



# Ingate Reference Guide

Version 6.1.4

# Table of Contents

Authors .....	1
Part I. Introduction .....	2
1. Introduction .....	3
1.1. What is a firewall? .....	3
1.2. What is a SIParator? .....	4
1.3. Configuration alternatives .....	4
1.4. Demilitarized zones .....	6
2. Getting started .....	8
2.1. Installation Overview .....	8
2.2. Configuration Overview .....	8
2.3. Settings Overview .....	9
3. Installation .....	11
3.1. Installation with a serial cable .....	11
3.2. Installation using the default IP address .....	17
3.3. Installation with the Startup Tool .....	17
3.4. Installation with magic ping .....	17
3.5. Turning off the unit .....	19
3.6. Remember to lock up the unit .....	19
4. Configuring .....	20
4.1. Logging on .....	20
4.2. Navigation .....	21
4.3. Overview of configuration .....	23
4.4. Preliminary and permanent configuration .....	24
4.5. Configuring IP addresses and masks .....	26
4.6. Name queries .....	27
4.7. Configuring the workstations .....	28
Part II. Graphical Interface .....	29
5. Administration .....	30
5.1. Save/Load Configuration .....	30
5.2. Show Configuration .....	33
5.3. User Administration .....	34
5.4. Upgrade .....	37
5.5. Downgrade .....	39
5.6. Fetch Licenses .....	39
5.7. Table Look .....	40
5.8. Date and Time .....	41
5.9. Restart .....	44
5.10. Change Language .....	45

6. Basic Configuration	47
6.1. Basic Configuration	47
6.2. Access Control	50
6.3. RADIUS	55
6.4. SNMP	59
6.5. DHCP Options	64
6.6. DHCP Server	68
6.7. DHCP Server Status	72
6.8. Router Advertisement	73
6.9. Dynamic DNS update	75
6.10. Certificates	78
6.11. TLS	83
6.12. Advanced Settings	86
6.13. SIParator Type	89
7. Network	91
7.1. Networks and Computers	91
7.2. Default Gateways	93
7.3. Interface (Eth0, Eth1, ...)	96
7.4. NAT	103
7.5. VLAN	105
7.6. Interface Status	106
7.7. PPPoE	108
7.8. Tunnels	110
7.9. Topology	113
8. Rules and Relays	116
8.1. Rules	116
8.2. Relays	119
8.3. DHCP Relay	123
8.4. Services	125
8.5. Protocols	127
8.6. Time Classes	129
9. SIP Services	131
9.1. Basic	132
9.2. Signaling Encryption	137
9.3. Media Encryption	140
9.4. Interoperability	145
9.5. Sessions and Media	167
9.6. Remote SIP Connectivity	178
9.7. VoIP Survival	183
9.8. VoIP Survival Status	186
10. SIP Traffic	187

10.1. SIP Methods	187
10.2. Filtering	189
10.3. Local Registrar	195
10.4. Authentication and Accounting	198
10.5. SIP Accounts	202
10.6. Dial Plan	204
10.7. Routing	213
10.8. SIP Status	227
10.9. SIP IDS/IPS	229
10.10. SIP IDS/IPS Status	234
11. SIP Trunks	236
11.1. SIP Trunks	236
11.2. Setting up SIP Trunking	237
11.3. Field Descriptions for the SIP Trunking Page	239
12. Failover	247
12.1. Introduction	247
12.2. Failover Setup	248
12.3. Failover Settings	251
12.4. Reference Hosts	256
12.5. Failover Status	258
12.6. Fault messages	260
13. Virtual Private Networks	262
13.1. Specification of Ingate VPN	262
13.2. Ingate VPN technology	263
13.3. IPsec Peers	263
13.4. IPsec Tunnels	270
13.5. IPsec Advanced	274
13.6. IPsec Cryptos	275
13.7. IPsec Certificates	279
13.8. IPsec Settings	280
13.9. Authentication Server	284
13.10. IPsec Status	286
13.11. PPTP	288
13.12. PPTP Status	292
14. QoS	293
14.1. Specification of Ingate QoS	293
14.2. Configuration of QoS	293
14.3. QoS and SIP	293
14.4. QoS Classes	296
14.5. QoS Interfaces	299
14.6. TOS Modification	302

15. Logging and Tools .....	305
15.1. Display Log .....	305
15.2. The log .....	313
15.3. Packet Capture .....	314
15.4. Check Network .....	317
15.5. Display Load .....	318
15.6. Logging Configuration .....	321
15.7. Log Classes .....	328
15.8. Log Sending .....	330
Part III. Serial Console .....	332
16. Basic Administration .....	333
16.1. Connecting to the serial console .....	333
16.2. Main Menu .....	334
16.3. Basic configuration .....	335
16.4. Save/Load configuration .....	339
16.5. Join a failover team and become slave .....	339
16.6. Leave the failover team and become standalone .....	340
16.7. Wipe email logs .....	341
16.8. Clear the log database .....	341
16.9. Set password .....	341
16.10. Exit admin .....	342
17. Command Line Reference .....	343
17.1. Command Reference .....	343
17.2. Table Definitions .....	348
17.3. Field Types .....	435
17.4. CLI command examples .....	485
Part IV. How To Guides .....	488
18. Network .....	489
18.1. Unit with two interfaces, using NAT .....	489
18.2. Unit with two interfaces, no NAT .....	497
18.3. Unit with four interfaces and DMZ .....	499
18.4. How To Configure VLANs .....	509
18.5. How To Configure a Semi-transparent FTP Relay .....	511
19. Administration .....	513
19.1. Changing Password .....	513
19.2. Changing Password for Software SIParator/Firewalls .....	517
19.3. Moving Configurations Between Ingate Units .....	518
20. SIP .....	523
20.1. SIP and IPv4/IPv6 .....	523
20.2. SIP Configuration .....	523
20.3. SIP server on the WAN .....	528

20.4. SIP server	530
20.5. SIP server on the LAN	536
20.6. How To Use Your SIP Operator Account Via the Ingate Unit	545
20.7. How To Use Your SIP Operator Account and Your IP-PBX Via the Ingate Unit	550
20.8. How To Use Multiple SIP Operators or IP-PBXs Via the Ingate Unit	556
20.9. How To Use Ingate Call Admission Control	561
20.10. How To Translate SIP Signaling Between UDP and TCP	564
20.11. How To Use RADIUS Accounting	568
20.12. How To Configure TLS	571
20.13. How To Use SIP Media Encryption	574
20.14. The DMZ SIParator Type	575
20.15. The DMZ/LAN SIParator Type	582
20.16. The Standalone SIParator Type	589
20.17. The WAN SIParator Type	597
20.18. The LAN SIParator Type	605
20.19. DMZ SIParator, SIP server on the WAN	611
20.20. DMZ SIParator, SIP server in the SIParator	615
20.21. DMZ SIParator, SIP server on the LAN	622
20.22. DMZ SIParator, SIP server in the SIParator, PSTN gateway inside	627
20.23. Standalone SIParator, SIP server on the WAN	635
20.24. Standalone SIParator, SIP server in the SIParator	638
20.25. Standalone SIParator, SIP server on the LAN	643
20.26. Standalone SIParator, SIP server in the SIParator, PSTN gateway inside	646
20.27. DMZ/LAN SIParator, SIP server on the WAN	653
20.28. DMZ/LAN SIParator, SIP server in the SIParator	656
20.29. DMZ/LAN SIParator, SIP server on the LAN	661
20.30. DMZ/LAN SIParator, SIP server in the SIParator, PSTN gateway inside	664
20.31. LAN SIParator	671
20.32. WAN SIParator	676
20.33. Manual SIParator	681
20.34. WebRTC	681
21. VPN	684
21.1. VPN between two Ingate Units	684
21.2. VPN connection with road warrior	688
21.3. How to configure PPTP connections	694
21.4. How to configure IPsec connections	697
21.5. How to configure IPsec connections from a road warrior	701
21.6. IPsec connections with RADIUS authentication	707
21.7. How to configure IPsec connections with NAT	714
21.8. IPsec Connection With NAT, Client Side has a Dynamic IP Address	722
21.9. IPsec Connection With NAT, Server Side has a Dynamic IP Address	731

21.10. How To Configure PPTP Passthrough . . . . .	739
21.11. VPN between Ingate and AWS (Amazon Web Services) . . . . .	743
21.12. IPsec with road warriors using extended authentication . . . . .	748
22. Cloud Environment . . . . .	758
22.1. Amazon Web Services (AWS) . . . . .	758
22.2. Openstack . . . . .	758
22.3. Azure . . . . .	758
22.4. Google Cloud Platform (GCP) . . . . .	758
Part V. Hardware Models . . . . .	760
23. Ingate SIParator/Firewall S21 rev A . . . . .	761
24. Ingate SIParator/Firewall S21 rev B . . . . .	763
25. Ingate SIParator/Firewall S51 . . . . .	765
26. Ingate SIParator/Firewall S52 . . . . .	766
27. Ingate SIParator/Firewall S95/S96/S97/S98 . . . . .	768
27.1. The front . . . . .	768
27.2. The back . . . . .	768
Appendix A: IP Firewall . . . . .	770
General . . . . .	770
Traffic Configuration . . . . .	770
NAT . . . . .	772
Relays . . . . .	773
Appendix B: Common services . . . . .	777
HTTP . . . . .	777
HTTPS . . . . .	778
FTP . . . . .	779
DNS . . . . .	781
SMTP . . . . .	783
NNTP . . . . .	785
Telnet . . . . .	785
SSH . . . . .	786
NTP . . . . .	786
Traceroute . . . . .	788
Incoming traceroute configuration . . . . .	790
Ping . . . . .	790
Real Audio/Video . . . . .	792
ICQ . . . . .	794
Appendix C: More About SIP . . . . .	796
The SIP Protocol . . . . .	796
Managing Your Own SIP Domain . . . . .	797
SIP Sessions . . . . .	804
SIP in Ingate SIParator/Firewall . . . . .	804

Appendix D: More About VPN	807
VPN protocols	807
VPN interoperability	807
VPN connections	808
VPN clients	808
Appendix E: More about security	812
Some of the most common types of attacks	812
Security resources on the Internet	813
Encryption	813
Appendix F: Troubleshooting	815
Network troubleshooting	815
Firewall troubleshooting	815
SIP troubleshooting	816
VPN troubleshooting	817
Administration troubleshooting	817
Log Messages	818
Performance Enhancements	820
Appendix G: Regular Expressions	822
Matching Characters	822
Modifiers and Operators	822
Using Regular Expressions	823
Appendix H: Format Descriptions	825
Log File Format	825
Ingate RADIUS Accounting	834
Appendix I: Definitions of terms	845
Appendix J: License Conditions	855
GNU Lesser General Public License (LGPL) v 2.1	855
GNU General Public License (GPL) v 2	864
GNU Lesser General Public License (LGPL) v 3	870
GNU General Public License (GPL) v 3	874
GNU Library General Public License (LGPL) v 2	886
GNU Free Documentation License (GFDL) v 1.3	895
License exceptions for libgcc	903
License exceptions for libstdc++	904
GCC RUNTIME LIBRARY EXCEPTION	904
Mozilla Public License Version 2.0	906
Python 2.7 license	912
The Vovida Software License, Version 1.0	918
Software developed by Cisco Systems	919
Software developed at University of California	920
zlib	923

ISC .....	924
License for bzip2 .....	925
License for lilo .....	926
Software in the GNU C distribution .....	928
Apache License .....	937
OpenSSL .....	941
License for ipmitool .....	944
License for libedit .....	944
License for libevent .....	945
License for libuuid .....	947
License for net-snmp .....	948
License for nginx .....	954
License for NTP .....	954
PCRE2 LICENCE .....	957
Software developed by Carnegie Mellon University .....	959
Software developed by Gregory M Christy .....	960
Software developed by Google, Inc .....	961
Software developed in the GIE DYADE cooperation .....	961
Software developed by Tommi Komulainen .....	963
Software developed by Paul Mackerras .....	963
Software developed by Pedro Roque Marques .....	964
Software developed by RSA Data Security, Inc .....	965
Software developed by Sun Microsystems, Inc .....	966
More software developed by Sun Microsystems, Inc .....	966
Software developed by Andrew Tridgell .....	967
License for dropbear .....	967
License for kerberos .....	970
License for libcom_err .....	971
License for libss .....	971
License for libcurl .....	972
License for libffi .....	972
License for libverto .....	973
License for libxml2 .....	974
License for ncurses .....	975
License for dnspython .....	976
License for pillow .....	977
License for wslay .....	978
License for libpcap .....	978
License for radvd .....	979
License for tcpdump .....	980
License for util-linux/agetty .....	981

License for util-linux/uuidgen .....	981
License for libselinux .....	982
License for tzdata .....	982
License for sqlite .....	983
Licenses for mediafw .....	984
Licenses for sipfw .....	986
Appendix K: References .....	988
Bibliography .....	988

# Authors

- Lisa Hallingström
- Paul Donald
- Bogdan Musat
- Adnan Khalid
- Per Johnsson
- Rickard Nilsson

The contents of this documentation may not be duplicated, in whole or in part, without the express written permission of Ingate Systems AB, according to copyright law. This includes all forms of duplications, including but not limited to printing, photocopying, dittoing, recording on tape, etc. Copyright © 2018 Ingate Systems AB

# Part I. Introduction

# Chapter 1. Introduction

Once upon a time, a few people decided that they wanted to share their computer systems, so they laid cables all across the country to interconnect their computers. They wanted to form a union where they could share their computers in different time zones so that CPU time could flow freely between them. Hackers created the network, and they saw that it was good. And the users did rejoice, and connected themselves from coast to coast to use one another's systems, send messages to SF-LOVERS and enjoy life on the Net.

The network grew over the years, and more and more systems joined it for the common good. Tourism flourished, every man his own armchair-tourist. Everyone sought CPU time on others' systems. Passwords did not exist. No one knew what a cracker was.

Suddenly, the network was so huge, the systems so many, that the number of hackers was not enough. Users found themselves alone on their systems, left to their own devices and their company management. Then somebody was seized with the fear that others would ruin something and began blocking out tourists, setting passwords to keep others from accessing what had once been common resources.

Suspicion spread: More and more users felt it necessary to put ID checks on their systems. Soon, no one but a handful of die-hard hackers thought there was anything strange about passwords and encryption.

Suspicion bred spite. Some individuals tried to use the ID checks and security systems for their own purposes, trying to convince the systems that they were other users.

They came to be called 'crackers,' spiteful individuals who wanted to break into systems for their own purposes, without wanting or even seeing the old feeling of camaraderie.

Security checks were developed. Soon, protocols were available on the network to interrogate distant systems on the users of certain network programs (IDENT), smart cards (CP/8), one-time passwords (S/Key) and similar things (SSH, PGP). This development included the creation of firewalls.

## 1.1. What is a firewall?

A firewall in a network works just like a firewall in the construction industry: Since it has no holes, it prevents a fire from spreading. In this case, the fire is the spiteful individuals and their programs.

Take a relatively large computer, add at least two network interfaces, and with the correct software, you have a bridge between two networks that lets all traffic pass from the one to the other. Block this bridge and you have a firewall.

However, this firewall is of limited benefit, because it prevents data packets from coming in as well as going out. This makes the connection between the internal network, which you are trying to protect, and the external network, which you want to reach, completely pointless. No traffic can move between them.

So, instead of completely cutting off traffic between the external and internal networks, we equip

the firewall with software to filter the traffic. Most anything is allowed to come out, but the road in is extremely restrictive.

## 1.2. What is a SIParator?

A SIParator is a device which processes traffic under the SIP protocol (see RFC 3261). The SIParator receives SIP requests, processes them according to the rules you have set up, and forwards them to the receiver.

The SIParator connects to an existing enterprise firewall through a DMZ port, enabling the transmission of SIP-based communications without affecting firewall security. SIP messages are then routed through the firewall to the private IP addresses of authorized users on the internal network.

The SIParator can also be used as an extra gateway to the internal network without connecting to the firewall, transmitting only SIP-based communications.

Some of the functions of Ingate SIParator are:

- SIP proxy: Forwarding of SIP requests.
- SIP registrar: Registration of SIP users.
- Protection against such attacks as address spoofing.
- Logging/alarm locally on the unit, via email and/or via syslog.
- Managing several logical/directly-connected networks and several network connections/physical networks.
- Administration of the unit through a web browser using http or https.
- Choice of language. Choose between Swedish and English.
- QoS - bandwidth limitation and traffic prioritizing (using the QoS module).
- Failover - connect two units in parallel; one handles traffic and the other acts as a hot standby.
- STUN server and Remote SIP Connectivity for SIP clients behind NAT boxes which are not SIP aware (using the Remote SIP Connectivity module).

## 1.3. Configuration alternatives

The Ingate SIParator can be connected to your network in four different ways, depending on your needs.

Note that if the Standalone type is used, the interface which should receive traffic from the outside must have a public IP address (no NAT).

For a DMZ or DMZ/LAN type which uses a private IP address on the interface connected to the DMZ of the firewall, its corresponding public IP address must be entered on the [Interoperability](#) page.

### 1.3.1. DMZ Configuration

Using this configuration, the unit is located on the DMZ of your firewall, and connected to it with only one interface. The SIP traffic finds its way to the unit using DNS or by setting the unit as an outbound proxy on the clients.

This is the most secure configuration, since all traffic goes through both your firewall and your unit. It is also the most flexible, since all networks connected to any of your firewall's interfaces can be SIP-enabled.

The drawback is that the SIP traffic will pass the firewall twice, which can decrease performance.

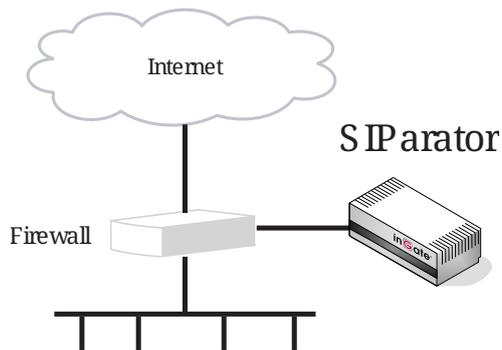


Figure 1. SIParator in DMZ configuration

### 1.3.2. DMZ/LAN Configuration

Using this configuration, the unit is located on the DMZ of your firewall, and connected to it with one of the interfaces. The other interfaces are connected to your internal networks. The unit can handle several networks on the internal interface even if they are hidden behind routers.

This configuration is used to enhance the data throughput, since the traffic only needs to pass your firewall once.

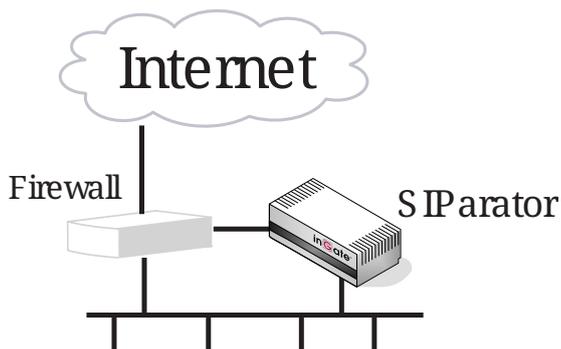


Figure 2. SIParator in DMZ/LAN configuration

### 1.3.3. Standalone Configuration

Using this configuration, the unit is connected to the outside on one interface and your internal networks on the others.

Use this configuration only if your firewall lacks a DMZ interface, or for some other reason cannot be configured for the DMZ or DMZ/LAN alternatives.

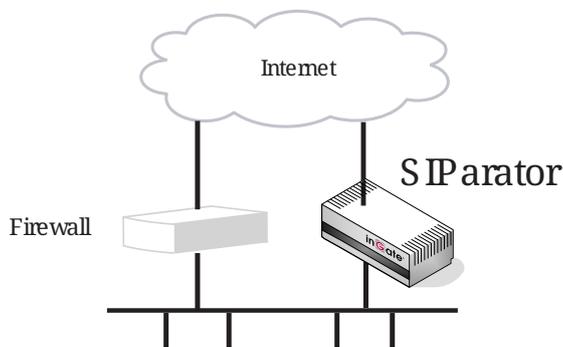


Figure 3. SIParator in Standalone configuration

### 1.3.4. WAN Configuration

Using this configuration, the unit is connected to the outside on one interface and your firewall on another interface. Between these two interfaces (marked as a Data Interfaces on the Topology page), only data will be sent. Other interfaces can be connected directly to your LAN, DMZ or other networks, and here SIP traffic will be sent.

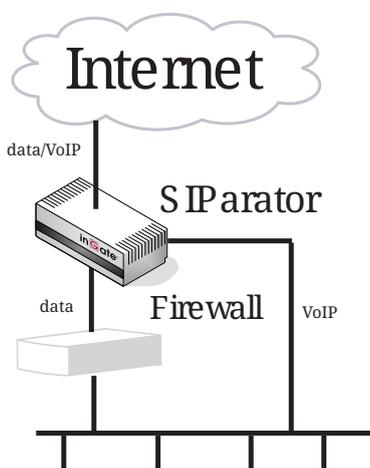


Figure 4. SIParator in WAN configuration

### 1.3.5. Manual Configuration

Using this configuration, the unit is connected to one or more networks. All the networks that you want to handle must be added to the Surroundings table (found on the page **Network** → **Topology**). If you have default gateways defined, the outside world will be automatically configured. The Manual SIParator can be used when none of the other types match your scenario.

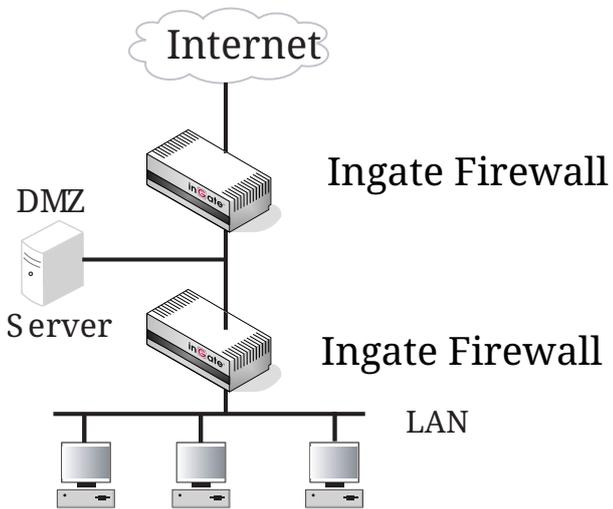
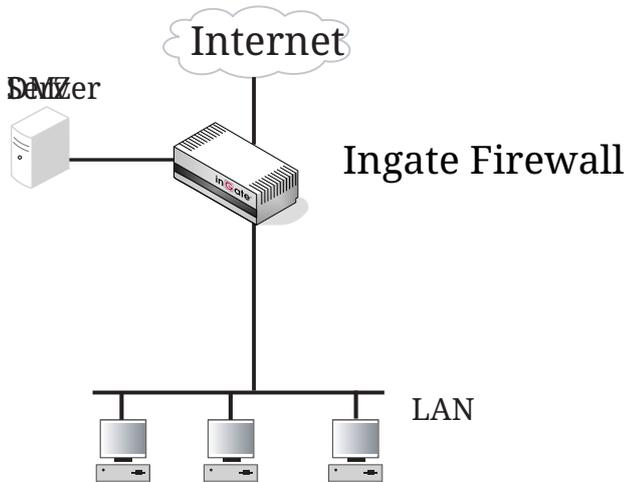
## 1.4. Demilitarized zones

In military and political situations there are buffer zones, demilitarized zones, between areas of unrest. One good example of this is the demilitarized zone between North and South Korea.

Demilitarized zones, or DMZs, are also found in computer networks. A DMZ is a computer network that is accessible from two other computer networks that have no direct contact with each other. Often, one of these networks is the Internet and the other is a local, internal network. There is no direct connection between the Internet and the local network, but both of them can access an intermediate network, a demilitarized zone.

DMZs are often used for special servers, such as WWW servers, which must be accessible from two separate networks.

It is easiest to create a DMZ using one firewall; the figure below shows an example. A DMZ can also be built as a network connected between two firewalls.



# Chapter 2. Getting started

## 2.1. Installation Overview

The recommended way to install the unit is to:

- Select an IP address for the unit on your network or use the default IP address set at factory (192.168.1.1 on Eth0).
- Plug in the power cord and turn on the unit.
- Wait while the unit boots up.
- Set the IP address of the unit and set a password.

This can be done in different ways:

- Use the default IP address (192.168.1.1 on Eth0).
- Connect to the unit with the serial cable. See [Installation](#).
- Run the StartUp Tool TG.
- Set the IP address with magic ping. See [Installation](#).
- Connect the network cables to the network interfaces.

The network interfaces are marked with Eth0, Eth1, .... These are the names of the physical interfaces and the ones which you should use in the installation program.

- Run the StartUp Tool TG.
- Register the product on <https://account.ingate.com>.
- Activate purchased licenses on <https://account.ingate.com>.

License codes are typically delivered by e-mail from Ingate and come with instructions how to register and install.

- Make extra configuration according to your requirements via the Web interface by directing your web browser to the IP address of the unit. See next chapter for the Configuration Overview.
- Save and backup the configuration.

## 2.2. Configuration Overview

This is an overview of the configuration needed to make your unit work.

Note that several of the steps below will be configured by StartUp Tool TG.

- Enter the IP address of the unit in your web browser. If you have set the IP address with magic ping you will be prompted to set a password for the unit admin user.
- The top page of the unit is the first page displayed. Go to the **Eth0** page under [Network](#) and

configure this interface. See also the [Interface \(Eth0, Eth1, ...\)](#) section.

- Then, move on to the other interface pages and give the unit at least one IP address per active interface and state the networks connected to each interface. See also the [Interface \(Eth0, Eth1, ...\)](#) section.
- Then, go to the [Default Gateways](#) page and enter the default gateway of the unit.
- Click on the SIParator Type link and select the configuration for your unit. The types are described on the corresponding help page.
- If NAT is wanted for some traffic through the unit, go to the [NAT](#) page and make settings for this. See also the [NAT](#) section. Note, the NAT page is only shown in Firewall Mode.
- Go to the [Networks and Computers](#) page to define the networks that will send and receive traffic through the unit. Usually, at least one network per interface of the unit is needed. Some computers should be handled separately, and they therefore need their own networks.
- Go to the Topology page (for the DMZ SIParator Type) and state the networks connected to your *firewall*. See also the [Topology](#) section.
- Go to the [Access Control](#) page and make settings for the configuration of the unit.
- By default, all traffic through the unit is blocked. Go to the [Rules](#) page under [Rules and Relays](#) and make rules to allow the traffic. Traffic over TCP (e.g. smtp) works without any reply rules, but traffic over UDP and ICMP needs rules for both directions in order to work correctly. However, if NAT is used, only rules for the "start direction" is needed. See also the [Rules](#) and [Services](#) sections.
- If NAT is used for traffic from an interface, relays are needed to get packets through to this interface. Go to the [Relays](#) page and define relays for the traffic allowed. See also the [Relays](#) section.
- Press the [Administration](#) button and go to the [Save/Load Configuration](#) page. Select **Apply configuration**. First the new configuration is tested. When it is satisfactory, it can be saved permanently. If the configuration is not satisfactory, select **Revert** or restart the unit. The old configuration will remain.
- When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

## 2.3. Settings Overview

The unit uses two sets of configurations: preliminary and permanent configuration. The permanent configuration is what is used in the active unit. The preliminary configuration is where you change and set the configuration. See [Configuring](#) for more instructions.

The changes you make in the preliminary configuration are not stored in the permanent configuration until you click on **Apply configuration** on the [Save/Load Configuration](#) page under [Administration](#).

The password configuration and time setting are the exceptions to this rule; they are saved immediately. Change the administrator passwords and create more administrator users on the [User Administration](#) page under [Administration](#).

The unit displays serious errors in red, e.g., if mandatory information is not entered. Blank fields are shown in red. Fields that you correct remain red until you select **Save**, **Add new rows** or update the page in some other way.

If you have a web session with the unit that is inactive for 10 minutes, it will ask for a password again.

Always log out from the unit administration interface when you are not using it. Press the **Log out** button on the top right to log out.

# Chapter 3. Installation

The recommended way to install the unit is to use a serial cable connected to the serial console at the unit and via it set the IP address and password for the unit.

Installation with a serial cable requires being at the same place as the unit, this will give most options for the start configuration and it will always work.

A new alternative from SW version 5.0.6 is to use the default IP address, connect to the unit with a web browser, and set the password as first action when connected.

Installation using the default IP address does not require being on the same place as the unit (but the computer has to be connected to the same logical network as the unit).

Any of the two ways above is followed by running the StartUP Tool TG, that gives help with network and SIP configuration for the combination of IP-PBX and ITSP that will be used.

Installation with the StartUp Tool TG does not require being on the same place as the unit (but the computer has to be connected to the same logical network as the unit). This tool includes also the possibility to set the IP address and password for the unit.

Finally further configurations are done through the web GUI.

One more alternative way to set the IP Address of the unit is to perform a magic ping followed by creating all configuration manually via the web interface.

Installation with magic ping does not require being on the same place as the unit (but the computer has to be connected to the same logical network as the unit), but restricts the start configuration.

## 3.1. Installation with a serial cable

Connect the unit to your workstation with the enclosed serial cable, plug in the power cord and turn the unit on. You will have to wait a few minutes while the unit boots up.

You need a serial cable (one was included with the product), a serial adapter cable, and a terminal program on your workstation.

Connect the serial port at the unit to your workstation with the serial cable, using a serial adapter suiting your workstation.

When communicating via serial links with Ingate products, use 19200bps, 8N1 (i.e. 8 data, No parity, 1 stop bit), VT100.

### 3.1.1. Windows

If you use a Windows workstation, connect like this:

1. Start PUTTY (of course other terminal programs can be used, however only PUTTY is described here).

2. Check which Serial Port that is used by checking in the Device manager, for example it can be COM3.
3. Write in Serial line: COM3 (use the port that is in use, in this example COM3)
4. Select Connection Type: Serial
5. Among the port settings make sure that the Speed is 19200 bit/s.
6. Use the default values for all other settings.
7. Connect by clicking Open.
8. Wait for a login prompt. (In some cases you have to press Return to get the login prompt.)

### 3.1.2. Linux

If you use a Linux workstation, connect like this:

1. Plug in your USB serial converter.
2. Determine the tty port the converter is on.

```
dmesg | grep tty
```

You should get something like this:

```
usb 2-1.5: pl2303 converter now attached to ttyUSB0
```

That means you should use `/dev/ttyUSB0`.

3. Use `minicom` to access the console.

```
minicom -8 -b 19200 -D /dev/ttyUSB0
```

You have to press Return to get the login prompt. If you get the following error:

```
minicom: cannot open /dev/ttyUSB0: Permission denied
```

You need to make sure you have permission to access the `ttyUSB0` device. Consult the manual of your particular distribution.

### 3.1.3. MAC

If you use a MAC workstation, connect like this:

1. Start Screen (of course other terminal programs can be used, however only Screen is described here).
2. Plug in your USB-serial adapter.

3. Find the right TTY device.

```
ls /dev/tty*
```

You should get something like this:

```
/dev/tty  
/dev/tty.Bluetooth-Incoming-Port  
/dev/tty.Bluetooth-Modem  
/dev/tty.usbserial
```

Look for something like usbserial (or similar). That means you should use `/dev/tty.usbserial`. Alternatively use :

```
dmesg | grep tty
```

You should get something like this:

```
usb 2-1.5: pl2303 converter now attached to ttyUSB0
```

That means you should use `/dev/ttyUSB0`.

4. Use Screen to access the console.

```
screen /dev/tty.usbserial 19200
```

You have to press Return to get the login prompt.

Log on from your workstation as the user admin. The first time you log on, no password is required. You set the password when you run the **1. Basic configuration** from the menu, that is presented when you have logged on.

Each network interface is marked with a name (Eth0, Eth1, ...), which corresponds to a tab under **Network**. All eth interfaces belong to ethernet cards and should only be connected using ethernet cables.

Decide which computer(s) are allowed to configure the unit and enter the name of the network interface to which they are connected, for example, eth0. You must use the physical device name (eth0, eth1, ...).

Enter the IP address of the unit on this interface and the network mask for the network.

A network mask can be written in two ways in the unit:

- The first looks just like an IP address, for example 255.255.192.0 or 255.255.254.0.

- The other way is as a number between 0 and 32. An IP address has 32 bits, where network mask number indicates how many bits are used in the network's addresses. The rest of the bits identifies the computer on the network.

Now, you can select to deactivate any network interfaces. Select `y` to deactivate all interfaces but the one you just configured. The remaining network interfaces can be activated later when you complete the configuration via the web interface from your work station. This only applies to interfaces which was previously active; you can't activate interfaces with this setting.

Now enter the computer or computers from which the unit may be configured (the configuration computers).

Then enter a password for the unit. This is the password you use in your web browser to access and change the unit's configuration. Finally, you can reset all other configuration if you want to.

Following is a sample run of the installation program.

```
Administration
=====

(Navigation tip: You may use Ctrl-d to skip back to this menu.)

1.      Basic configuration
2.      Download/Upload
3.      Join a failover team and become slave
5.      Wipe email logs
6.      Set password
7.      Command line interface
8.      Clear the log database
a.      About
reboot. Reboot
reset.  Factory reset
q.      Exit admin

==>
```

Select 1 to install your unit.

```
Basic unit installation program version 6.1.4
```

```
Press return to keep the default value
```

```
Network configuration inside:
```

```
Physical device name[eth0]:
```

```
IP address [0.0.0.0]: 10.47.2.242
```

```
Netmask/bits [255.255.255.0]: 255.255.0.0
```

```
Deactivate other interfaces? (y/n) [n]
```

```
Computers from which configuration is allowed:
```

```
You can select either a single computer or a network.
```

```
Configure from a single computer? (y/n) [y]
```

If you choose to allow only one computer to configure the unit, you are asked for the IP address (the mask is set automatically).

```
IP address [0.0.0.0]: 10.47.2.240
```

If this IP address is not on the same network as the IP address of the unit, you are asked for the router. Enter the IP address of the router on the network where the unit is connected. Then enter the network address and mask of the network containing the *configuring computer*.

```
Static routing:
```

```
The computer allowed to configure from is not on a network local to  
this unit. You must configure a static route to it. Give  
the IP address of the router on the network the unit is on.
```

```
The IP address of the router [0.0.0.0]: 10.47.3.1
```

```
Network address [10.47.0.0]: 10.10.0.0
```

```
Netmask [255.255.255.0]:
```

You can choose to allow several computers to configure the unit, by answering no to the question:

```
Configure from a single computer? (y/n) [y] n
```

The installation program then asks for the network number. The configuration computers must be entered as a complete subnet, i. e. a range which can be written as a network number and a netmask (like 10.47.2.128 with netmask 255.255.255.128, which means the computers 10.47.2.128-10.47.2.255). All computers on this subnet will be allowed to configure the unit. For more information about network numbers and netmasks, see [Configuring](#).

```
Network number [0.0.0.0]: 10.47.2.0
Netmask/bits [255.255.255.0]: 255.255.255.0
```

If the network or partial network is not directly connected to the unit, you must enter the IP address of the router leading to that network. Then enter the network's address and mask.

```
Static routing:
The network allowed to configure from is not on a network local to this
unit. You must configure a static route to it. Give the
IP address of the router on the network this unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1
Network address [10.47.0.0]: 10.10.0.0
Netmask [255.255.255.0]:
```

Then enter a password.

```
Password []:
```

Finally, you are asked if you want to reset other configuration.

```
Other configuration
Do you want to reset the rest of the configuration? (y/n) [n]
```

If you answer n, nothing is removed. If you answer y, you have three alternatives to select from:

1. Clear as little as possible. This is the alternative that is used if you answer n to the question above. Both the preliminary and the permanent configurations will be updated with the configuration specified above.
2. Revert to the factory configuration and then apply the configuration specified above. This will affect the permanent but not the preliminary configuration.
3. Revert to the factory configuration and empty all logs and then apply the configuration specified above. Both the preliminary and the permanent configurations will be affected.

Select the update mode, which is what you want to remove.

```
Update mode (1-3) [1]:
```

All configuration is now complete. The installation program shows the configuration and asks if it is correct.

yes saves the configuration.

no runs the installation program over again.

abort ends the installation program without saving.

```
You have now entered the following configuration
```

```
Network configuration inside:
```

```
Physical device name: eth0
```

```
IP address: 192.168.150.2
```

```
Netmask: 255.255.255.0
```

```
Deactivate other interfaces: no
```

```
Computer allowed to configure from:
```

```
IP address: 192.168.128.3
```

```
Password: eeyore
```

```
The rest of the configuration is kept.
```

```
Is this configuration correct (yes/no/abort)? yes
```

Now, finish configuration of the unit from the computer/computers specified in the installation program by log on to the web interface as admin, using the new password.

Connect the network cables to the network interfaces.

## 3.2. Installation using the default IP address

A new alternative from SW version 5.0.6 is to use the default IP address, connect to the unit with a web browser, and set the password as first action when connected.

The default IP address is 192.168.1.1 with netmask 255.255.255.0.

The configuration computer has to be connected to the same logical network as the unit.

There is no default password set from factory. You will be asked to set a password via the web user interface when you connect the first time.

## 3.3. Installation with the Startup Tool

The Ingate StartUp Tool TG is delivered on the CD you got with the unit. You can also download the latest Startup Tool version from <https://account.ingate.com/>.

The Startup Tool helps you to set the initial IP address, and with network and SIP configuration including SIP Trunking for the combination of IP-PBX and ITSP that will be used.

## 3.4. Installation with magic ping

You can use the magic ping to set an IP address for the unit. This is how to perform a magic ping:

- Plug in the power cord and turn the unit on.
- Wait while the unit boots up.
- Connect the network cables to the network interfaces.
- Find out the MAC address of the unit (printed on the unit label). This is the MAC address of Eth0.
- Add a static entry in your local ARP table consisting of the unit's MAC address and the IP address it should have on eth0. See below how to add the entry on a Windows workstation.
- Perform the magic ping:

Ping this IP address to give the unit its new IP address. You should receive one ping reply if the address distribution was successful.

The magic ping will not set any password. Set a password immediately via the web user interface. Before any configuration has been made, only the computer which performed the magic ping will be able to configure the unit.

### 3.4.1. How to add a static ARP entry in Windows 7+

- Start a command (or cmd) window as administrator.
- In the command window, enter the command:

```
netsh interface ipv4 show addresses
```

by this you get the network adaptor name for which you want to add the route/static MAC mapping

- Then enter the command:

```
netsh interface ip add neighbors "networkadaptor" "ipaddress" "macaddress"
```

where **networkadaptor** is the network adaptor name that you just read out in previous step, **ipaddress** is the new IP address for the eth0 interface, and **macaddress** is the MAC address printed on the unit, but with all colons (:) replaced with dashes (-).

For example:

```
netsh interface ip add neighbors "USBeth" "10.10.10.1" "00-90-fb-3c-83-16"
```

### 3.4.2. How to add a static ARP entry in older Windows

This is how to add a static ARP entry if you use an older Windows version.

- Start a command (or cmd) window as administrator.
- In the command window, enter the command:

```
arp -s ipaddress macaddress
```

where **ipaddress** is the new IP address for the eth0 interface, and **macaddress** is the MAC address printed on the unit, but with all colons (:) replaced with dashes (-).

## 3.5. Turning off the unit

Backup the unit configuration (just in case something should happen). You do this on the Save/Load Configuration page under Administration. Once this is done, just turn the computer off. The unit is specially designed so that you can switch it off without causing any problems in the file structure.

## 3.6. Remember to lock up the unit

The Ingate SIParator/Firewall is a computer with special software, and must be protected from unauthorized physical access just as other computers performing critical tasks. A locked up unit protects against:

- connecting to the console
- changing the administrator password using a reboot and the unit buttons.

For more information about the necessary configuration, see [Configuring](#).

# Chapter 4. Configuring

You connect to your unit by entering its name or IP address in the Location box of your web browser.

## 4.1. Logging on

Before you can configure the unit, you must enter your administrator username and password or RADIUS username and password. The *admin* user is predefined with complete administration privileges.

You were not logged on.

### Local password

Username:   
Password:

### 4.1.1. Log on again

If you have a web connection for unit configuration that is inactive for more than 10 minutes, you must enter the password again and click on one of the buttons **Keep changes below** and **Abandon changes below**.

You have been away more than 10 minutes.  
Please enter the local password for admin:

On all pages where changes have been made, the two buttons **Keep changes below** and **Abandon changes below** will be shown when you log on again. **Keep changes below** connects you to the unit and stores the preliminary configuration you have changed. **Abandon changes below** connects you to the unit and discards the changes you have made on this page.

On pages where nothing has been changed, the **Log in again** button is displayed. Enter the password and click on the button to re-connect to the unit.

The unit's encryption key is changed every 24 hours. If you have a web connection for unit configuration when this happens, you must enter the password again. This works in the same way as when your connection has been inactive for more than 10 minutes (see above).

### 4.1.2. Log out

When you have finished looking at or adding settings, you should log out from the unit. At the top right of each web page there is a Log out button which will end your session.

## WARNING

You will not be logged out automatically just by directing your web browser to a different web address. You should log out using the button to make the browser forget your username and password.

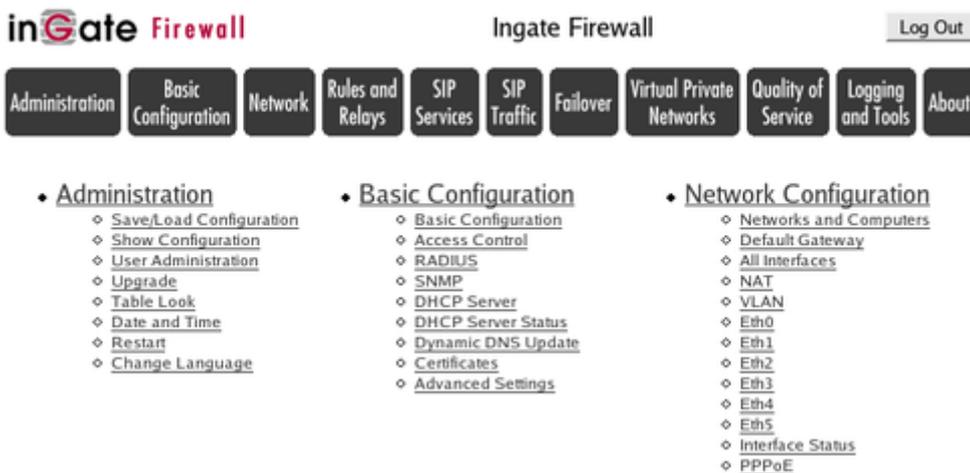
## 4.2. Navigation

All pages have buttons for quick navigation to the other main pages. You also see the name of the unit above the line of buttons.



### 4.2.1. The top page

The top page is the first page displayed when you have logged on the unit. From this page, you can access **Basic Configuration**, **Administration**, **Network**, **Rules and Relays**, **Logging and Tools**, **SIP Services**, **SIP Traffic**, **Failover**, **Virtual Private Networks**, and **Quality of Service**. You can also access a special page by the text links below each category name. Go to the top page by clicking the logotype at the top left of a web page.



### 4.2.2. Administration Tab

Under **Administration**, you store or load a configuration. You can also test your configuration to see if it works the way you planned, upgrade or reboot your unit, set date, time and language, and configure administration users and passwords.

### 4.2.3. Basic Configuration Tab

Under **Basic Configuration**, enter the name of the unit and make settings for the configuration traffic. You can also enter IP addresses for DNS server, and switch the version control on or off. Here you also configure if the unit should interact with a RADIUS, a DynDNS or an SNMP server, and if it should run a DHCP server.

#### 4.2.4. Network Tab

Under **Network**, you enter the unit's IP address, the routing for the different networks, and define groups of IP addresses which are used in various settings of the unit.

You also define what traffic should be NAT:ed through the unit.

#### 4.2.5. Rules and Relays Tab

Under **Rules and Relays**, you create names for services, define protocols and time classes, and then set rules and relays that define what traffic is allowed or blocked from one net to another.

The DHCP relay is also configured here.

#### 4.2.6. SIP Services Tab

Under **SIP Services**, you configure SIP encryption, interoperability settings, Remote SIP Connectivity and VoIP Survival.

#### 4.2.7. SIP Traffic Tab

Under **SIP Traffic**, you configure the SIP traffic and the SIP registrar in the unit. You can also view current user registrations and SIP sessions.

#### 4.2.8. Failover Tab

Under **Failover**, you configure the failover team and its dedicated network. You can also view the status of the other team member.

#### 4.2.9. Virtual Private Networks Tab

Under **Virtual Private Networks**, you configure the encrypted traffic between your unit and other VPN gateways and clients. VPN connections can be made using IPsec or PPTP.

#### 4.2.10. Quality of Service Tab

The Quality of Service module enables bandwidth limitation and prioritizing for different kinds of traffic through the unit. For each interface you can state a guaranteed and a maximum bandwidth for classes of traffic.

You can also set bandwidth limits for SIP calls and ensure that when there is not enough bandwidth for call media, the call will not be set up at all.

#### 4.2.11. Logging and Tools Tab

Under **Logging and Tools**, you specify the type of traffic you want to log/alarm and how it should be logged. You can also view the logs and the traffic load here.

## 4.2.12. About Tab

Under About, you get basic information about the unit's serial number, software version, installed licenses and patches, and links to more information.

## 4.3. Overview of configuration

Start by installing the unit as described in [Installation](#).

The unit must have at least one IP address per active network card to work. You must also set a routing, or path, for other networks on the **Interface** pages.

If you want the unit to have several IP addresses on one network, specify this under **Alias**, which is on the **Interface** pages under **Network**. When you use NAT, it is a good idea to have several IP addresses on the outside. For example, you can have several web servers that appear to be on these IP addresses but are actually on several machines on the other side of the unit.

If you want to hide the logical networks in the organization so that only the outside of the unit is visible, configure NAT on the NAT page under **Network**.

Once you have set the IP address and routing, it is time to name the networks. Make up good names and enter the network addresses for them. All these settings are configured on the **Networks and Computers** page under **Network**.

You must also define several services that you will use on the network. Some examples are WWW, email and file transfer. Many common services are already predefined. You define services on the **Services** page under **Rules and Relays**.

The Services are based on protocols, defined on the Protocols page under **Rules and Relays**. The common protocols TCP, UDP and ICMP are predefined.

You must also define time classes, which will make it possible to define rules that, for example, are active only during weekdays, or parts of a day. You define these on the **Time Classes** page under **Rules and Relays**.

Once you have defined networks, machines, protocols, time classes and services, you can set up firewall rules for the traffic to be allowed and blocked. Traffic that is not allowed by any rule is blocked. You set firewall rules on the **Rules** page.

If NAT is on, you must set relays for the services on the NAT'ed network that you want to expose to the outside world. Relays can also be used without NAT. You configure them on the Relays page.

Use logging to analyze the traffic that passes through the unit. Logging can be set to off, log all, or log only for the rules and relays for which you specified logging. A new unit logs for marked rules and relays; see [Rules](#) and [Relays](#). You can choose to log locally on the unit, send logs to a syslog server or send them by e-mail to an e-mail address. Specify the type of logging you want under **Logging and Tools**. This is also where you view the logs of traffic through the unit.

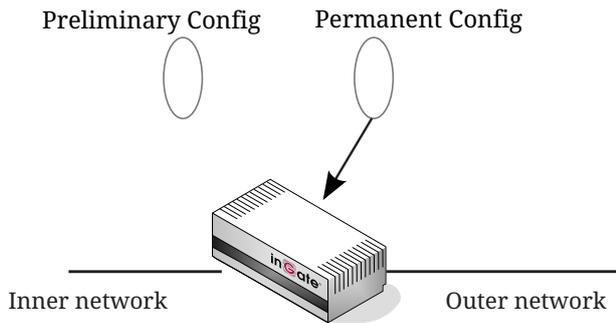
When you have completed the configuration, apply it. Go to **Administration** and select the **Save/Load Configuration** tab. Select **Apply configuration**. Now you can test your new

configuration and save it permanently if you are satisfied with it. If the configuration is not satisfactory, select **Revert** or restart the unit. The old configuration will remain.

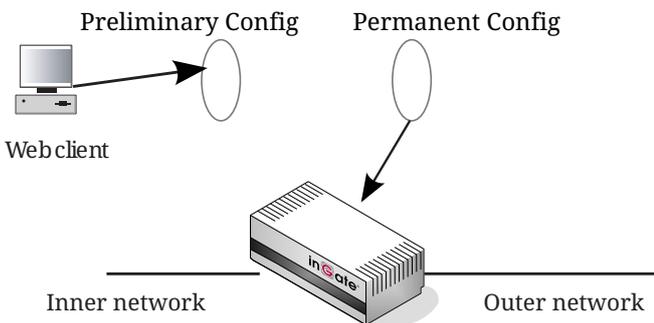
When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

## 4.4. Preliminary and permanent configuration

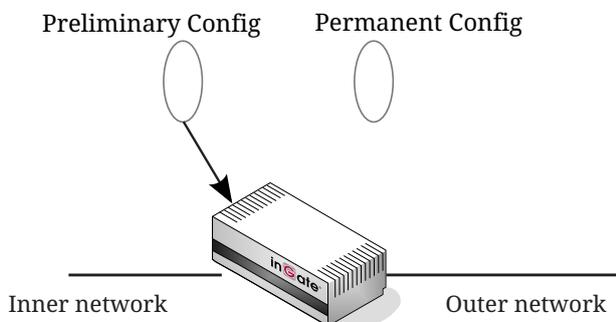
The unit has two kinds of settings: preliminary and permanent configuration. When the unit is running, the permanent configuration controls the unit functions.



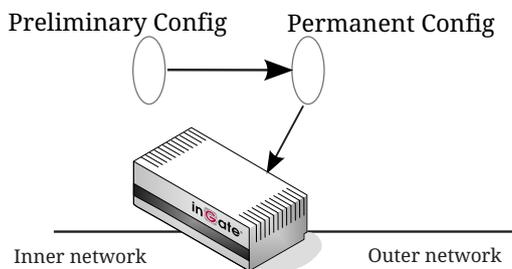
When you configure your unit, you are working with the preliminary configuration. As you change the preliminary configuration, the permanent configuration continues to control the unit functions.



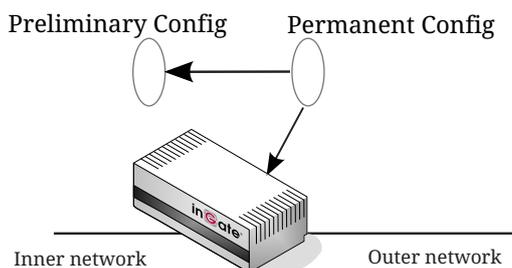
When you are done with the preliminary configuration, you can test it by selecting Apply configuration on the Save/Load Configuration page. Now the preliminary configuration controls the unit functions.



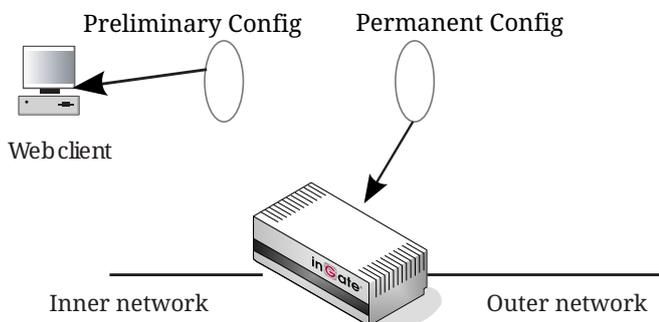
When you are satisfied with the preliminary configuration, you can apply it permanently, which copies the preliminary configuration to the permanent configuration. Now the new configuration controls the unit functions.



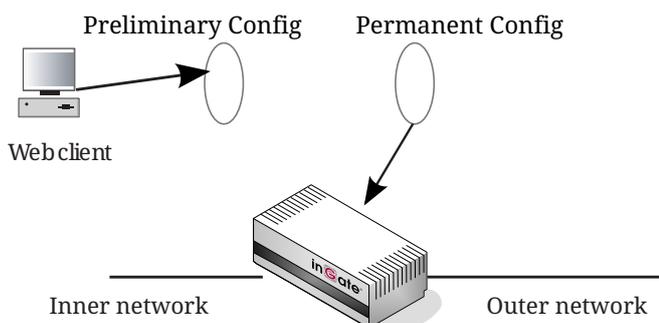
You can also copy the permanent configuration to the preliminary configuration. This does not affect the permanent configuration or the unit functions, which are still being run by the permanent configuration. You do this by selecting **Abort all edits** on the **Save/Load Configuration** page under **Administration**. This will discard all changes made in the preliminary configuration since last time you applied a configuration by pressing **Save configuration**.



You can save the preliminary configuration to a file on your work station (the computer that is running your web browser). Select **Save to local file** or **Save config to CLI file** on the **Save/Load Configuration** page.



A saved configuration can be loaded to the preliminary configuration. Use Browse to search your local computer or enter path and file name in the box. When you have chosen the file you want to load, select **Load from local file** or **Load CLI file** on the **Save/Load Configuration** page.



You can perform all of these functions on the **Save/Load Configuration** page under

## 4.5. Configuring IP addresses and masks

### 4.5.1. IP address

IP addresses are written as four groups of numbers with dots between them. The numbers must be between 0 and 255 (inclusive); for example, 192.168.129.17.

### 4.5.2. Mask/Bits

The binary system uses the numbers 0 and 1 to represent numbers. A binary digit is called a bit. Eight bits in the binary system can represent numbers from 0 to 255.

The mask indicates how much of the IP address is used for the network address and the computers' individual addresses, respectively. A mask consists of  $8+8+8+8 = 32$  bits. Below is a mask with 26 bits set to 1, which means that 26 bits of the IP address is locked to the network address and can't be changed within the network.

<b>Bits</b>	11111111	11111111	11111111	11000000
<b>No.</b>	255	255	255	192

In the unit, a mask is written either as the number of bits that are 1 or as four numbers (0-255) with dots between the numbers.

Sometimes it can be convenient to give a group of computers a network name, such as Administration, or specify that only a handful of computers can change the unit configuration.

You can form a group of computers with a network name, if the computers have consecutive IP addresses. In order to do this, you must set the mask to indicate that the network group consists of those computers only. The lowest IP address for these computers tells the network number of the group.

This is easiest to explain with a simple example. You have 7 computers that will make up a group called Administration.

Take the nearest power of two above the amount of computers you want to include: 2, 4, 8, 16, 32, 64, 128 or 256. Since you have 7 computers, 8 is the nearest. In this example, one IP address is free for future use.

Give the computers consecutive IP addresses. Make the first IP address a multiple of the power of two number you selected, but under 255. In the above example, this means 0, 8, 16, 24, 32, 40, 48 and so on, up to 248. You might choose to start with 136 ( $17 \times 8$ ). This would give the computers the IP addresses 196.176.1.136, 196.176.1.137, 196.176.1.138, 196.176.1.139, 196.176.1.140, 196.176.1.141, 196.176.1.142 and 196.176.1.143.

One of the IP addresses is free and can be used for an eighth computer in the future. You must enter the first IP address in the series, 196.176.1.136, in the **Network/IP address** field.

Now you must set the mask so that only the computers with these eight IP addresses are included in this network. Take 256 and subtract the amount of IP addresses in the named network. In the example, we would have  $256 - 8 = 248$ . The complete mask is 255.255.255.248.

Now you have created a group of computers (IP addresses) that you can give a single name, such as Administration.

Table 1. Table of netmasks

No. of computers	Mask	Bits
1	255.255.255.255	32
2	255.255.255.254	31
4	255.255.255.252	30
8	255.255.255.248	29
16	255.255.255.240	28
32	255.255.255.224	27
64	255.255.255.192	26
128	255.255.255.128	25
256	255.255.255.0	24

## 4.6. Name queries

A firewall should be as independent of other computers as possible. At the same time, the person who changes the configuration of the unit may want to use names for the computers instead of IP addresses. Also, the SIP module needs to look up names of SIP domains. This makes it necessary to use a DNS (name server) for SIP requests.

There are three instances when the unit uses a DNS server:

- When it receives a SIP request for a SIP domain.

The results of these DNS queries are stored for a short while in the unit.

- When you change names/IP addresses and save the page.

The results of these DNS queries are stored in the unit.

- When you click on **Look up all IP addresses again**.

The results of these DNS queries are stored in the unit.

- When negotiations start for an IPsec tunnel where the IPsec peer has a dynamic DNS name.

The results of these DNS queries are stored in the unit.

The unit is dependent of a working name server for the SIP functions. However, it doesn't automatically look up IP addresses in the configuration, which makes it necessary to click on **Look up all IP addresses again** every time a computer changes its IP address.

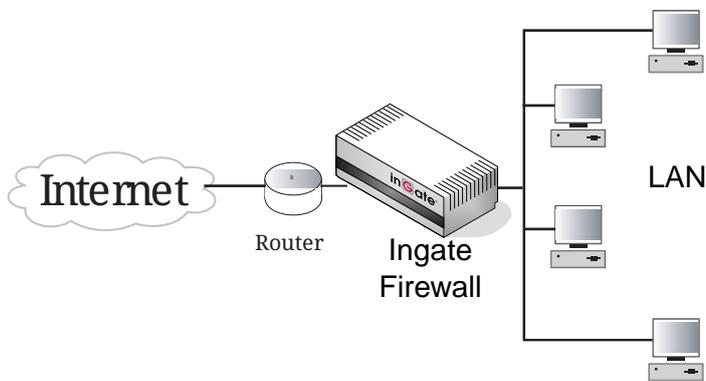
An exception to this is the **IPsec Peers** page, where you can configure the unit to look up IP addresses dynamically. The IP address of the peer is then looked up whenever an IPsec connection is negotiated.

When you enter IP addresses in the unit, they are not updated automatically. If you change a name/IP address in a row, the row is updated when you click on **Save**, switch to another page of the unit user interface, or click on **Look up all IP addresses again**.

## 4.7. Configuring the workstations

When the unit is connected to a network between a router and the organization's workstations, the default gateway of the work stations must be changed to be the unit's IP address instead.

In the figure below, a unit was connected between the router, which connects the organization to the Internet, and the organization's workstations. The workstations' settings must be changed so that the default gateway is no longer the router, but the unit's identity towards the internal network.



# Part II. Graphical Interface

This part contains complete descriptions of settings in the unit's GUI. The descriptions are grouped in the same way as they are in the GUI.

# Chapter 5. Administration

Under Administration, you

- apply your configuration
- define administrator users and change their passwords
- save the preliminary configuration to file
- load a saved configuration
- view the configuration
- reboot your unit
- restart the SIP module on your unit
- upgrade your unit
- set table formats
- set date, time, and time zone (manually or via NTP)
- select a language for the administration web pages

## 5.1. Save/Load Configuration

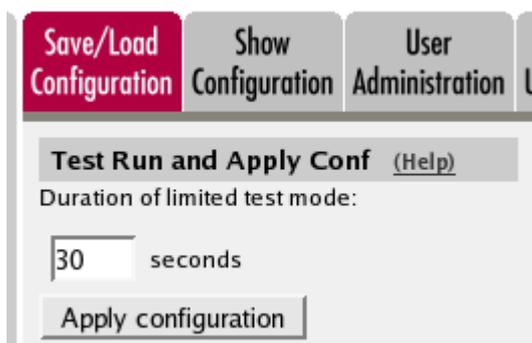
Here, you work with the preliminary and permanent configurations, save them and load new configurations from previously saved configurations.

### 5.1.1. Test Run and Apply Conf

The settings you make in the web GUI will not be used automatically, but you must apply them first. When there are settings which are not yet applied, a warning about this will be shown on the web pages.

When **Apply configuration** is pressed, the unit will test the configuration before you make it permanent.

During test, the unit waits for you to press one of the three buttons displayed. If you never see the three buttons, something in your preliminary configuration (now tested) is wrong, which makes it impossible for you to access the configuration web interface.



## Duration of limited test mode

Here, you enter the time limit for the testing. If you do not press any button within this time, the unit will assume that some part of your preliminary configuration makes connecting impossible. When the timeout is reached, the unit automatically reverts to the old permanent configuration. If this occurs, you will be informed when trying to press a button.

## Apply configuration

Saves the preliminary configuration to the permanent configuration and puts it into use. You can test your preliminary configuration before finalizing it.

Three buttons are displayed during the test:



**Save configuration** saves your preliminary configuration to the permanent configuration and puts it into use.

**Continue testing** shows a new page with only the other two buttons.

**Revert** cancels this test of the preliminary configuration without saving.

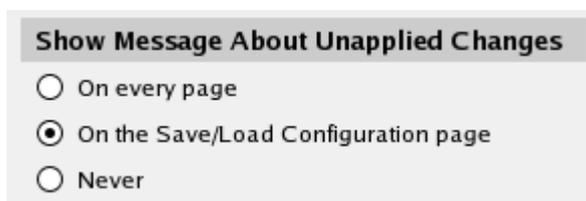
If you do not press any button within the time limit, the unit will revert to the old permanent configuration, just as if you had pressed **Revert**. This is useful if you happen to configure your unit so it isn't accessible from your browser.

After the timeout, pressing either of the three buttons will show a new page which will inform you that the test run was aborted.

Restarting the unit by cycling the power or pressing the RESET button also cancels the test.

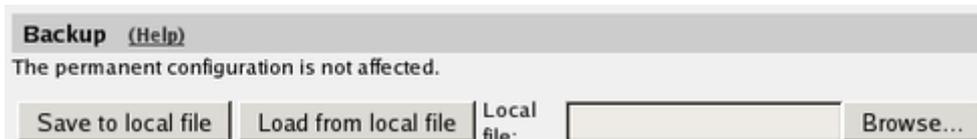
## 5.1.2. Show Message About Unapplied Changes

When there are settings which are not yet applied, a warning about this will be shown on the web pages. Select here where this message should be shown. The options are **On every page**, **On the Save/Load Configuration page** (this page) and **Never**.

A light gray rectangular box with a title bar at the top that reads 'Show Message About Unapplied Changes'. Below the title bar are three radio button options: 'On every page', 'On the Save/Load Configuration page' (which is selected with a filled circle), and 'Never'.

## 5.1.3. Backup

All configurations can be saved to and loaded from file. This does not affect the permanent configuration.



### Save to local file

Press **Save to local file** to save the preliminary configuration to the file you have selected. A new window is opened where you enter the name of the file.

### Load from local file

Press **Load from local file** to load a new preliminary configuration from the file you have selected.

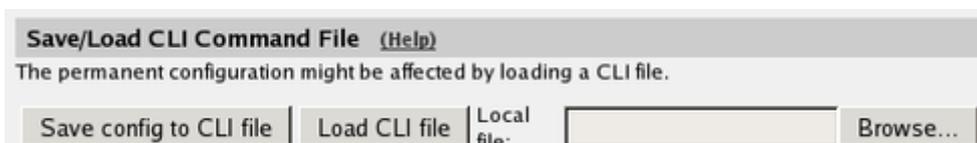
### Browse

**Browse** is used to scan your local disk. The web browser opens a new window where you can search among files and directories. Go to the right directory and select the file you want to upload.

## 5.1.4. Save/Load CLI Command File

All configurations can be saved to and loaded from a CLI file (see [Command Line Reference](#), for more information about the CLI). You can also edit the CLI file before it is uploaded again.

Uploading a CLI file might affect the permanent configuration, as the CLI file can contain commands that applies the configuration.



### Save config to CLI file

Press **Save config to CLI file** to save the preliminary configuration to the file you have selected. A new window is opened where you enter the name of the file.

### Load CLI file

Press **Load CLI file** to upload a CLI file to the unit.

### Browse

**Browse** is used to scan your local disk. The web browser opens a new window where you can search among files and directories. Go to the right directory and select the file you want to upload.

## 5.1.5. Revert to Old Configurations

You can revert to old configurations of the unit, either back to the last configuration successfully applied, or to the configuration delivered with your unit from the factory.



### Abort All Edits

**Abort all edits** copies the permanent configuration to the preliminary configuration. All changes made in the preliminary configuration are deleted.

### Reload Factory Configuration

The factory configuration is the standard configuration that is delivered with the unit. Click on this button to load this configuration into the preliminary configuration. The permanent configuration is not affected.

## 5.2. Show Configuration

Shows both the preliminary and permanent configurations, in that order. Before the preliminary configuration, you see the unit's version, serial number, the time zone, language and table format you selected.

If there are any differences between the preliminary and the permanent configuration, the message "This setting has been changed but not applied." will be shown in red at the setting in question, in the Preliminary section. If there are any errors in the preliminary configuration, this will also be marked in red in the Preliminary section.

The heading before each table for the preliminary configuration is clickable and accesses the corresponding configuration page.

Print this list from your web browser and store it in a safe place.

Save/Load Configuration	<b>Show Configuration</b>	User Administration	Upgrade	Table Look	Date and Time	Restart	Change Language
-------------------------	---------------------------	---------------------	---------	------------	---------------	---------	-----------------

Installed system: Ingate Firewall 4.8.2  
 Serial number: IG-400-205-2001-7

**Failover - Failover Status**

Failover type: Standalone  
 Dedicated interface: N/A  
 Dedicated network: N/A

**User Interface Settings**

**Administration - Save/Load Configuration**

Show message about unapplied changes: On every page  
 Duration of limited test mode (s): 30

**Administration - Table Look**

Table look: Always have an "Edit" column  
 Tables with at least this many rows have an Edit column: 10

**Administration - Date and Time**

Time zone: Linköping (Europe)

**Administration - Change Language**

Language: English

## 5.3. User Administration

On the **User Administration** page, you change the administration password for the admin account on your unit and create other administrator user accounts. The characters in the password are displayed as little stars. Remember that the password is sent unencrypted over the network if you use HTTP instead of HTTPS.

Settings made on this page (the admin password and other accounts) will not be included when saving the configuration to file. This means that you cannot move accounts defined on one unit onto another one.

You can authenticate administrators using a RADIUS server instead of a local password (select this on the **Access Control** page under **Basic Configuration**). When RADIUS is used, you must also enter a RADIUS server on the **RADIUS** page under **Basic Configuration**.

More information about how to configure the RADIUS server to authenticate administrators can be found in the [RADIUS](#) section.

### 5.3.1. Password For the *admin* Account

The *admin* user is predefined. That user can make changes, load configurations, apply configurations and log on the unit via the serial cable. You can't remove this user or change its privileges, only change its password.

Save/Load Configuration	Show Configuration	User Administration	Upgrade	Table Look	Date and Time	Restart	Change Language
-------------------------	--------------------	---------------------	---------	------------	---------------	---------	-----------------

**Password For the 'admin' Account**

Old password:

New password:

Confirm password:

### Old password

Enter the old password for the *admin* user.

### New password, Confirm password

Enter the new password in both fields. You must enter the exact same password in both fields, to make sure that you did not make a mistake.

### Change administration password

Click on this button to change the password for the *admin* user. The new password is now saved on the unit.

## 5.3.2. Other Accounts

Here, you define other user accounts that can access the unit. A user account can be restricted to only look at settings, or to change only some settings. Changes of configuration are logged by user name.

Changes in restrictions for an existing user account are immediate. The exception is changes for a currently logged on user, for which the changes will have effect the next time he/she logs on.

**Other Accounts**

Here, you define more accounts that should be able to access the firewall administration interface.

Edit row	User	Password	Account Type	Delete row
<input checked="" type="checkbox"/>	VPN-user	Change Password	VPN Admin ▾	<input type="checkbox"/>
<input checked="" type="checkbox"/>	guest	Change Password	View Config Only ▾	<input type="checkbox"/>
<input checked="" type="checkbox"/>	hasse	Change Password	SIP Admin ▾	<input type="checkbox"/>

rows.

### User

Enter the user name for this account. The name is used when the user logs on and for logging the changes.

### Password

Press the **Change password** button to enter the password for this user.

## Account Type

Select what privileges this user should have.

**View Config Only** means that the user can view any configuration and make log searches, but can't change any configuration.

**Debug** means that the user can view the unit logs.

**Backup/Restore Config** means that the user can download the configuration to file, and upload a configuration file to the unit. The user is also allowed to apply configurations.

**Full Access** means that the user can make any changes to the configuration. This is the same privileges as the admin user has in the web GUI, but only the admin user can log on via the serial cable.

**SIP Admin** means that the user can make any changes on the **SIP Services** and **SIP Traffic** pages and apply configurations, but can't change any other configuration.

**VPN Admin** means that the user can make any changes on the **Virtual Private Networks** pages and apply configurations, but can't change any other configuration.

**VPN Renegotiator** means that the user is allowed to press the **Renegotiate IPsec tunnels** button to negotiate new IPsec tunnels, but can't change any configuration.

**Off** means that the user is not allowed to log on to the web interface of the unit.

### 5.3.3. Currently Logged In Administrators

Here, all users logged on the unit web interface are shown. If your user has full access, you can log out other users here.

Currently Logged In Administrators						
Account	Type	From	Logged in	Last access	Status	Log out
admin	Full Access	193.180.23.109	2005-10-03 18:06:21	2005-10-03 18:15:07	Active	
admin	Full Access	193.180.23.181	2005-10-03 18:14:27	2005-10-03 18:14:27	Active	Log out

#### Account

The name of the logged on user.

#### Type

Here, the account type for the user is shown. The account type tells you the user's access rights for the unit web interface.

#### From

Here you see from which IP address the user connected to the unit.

## Logged In

Here you see when the user logged on to the unit.

## Last Access

Here you see when the user last accessed the unit web interface. Accesses could be a change of a parameter, a change of web page or a log search.

## Status

Here you see if the user is active or idle. The unit marks a user as idle if the user has not accessed the web interface in ten minutes.

## Log Out

If your user has full access to the web interface, you can log out other users. However, if you do not change their password (or change the Account type to Off), they can just log on again.

# 5.4. Upgrade

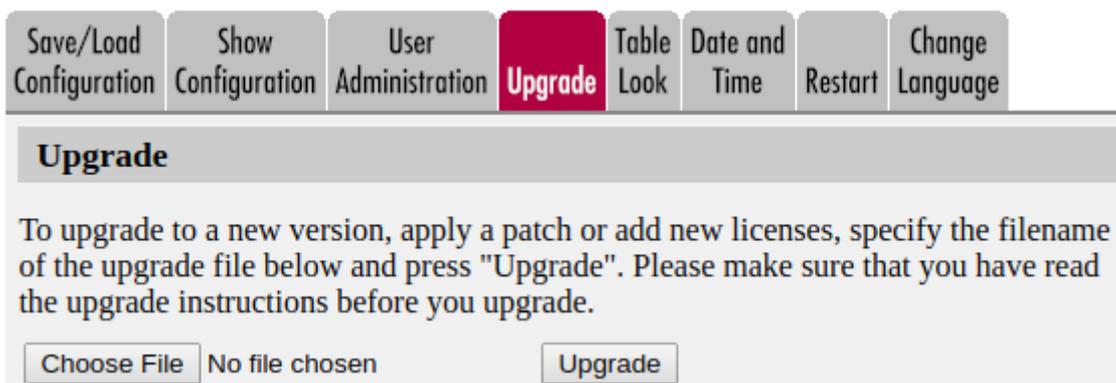
Read these instructions carefully before upgrading. You can find version upgrades for the unit at <https://account.ingate.com/>. The upgrade is signed with GNU Privacy Guard. When the unit is upgraded, it automatically checks the signing before accepting the upgrade. At <https://account.ingate.com/> you will also find User Manuals for the unit.

At <https://account.ingate.com/>, you also find upgrade instructions for this particular upgrade. These instructions tell you exactly how to upgrade your unit. They also contain information about special things to do before upgrading. Read it carefully.

You should always upgrade your unit to the latest version. The unit can check for new versions automatically. See [Basic Configuration](#).

Here, you also upgrade with extension modules (e.g. QoS) and licenses. Upgrading in this way is exactly the same procedure as upgrading to a new version.

Download the upgrade and browse to the downloaded file in the unit's interface. When you are ready to upgrade, select **Upgrade**, and await output messages.



The screenshot shows a navigation bar with buttons: Save/Load Configuration, Show Configuration, User Administration, Upgrade (highlighted in red), Table Look, Date and Time, Restart, and Change Language. Below the navigation bar is a dialog box titled "Upgrade" with the following text: "To upgrade to a new version, apply a patch or add new licenses, specify the filename of the upgrade file below and press "Upgrade". Please make sure that you have read the upgrade instructions before you upgrade." At the bottom of the dialog box, there is a "Choose File" button, a text field containing "No file chosen", and an "Upgrade" button.

## 5.4.1. Upgrade

This is the procedure to follow when upgrading the unit.

### Step 1

First save the upgrade to a file on your workstation. Enter the file name and path in the box or press **Browse** to search the disk. When you have selected a file, press **Upgrade**. The unit will read the upgrade file and check that it was correctly signed and is compatible with the current unit version.

### Step 2

If the upgrade file is correct, a text will appear at the top of the web page, informing about what version the upgrade is. Two new buttons will also be shown; **Apply upgrade** and **Remove upgrade**. You can still load new upgrades replacing the old one, which is useful if you for example have selected an upgrade which is too old.

#### Apply upgrade

Pressing **Apply upgrade** will make the unit install the new upgrade.

#### Remove upgrade

**Remove upgrade** removes the loaded upgrade from the unit. The upgrade will not be installed.

### Step 3

If **Apply upgrade** was pressed, the buttons **Try the upgrade** and **Remove upgrade** will appear.

#### Try the upgrade

**Try the upgrade** will reboot the unit and test the loaded upgrade. When the reboot is done, log on to continue upgrading the unit.

#### Remove upgrade

**Remove upgrade** removes the loaded upgrade from the unit. The upgrade will not be installed.

### Step 4

When you have pressed **Try the upgrade** and the unit has rebooted, you will see two buttons on top of every web page: **Accept upgrade** and **Abort upgrade**.

Now, you can choose to make the upgrade permanent or to revert to the old version. You can check the configuration, but no changes can be done before the upgrade is permanent. If the unit is rebooted before the upgrade is made permanent, it will revert to the old version.

#### Accept upgrade

**Accept upgrade** will complete the upgrade. When you have accepted the upgrade, you must also go to **Save/Load Configuration** and **Apply configuration**, i. e. the new upgrade.

## Abort upgrade

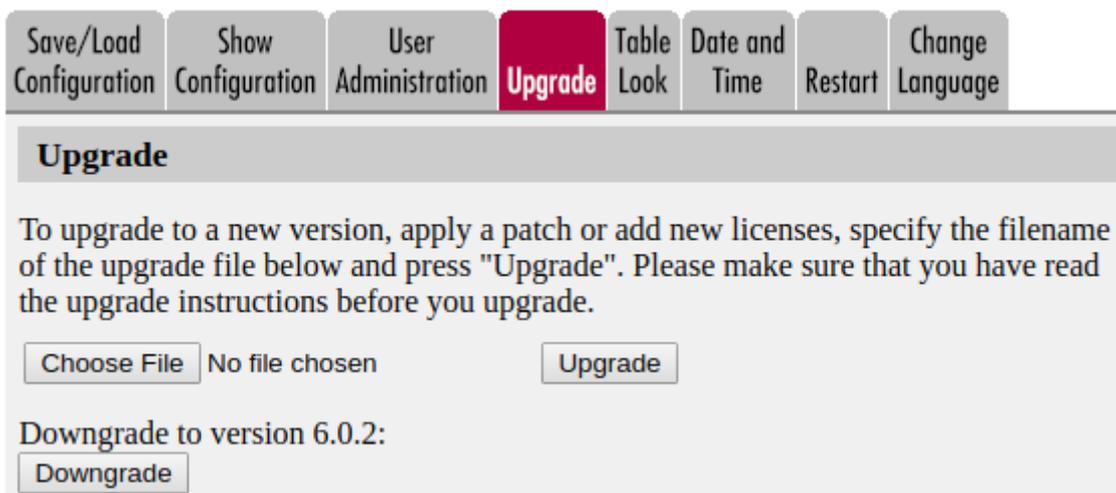
**Abort upgrade** aborts the upgrade. The unit will revert to the old version.

## 5.5. Downgrade

If the unit has been upgraded before, it is possible to downgrade to the previous version.

When you downgrade, the unit will revert to the configuration it had before upgrading. All configuration changes made after the upgrade will be lost.

When you want to upgrade, the upgrade file must be uploaded again.



The screenshot shows a navigation menu at the top with buttons for 'Save/Load Configuration', 'Show Configuration', 'User Administration', 'Upgrade' (highlighted in red), 'Table Look', 'Date and Time', 'Restart', and 'Change Language'. Below the menu is a section titled 'Upgrade' with the following text: 'To upgrade to a new version, apply a patch or add new licenses, specify the filename of the upgrade file below and press "Upgrade". Please make sure that you have read the upgrade instructions before you upgrade.' There is a file selection area with a 'Choose File' button, the text 'No file chosen', and an 'Upgrade' button. Below this is a section titled 'Downgrade to version 6.0.2:' with a 'Downgrade' button.

## 5.6. Fetch Licenses

**NOTE** | This section is only shown in supported browsers.

Here you can fetch licenses if you have a license code (XXXX-XXXX-XXXX).

The licenses are fetched by your browser and not by the unit. Thus, you can only fetch licenses if your browser has internet access.

Enter your credentials for your account at [ingate.com](https://account.ingate.com/). If you do not have an account you can create one here: <https://account.ingate.com/>

Fill in the license code and click on **Fetch**.

Save/Load Configuration   Show Configuration   User Administration   **Upgrade**   Table Look   Date and Time   Restart   Change Language

### Upgrade

To upgrade to a new version, apply a patch or add new licenses, specify the filename of the upgrade file below and press "Upgrade". Please make sure that you have read the upgrade instructions before you upgrade.

Choose File   No file chosen   Upgrade

### Fetch Licenses

You can only fetch licenses if your browser has internet access.  
Enter your credentials for your account at ingate.com.

Username:

Password:

License code:

Fetch

## 5.7. Table Look

There are two alternatives for tables in the unit: Either you can change the contents of the table directly, or else you must click on a box in the **Edit** column to allow the row to be changed. The image below shows how tables with an **Edit** column can look.

Networks and Computers   Default Gateways   All Interfaces   NAT   VLAN   Eth0   Eth1   Eth2   Interface Status   PPPoE   Topology

### Networks and Computers

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ Any	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
+ LAN	-	10.10.10.0	10.10.10.0	10.10.10.255	10.10.10.255	-	<input type="checkbox"/>
+ WAN	-	10.48.0.0	10.48.0.0	10.48.255.255	10.48.255.255	-	<input type="checkbox"/>

Add new rows    groups with  rows per group.

To change a row, click in the **Edit** box for that row and click on **Save**, **Add new rows**, or the tab for the desired configuration page. The page is updated so that you can change the configurations on the row. You can select several rows to change.

With an Edit column, tables with many rows are loaded faster, provided that only few of the Edit boxes are checked.

### 5.7.1. Edit Column

Select if all, some or none of the unit tables should have an Edit column. If you select that some tables have an Edit column, you also enter the size required to add the Edit column.

If a table has an Edit column, and the **Edit** check box is not checked for one row, this row will still be editable if there are any errors on the row.

**Save/Load Configuration** **Show Configuration** **User Administration** **Upgrade** **Table Look** **Date and Time** **Restart** **Change Language**

**Edit Column**

Tables in Ingate Firewall can be edited in one of two ways: either all contents of the table can be edited at all times, or there is an **Edit** column that you must mark to make the contents of the row editable. Many web browsers have problems handling large tables. They work better if the **Edit** column is used, and not marked in too many rows.

Always have an Edit column

Sometimes have an Edit column

Never have an Edit column

Tables with at least this many rows have an **Edit** column:

### Always have an Edit column

Regardless of the table size, all tables will have an Edit column.

### Sometimes have an Edit column

Only the tables of the size entered below will have an Edit column.

### Never have an Edit column

Regardless of the table size, no table will have an Edit column.

### Tables with at least this many rows have an Edit column

This is an additional setting which only takes effect if you selected **Sometimes have an Edit column** above. Tables with at least the amount of rows as you enter in the box will have an **Edit** column. Tables with less rows than this are changeable directly.

The standard setting for new the unit is Tables with at least **10** rows have an Edit column.

It is not advisable to enter a value higher than 15 here, or the web browser won't be able to satisfactorily manage the tables.

## 5.7.2. Save

Saves the Table Look configuration to the preliminary configuration. The change takes effect immediately.

## 5.7.3. Undo

Reverts to the previous table configuration.

## 5.8. Date and Time

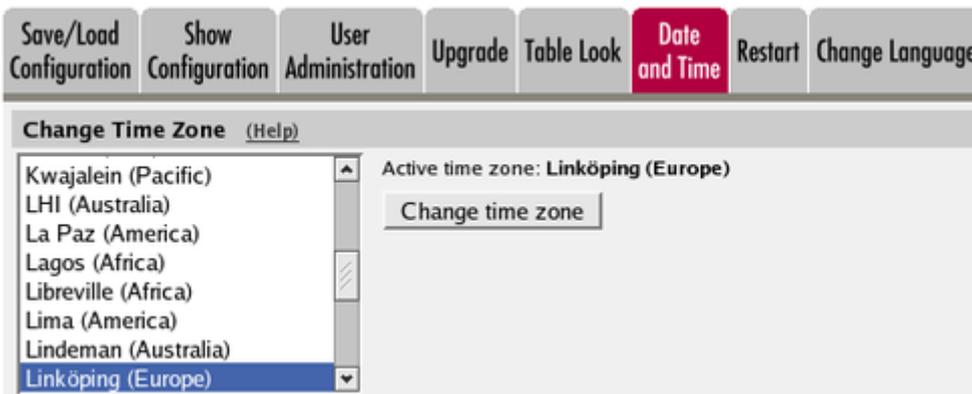
Set the unit clock to ensure that the information in the logs has the right date and time. The date

and time are displayed at the bottom of all pages. You can set the date and time manually or let the unit get the correct time from an NTP server.

Note that the unit will use these time settings when deciding whether a time class is active or not. If you change settings, configuration controlled by time classes will be affected.

### 5.8.1. Change Time Zone

Before you change the time in the unit, check that it uses the correct time zone. A change of time zone only affects the time displayed on the unit web pages; the unit clock is not changed. An effect of a time zone change is that time classes are applied differently, as they are used according to the time shown on the web pages.



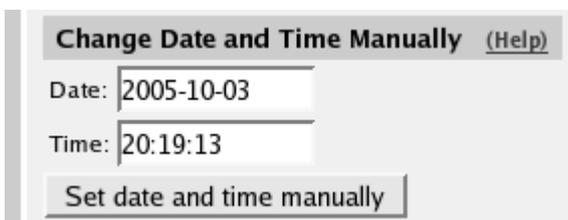
**Active time zone** shows the current time zone setting. Change time zone by selecting one in the left-hand box and press the **Change time zone** button.

Preferably, select a city in your country as opposed to selecting a GMT time zone. With the location selection, the unit will also compensate for things like Daylight Saving Time.

### 5.8.2. Change Date and Time Manually

Here you change the unit clock manually. When you change time here, there will be a time gap in the log files (if you change time forwards) or the same time will be shown twice (if you change time backwards).

N.B. Before you change time here, make sure that the unit uses the correct time zone above.



#### Date

The date is written as four digits for the year, two for the month and two for the day. The punctuation between year, month and day must be dashes (-).

## Time

Time is written as two digits for the hour, two digits for the minute and two digits for the second, although seconds can be left out. The punctuation between hours, minutes and seconds must be colon (:), or period (.). A 24-hour clock is used.

### Set date and time manually

Click on **Set date and time manually** to change the clock in the unit to what you entered in the **Date** and **Time** fields.

### 5.8.3. Change Date and Time With NTP

Instead of setting the time manually, you can let the unit get the correct time from an NTP server. The time for synchronizing will be notably shorter if the unit time is approximately correct when NTP is activated.

N.B. Before you change time here, make sure that the unit uses the correct time zone above.

**Change Date and Time With NTP** [\(Help\)](#)

Synchronize time with NTP:  Yes  No

**NTP Servers To Use If NTP Is Enabled**

Dynamic	DNS Name or IP Address	IP Address	Delete Row
-	10.47.3.222	10.47.3.222	<input type="checkbox"/>
Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

### Synchronize time with NTP

Here, select if NTP synchronizing should be enabled or not.

Enter servers to sync with in the table below.

#### Dynamic

If an interface will receive its IP address from a DHCP server, the unit can also get information about its NTP server from that server. In this case, select the corresponding IP address here and leave the other fields empty.

### 5.8.4. NTP Servers To Use If NTP Is Enabled

#### DNS Name or IP Address

The name/IP address of the NTP server to which the unit should connect. If a name is entered, you must enter the IP address for a name server on the **Basic Configuration** page.

## **IP Address**

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

## **Delete**

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## **Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## **5.8.5. Save**

Saves all Date and Time configuration to the preliminary configuration.

## **5.8.6. Undo**

Clears and resets all fields in new rows and resets changes in old rows.

## **5.8.7. Look up all IP addresses again**

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## **5.9. Restart**

Here, you can reboot the unit or restart certain modules.

When the unit is rebooted, all active sessions, including SIP sessions (SIP calls, video conferences etc), will be torn down. SIP user registrations are not affected.

When the SIP module is restarted, all active SIP sessions (SIP calls, video conferences etc) will be torn down and all SIP user registrations will be removed.

N.B! The reboot/restart will be instantaneous when the button is pressed.

Save/Load Configuration Show Configuration User Administration Upgrade Table Look Date and Time **Restart** Change Language

Here, you can reboot the firewall or restart selected modules.

**Reboot Your Software SIParator/Firewall**

When you reboot the firewall, all active sessions (including SIP sessions) are torn down.

Pressing the button will immediately reboot the firewall.

**Force Checking Log Database on Reboot** [\(Help\)](#)

Check log database on reboot:  Yes  No

**Restart the SIP Module**

When you restart the SIP module, all active SIP sessions are torn down and all SIP registrations are removed.

Pressing the button will immediately restart the SIP module.

**Automatic Restart of the SIP Module** [\(Help\)](#)

Automatically restart SIP module:  Yes  No

### 5.9.1. Reboot Your Ingate SIParator/Firewall

When this button is pressed, the unit will immediately reboot.

All active sessions, including SIP sessions, will be torn down at the reboot.

### 5.9.2. Force Checking Log Database on Reboot

When this option is enabled the log database will always be checked for errors when the the firewall reboots. Checking the database will increase the boot time. Note, you need to **save any change** to this option before clicking the **Reboot** button in this configuration tab.

### 5.9.3. Restart the SIP Module

When this button is pressed, the SIP module of the unit will restart and all SIP registrations will be removed.

All active SIP sessions will be torn down and all SIP registrations will be removed at the restart.

### 5.9.4. Automatic Restart of the SIP Module

You can make the unit monitor the SIP module. If the module stops responding, it will be restarted.

This restart will not have the same effect as when you press the **Restart SIP module** button: all active SIP sessions are torn down, but SIP registrations will not be removed. If the module is not restarted, ongoing calls will usually be unharmed, but no new calls can be set up.

## 5.10. Change Language

Here, you can choose whether to display all configuration web pages text in English or Swedish. Select the language you want to use, then click on **Change language** to change.

Save/Load Configuration   Show Configuration   User Administration   Upgrade   Table Look   Date and Time   Restart   **Change Language**

### Change Language

Select the language to use in your Ingate Firewall:

English

# Chapter 6. Basic Configuration

Under **Basic Configuration**, you configure:

- The name of the unit
- The computers and networks from which the unit can be administered
- Policies for ping packets and packets not matching any rules
- Default domain
- DNS servers
- DNS Lookup Preference
- Version control
- RADIUS configuration
- SNMP configuration
- DHCP server options
- DHCP server
- Router Advertisement
- If the unit should use external services to update a DNS server dynamically when the unit changes its own IP address.
- Creation of unit certificates and upload of CA certificates
- TLS settings
- SIParator Type

This configuration is usually not changed very often.

## 6.1. Basic Configuration

On the **Basic Configuration** page, general settings for the unit are made. The most important one for getting started is the DNS server.

### 6.1.1. General

<b>Basic Configuration</b>	Access Control	RADIUS	SNMP	DHCP Options	DHCP Server	DHCP Server Status	Router Advertisement	Dynamic DNS Update	Certificates	TLS	Advanced	SIParator Type
----------------------------	----------------	--------	------	--------------	-------------	--------------------	----------------------	--------------------	--------------	-----	----------	----------------

**General**

Name of this firewall:

Default domain:

**IP Policy**

Discard IP packets  
 Reject IP packets

**Version of Software SIParator/Firewall**

Check for new versions of Software SIParator/Firewall:  Yes  No

Date of last successful version check: **Not available**

Software version in use: **5.1.0-beta5**

**Policy For Ping To the firewall**

Never reply to ping  
 Only reply to ping to the same interface  
 Reply to ping to all IP addresses

### Name of this unit

Here, you can give your unit a name. The name of the unit is displayed in the title bar of your web browser. This can be a good idea if you administer several units. The name is also used if you use SNMP and when you export log files into the WELF format.

### Default domain

Here, you can enter a default domain for all settings. If a default domain is entered, the unit will automatically assume that an incomplete computer name should be completed with the default. If, for example, **Default domain** contains **company.com**, you could as the name of the computer **axel.company.com** use only **axel**. If no default domain should be used, the\* **Default domain\*** field should contain a single dot (.).

### 6.1.2. IP Policy

Here, you specify what will happen to IP packets that do not match any of the defined firewall rules (defined on the **Rules** page). This applies to all traffic in all directions between the different networks. **Discard IP packets** means that the unit ignores the IP packets without replying that the packet did not arrive. **Reject IP packets** makes the unit reply with an ICMP packet telling that the packet did not arrive.

### 6.1.3. Version

You can choose to turn the unit's version checker **On** or **Off** at **Check for new versions**. You must enter a **Default gateway** to enable the version checker. If a new version exists, the text "A new version exists. Check here for upgrades." will appear at the top of each configuration web page.

The unit checks for new versions every 24 hours and at reboot. **Date of last successful version check** shows when the last check was made.

### 6.1.4. Ping Policy

Here, you specify how the unit should reply to ping packets to its IP addresses. You can choose between **Never reply to ping**, **Only reply to ping from the same interface** and **Reply to ping to**

**all IP addresses. Only reply to ping from the same interface** means that the ping request should originate from a network which is directly-connected to the pinged interface of the unit or from a network to which there exists a static route from the pinged interface, or the request will be ignored.

*Ping* is a way of finding out whether a computer is working. See [Definitions of terms](#), for further information on ping.

### 6.1.5. DNS Servers

Here, you configure DNS servers for the unit. The servers are used in the order they appear in this table, which means that the unit uses the top server to resolve DNS records until it doesn't reply. Only then is server number two contacted.

DNS Servers <a href="#">(Help)</a>				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

**No.**

The DNS servers are used in the order they are presented in the table. To move a server to a certain row, enter the number on the row to which you want to move it. You need only renumber servers that you want to move; other servers are renumbered automatically. When you click on Save, the DNS servers are re-sorted.

#### Dynamic

If an interface will receive its IP address from a DHCP server, the unit can also get information about its DNS server from that server. In this case, select the corresponding IP address here and leave the other fields empty.

#### DNS Name or IP Address

The DNS name/IP address of the DNS server which the unit should use. Note that to use DNS names here, there must exist a DNS server in the unit's permanent configuration.

#### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 6.1.6. DNS Lookup Preference

Select the DNS Lookup Preference the unit should use. The selected preference determines in which order the DNS records (A and AAAA) in the DNS response should be treated.

**DNS Lookup Preference** [\(Help\)](#)

Auto ▼

The following preferences are available:

Setting	Description
Auto	If the unit is configured with IPv4 addresses only, A records will be considered (no AAAA records). If configured with IPv6 addresses only, AAAA records will be considered (no A records). If the unit is configured with both IPv4 and IPv6 addresses, AAAA records will be favoured.
Only IPv4	Only A records will be considered.
Prefer IPv4	A records will be favoured over AAAA records.
Only IPv6	Only AAAA records will be considered.
Prefer IPv6	AAAA records will be favoured over A records.

### 6.1.7. Save

Saves the Basic Configuration configuration to the preliminary configuration.

### 6.1.8. Undo

Reverts all the above fields to their previous configuration.

### 6.1.9. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered above.

## 6.2. Access Control

On the **Access Control** page, settings are made which controls the access to the unit administration interfaces. The unit can be configured via the web (http and https) and via ssh or the serial cable (using the CLI, see [Command Line Reference](#)).

Select one or more configuration IP addresses for the unit. The configuration address is the IP address to which you direct your web browser to access the web interface of the unit, or connect your ssh client to.

For each network interface, you also specify whether or not the unit can be configured via this network interface.

You also select what kind of authentication will be performed for the users trying to access the administration interfaces.

To further increase security, the unit can only be configured from one or a few computers that are accessed from one of these interfaces. Enter the IP address or addresses that can configure the unit. The IP addresses can belong to one or more computers. For each IP address or interval of addresses, select which configuration protocols are allowed.

### 6.2.1. Configuration Transport

Here you define on which protocol, address and port configuration traffic should be available. You can choose between the protocols HTTP, HTTPS and SSH.

For HTTPS you need to select a local certificate and a TLS protocol. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

For SSH configuration, the Command Language Interface is used. See [Command Line Reference](#).

You can use different IP addresses for HTTP, HTTPS, and SSH configuration.

Protocol	IP Address	Port	Cert	TLS	Delete Row
HTTP ▼	eth0 (10.48.28.61) ▼	80	- ▼	- ▼	<input type="checkbox"/>
HTTPS ▼	eth1_inet6 (2001:470:dc8c:1000::28:61) ▼	443	httpsconfig ▼	TLSv1.x ▼	<input type="checkbox"/>
SSH ▼	eth0 (10.48.28.61) ▼	22	- ▼	- ▼	<input type="checkbox"/>

Add new rows  rows.

#### Protocol

The protocol used for configuration traffic. Available protocols are HTTP, HTTPS and SSH.

#### IP Address

The unit's IP addresses configured on the **Interface** pages under **Network**.

#### Port

The port that will be used for configuration traffic. Default port for HTTP is 80, default for HTTPS is 443 and default for SSH is 22.

#### Cert

A local private certificate. A certificate must be selected if you use HTTPS.

## TLS

Select the TLS protocol that will be used when configuring via HTTPS.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.2.2. Configuration Allowed Via Interface

This setting specifies whether configuration traffic is allowed via this interface. If you only allow configuration via eth1, configuration traffic will only be allowed from computers connected to the eth1 interface, regardless of which IP address the configuration traffic is directed to or which IP addresses the computers have. This configuration is a complement to the **Configuration Computers** setting below.

Configuration Allowed Via Interface <a href="#">(Help)</a>		
Interface or Tunnel	Allowed	Delete Row
Ethernet0 (eth0) ▾	Yes ▾	<input type="checkbox"/>
Ethernet1 (eth1) ▾	Yes ▾	<input type="checkbox"/>

rows.

### Interface or Tunnel

Interface or Tunnel on which configuration traffic should allowed/disallowed.

### Allowed

Allow configuration traffic on this **Interface or Tunnel**.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.2.3. User Authentication For Web Interface Access

**User Authentication For Web Interface Access** [\(Help\)](#)

Local users  
 RADIUS database  
 Local users or RADIUS database

Select the mode of administrator authentication for logins via the web interface: **Local users**, via a **RADIUS database**, or a choice between the two alternatives at login (**Local users or RADIUS database**).

Local administrator users and their passwords are defined on the **User Administration** page under **Administration**. If the authentication should be made by help of a RADIUS server, you must enter one on the **RADIUS** page.

When connecting to the administration interface via SSH, you can only log in as admin.

### 6.2.4. Web Interface Access Settings

**Web Interface Access Settings** [\(Help\)](#)

Login timeout:  seconds

The Login timeout setting specifies how long (in seconds) before a logged in web GUI user needs to re-authenticate. The range is 300-28800 seconds.

### 6.2.5. Configuration Computers

Enter the IP address or addresses that can configure the unit. The IP addresses can belong to one or more computers.

Note that you must also allow configuration via the unit interface that the computers are connected to. See [Configuration Allowed Via Interface](#) above.

**Configuration Computers** [\(Help\)](#)

No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0 - 255.255.255.255	- ▾	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	- ▾	<input type="checkbox"/>
2	2001:470:dc8c:1000::	2001:470:dc8c:1000::	64	2001:470:dc8c:1000: - 2001:470:dc8c:1000:ffff:ffff:ffff:ffff	- ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	- ▾	<input type="checkbox"/>

Add new rows  rows.

**No.**

The **No.** field determines the order of the lines. The order is important in deciding what is logged and warned for. The unit uses the first line that matches the configuration traffic.

Perhaps you want to configure the unit so that configuration traffic from one specific computer is simply logged while traffic from the rest of that computer's network is both logged and generates alarms.

The rules are used in the order in which they are listed, so if the network is listed first, all configuration traffic from that network is both logged and generates alarms, including the traffic

from that individual computer. But if the individual computer is listed on a separate line before the network, that line will be considered first and all configuration traffic from that computer is only logged while the traffic from the rest of the computer's network is both logged and generates alarms.

### **DNS Name or Network Address**

Enter the DNS name or IP address of the computer or network from which the unit can be configured. Avoid allowing configuration from a network or computer on the Internet or other insecure networks, or use HTTPS or IPsec to connect to the unit from these insecure networks.

### **Network Address**

Shows the network address of the **DNS Name or Network Address** you entered in the previous field.

### **Netmask/Bits**

**Netmask/Bits** is the mask that will be used to specify the configuration computers. See [Configuring](#), for instructions on writing the netmask. To limit access so that only one computer can configure, use the netmask 255.255.255.255. You can also specify the netmask as a number of bits, which in this case would be 32. To allow configuration from an entire network, you must enter the network address under **Network Address**, and a netmask with a lower number here. To allow configuration from several computers or networks, create several lines for the information.

### **Range**

The **Range** shows all IP addresses from which the unit can be configured. The range is calculated from the configuration under **DNS Name or Network Address** and **Netmask/Bits**. Check that the correct information was entered in the **DNS Name or Network Address** and **Netmask/Bits** fields.

### **Via IPsec Peer**

Here, you can select an **IPsec Peer** from which this connection must be made. If an IPsec peer is selected, you will only be able to configure the unit from this IP address through an IPsec tunnel.

### **SSH**

Check the check box if this computer/network should be allowed to configure the unit via SSH.

### **HTTP**

Check the check box if this computer/network should be allowed to configure the unit via HTTP.

### **HTTPS**

Check the check box if this computer/network should be allowed to configure the unit via HTTPS.

### **Log Class**

Here, you enter what log class the unit should use to log the configuration traffic to the unit's web

server. Log classes are defined on the **Log Classes** page under **Logging and Tools**. See also [Logging and Tools](#).

### **Delete**

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### **Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### **6.2.6. Save**

Saves the Access Control configuration to the preliminary configuration.

### **6.2.7. Undo**

Reverts all the above fields to their previous configuration.

### **6.2.8. Look up all IP addresses again**

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## **6.3. RADIUS**

RADIUS (Remote Authentication Dial-In User Service) is an authentication system consisting of one or more servers, and clients using the servers to authenticate users. You could, for example, equip the company modems with RADIUS clients, demanding that a user connecting to a modem first identifies himself to the RADIUS server. Servers and clients communicate via UDP.

The unit uses RADIUS for authentication for administration, for SIP users, and VPN connections from road warriors. If RADIUS is used for user authentication from VPN connections, you must do additional configuration on the **Authentication Server** page.

The unit can also send accounting information about SIP calls to a RADIUS server.

### **6.3.1. RADIUS Servers**

Enter the server(s) that the unit should use. When more than one RADIUS server is entered, make sure that their databases contain the same data, since the unit regards them all alike and uses the server which first replies to a request.

Basic Configuration	Access Control	<b>RADIUS</b>	SNMP	DHCP Server	DHCP Server Status	Dynamic DNS Update	Certificates	Advanced
---------------------	----------------	---------------	------	-------------	--------------------	--------------------	--------------	----------

**RADIUS Servers** [\(Help\)](#)

Edit Row	RADIUS Server		Port	Secret	Delete Row
	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	193.180.23.77	193.180.23.77	1645		<input type="checkbox"/>

Add new rows  rows.

## RADIUS server

Enter the **DNS Name or IP Address** for the RADIUS server used for authentication.

In IP Address, the IP address of the server is shown. It is updated whenever **Look up all IP addresses** again is pressed, or the **DNS Name or IP Address** field is changed.

## Port

The official port for RADIUS is UDP port 1812. However, several RADIUS servers use port 1645, so you may have to change the port number either on the RADIUS server or in the table.

## Secret

A RADIUS authentication requires a *shared secret*, which must be the same on both sides. Since the secret is used as an encryption key, it is important that it is kept a secret. Since the secret is saved unencrypted in the unit configuration, you should be careful with where you store the configuration.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.3.2. Contact IP Address

Select the IP address from which the unit should make connections to RADIUS servers.

<p><b>Contact IP Address</b> <a href="#">(Help)</a></p> <p>Contact RADIUS servers from:</p> <p><input type="text" value="Outside (193.12.253.115)"/></p>	<p><b>Identifier</b> <a href="#">(Help)</a></p> <p>Use NAS-IP-Address: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>NAS-Identifier: <input type="text"/></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Contact RADIUS servers from

Select an IP address from which the unit should make connections to the RADIUS server. A

convenient choice of address is one on the interface closest to the server. Select from the IP addresses configured for the unit interfaces under **Directly Connected Networks** and **Alias**.

### 6.3.3. Identifier

A RADIUS client may use either of two ways to identify itself for the RADIUS server: an IP address or a name (identifier). You must use at least one of these ways, or the authentication will fail.

Select here which method to use. The address or name in use must be registered at the RADIUS servers specified in the top table, and must be unique in that RADIUS database.

#### Use NAS-IP-Address

If you select **Yes**, the unit's IP address (the address selected under **Contact IP Address**) will be enclosed as identity. If you select **No**, you must enter a **NAS-Identifier** for the unit.

#### NAS-Identifier

You can enter a special identifier into this field. All characters except space are allowed according to the unit, but your RADIUS server may have some restrictions on the identifier.

### 6.3.4. Status for RADIUS Servers

At the bottom of the page the status for the RADIUS servers is shown. Radiusmux is the part that connects to the RADIUS servers.

If no authentication by RADIUS is configured, the radiusmux is not run. When you apply a configuration which involves contacting a RADIUS server, the radiusmux is started.

Status for RADIUS Servers						
RADIUS server	Score	Sent requests	Received replies	Consecutive sends	Recent average response time	Free slots
193.180.23.239	8.41	14	14	0	0.005755 s	256

(Counters are reset when any RADIUS server is reconfigured or when the firewall reboots.)

#### RADIUS server

The IP address for this RADIUS server.

#### Score

Radiusmux gives points (the scale is 1 to 40, inclusive) to the different servers according to their performance. The better server performance, the higher score. Radiusmux uses the score to select which server to query primarily.

#### Sent requests

The number of UDP packets sent to this server.

### **Received replies**

The number of UDP packets received from this server.

### **Consecutive sends**

The number of consecutive UDP packets sent without response from the server.

### **Recent average response time**

A calculated average of response time for packets for which response has been received.

### **Free slots**

The RADIUS server allocates a certain number of slots for each RADIUS client, and every pending request from the unit occupies a slot. Here you see the current number of free slots.

### **6.3.5. Save**

Saves the RADIUS configuration to the preliminary configuration.

### **6.3.6. Undo**

Reverts all of the above fields to their previous configuration.

### **6.3.7. Look up all IP addresses again**

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

### **6.3.8. Configuration of a RADIUS server**

In this section it is assumed that you know how to configure your RADIUS server. Consult your RADIUS manual for details.

Add the unit as a client in the RADIUS server. Make sure that the shared secret here is the same as in the unit.

The unit checks the permissions for a user by looking at its RADIUS attribute *Service-Type*.

If the *Service-Type* has the value *Administrative (6)*, the user is allowed to configure the unit.

If the value is *Framed (2)*, the user is allowed to connect via VPN.

For the various privileges for users, there is an Ingate-specific RADIUS attribute defined thus:

```

VENDOR Ingate 13465

ATTRIBUTE IG-Admin-Account 1 integer Ingate

#
# Type of administrator account.
#
VALUE IG-Admin-Account Full-Access-Admin 1
VALUE IG-Admin-Account Backup-Admin 2
VALUE IG-Admin-Account Read-Only-Admin 3
VALUE IG-Admin-Account VPN-Admin 4
VALUE IG-Admin-Account SIP-Admin 5
VALUE IG-Admin-Account VPN-Reneg-Admin 6

```

To be able to authenticate SIP users, the RADIUS server must support Digest authentication. You find a description of this in draft-sterman-aaa-sip-02 (Internet draft). This is all that is required for it to work with the unit.

More information about RADIUS can be found in RFC 2865.

## 6.4. SNMP

SNMP is a network monitoring protocol, which enables a single server to monitor one or more networks, including all network equipment like routers and firewalls. The unit supports SNMP and can accordingly be monitored automatically.

The monitoring signaling consists of two main parts. The SNMP server sends requests to the unit, which replies with a list of network parameters and their values for the unit. The unit can also send messages (traps) without the server prompting, when someone sends a request without valid authentication and when the unit boots. You can also configure the unit to send traps when certain threshold values are reached.

The unit can only send parameters to the server; no changes of configuration can be made through SNMP requests.

For more information about SNMP, read RFC 1157.

### 6.4.1. General

Here, select the IP addresses (local and remote) involved in the SNMP signaling. You can also enter contact information for the unit.

Basic Configuration	Access Control	RADIUS	<b>SNMP</b>	DHCP Server	DHCP Server Status	Dynamic DNS Update	Certificates	Advanced
---------------------	----------------	--------	-------------	-------------	--------------------	--------------------	--------------	----------

---

**General**

The firewall IP address to respond to SNMP requests:  Contact person:

Servers allowed to contact the firewall via SNMP:  Node location:

### The firewall IP address to respond to SNMP requests

Select the IP address of the unit to which the SNMP servers should direct their requests. Select from the addresses defined on the **Interface** pages under **Network**.

### Servers allowed to contact the firewall via SNMP

Select the SNMP server(s) which are allowed to contact the unit. You select from the network groups defined on the **Networks and Computers** page under **Network**.

### Contact person

Enter the name of the contact person for this unit. This information is sent with the parameter list as reply to an SNMP request from the server.

### Node location

Enter the location of the unit. This information is sent with the parameter list as reply to an SNMP request from the server.

## 6.4.2. SNMP v1 and v2c

In SNMP version 1 and 2c, the authentication is managed through an unencrypted password, a community. Here, you select if the unit should accept access via v1 or v2c, and enter the valid communities.

**SNMP v1 and v2c**

Access via SNMPv1 and SNMPv2c:  On  Off

Edit Row	Community	Delete Row
<input type="checkbox"/>	ingate-common	<input type="checkbox"/>

Add new rows  rows.

### Access via SNMPv1 and SNMPv2c

Select if access via SNMP version 1 or 2c (using communities as the authentication method) should be On or Off.

## Community

Enter a password. Note that this password is stored unencrypted.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

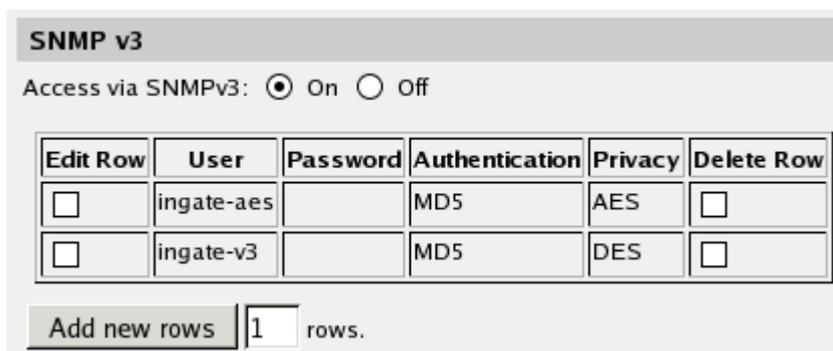
## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 6.4.3. SNMP v3

In SNMP version 3, the authentication is managed through the server sending a username and an (in most cases) encrypted password to the unit, which verifies the validity of them.

Here, you select if the unit should accept access via v3, and select the authentication and encryption used for the SNMP requests.



The image shows a configuration interface for SNMP v3. At the top, there is a header 'SNMP v3'. Below it, there is a label 'Access via SNMPv3:' followed by two radio buttons: 'On' (which is selected) and 'Off'. Below this is a table with six columns: 'Edit Row', 'User', 'Password', 'Authentication', 'Privacy', and 'Delete Row'. There are two rows of data in the table. The first row has an unchecked checkbox, the user 'ingate-aes', an empty password field, 'MD5' for authentication, 'AES' for privacy, and an unchecked checkbox. The second row has an unchecked checkbox, the user 'ingate-v3', an empty password field, 'MD5' for authentication, 'DES' for privacy, and an unchecked checkbox. Below the table, there is a button labeled 'Add new rows' followed by a text input field containing the number '1' and the text 'rows.'.

Edit Row	User	Password	Authentication	Privacy	Delete Row
<input type="checkbox"/>	ingate-aes		MD5	AES	<input type="checkbox"/>
<input type="checkbox"/>	ingate-v3		MD5	DES	<input type="checkbox"/>

Add new rows  rows.

## Access via SNMPv3

Select if access via SNMP version 3 (using usernames and encrypted passwords as the authentication method) should be **On** or **Off**.

## User

Enter a username which the server should use when contacting the unit.

## Password

Press the **Change password** button to enter a password for this user.

## Authentication

Select the authentication algorithm to use for SNMP requests. The unit supports the **MD5** and **SHA-1** algorithms.

## Privacy

Select whether the SNMP request should be encrypted using AES or DES, or not be encrypted at all.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.4.4. SNMP Traps

If **Trap sending function** is On, the unit will send messages (traps) to the server(s) entered below whenever an SNMP authentication fails or the unit boots. They are also sent when the status is changed for an IPsec tunnel, and when the unit discovers that a new software version is available.

You can also configure the unit to send traps when certain levels are reached (see Resource Monitoring).

SNMP traps are sent from the IP address closest to the receiving SNMP server. If the unit has been assigned more than one IP address on that network, the address given in the **Directly Connected Networks** table will be used.

If the trap sending is disabled, no traps will be sent.

**SNMP Traps**

Trap sending function:  On  Off

Edit row	Trap receiver		Community	Version	Delete row
	DNS name or IP address	IP address			
<input type="checkbox"/>	10.47.2.13	10.47.2.13	server-mode	v2c	<input type="checkbox"/>

Add new rows  rows.

## Trap sending function

Select if trap sending (at boot and failed SNMP authentication) should be **On** or **Off**.

## Trap receiver

Enter the IP address, or a name in the DNS, of the server to which the unit should send traps. If you enter a DNS name instead of an IP address, you must enter the IP address of a DNS server on the **Basic Configuration** page.

IP Address shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

## Community

Enter the password (community) which the unit should use when sending traps. The community is sent unencrypted over the network.

## Version

Select the SNMP version to be used for traps. You can select v1 or v2c.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.4.5. Resource Monitoring

Your unit can send SNMP traps when usage passes certain levels. Set the levels here. The trap receivers are configured in the **SNMP Traps** table.

For each usage, there is an **Alarm by** and a **Resume by** level. When the usage hits the **Alarm by** level, the unit sends a trap about this and locks the trap sending for that usage, which means that as long as the level stays high, no more traps are sent. When the level goes down to below the **Resume by** level, the lock is released. Next time the **Alarm by** level is reached, a new trap is sent.

To avoid excessive trap sending, it is recommended that the **Alarm by** and **Resume by** levels for a resource are not set too close.

<b>SIP Sessions Trap Levels</b> <a href="#">(Help)</a>	<b>CPU Load Trap Levels</b> <a href="#">(Help)</a>
Alarm by: <input type="text" value="60"/> Resume by: <input type="text" value="50"/>	Alarm by: <input type="text" value="70"/> % Resume by: <input type="text" value="50"/> %
<b>SIP User Registrations Trap Levels</b> <a href="#">(Help)</a>	<b>Memory Usage Trap Levels</b> <a href="#">(Help)</a>
Alarm by: <input type="text" value="150"/> Resume by: <input type="text" value="120"/>	Alarm by: <input type="text" value="70"/> % Resume by: <input type="text" value="50"/> %

### SIP Sessions Trap Levels

Enter the SIP sessions levels here. When the amount of SIP sessions reaches the Alarm by level, an SNMP trap is sent.

### SIP User Registrations Trap Levels

Enter the SIP user registrations levels here. When the amount of registered SIP users reaches the Alarm by level, an SNMP trap is sent.

### CPU Load Trap Levels

Enter the CPU load levels here. When CPU usage increases above the Alarm by limit, an SNMP trap is sent.

### Memory Usage Trap Levels

Enter the memory usage levels here. When memory usage increases above the Alarm by limit, an SNMP trap is sent.

### 6.4.6. Download the Ingate MIB

This link leads to the Ingate-specific MIB (Management Information Base) definition for your unit.

The unit also supports these standard MIBs:

- mibII.system
- mibII.interfaces
- mibII.at
- mibII.ip
- mibII.icmp
- mibII.tcp
- mibII.udp
- mibII.snmp

### 6.4.7. Save

Saves the SNMP configuration to the preliminary configuration.

### 6.4.8. Undo

Reverts all of the above fields to their previous configuration.

### 6.4.9. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 6.5. DHCP Options

If you want your DHCP Server to pass custom DHCP options to the clients you can define them here.

### 6.5.1. DHCP Data Types

In this table you can define new DHCP data types and create structures (a.k.a. Records) using the built in standard types. Records can contain arbitrary number of standard types. STRING and TEXT types can only be present once within the same record. These types must be the last type in a record (highest order).

## DHCP Data Types [\(Help\)](#)

Edit Row	Name	Order	Type	Delete Row
<input type="checkbox"/>	+ Boolean	1	BOOLEAN	<input type="checkbox"/>
<input type="checkbox"/>	+ IPv4 address	1	IPv4	<input type="checkbox"/>
<input type="checkbox"/>	+ IPv6 address	1	IPv6	<input type="checkbox"/>
<input type="checkbox"/>	+ Integer (16)	1	INT16	<input type="checkbox"/>
<input type="checkbox"/>	+ Integer (32)	1	INT32	<input type="checkbox"/>
<input type="checkbox"/>	+ Integer (8)	1	INT8	<input type="checkbox"/>
<input type="checkbox"/>	+ String	1	STRING	<input type="checkbox"/>
<input type="checkbox"/>	+ Text	1	TEXT	<input type="checkbox"/>
<input type="checkbox"/>	+ Unsigned Integer (16)	1	UINT16	<input type="checkbox"/>
<input type="checkbox"/>	+ Unsigned Integer (32)	1	UINT32	<input type="checkbox"/>
<input type="checkbox"/>	+ Unsigned Integer (8)	1	UINT8	<input type="checkbox"/>
<input type="checkbox"/>	+ sip-server	1	UINT8	<input type="checkbox"/>
<input type="checkbox"/>		2	IPv4	<input type="checkbox"/>

Add new rows  groups with  rows per group.

### Name

A name for the Data Type. The name is used in the **Data Type** column when you create [DHCP Options](#).

### Order

The order is used to specify the order of a **Type** within a record (structure). The **Type** with the lowest number will be first and the one with the highest number will be last.

### Type

The type determines how the data type should be interpreted. The following types are available:

Type	Description	Example
BOOLEAN	A flag value that can be on or off (true or false).	true
UINT8	Unsigned integer with width 8 (min: 0, max: 255).	250
UINT16	Unsigned integer with width 16 (min: 0, max: 65535).	33500
UINT32	Unsigned integer with width 32 (min: 0, max: 4294967295).	1421331872
INT8	Signed integer with width 8 (min: -128, max: 127).	120
INT16	Signed integer with width 16 (min: -32768, max: 32767).	-20000

Type	Description	Example
INT32	Signed integer with width 32 (min: -2147483648, max: 2147483647).	145324
IPv4	An IPv4 address. Can be expressed as a domain name or in dotted quad format.	192.168.1.1 or sip.example.com
IPv6	An IPv6 address.	::1 or 2001:470:dc8c:1000::66:22
TEXT	An ASCII text string. Must be quoted.	"tftp.example.com"
STRING	A collection of bytes. Can be specified as quoted text or as a colon separated hexadecimal list.	9f:b6:54:ed:fa:b3 or "String of text"

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.5.2. DHCP Options

A DHCP option has a **Name**, a **Code** and a **Value**. The **Value** must match the selected **Data Type**. E.g. *true* for **BOOLEAN** and *"example text"* for **TEXT**.

Options can contain an **Array** of values (except for **STRING** and **TEXT** types). Multiple values are separated by comma. When adding values to a record all the values must be set. E.g. for a record of type *{IPv4, BOOLEAN, UINT8}* one legal value is *192.168.1.1, true, 254*. A legal array value for the same record could be *192.168.1.1, true, 254, 192.168.100.10, off, 0*.

**NOTE** | A DHCPv6 option **Name** must be prefixed with *ipv6-*. E.g. *ipv6-vendor-opts*.

In order to use the created options, invoke the created *"opts-subnet-A"* or *"opts-subnet-B"* via the setting **Options** found in [IP Ranges](#).

**DHCP Options** [\(Help\)](#)

Group Name	Name	Code	Value	Data Type	Array	Delete Row
+ opts-subnet-A	tftp-server	66	"tftpserver.example.com"	Text	No	<input type="checkbox"/>
	tftp-file	67	"/my/path/file.cfg"	Text	No	<input type="checkbox"/>
	sip-options	120	1,192.168.1.1	sip-server	No	<input type="checkbox"/>
+ opts-subnet-B	ipv6-sip-servers-ad	22	2001:470:dc8c:1100::1	IPv6 address	Yes	<input type="checkbox"/>

Add new rows  groups with  rows per group.

### Group Name

The group name is the name that will be used when the options in this group is referenced from other parts of the configuration, see [IP Ranges](#). A group can contain one or more DHCP options.

### Name

The name of the DHCP option. Note that DHCPv6 option names must be prefixed with *ipv6-*.

### Code

The DHCP option code. The codes for different options are defined by the DHCP protocol.

### Value

The value that should be passed to the DHCP client. The value entered must match the selected **Data Type**.

### Data Type

A data type is defined in [DHCP Data Types](#). Select the appropriate data type for the entered **Value**.

### Array

Set the array setting to *Yes* if the **Value** contains multiple values or if the DHCP option is defined as an *array* of a certain type.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 6.5.3. Save

Saves the DHCP Options configuration to the preliminary configuration.

## 6.5.4. Undo

Reverts all of the above fields to their previous configuration.

## 6.6. DHCP Server

The unit can act as a DHCP server for clients on one or more of its interfaces.

The DHCP server can not listen on an interface where the unit obtains its IP address dynamically. It is also not possible for it to listen to the same interface as the DHCP relay.

Note: Do not create DHCP ranges larger than 24 bits (256 addresses) on flash memory models, and lower internal memory. Doing so, you will receive strange errors and performance issues.

### 6.6.1. General

Turn the DHCP server in the unit on or off, and enter client lease times for the DHCP clients.

The screenshot shows a web interface for configuring the DHCP server. At the top, there are several tabs: Basic Configuration, Access Control, RADIUS, SNMP, DHCP Server (highlighted in red), DHCP Server Status, Dynamic DNS Update, Certificates, and Advanced. Below the tabs, the 'DHCP server' section is expanded, showing two radio buttons: 'Enable DHCP server' (selected) and 'Disable DHCP server'. Below this, there is a 'Domain' field with the value 'ingate.com'. To the right of the domain field is a 'Client Lease Time' section with three rows: 'Minimum' with a value of 60 seconds, 'Default' with a value of 43200 seconds, and 'Maximum' with a value of 86400 seconds.

#### General

Select to turn the DHCP server **On** or **Off**.

#### Domain

Enter the domain that the DHCP clients should use.

#### Client Lease Time

Enter values for the client lease time. Clients can send a suggested lease time in their DHCP requests. If this time is lower than **Minimum**, the Minimum time is used as the lease time. If the suggested time is higher than **Maximum**, the Maximum time is used as the lease time. If the client does not suggest a lease time, the **Default** value is used. In other cases, the client's suggestion is used as the lease time.

## 6.6.2. IP Ranges

Here, you select the interface(s) on which the unit should listen for DHCP requests. For each interface selected, enter a range of IP addresses, which the DHCP server can lease to the clients on that interface, and a default gateway for the clients.

Listen To ...	IP Range (lower limit)		IP Range (upper limit)		Gateway		Options	Delete Row
	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
Ethernet1 (eth1 untagged) ▾	<input type="text" value="10.5.1.20"/>	<input type="text" value="10.5.1.20"/>	<input type="text" value="10.5.1.200"/>	<input type="text" value="10.5.1.200"/>	<input type="text"/>	<input type="text"/>	opts-subnet-A ▾	<input type="checkbox"/>

Add new rows  rows.

### Listen To

Select an interface on which the unit DHCP server should listen for DHCP requests. Note that the DHCP server and the DHCP relay can't listen to the same interface.

### IP Range (lower limit)

Enter the first IP address in the range, or a corresponding DNS name.

### IP Range (upper limit)

Enter the last IP address in the range, or a corresponding DNS name.

### Gateway

Enter the default gateway for this IP range, or a corresponding DNS name. If the unit should send its own IP as gateway, you enter "\*" here.

### Options

Select an option that is defined in [DHCP Options](#)

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.6.3. DNS Servers

Select how the DHCP clients should get DNS server information. You can use separate DNS servers for the DHCP clients. The Manual DNS Servers table will only be used if **Assign DNS servers** was set to **Manual**.

**DNS Servers** [\(Help\)](#)

Assign DNS servers: **Manual DNS Servers**

Auto Assign  
 **Manual**  
 Don't assign

Edit Row	No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
<input type="checkbox"/>	2	Internet		Internet	<input type="checkbox"/>

**Add new rows**  rows.

## Assign DNS servers

Select if the unit should assign DNS servers for the DHCP clients. **Auto Assign** will make the unit send the DNS servers entered on the **Basic Configuration** page. **Manual** will make it send the DNS servers entered in the table below. If **Off** is selected, no DNS servers are assigned.

## Manual DNS Servers

### No.

The DNS servers are assigned to the clients in the order presented in the table. To move a server to a certain row, enter the number on the row to which you want to move it. You need only renumber servers that you want to move; other server are renumbered automatically. When you click on **Save**, the DNS servers are re-sorted.

### Dynamic

If an interface will receive its IP address from a DHCP server, the unit can also get information about DNS servers from the server for further distribution to the DHCP clients. In this case, select the corresponding IP address here.

### DNS Name or IP Address

Enter the DNS name or IP address for the DNS server.

### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.6.4. NetBIOS Settings

Select NetBIOS node type and enter WINS servers for the DHCP clients.

The screenshot shows the 'NetBIOS Settings' window. On the left, under 'Assign NetBIOS node type:', a dropdown menu is set to 'Hybrid - WINS, then broadcast'. Below it, 'NetBIOS over TCP/IP:' has three radio buttons: 'Send option with value "Enabled"', 'Send option with value "Disabled"', and 'Don't send this option' (which is selected). On the right, 'Manual WINS Servers' contains a table with one row: No. 1, DNS Name or IP Address 10.5.1.4, IP Address 10.5.1.4. Below the table is an 'Add new rows' button and a text box containing '1' followed by 'rows.'.

Edit Row	No.	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	1	10.5.1.4	10.5.1.4	<input type="checkbox"/>

### Assign NetBIOS node type

The unit can tell the clients how to look up NetBIOS names by setting their NetBIOS node type. Available options are: **Off** (no node type is set), **Broadcast - no WINS**, **Peer - WINS only**, **Mixed - Broadcast, then WINS**, and **Hybrid - WINS, then broadcast**.

### NetBIOS over TCP/IP

If you run a modern network without NetBIOS, you can use a Microsoft specific DHCP option to request clients to disable NetBIOS. Select *Send option with value "Disabled"* to do this.

### Manual WINS Servers

#### No.

The WINS servers are assigned to the clients in the order presented in the table. To move a server to a certain row, enter the number on the row to which you want to move it. You need only renumber servers that you want to move; other server are renumbered automatically. When you click on Save, the WINS servers are re-sorted.

#### DNS Name or IP Address

Enter the DNS name or IP address for the WINS server.

#### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.6.5. Save

Saves all DHCP Server configuration to the preliminary configuration.

## 6.6.6. Undo

Clears and resets all fields in new rows and resets changes in old rows.

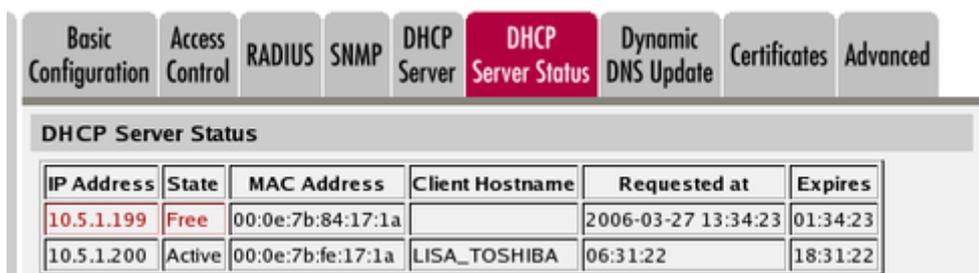
## 6.6.7. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 6.7. DHCP Server Status

On this page, details are shown about the IP addresses the unit DHCP server has leased out.



The screenshot shows a web interface with a navigation bar containing tabs: Basic Configuration, Access Control, RADIUS, SNMP, DHCP Server, DHCP Server Status (highlighted in red), Dynamic DNS Update, Certificates, and Advanced. Below the tabs is a section titled "DHCP Server Status" containing a table with the following data:

IP Address	State	MAC Address	Client Hostname	Requested at	Expires
10.5.1.199	Free	00:0e:7b:84:17:1a		2006-03-27 13:34:23	01:34:23
10.5.1.200	Active	00:0e:7b:fe:17:1a	LISA_TOSHIBA	06:31:22	18:31:22

### 6.7.1. DHCP Server Status

#### IP Address

The IP address leased to the DHCP client.

#### State

The state for this IP address is shown here. If the client uses the address, the state is Active. If the client was assigned this address before, but isn't using it right now, the state is Free. The next time the same client requests an IP address, the same address will be assigned, provided that the unit did not run out of DHCP addresses during its absence.

#### MAC Address

The MAC address for the client leasing, or which most recently leased, the IP address.

#### Client Hostname

The hostname for the client leasing the IP address.

## Requested at

The time when this IP address was leased to the client.

## Expires

The time when this lease will expire.

# 6.8. Router Advertisement

If enabled the unit will listen to ICMPv6 *Router Solicitation* messages and respond with a ICMPv6 *Router Advertisement* message. The unit will also send periodic *Router Advertisement* messages. These messages are part of the IPv6 *Neighbor Discovery Protocol* (NDP). In addition to IPv6 router discovery the unit also supports *Stateless Address Autoconfiguration* (SLAAC).

### IPv6 Router Advertisement [\(Help\)](#)

- Enable IPv6 Router Advertisement
- Disable IPv6 Router Advertisement

## 6.8.1. Interface Settings

Here you specify which interfaces and VLANs that should be enabled for processing Router solicitation and advertisement messages.

### Interface Settings [\(Help\)](#)

Name	Interface	Default Router	Managed	Other Config	RDNSS	Delete Row
lan_slaac	Ethernet1 (eth1 untagged) ▼	Yes ▼	No ▼	No ▼	Yes ▼	<input type="checkbox"/>

Add new rows  rows.

### Name

The name of the interface. This name will be referenced in setting **Interface** in table [Prefix Settings](#).

### Interface

The interface or VLAN that should listen for *Router Solicitation* messages and send *Router Advertisement* messages

### Default Router

Advertise as default router.

### Managed

Set the managed address configuration flag (M-bit).

## Other Config

Set the other configuration flag (O-bit).

## RDNSS

Send RDNSS (Recursive DNS Server) if available. DNS servers are read from **DNS Servers** on **Basic Configuration** page.

## Delete

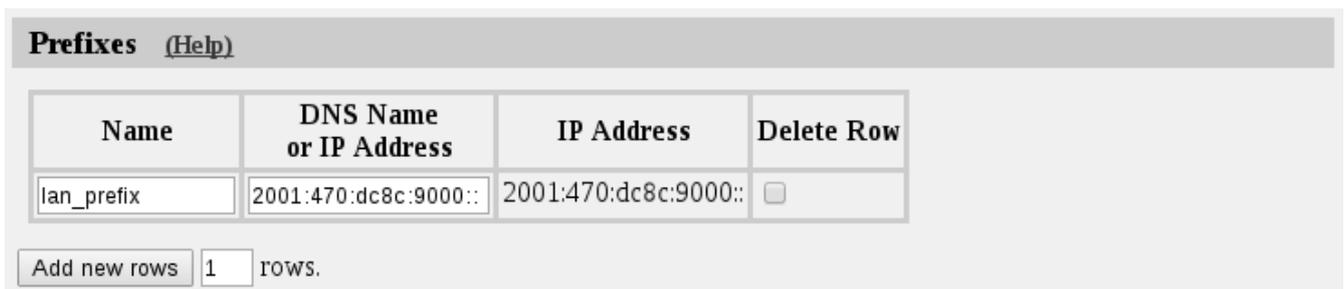
If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.8.2. Prefixes

Here you define network prefixes that should be advertised via router advertisement. The prefixes should have a 64 bit prefix length.



Name	DNS Name or IP Address	IP Address	Delete Row
lan_prefix	2001:470:dc8c:9000::	2001:470:dc8c:9000::	<input type="checkbox"/>

Add new rows  rows.

### Name

The name of the prefix. This name will be referenced in setting **Prefix** in table [Prefix Settings](#).

### DNS Name or IP Address

The prefix to be advertised.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.8.3. Prefix Settings

Here you specify which prefixes that should be advertised. Select the interface where you want the

prefix to be advertised on.

Prefix Settings <a href="#">(Help)</a>		
Prefix	Interface	Delete Row
lan_prefix ▼	lan_slaac ▼	<input type="checkbox"/>
Add new rows <input type="text" value="1"/> rows.		

### Prefix

Select a prefix from [Prefixes](#).

### Interface

Select an interface from [Interface Settings](#).

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.8.4. Save

Saves all Router Advertisement configuration to the preliminary configuration.

## 6.8.5. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 6.9. Dynamic DNS update

Usually, static DNS servers are used to associate a domain or host name with an IP address. If the unit gets its public IP address via DHCP or PPPoE, the static DNS servers will not work, as they do not automatically change bindings when the unit gets a new IP address.

The unit supports dynamic DNS update at DynDNS.org and Hurricane Electric Free DNS. You must purchase the update service at DynDNS.org before you can use it.

On this page you can also configure dynamic update of the client IPv4 address for the service *Hurricane Electric IPv6 Tunnel Broker*. Please refer to the GUI help for more information.

### 6.9.1. Dynamic DNS General Configuration

Here, make settings which the unit will use when updating IP addresses at DynDNS.org or Hurricane Electric. In the descriptions below, the example domain example.com is used.

Basic Configuration	Access Control	RADIUS	SNMP	DHCP Options	DHCP Server	DHCP Server Status	Router Advertisement	<b>Dynamic DNS Update</b>	Certificates	TLS	Advanced	SIParator Type
---------------------	----------------	--------	------	--------------	-------------	--------------------	----------------------	---------------------------	--------------	-----	----------	----------------

**Dynamic DNS** [\(Help\)](#)

Enable Dynamic DNS  
 Disable Dynamic DNS

Dynamic DNS service: Use wildcard hostnames:  Yes  No

Hurricane Electric Free DNS ▼ Offline URL redirection:  Yes  No

IP address for updates:

eth0 (10.48.28.61) ▼

## Enable Dynamic DNS

Select if the unit should use Dynamic DNS services to update IP addresses.

## Dynamic DNS service

Select which service you use at DynDNS or Hurricane Electric.

## IP address for updates

Select the IP address which the unit should send. If a dynamic IP address is selected, the unit will update the Dynamic DNS service every time the address changes.

## Wildcard hostnames

If you select to turn this feature **On**, all DNS queries for any *hostname.example.com* will return your IP address. If this feature is **Off**, only queries for *example.com* will return your IP address.

## Offline URL redirection

If **Offline URL redirection** is on, queries for your domain will be redirected to another URL if your server is down. The URL is entered on the dyndns.org web site. If no URL is set, queries will be redirected to a general web page at dyndns.org.

This is an add-on service at DynDNS.

## 6.9.2. User, SMTP Server

Enter user details needed when the unit updates information at the Dynamic DNS service.

You can also enter an SMTP server to report to DynDNS.

User	SMTP Server
Username: <input type="text" value="dmlisa"/>	SMTP server: <input type="text" value="mail.ingate.com"/>
Password: <input type="button" value="Change Password"/>	SMTP server is backup: <input type="radio"/> Yes <input checked="" type="radio"/> No

### Username

Enter your Dynamic DNS service username. This is needed when the unit updates its IP address.

### Password

Press the button to enter your Dynamic DNS service password. This is needed when the unit updates its IP address.

### SMTP server

Enter the host name of your SMTP server. This is the name that SMTP DNS queries for *example.com* should return.

You can't enter an IP address here; neither can you enter a host name that is a CNAME (a kind of DNS alias), but must enter the server's primary name.

### SMTP server is backup

If you selected **No** here, the DynDNS server will assume that the SMTP server entered above is the primary email server for *example.com*.

If you selected **Yes**, the DynDNS server will assume that your primary email server is the one associated with the DNS name *example.com*, and that the SMTP server entered above is a backup server to take over when the primary server is unreachable.

## 6.9.3. CA Certificate

Select a previously imported CA Certificate that is needed to verify the server certificate of the Dynamic DNS service. No verification will be done unless one is selected.

## 6.9.4. DNS Names to Update

Enumerate the domain and host names that should be connected to the IP address selected above. If **Wildcard hostnames** was selected as **On**, you only need to enter domain names; the Dynamic DNS server will return the same IP address for every hostname under the domain. If it is **Off**, you need to enter every hostname separately.

**CA Certificate** [\(Help\)](#)

ca\_bundle\_mozilla ▾

**DNS Names to Update** [\(Help\)](#)

DNS Name	Delete Row
ighome.dyndns.org	<input type="checkbox"/>
tunnel282506.tunn	<input type="checkbox"/>

Add new rows  rows.

### DNS Name

Enter the DNS name to be associated to the unit IP address.

### Delete

If you select this box, the row is deleted when you click on Add new rows or Save.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on Add new rows.

### 6.9.5. Save

Saves the Dynamic DNS update configuration to the preliminary configuration.

### 6.9.6. Undo

Reverts all of the above fields to their previous configuration.

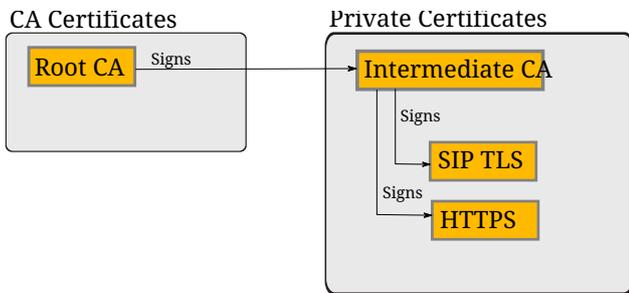
## 6.10. Certificates

Here, you create X.509 certificates for the unit, to be used for authentication in various applications, like when configuration over HTTPS is performed.

On this page you also upload CA certificates to the unit. For the applications (HTTPS, VPN, RADIUS authentication of road warriors, and SIP over TLS), you select one or more CA certificates to trust.

Certificates can be built up from certificate chains. A certificate chain is a sequence of certificates, where each certificate in the chain is signed by the subsequent certificate.

Root Certificates are entered into **CA Certificates** while all other Certificates (including Intermediate Certificates and Peer Certificates) are entered into **Private Certificates**.



You do not upload certificates here for IPsec peers where you have the peer's own certificate (as opposed to a CA certificate). These certificates are uploaded on the **IPsec Peers** page.

### 6.10.1. Private Certificates

Here the private X.509 certificates of the unit are created. You can use the same certificate for all authentication purposes, or create different certificates for the various functions in the unit.

Basic Configuration   Access Control   RADIUS   SNMP   DHCP Server   DHCP Server Status   Dynamic DNS Update   <b>Certificates</b>   Advanced						
Private Certificates (Help)						
Edit Row	Name	Certificate			Information	Delete Row
<input checked="" type="checkbox"/>	Inside	Create New	Import	View/Download	Subject: /CN=10.47.3.243 Issuer: /CN=10.47.3.243 MDS Fingerprint: F0:28:F2:F6:96:D0:A2:EE:AD:A6:0F:D1:8B:97:9A:99 Valid to: 2008-03-05 13:58:07	<input type="checkbox"/>
<input type="checkbox"/>	RADIUS				Subject: /ST=sweden/O=ingate/CN=sip.ingate.com Issuer: /ST=sweden/O=ingate/CN=sip.ingate.com MDS Fingerprint: 0C:23:74:2F:BA:73:96:9B:2B:E0:46:CC:3A:79:C4:18 Valid to: 2009-04-29 13:02:50	<input type="checkbox"/>
<input type="checkbox"/>	VPN cert				Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MDS Fingerprint: B6:F3:5D:88:DC:90:86:96:E2:F8:AA:E9:BC:7A:15 Valid to: 2010-02-07 13:03:58	<input type="checkbox"/>
<input type="checkbox"/>	main cert				Subject: /O=ingate/CN=sip.ingate.com Issuer: /O=ingate/CN=sip.ingate.com MDS Fingerprint: 57:45:30:EC:A3:B7:5C:65:87:21:86:58:82:4F:84:80 Valid to: 2008-02-26 12:51:17	<input type="checkbox"/>

Add new rows | 1 rows.

#### Name

Enter a name for this certificate. The name is only used internally in the unit.

#### Certificate

Create, import or download a private certificate. See more information about creating certificates below. Under **Import**, you upload unit certificates signed by an external CA or external intermediate CA.

Under **View/Download**, you download the private certificate, and you can also download the key pair.

#### Information

Information about this certificate, such as the signing CA and expiration date.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.10.2. Create certificate or certificate request

Press **Create New** to create a new X.509 certificate. A new page with a form appears, requesting information about the unit. Fill in the form to apply for a certificate or create a self-signed certificate. Fields marked \* are mandatory.

### Create Certificate or Certificate Request

Fill in the certificate data for "" below, then create either a certificate or a certificate request.  
After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days):	Country code (C):	Organization (O):
* <input type="text" value="365"/>	<input type="text"/>	<input type="text"/>
Common Name (CN):	State/province (ST):	Organizational Unit (OU):
* <input type="text"/>	<input type="text"/>	<input type="text"/>
Email address	Locality/town (L):	
<input type="text"/>	<input type="text"/>	

### SubjectAltName Extension

Enter the alternative names that you want to add to a certificate or a certificate request. Multiple values can be added by using comma separation.

Email:	<input type="text"/>
URI:	<input type="text"/>
DNS:	<input type="text"/>
IP:	<input type="text"/>

### Key Length and Signature Algorithm

Select the key length and the signature algorithm that you want to use when creating a certificate or a certificate request.

Key length (bits):	<input type="text" value="2048"/>
Signature algorithm:	<input type="text" value="SHA-256"/>

If you generate several certificates with identical data you should make sure they have different serial numbers. Below you can enter an optional challenge password.

Serial number:	Challenge password:
* <input type="text" value="0"/>	<input type="text"/>
Challenge password again:	<input type="text"/>

Fields marked with "\*" are mandatory.

## Expire in

The expiration time defines how many days the certificate will last. Default time is 365 days, one year.

## Common Name

Here, you enter the host name or IP address of the unit.

## Email address

Enter the email address of the unit administrator.

**Country code**

Here, you enter the country code - not the top domain - for the country where the unit is located. The country code for the USA is US.

**State/province**

The state or province where the unit is located.

**Locality/town**

The city or town where the unit is located.

**Organization**

The name of the organization/company owning the unit.

**Organizational Unit**

The department using the unit.

**SubjectAltName Extension**

Enter the alternative names that you want to add to a certificate or a certificate request. Multiple values can be added by using comma separation.

**Email:**

Enter one or more email addresses

**URI:**

Enter one or more URI's

**DNS:**

Enter one or more DNS names

**IP-Addresses**

Enter one or more IP-Addresses

**Key Length and Signature Algorithm**

Select the key length and the signature algorithm that you want to use when creating a certificate or a certificate request.

**Key length (bits):**

The length of the generated keys.

## Signature algorithm:

The hashing algorithm to use when signing the certificate.

## Serial number

If you generate more than one certificate with the same information, and you want to give them separate names and treat them as different certificates, you need to give them different serial number. Enter a serial number for this certificate here.

## Challenge password

Enter a password. This will be used only when revoking a signed certificate.

## Create a self-signed X.509 certificate

By entering the requested information above and pressing this button, you can create a certificate that isn't signed by any certificate authority (CA). Self-signed certificates are for free, while certificates signed by an official CA normally are not. Certificates signed by CAs are automatically accepted by web browsers, while you have to accept self-signed certificates manually when using them in your web browser.

## Create an X.509 certificate request

When pressing this button, you make a certificate request which can be sent to a certificate authority for signing. The request is downloaded under View/Download on the certificate page. The signed certificate is uploaded under Import.

## Abort

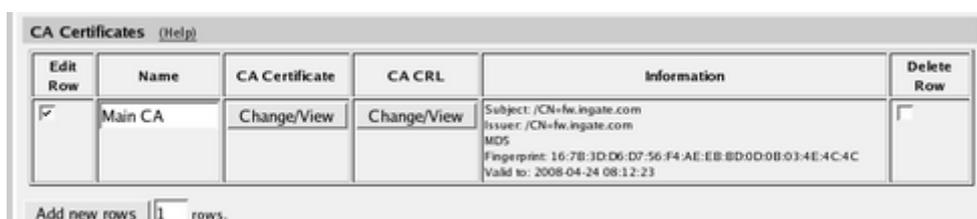
Press the Abort button to return to the Certificates page without creating a new certificate or certificate request.

## 6.10.3. CA Certificates

Here, you upload CA certificates and CRLs (Certificate Revocation Lists).

The CAs are used to authenticate peers using IPsec VPN or TLS. Upload one or more CA certificates here, and then select which CAs to trust for each function in the unit.

CRLs are used to let the unit know that some of the certificates signed by a certain CA should not be accepted. This could be useful when laptops with certificates are stolen. See instructions for your CA on how to make a CRL.



Edit Row	Name	CA Certificate	CA CRL	Information	Delete Row
<input checked="" type="checkbox"/>	Main CA	Change/View	Change/View	Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MOS Fingerprint: 16:7B:3D:D6:D7:56:F4:AE:EB:8D:0D:0B:03:4E:4C:4C Valid to: 2008-04-24 08:12:23	<input type="checkbox"/>

Add new rows  rows.

## **Name**

Enter a name for this CA certificate. The name is only used internally in the unit.

## **CA Certificate**

You upload the CA certificate to the unit, inspect the current certificate, or download it to use somewhere else, by pressing the **Change/View** button.

## **CA CRL**

A CRL (Certificate Revocation List) is used to tell the unit that some certificates issued by this CAs are not valid, even though they may not have expired yet. Upload a CRL for this CA by pressing the Change/View button.

## **Information**

Information about this certificate, such as the signing CA and expiration date.

## **Delete**

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## **Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## **6.10.4. Save**

Saves all Certificates configuration to the preliminary configuration.

## **6.10.5. Undo**

Clears and resets all fields in new rows and resets changes in old rows.

# **6.11. TLS**

## **6.11.1. TLS Settings**

Here you group the TLS protocols, ciphers, Diffie-Hellman Group and ECDH Curve to a name that can be referenced from other pages.

**TLS Settings** [\(Help\)](#)

Name	Protocols	Ciphers	Diffie-Hellman Group	ECDH Curve	Delete Row
DTLSv1.x	DTLSv1.x ▼	HIGH ▼	MODP2048 (Group 14) ▼	NIST P-256 (secp256r1) ▼	<input type="checkbox"/>
SSLv3.0	SSLv3.0 ▼	HIGH ▼	MODP2048 (Group 14) ▼	NIST P-256 (secp256r1) ▼	<input type="checkbox"/>
TLSv1.x	TLSv1.x ▼	HIGH ▼	MODP2048 (Group 14) ▼	NIST P-256 (secp256r1) ▼	<input type="checkbox"/>
TLSv1.x & SSLv3.	TLSv1.x & SSLv3.0 ▼	HIGH ▼	MODP2048 (Group 14) ▼	NIST P-256 (secp256r1) ▼	<input type="checkbox"/>

Add new rows  rows.

### Name

Enter a name for this TLS setting. The name can be referenced from other pages.

### Protocols

Here you select the protocols for this setting. The protocols are defined in the **Protocols** table.

### Ciphers

Here you select the ciphers for this setting. The ciphers are defined in the **Ciphers** table.

### Diffie-Hellman Group

Here you optionally select the Diffie-Hellman Group for this setting.

### ECDH Curve

Here you select the ECDH curve for this setting.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.11.2. Protocols

Here you name a group of TLS protocols. The name can be referenced from the **TLS Settings** table.

**Protocols** [\(Help\)](#)

Name	Protocol	Delete Row
+ DTLSv1.x	DTLSv1.0 ▼	<input type="checkbox"/>
	DTLSv1.2 ▼	<input type="checkbox"/>
+ SSLv3.0	SSLv3.0 ▼	<input type="checkbox"/>
+ TLSv1.x	TLSv1.1 ▼	<input type="checkbox"/>
	TLSv1.2 ▼	<input type="checkbox"/>
+ TLSv1.x & SSLv3	SSLv3.0 ▼	<input type="checkbox"/>
	TLSv1.0 ▼	<input type="checkbox"/>
	TLSv1.1 ▼	<input type="checkbox"/>
	TLSv1.2 ▼	<input type="checkbox"/>

Add new rows  groups with  rows per group.

**Name**

Enter a name for this protocol group. The name can be referenced from the **TLS Settings** table.

**Protocol**

Here you select the protocol to use in this group. By clicking on the plus sign beside the name, you add more rows where you can specify more protocols for this group.

**Delete**

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

**Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

**6.11.3. Ciphers**

Here you name a cipher list. The name can be referenced from the **TLS Settings** table.

**Ciphers** [\(Help\)](#)

Name	Ciphers	Delete Row
HIGH	HIGH:!aNULL:!MD5	<input type="checkbox"/>

Add new rows  rows.

**Name**

Enter a name for this cipher list. The name can be referenced from the **TLS Settings** table.

## Ciphers

Here you enter a cipher list. The cipher list format is defined by OpenSSL.

[You can read more about the cipher list format in the OpenSSL manual.](#)

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 6.11.4. Save

Saves all TLS configuration to the preliminary configuration.

## 6.11.5. Undo

Clears and resets all fields in new rows and resets changes in old rows.

# 6.12. Advanced Settings

## 6.12.1. Timeouts

The unit saves information (for example NAT information) about all connections made to other units. Here, you can set timeouts for different types of connections. The timeout defines how long the unit should wait after sending or receiving a packet for the connection before it discards the information about the connection.

Long timeouts consume memory for all connections.

They also keep holes open in the unit long after the traffic has ceased to flow.

Short timeouts kill connections that you might want to keep alive, like ssh tunnels through the unit.

Basic Configuration	Access Control	RADIUS	SNMP	DHCP Options	DHCP Server	DHCP Server Status	Router Advertisement	Dynamic DNS Update	Certificates	TLS	<b>Advanced</b>	Separator Type
---------------------	----------------	--------	------	--------------	-------------	--------------------	----------------------	--------------------	--------------	-----	-----------------	----------------

**Timeouts** [\(Help\)](#)

Timeout for one-way UDP connections:  seconds

Timeout for established TCP connections:  seconds

Timeout for two-way UDP connections:  seconds

Timeout for ICMP connections:  seconds

Timeout for ICMPv6 connections:  seconds

### Timeout for one-way UDP connections

The Timeout for one-way UDP connections regards UDP connections where packets have only been sent in one direction.

### Timeout for two-way UDP connections

The Timeout for two-way UDP connections regards UDP connections where packets have been sent in both directions.

### Timeout for established TCP connections

The Timeout for established TCP connections regards TCP connections where the three-way (SYN, SYN+ACK, ACK) handshake has been completed, which means that the connection is fully established.

### Timeout for ICMP connections

The Timeout for ICMP connections regards ICMP connections, like ping.

### Timeout for ICMPv6 connections

The Timeout for ICMPv6 connections regards ICMPv6 connections, like ping6.

## 6.12.2. Port Allocation Ranges

Local ports used by the unit for outgoing connections.

Any changes here require a restart of the unit to take full effect.

Port Allocation Ranges <a href="#">(Help)</a>		
Auto:	<input type="text" value="1024"/>	- <input type="text" value="32767"/>
FTP:	<input type="text" value="57000"/>	- <input type="text" value="58023"/>
NAT:	<input type="text" value="61000"/>	- <input type="text" value="65096"/>
RADIUS:	<input type="text" value="65097"/>	- <input type="text" value="65200"/>

#### Auto

The port range that is used to automatically choose the local port for outgoing connections for services not listed below.

#### FTP

The port range that is used to choose the local port for the FTP relay.

#### NAT

The port range that is used to choose the local port for NAT.

## RADIUS

The port range that is used to choose the local port for the RADIUS client.

### 6.12.3. IP Fragments

Select whether to discard weird IP fragments or process them. Weird IP fragments are fragments that shouldn't appear normally, e.g. overlapping fragments.

#### IP Fragments [\(Help\)](#)

- Process weird fragments
- Discard weird IP fragments

### 6.12.4. Enforce RFC 4890 ICMPv6 filter recommendations

Select *Yes* (the default) to enforce the ICMPv6 filter recommendations specified in RFC 4890 (section 4.3.1). The section specifies ICMPv6 messages that must not be dropped by the firewall. If these messages are dropped IPv6 communication to and from the unit might not work as expected. Note that this setting doesn't affect traffic flowing through the unit.

#### Enforce RFC 4890 ICMPv6 filter recommendations [\(Help\)](#)

- Yes
- No

The following ICMPv6 messages will be allowed to and from the unit:

Name	Type	Code
Destination Unreachable	1	All
Packet Too Big	2	All
Time Exceeded	3	0
Parameter Problem	4	1, 2
Echo Request	128	All
Echo Response	129	All

### 6.12.5. Options

Table for entering advanced options after consultation with the Ingate support team.

#### Options [\(Help\)](#)

Name	Value	Delete Row
------	-------	------------

Add new rows  rows.

## 6.12.6. Save

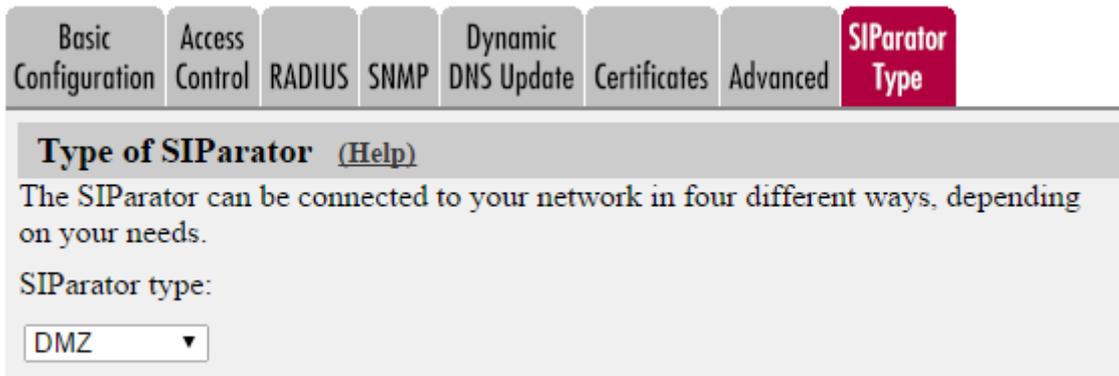
Saves the Advanced Settings configuration to the preliminary configuration.

## 6.12.7. Undo

Reverts all of the above fields to their previous configuration.

# 6.13. SIParator Type

## 6.13.1. Type of SIParator (SIParator Mode)



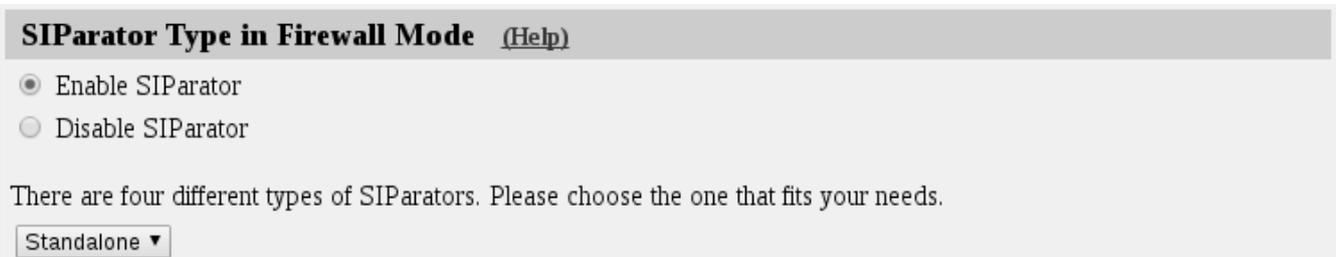
The screenshot shows a configuration interface with a top navigation bar containing tabs: Basic Configuration, Access Control, RADIUS, SNMP, Dynamic DNS Update, Certificates, Advanced, and SIParator Type (which is highlighted in red). Below the tabs is a header for "Type of SIParator" with a "(Help)" link. The main content area contains the text: "The SIParator can be connected to your network in four different ways, depending on your needs." followed by "SIParator type:" and a dropdown menu currently set to "DMZ".

### SIParator Type

There are five different types of SIParators. Please choose the one that fits your needs.

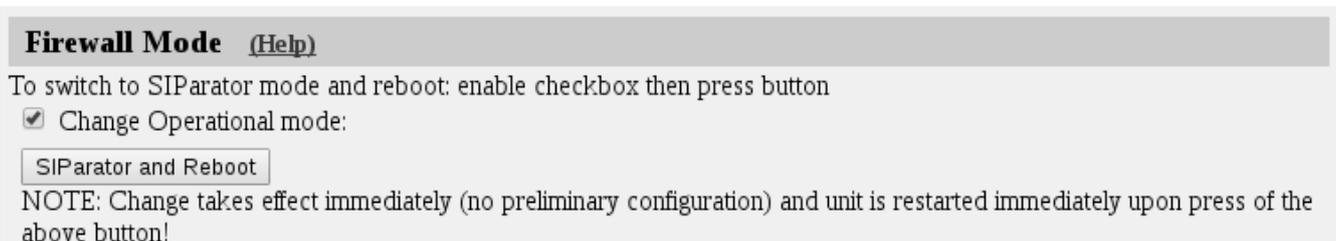
## 6.13.2. Type of SIParator (Firewall Mode)

Enable this setting if you want to use SIParator types in Firewall mode. There are five different types of SIParators. Please choose the one that fits your needs. When this setting is active, SIParator functionality is available in Firewall mode.



The screenshot shows a configuration interface for "SIParator Type in Firewall Mode" with a "(Help)" link. It features two radio button options: "Enable SIParator" (which is selected) and "Disable SIParator". Below the options is the text: "There are four different types of SIParators. Please choose the one that fits your needs." followed by a dropdown menu currently set to "Standalone".

## 6.13.3. Change Operational Mode



The screenshot shows a configuration interface for "Firewall Mode" with a "(Help)" link. It contains the text: "To switch to SIParator mode and reboot: enable checkbox then press button" followed by a checked checkbox labeled "Change Operational mode:". Below the checkbox is a button labeled "SIParator and Reboot". A note at the bottom states: "NOTE: Change takes effect immediately (no preliminary configuration) and unit is restarted immediately upon press of the above button!"

Check the Change Operational mode box, then press the button to set the new mode. This product can operate in two different operational modes: Firewall or SIParator. In Firewall mode all traffic (both SIP and data traffic) is going through this unit. In SIParator mode this unit only deals with SIP traffic - normal data traffic is handled by another firewall. There are several different SIParator modes available.

**NOTE**

When pressing the button to switch operational mode the change is instant and the unit is immediately rebooted! The unit shall be in factory default mode when performing the operational mode change.

# Chapter 7. Network

Under **Network**, you configure:

- Network groups which are used for the unit configuration
- The unit's IP addresses on all network interfaces
- Routings for the networks so that computers behind routers can be contacted
- NAT (IP masquerading)
- VLAN settings
- PPPoE settings
- IPv4 → IPv6 transition tunnels.

## 7.1. Networks and Computers

### 7.1.1. Networks and Computers

Here, you name groups of computers and networks. Sometimes it can be useful to give a group of computers a network name, such as Administration. If you want to group some computers, this can be done here, even if they do not have consecutive IP addresses. You can also include a subgroup when defining a new network group.

These names are used when you configure **Rules**, **Filtering**, **Local Registrar** and other settings.

The rows are sorted in alphabetical order, except that all upper case letters are sorted before lower case letters (B comes before a).

When using an already defined group as a subgroup, select the name of the group under **Subgroup**. Set **Interface/VLAN** to "-" and leave the other fields empty.

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ Any	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
+ LAN	-	10.10.10.0	10.10.10.0	10.10.10.255	10.10.10.255	-	<input type="checkbox"/>
+ WAN	-	10.48.0.0	10.48.0.0	10.48.255.255	10.48.255.255	-	<input type="checkbox"/>

Add new rows  groups with  rows per group.

#### Name

Enter a name for the group of computers. You can use this name when you change configuration on the pages mentioned above. A group can consist of several rows of IP addresses or series of IP addresses. By clicking on the plus sign beside the name, you add more rows where you can specify more IP addresses for this group.

## Subgroup

An already defined group can be used as a subgroup to new groups. Select the old group here and leave the fields for **DNS name** empty. Select "-" as **Interface**. If you don't want to use a subgroup, select "-" here.

## Lower Limit

### DNS Name or IP Address

Enter the **DNS name or IP address** of the network or computer. For computers in an IP range that you want to give a network name, enter the first IP address in the range. DNS Name or IP Address must not be empty if you are not using a subgroup.

### IP Address

The IP address of the object you entered in the DNS Name or IP Address field is displayed here. This field is not updated until you click on **Look up all IP addresses again** or make changes in the **DNS Name or IP Address** field.

## Upper Limit

### DNS Name or IP Address

Here, enter the last DNS name/IP address of the network or group. For computers in an IP range that you want to give a network name, enter the last IP address in the seriesrange. The IP address in **Upper Limit** must be at least as high as the one in **Lower Limit**. If this field is left empty, only the IP address in **Lower Limit** is used. If you use a subgroup, leave this field empty.

### IP Address

The IP address of the object you entered in the **DNS Name or IP Address** field is displayed here. This field is not updated until you click on **Look up all IP addresses again** or make changes in the **DNS Name or IP Address** field.

## Interface/VLAN

Here, you can select an interface or a VLAN to restrict the IP range.

If "-" is chosen, the group will consist of all IP addresses in the interval between **Lower Limit** and **Upper Limit**, regardless of what interface they are connected to. By selecting an interface or a VLAN, you constrain the group to consist only of the IP addresses in the interval that really are connected to the selected interface/VLAN.

For example, if 10.20.0.0 - 10.20.0.255 are IP addresses behind the interface DMZ-1 and the lower and upper limits are 10.10.10.20 and 255.255.255.255 respectively, choosing DMZ-1 as Interface will cause the group to consist of the IP addresses 10.20.0.0 - 10.20.0.255, being the IP addresses in the interval actually connected to the selected interface.

If you have selected a subgroup, the **Interface/VLAN** should be "-". If you want to define a network group at the remote side of a VPN connection, the **Interface/VLAN** should be "-".

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

### 7.1.2. Save

Saves the Networks and Computers configuration to the preliminary configuration.

### 7.1.3. Undo

Clears and resets all fields in new rows and reset changes in old rows.

## 7.2. Default Gateways

### 7.2.1. Main Default Gateways

**Main Default Gateways** are IP addresses of routers that are used to contact the outside world. This IP address is usually assigned by your network provider. **Main Default Gateways** must be IP addresses from one of the Directly Connected Networks of the unit's interfaces. See [Definitions of terms](#), for further description of routers/gateways.

If the **SIP module** is active, you must enter at least one default gateway.

If an interface gets its IP address dynamically, the default gateway is also assigned by the DHCP/PPPoE server. In this case, select the corresponding IP address under **Dynamic**.

You can enter more than one default gateway. The unit will use the one with the highest priority until it stops responding, and then switch to the next one.

Main Default IPv4 Gateways <a href="#">(Help)</a>					
Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
<input type="text"/>	<input type="checkbox"/>	<input type="text" value="10.48.255.1"/>	<input type="text" value="10.48.255.1"/>	<input type="text" value="Ethernet0 (eth0)"/>	<input type="checkbox"/>

Add new rows  rows.

Main Default IPv6 Gateways <a href="#">(Help)</a>					
Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
<input type="text"/>	<input type="checkbox"/>	<input type="text" value="2001:470:dc8c:1000::1"/>	<input type="text" value="2001:470:dc8c:1000::1"/>	<input type="text" value="Ethernet0 (eth0)"/>	<input type="checkbox"/>

Add new rows  rows.

### Priority

If you entered more than one default gateway, you can assign a priority to each of them. The unit will use the gateway with the highest priority (lowest number) when it works. If it stops working, the unit will switch to the next in priority, while checking the first for availability. When the first gateway works again, the unit will switch back to using that.

### Dynamic

If an interface will receive its IP address from a DHCP server, the unit will get its default gateway from the server. In this case, select the corresponding IP address here.

### DNS Name or IP Address

Enter the DNS name or IP address for the default gateway. If an interface will receive its IP address from a DHCP server, the unit will get its default gateway from the server. In this case, leave this field empty.

### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

### Interface

Select the interface connected to the unit default gateway.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.2.2. Additional Default Gateways

You can list additional default gateways to be used for SIP traffic.

If an interface gets its IP address dynamically, the default gateway can also be assigned by the DHCP/PPPoE server. In this case, select the corresponding IP address under **Dynamic**.

Additional Default Gateways <a href="#">(Help)</a>						
Edit Row	Name	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
<input type="checkbox"/>	SIP operator	-	15.22.3.30	15.22.3.30	SIP-1 (eth4)	<input type="checkbox"/>
<input type="checkbox"/>	SIP-2	-	10.20.30.29	10.20.30.29	SIP-2 (eth5)	<input type="checkbox"/>

Add new rows  rows.

### Dynamic

If an interface will receive its IP address from a DHCP server, the unit can also get its default gateway from the server. In this case, select the corresponding IP address here.

### DNS Name or IP Address

Enter the DNS name or IP address for the default gateway. If an interface will receive its IP address from a DHCP server, the unit can also get its default gateway from the server. In this case, leave this field empty.

### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

### Interface

Select the interface connected to the unit default gateway.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.2.3. Policy For Packets From Unused Gateways

This policy controls how packets from the currently unused gateway(s) should be treated. The packet can be allowed (subject to the rest of the configuration) or discarded.

Policy For Packets From Unused Gateways <a href="#">(Help)</a>	
<input checked="" type="radio"/>	Discard IP packets
<input type="radio"/>	Accept IP packets

The **Discard IP packets** selection means that the unit ignores the IP packets without replying that the packet did not arrive.

The **Allow IP packets** selection makes the unit use the rest of the configuration to decide if the

packet should be allowed.

## 7.2.4. Gateway Reference Hosts

The gateway reference hosts are used by the unit to check if the gateways are alive. For each reference host, test ping packets are sent, using the different gateways.

Reference hosts are not needed if you have entered a single default gateway.



The screenshot shows a web interface titled "Gateway Reference Hosts" with a "(Help)" link. It contains a table with three columns: "DNS name or IP address", "IP address", and "Delete row". The first row of the table has the values "193.180.23.12", "193.180.23.12", and a checkbox. Below the table is a button labeled "Add new rows" followed by a text input field containing the number "1" and the text "rows.".

DNS name or IP address	IP address	Delete row
193.180.23.12	193.180.23.12	<input type="checkbox"/>

Add new rows  rows.

### DNS Name or IP Address

Enter the DNS name or IP address for the reference host. The reference host must be located on the other side of the default gateway.

### IP Address

Shows the IP address of the DNS Name or IP Address you entered in the previous field.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.2.5. Save

Saves the Default Gateways configuration to the preliminary configuration.

## 7.2.6. Undo

Clears and resets all fields in new rows and reset changes in old rows.

## 7.3. Interface (Eth0, Eth1, ...)

There is a page for each network interface (Eth0, Eth1, ...) on the unit. Select a page to make configuration for that interface. There is also a page where configuration for all interfaces can be viewed and changed.

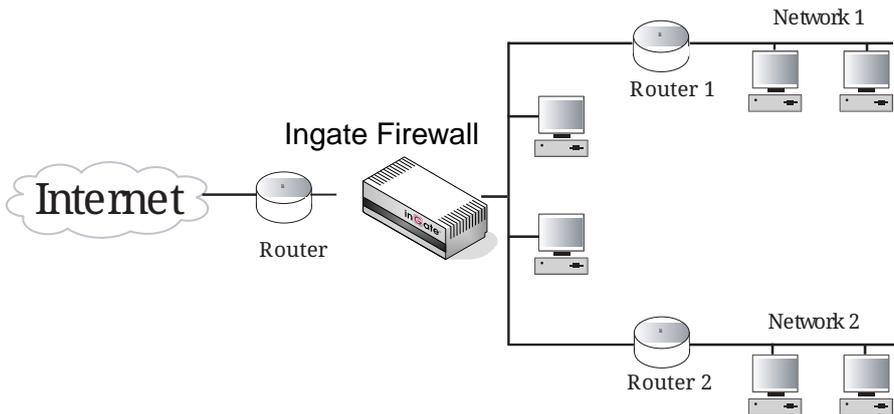
Here, you set the interface name, whether the interface is on or off, the IP address, alias, and static routing.

For each interface, go to **Directly Connected Networks** and state the IP address of the unit and the size of the network connected to this interface.

The figure below shows an example with two network interfaces. One of the interfaces is connected to the Internet via the provider’s router, your default router, and the other is connected to the internal networks.

In the figure below, to access the two networks on the inside, the unit must know that Network 1 is accessible via Router 1 and that Network 2 is accessible via Router 2.

You do not need to enter a route for the computers on any of the unit’s directly connected networks.



### 7.3.1. General

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	<b>Eth0</b>	Eth1	Eth2	Interface Status	PPPoE	Topology
<b>General</b>					<b>Speed and Duplex</b>					
Physical device: <b>eth0</b>					<input checked="" type="radio"/> Automatic negotiation <input type="radio"/> 100 Mbit/s, full duplex <input type="radio"/> 100 Mbit/s, half duplex <input type="radio"/> 10 Mbit/s, full duplex <input type="radio"/> 10 Mbit/s, half duplex					
This interface is: <input checked="" type="radio"/> Active <input type="radio"/> Inactive										
Interface name: <input type="text" value="Internal"/>										

#### Physical device

**Physical device** tells the physical device name of the network interface.

#### This interface is

Specify if this network interface is **On** or **Off**. If the interface is off, all configuration on this page is ignored, and the unit will behave as if this interface wasn’t present (except when used for failover).

If the interface should be used for failover, you should select **Off**. In this case, it won’t be available for other traffic than the synchronizing within the failover team. Read more about failover in [Failover](#).

## Interface name

The network **Interface name** is only used internally in the unit, e. g. when configuring **Networks and Computers**.

### 7.3.2. Obtain IP Address Dynamically

Specify if this network interface should obtain its IP address from a DHCP or PPPoE server instead of an address entered on this page. If **DHCP client ON** is selected, the unit will send out a DHCP request when you apply the configuration and at boot. The request is sent out to the network connected to this interface. If no IP address is obtained, the unit will keep on sending requests until an address lease is received.

The unit will accept an IP address and a netmask via DHCP. It will also accept a default gateway, if you configured for that in the **Main Default Gateways** table on the **Default Gateways** page.

If **PPPoE client ON** is selected, the unit will send out a PPPoE request both when you apply the configuration, and also at boot time. To obtain an IP address via PPPoE, you also need to enter the configuration on the **PPPoE** page.

More than one interface can obtain its IP address dynamically.

### 7.3.3. Speed and Duplex

The unit can negotiate interface speed and duplex automatically for Gbit interfaces, this setting must be set to *Automatic negotiation* to achieve Gbit speed.

Note that link partner must also be set to Automatic negotiation.

### 7.3.4. Directly Connected Networks

The unit must have an IP address on every network to which it is directly connected. This applies to all networks on the same physical network to which this interface is connected.

When the DHCP client is on, there must be a directly connected network with "\*" as the **DNS name/IP address**, and where the **Netmask/bits** field is left empty. No other directly connected networks are allowed for this interface.

Directly Connected Networks <small>(Help)</small>										
Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Admin-1	Static	192.168.1.1	192.168.1.1	24	192.168.1.0	192.168.1.255	27	Admin	<input type="checkbox"/>
<input type="checkbox"/>	Admin-2	Static	192.168.20.1	192.168.20.1	24	192.168.20.0	192.168.20.255	27	Admin	<input type="checkbox"/>
<input type="checkbox"/>	Inside	Static	10.47.2.243	10.47.2.243	16	10.47.0.0	10.47.255.255		-	<input type="checkbox"/>

Add new rows  rows.

## Name

A name for this IP address. You can use this name when configuring relays and VPN. This name is only used internally in the unit.

## DNS Name or IP Address

The name/IP address of the unit on this network interface on this directly connected network. If a name is entered, you must enter the IP address for a name server on the **Basic Configuration** page.

## IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

## Netmask/Bits

Enter the mask of the network where the **DNS Name or IP Address** applies.

## Network Address

The IP address of the network where the **DNS Name or IP Address** applies.

## Broadcast Address

Shows the broadcast address of the network in the **Network address** field.

## VLAN Id

VLANs are used for clustering IP ranges into logical networks. A VLAN id is simply a number, which identifies the VLAN uniquely within your network.

Enter a VLAN id for this network. You don't need to use a named VLAN (defined on the **VLAN** page).

## VLAN Name

If you entered the VLAN id of a named VLAN, the name will show here.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

If the interface should obtain its IP address from a DHCP server, the settings should be like in the image below. With a DHCP IP, no aliases can be defined for the interface.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | **Eth2** | Interface Status | PPPoE | Topology

**General**  
 Physical device: **eth2**  
 This interface is:  Active  Inactive  
 Interface name:

**Speed and Duplex**  
 Automatic negotiation  
 100 Mbit/s, full duplex  
 100 Mbit/s, half duplex  
 10 Mbit/s, full duplex  
 10 Mbit/s, half duplex

**Directly Connected Networks** [\(Help\)](#)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
Internet	DHCP		*		-	-		-	<input type="checkbox"/>

Add new rows  rows.

### 7.3.5. Alias

The unit can use extra IP addresses, aliases, on its interfaces. All alias IP addresses must belong to one of the **Directly Connected Networks** you have specified.

Aliases are necessary for setting up multiple relays on different IP addresses.

If the interface obtains its IP address dynamically, no aliases can be defined.

**Alias** [\(Help\)](#)

Below are the ranges from which you can select aliases.

10.47.0.1-10.47.255.254
192.168.1.1-192.168.1.254
192.168.20.1-192.168.20.254

Edit Row	Name	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	Inside-2	10.47.2.244	10.47.2.244	<input type="checkbox"/>
<input type="checkbox"/>	SIP-1	10.47.3.1	10.47.3.1	<input type="checkbox"/>
<input type="checkbox"/>	SIP-2	10.47.3.2	10.47.3.2	<input type="checkbox"/>

Add new rows  rows.

#### Name

Enter the name of your alias. You can use this name when configuring relays and VPN. This name is only used internally in the unit.

#### DNS Name or IP Address

Enter the IP address of this alias, or a name in the DNS. If you enter a DNS name instead of an IP address, you must enter the IP address of a DNS server on the **Basic Configuration** page.

#### IP Address

Shows the IP address of the DNS Name or IP Address you entered in the previous field.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 7.3.6. Proxy ARP

Proxy ARP <small>(Help)</small>							
Edit Row	Get Network From	Proxy ARPed Network			VLAN Id	VLAN Name	Delete Row
		DNS Name or Network Address	Network Address	Netmask / Bits			
<input checked="" type="checkbox"/>	boogah (10.48.49.50) ↕	10.48.49.51	10.48.49.51	32		-	<input type="checkbox"/>

You can use parts of the same network on several interfaces.

This is especially useful if you want to split your public IP addresses, and use one part on the outside, and the rest on your DMZ.

Under Get Network From, you select from which directly connected network you want to use IP addresses. The network you select should not be located on this interface. Then enter the Proxy ARPed Network that you want to use on this interface.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 7.3.7. Static Routing

If there is a router between the unit and a computer network which the unit is serving, you must name the router and the network here. The table is sorted by network number and network mask.

The **Default gateway**, configured on the **Default Gateways** page, will automatically be entered in this table on the corresponding interface page, when added to the **Main Default Gateways table**.

If the interface obtains its IP address dynamically, no other static routes can be defined.

Static Routing <small>(Help)</small>							
Edit Row	Routed Network			Router			Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
<input type="checkbox"/>	10.10.0.0	10.10.0.0	24	-	10.47.3.14	10.47.3.14	<input type="checkbox"/>

Add new rows  rows.

## Routed network

Enter the DNS name or IP address of the routed network under **DNS Name or Network Address**.

The IP address of the routed network is shown under **Network Address**.

In the **Netmask/Bits** field, enter the netmask of the network.

## Router

The name or IP address of the router that will be used for routing to the network. If there are several routers between the unit and the network, fill in the router closest to the unit.

If an interface will receive its IP address from a DHCP server, the unit will get its default gateway from the server. In this case, select the corresponding IP address under **Dynamic**.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.3.8. Unreachable

Add IP networks to the Unreachable table for which the firewall never should allow traffic to or from, unless a more specific network (longer bit mask) is defined in **Directly Connected Networks** or **Static Routing**.

For example if a /48 IPv6 network is routed to the firewall, then it should be added to avoid route loops unless there exists a route in the **Static Routing** for the complete /48 network.

You may want to add the private networks from RFC 1918 here, i.e. 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16.

Unreachable <a href="#">(Help)</a>			
Unreachable Network			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	
<input type="text" value="172.16.0.0"/>	<input type="text" value="172.16.0.0"/>	<input type="text" value="12"/>	<input type="checkbox"/>
<input type="text" value="2002:470:dc8c::"/>	<input type="text" value="2002:470:dc8c::"/>	<input type="text" value="48"/>	<input type="checkbox"/>

rows.

## DNS Name or Network Address

A network for which the firewall never should allow traffic to or from.

## Netmask / Bits

The netmask for the network.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.3.9. Save

Saves all Interface configuration to the preliminary configuration.

## 7.3.10. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 7.3.11. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

# 7.4. NAT

To hide IP addresses located behind one interface for a network behind another interface, turn on NAT (Network Address Translation, also known as masquerading) for that interface or only for that network.

NAT makes it more difficult to access the computers on a network directly from another network. For example, internal networks can be hidden from external networks such as the Internet. To access computers (e.g. a web server) you need a relay. See [IP Firewall](#), for more information on how NAT and relays work.

If a network with private IP addresses is connected to eth0, traffic from these addresses must be NAT:ed when sent out to the Internet. You can also select to NAT traffic bound to a specific network behind the destination interface.

If you want to NAT traffic through an IPsec tunnel, configure this on the **IPsec Tunnels** page.

## 7.4.1. NAT

**NAT**  
 Select if packets that originate from a unit behind the **From** interface should be NAT:ed when they are sent to a unit behind the **To** interface. Optionally you can also select specific networks to be NAT:ed, as well as the address to use.

No.	From				To				NAT As (optional)	Delete Row
	Interface	Network (optional)			Interface	Network (optional)				
		DNS Name or Network Address	Network Address	Netmask / Bits		DNS Name or Network Address	Network Address	Netmask / Bits		
1	Internal (eth0)				External2 (eth2)				.	<input type="checkbox"/>

Add new rows:  rows.

**No.**

This is a number that is used to identify each individual NAT rule. Rules are sorted in numerical order. To move a rule to a certain row, enter the number on the row to which you want to move it. You need only renumber rules that you want to move; other rules are renumbered automatically. When you click on Save, the rules are re-sorted. The order of the rules is important. Rules are used in the order in which they are displayed in the table; rule number 1 is first.

**From**

Select the interface and network from which traffic should originate if it should be NAT:ed. If the network is omitted, all traffic from this interface will be NAT:ed when sent to the destination under **To**.

**Interface**

Select the interface from which traffic should originate to be NAT:ed.

**Network**

Enter the DNS name or network address for the network to be NAT:ed. If the network is omitted, all traffic from any computer connected to this interface will be NAT:ed when sent to the destination under **To**.

Under **Netmask/Bits**, enter the netmask for the network to be NAT:ed.

**To**

Select the interface and network to which traffic should be destined if it should be NAT:ed. If the network is omitted, all traffic to this interface will be NAT:ed when originating from the network specified under **From**.

**Interface**

Select the interface behind which the destination network is located.

**Network**

Enter the DNS name or network address for the destination network. If no network is entered, all traffic to this interface will be NAT:ed when originating from the network specified under **From**.

Under **Netmask/Bits**, enter the netmask for the destination network.

## NAT as

You can select the IP address to be used when traffic is NAT:ed. Select from the IP addresses given to the unit under **Directly Connected Networks** and **Alias** for the destination interface. If no IP address is selected, the unit selects one at random.

### 7.4.2. Save

Saves all NAT configuration to the preliminary configuration.

### 7.4.3. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 7.5. VLAN

VLANs are used for clustering IP ranges into logical networks. A VLAN id is simply a number, which identifies the VLAN uniquely within your network.

### 7.5.1. Named VLANs

Here, you can list the VLANs you wish to use and give them names, to make administration easier.

Named VLANs can also be selected instead of interfaces on the **Networks and Computers** page.

See also [Part IV. How To Guides](#) for more information about how to configure VLANs on your unit.

Name	Interface	VLAN Id	Status	Delete Row
------	-----------	---------	--------	------------

Add new rows  ROWS.

#### Name

The name of this VLAN. The name is only used in the unit web interface to help you keep track of the different VLANs.

#### Interface

Select an interface for this VLAN.

#### VLAN Id

Enter a VLAN id. A VLAN id is just a number. All packets for this VLAN are then marked with this number, enabling all network devices to recognize and route packets for the VLAN.

## Status

The status for this VLAN. Status can be **On** (the VLAN is used on an active interface), **Off** (the VLAN is used on an inactive interface) and **Unused** (no **Directly Connected Networks** has been selected for this VLAN).

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.5.2. Save

Saves all VLAN configuration to the preliminary configuration.

## 7.5.3. Undo

Clears and resets all fields in new rows and resets changes in old rows.

# 7.6. Interface Status

On this page, status about the physical interfaces and links are shown.

Status of dynamic IP addresses is also shown here.

## 7.6.1. Interface Status

Physical Device	Interface Name	MAC Address	Configured State	Configured Speed/Duplex	Active	Link	Type	Speed	Duplex
eth0	Ethernet0	00:d0:c9:b3:4e:44	Yes	Autonegotiation	Yes	Yes	10/100	100 Mbit/s	Full
eth1	Ethernet1	00:d0:c9:b3:4e:45	No	Autonegotiation	No		10/100		
eth2	Ethernet2	00:d0:c9:b3:4e:46	No	Autonegotiation	No		10/100		

### Physical Device

The name of the physical network interface.

### Interface Name

The name you gave this interface.

## MAC Address

The MAC address of the interface.

## Configured State

Shows if the interface is configured to be On or Off.

## Active

Shows if the interface is activated or not.

## Link

Here you can see if the interface has physical link to the network.

## Type

Here the speed options for the interface are shown.

## Speed

Here you can see the negotiated speed on the interface network.

## Duplex

Here you can see the negotiated duplex for the interface.

## 7.6.2. DHCP Client Status

When an interface is configured to obtain its IP via DHCP, the **DHCP Client Status** section is shown. Here you find information about the DHCP lease.

DHCP client status	
IP address:	193.12.253.122
Netmask:	255.255.255.240
Default gateway:	193.12.253.115
Lease obtained from:	193.12.253.115
Lease time (seconds):	43200
Lease expires:	2005-10-21 22:23:37

### IP address

The IP address obtained via DHCP.

### Netmask

The netmask for the network on which the IP address is.

## Default gateway

Default gateway for the network on which the IP address is.

## Lease obtained from

The DHCP server which served the IP address to the unit.

## Lease time

The time interval (in seconds) which the lease can be held.

## Lease expires

The time when this lease expires. The unit will renew the lease automatically.

### 7.6.3. PPPoE Client Status

When an interface is configured to obtain its IP via PPPoE, the **PPPoE Client Status** section is shown. Here you find information about the PPPoE address.

PPPoE client status	
IP address:	193.12.253.123
PPPoE server:	193.12.253.107

#### IP address

The IP address of the unit obtained via PPPoE.

#### PPPoE server

The PPPoE server which leased the IP address.

## 7.7. PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a modification of PPP and is used to assign an IP address to a computer as long as it is connected to the PPPoE server. When it disconnects, it instantly loses the IP address.

Many Internet providers use PPPoE instead of DHCP to distribute IP addresses.

### 7.7.1. Authentication

The unit must be authenticated to get an IP address. Here, you enter authentication information for the unit to use.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Interface Status	<b>PPPoE</b>	Topology
------------------------	------------------	----------------	-----	------	------	------	------	------------------	--------------	----------

### Authentication

User:

PPPoE password:

Service Name (rarely used):

Confirm password:

### User

Enter the user name which the unit should use to identify itself to the PPPoE server.

### Service Name

If your PPPoE server supports this, you can ask for a certain service. This parameter is rarely used.

### PPPoE password, Confirm password

Enter the password for the user above. You must enter the same password in both fields. Press the **Change password** button to change to the entered password (do not press enter).

## 7.7.2. Keep Alive

The unit can check the status of the PPPoE connection by sending LCP echo requests to the PPPoE server with regular intervals. If the server does not reply to three consecutive requests, the connection is assumed to be down, and the unit starts a new PPPoE negotiation.

**Keep Alive** [\(Help\)](#)

LCP echo-request interval:

seconds

### LCP echo-request interval

Enter the interval (in seconds) between two requests. Leave the field empty to turn this function off.

## 7.7.3. Logging

The PPPoE negotiations generate log messages. Here, you can select how to log these messages.

**Logging** [\(Help\)](#)

Log class for PPPoE negotiations:

▼

## Log class for PPPoE negotiations

Select a log class for PPPoE negotiations. Select from the log classes defined on the **Log Classes** page.

### 7.7.4. Save

Saves all PPPoE configuration to the preliminary configuration.

### 7.7.5. Undo

Reverts all of the above fields to their previous configuration.

## 7.8. Tunnels

Here you can configure IPv4 → IPv6 transition tunnels. The unit supports three different type of tunnels - *6in4*, *6to4* and *6rd*.

### 7.8.1. 6in4 Tunnels

These statically configured tunnels encapsulate IPv6 in IPv4 - defined by standard RFC 4213.

To make use of the tunnel add the IPv6 address (supplied by the tunnel broker) to a **Directly Connected Network** (found on the page **Network** → **All Interfaces**). The selected interface should be the **Name** of the tunnel.

You should also add the default IPv6 gateway that is given by the tunnel broker. Create a new **Main Default IPv6 Gateway** entry (found on the page **Network** → **Default Gateways**), add the IPv6 gateway address and select the tunnel interface you created here.

6in4 Tunnels <a href="#">(Help)</a>					
Name	Active	Local Side	Remote Side		Delete Row
			DNS Name or IP Address	IP Address	
<input type="text" value="he"/>	<input type="text" value="Yes ▼"/>	<input type="text" value="eth0 (10.48.28.61) ▼"/>	<input type="text" value="192.168.171.4"/>	<input type="text" value="192.168.171.4"/>	<input type="checkbox"/>

rows.

#### Name

Name used for the interface, in **All Interfaces**.

#### Active

Set whether this tunnel is an active interface.

## Local Side

Assign your local IPv4 address (usually your public IPv4 IP).

## Remote Side

Assign your 6in4 tunnel provider IPv4 address.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.8.2. 6to4 Tunnels

These tunnels are automatically configured, and encapsulate IPv6 within IPv4, with the address prefix 2002::/16 and where specific IPv4 hops are represented in IPv6 using the 32 bits following the prefix 2002::/16 using a defined method. The IPv4 address 192.0.2.119 becomes IPv6 hex representation 192→C0 0→00 2→02 119→77 thus 2002:C000:0277::/48. RFC 1918 private IPv4 addresses are undefined in this tunnel method. 6to4 relays are usually available via the standard 6to4 Anycast IP address which according to RFC 3068 is 192.88.99.1 e.g. 2002:c058:6301::/48. These tunnels typically route your local IPv6 network to the global IPv6 network via an IPv4 segment.

If your IPv4 address is **192.0.2.119** your 6to4 prefix will be **2002:c000:0277::/48**. The IPv6 address on the tunnel will be **2002:c000:0277::1/64**. If you want to have a IPv6 network on your LAN (protected by the unit) you can as an example choose the network **2002:c000:0277:1000::/64**.

To make use of the tunnel add the IPv6 address **2002:c000:0277::1/64** to a **Directly Connected Network** (found on the page **Network**→**All Interfaces**). The selected interface should be the **Name** of the tunnel.

In order to reach other 6to4 IPv6 addresses you should add a static route. Create a new **Static Routing** entry (found in the tab **Network**→**All Interfaces**), enter 2002:: in **Network Address**, 16 in **Bits** and select the tunnel interface you created here. No IPv6 gateway address should be given.

In order to reach other IPv6 addresses than 2002::/16 you should add a default IPv6 gateway. Create a new **Main Default IPv6 Gateway** entry (found on the page **Network**→**Default Gateways**) and select the tunnel interface you created here. No IPv6 gateway address should be given.

6to4 Tunnels <a href="#">(Help)</a>			
Name	Active	Local Side	Delete Row
6to4tunnel	Yes ▼	eth0 (10.48.28.61) ▼	<input type="checkbox"/>

rows.

## Name

Name used for the interface, in **All interfaces**.

## Active

Set whether this tunnel is an active interface.

## Local Side

Choose your local IPv4 address as your Local side.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.8.3. 6rd Tunnels

IPv6 Rapid Deployment tunnels defined in RFC 5969. Similar to the above 6to4 tunnel method. 32 bit IPv4 addresses are mapped into the IPv6 address space with the provider ASN IPv6 prefix. You will need the prefix, e.g. 2001:DB8::/32, prefix length e.g. 32, the IPv4 address of the 6rd border router, then the amount of high-order bits (e.g. 10.0.0.0/8) that are identical across and available to all customer equipment (CE) IPv4 addresses within a given 6rd domain, eg. 8. RFC 1918 private IPv4 addresses are defined in this tunnel method, meaning that you and 6rd providers can use private IPv4 addresses.

For a full IPv4/32 address representation in an IPv6rd prefix, the IPv4 address 192.0.2.119/32 becomes the IPv6 hex representation 192 → C0 0 → 00 2 → 02 119 → 77 thus 2001:DB8:C000:0277::/64 with IPv4 bits 32-32 = 0.

6rd Tunnels <small>(Help)</small>									
Name	Active	Local Side	Remote Side		Network			IPv4 bits	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or Network Address	Network Address	Netmask / Bits		
my6rd	Yes ▼	eth0 (10.48.28.61) ▼	192.168.171.4	192.168.171.4	2001:DB8:C000:0277:	2001:db8:c000:277::	64	0	<input type="checkbox"/>

Add new rows  rows.

## Name

Name used for the interface, in **All interfaces**.

## Active

Set whether this tunnel is an active interface.

## Local Side

Assign your local customer equipment (CE) IPv4 address.

## Remote Side

Assign your 6rd tunnel provider IPv4 address.

## Network

Specify the parameters of the 6rd subnet assigned to you, including the size of the IPv6 subnet you will use, usually a 64 bit prefix.

## IPv4 bits

Specify the amount of high-order bits that are identical across and available to all customer equipment (CE) IPv4 addresses within a given 6rd domain.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 7.8.4. Save

Saves all Tunnel configuration to the preliminary configuration.

### 7.8.5. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 7.9. Topology

State the topology around the unit on this page. Which type of topology is needed depends on which SIParator Type was selected.

### 7.9.1. Surroundings

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the unit.

All computers that can reach each other without having to go through the firewall connected to the unit should be grouped in one network. When you are finished, there should be one line for each of

your firewall's network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the firewall.

For DMZ and Manual units, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

**Surroundings** [\(Help\)](#)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
---------	------------------------	------------

Add new rows  rows.

### Network

Select a network. The alternatives are the networks you defined on the **Networks and Computers** page.

### Additional Negotiators

Sometimes you have SIP devices on a different network that needs to negotiate for this network. This happens when there is a SIP server on one network, and SIP-unaware phones on another. In this case, select the phone network under Network, and the SIP server as an Additional Negotiator. Select from the networks defined on the **Networks and Computers** page.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 7.9.2. Data Interfaces

Settings in the **Data Interfaces** table are only required when the unit has been made the **WAN** type.

Between the Data Interfaces listed here, the unit will act as a plain router, and only forward traffic, with the exception that QoS will be performed if configured for the traffic in question.

The traffic sent between Data Interfaces will not be logged by the unit.

The unit will only send SIP traffic between the other interfaces.

## Data Interfaces [\(Help\)](#)

If your firewall type is not set to **WAN**, the settings in this section will have no effect.

**Interface** **Delete Row**

**Add new rows**  ROWS.

### Interface

Select a data interface here.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 7.9.3. Save

Saves all Topology configuration to the preliminary configuration.

### 7.9.4. Undo

Clears and resets all fields in new rows and resets changes in old rows.

# Chapter 8. Rules and Relays

Under **Rules and Relays**, you configure which traffic is allowed from one network to another; for example, from an internal network to the Internet. You must use NAT and relays to transmit traffic to IP address series that can only be used locally.

Remember that the order of the firewall rules is important. The unit always uses the first rule that applies to a certain type of traffic.

All traffic that does not fit into any of the rules is rejected or discarded. Specify whether such traffic should be rejected or discarded under **IP Policy** on the **Basic Configuration** page.

Before you set the **Rules and Relays**, you must enter configuration for **Networks and Computers**, and maybe also for **Time Classes** and **Services**. Under **Networks and Computers**, specify the network interface where a computer or network can be accessed.

If NAT is not used, the rules for UDP traffic apply to one direction only. This means that you must set up a rule for each direction. In contrast to TCP traffic, UDP traffic requires no connections. All packets are sent as separate, small units. This makes this type of traffic harder to monitor.

The unit has a number of relay types: FTP relay, TCP relay, TCP port forwarding, semi-transparent TCP port forwarding, UDP relay, UDP port forwarding, semi-transparent UDP port forwarding, DHCP relay, and address rewriting HTTP relay. See [IP Firewall](#), for more information on how these relays work.

## 8.1. Rules

On the **Rules** page, you set all the rules for traffic between the different network interfaces. The rules are made by combining the information from other pages (see below). Make sure that you have done all the necessary configuration on the **Networks and Computers**, **Time Classes** and **Services** pages before you set the rules. A rule regulates the traffic for a certain service from one network to another.

**NOTE** The order of the rules is important. The unit uses the first rule that matches to decide how to handle received traffic.

If FTP or PPTP should be allowed through the unit, special rules for this (using services with Dynamic FTP or PPTP management) should be placed before any other, more general rules, allowing TCP between the same networks.

### 8.1.1. Rules

Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Office network	-	Internet	-	Internal -> External (NAT:ed)	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Email server	-	Internet	-	External2 -> External (NAT:ed)	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Office network	-	Email server	-	Internal -> External2	pop-3	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	4	Yes	DNS server	-	Office network	-	External2 -> Internal	dns-reply	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	5	Yes	DHCP clients	-	Internet	-	DHCP clients -> External (NAT:ed)	icmp/udp/tcp	Allow	office hours	Local		<input type="checkbox"/>
<input type="checkbox"/>	6	Yes	Atlantic VPN	Atlantic City	DMZ	-	(VPN) -> External2	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	7	Yes	DNS server	-	Internet	-	External2 -> External (NAT:ed)	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	8	Yes	Office network	-	Email server	-	Internal -> External2	imap	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	9	Yes	Office network	-	DNS server	-	Internal -> External2	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	10	Yes	DMZ	-	Atlantic VPN	Atlantic City	External2 -> (VPN)	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	11	Yes	DMZ	-	All	-	External2 -> Indeterminate interface (partly NAT:ed)	icmp/udp/tcp	Discard	24/7	Local+Syslog		<input type="checkbox"/>

Add new rows | 1 rows.

### Rule No.

This is a number that is used to identify each individual rule. Rules are sorted in numerical order. To move a rule to a certain row, enter the number on the row to which you want to move it. You need only renumber rules that you want to move; other rules are renumbered automatically. When you click on Save or add a new row, the rules are re-sorted. The order of the rules is important. Rules are used in the order in which they are displayed in the table; rule number 1 is first.

### Rule State

Select if this rule should be enabled or disabled. When disabled, the rule will remain in the same place in this rule list, but the unit will ignore it.

### Client

Under **Client**, you can select one of the defined **Networks and Computers**. The rule regulates the traffic from **Client** to **Server**. If you want to define a connection with an IPsec peer, you must use a **Client** network with the interface "-".

### From IPsec Peer

By selecting an **IPsec peer** here, the rule is restricted to only matching encrypted packets from a computer using this peer. In addition to this, the packets must originate from an IP address in the range of the selected **Client**. If no IPsec peer is selected ("-"), this rule will match regardless of whether the packet arrives via an IPsec connection or not.

When an IPsec peer is selected, the **Client** network must use "-" as interface. This is defined on the **Networks and Computers** page.

## Server

Under **Server**, you can select one of the defined **Networks and Computers**. This regulates which computer(s) receive traffic under this rule. If you want to define a connection with an IPsec peer, you must use a **Server** network with the interface "-".

## To IPsec Peer

If the **Server** should only be accessed via an IPsec connection, you select the **IPsec peer** here. The **Server** must have an IP address within the range of the **IPsec Tunnels** of the selected **IPsec peer**. This is used when a client behind the unit wants to access a network or a computer through an IPsec tunnel.

If the server receiving traffic is not behind an IPsec tunnel (from the unit's point of view), you select "-" here.

## Direction

The direction shows from what network interface, to what network interface this rule regulates traffic. One example can be Outside → Inside. If a rule regulates traffic to or from a network defined on several interfaces or no interface, the text "Indeterminate interface" is shown.

## Service

The network service which should be let through/blocked with this rule. You configure services on the **Services** page. Examples of services are WWW and telnet.

## Action

Here, you determine the action that the unit should take when a matching packet arrives. **Allow** lets all traffic of this type through the unit. **Reject** blocks all traffic of this type and sends an error message back as response, an ICMP packet. **Discard** blocks all traffic of this type and sends no response.

## Time Class

For each rule you select a **Time class**, which regulate on what days and at what time of a day the rule will be active. Inactive rules are ignored when deciding what should be done with an arriving packet. You define the different time classes on the **Time Classes** page.

## Log Class

Here, you set the **Log Class** to be used for packets matching this rule. For traffic let through by a dynamic management rule (that is, a rule where the service has a Dynamic management firewall type), only the first packet and rejected/discarded packets in the connection is logged.

Log classes are defined on the **Log Classes** page under **Logging and Tools**. See also [Logging and Tools](#).

## Comment

Enter a comment to remind yourself what this rule is meant to do.

## Delete

If you select this box, the row is deleted when you click on Add new rows or Save.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 8.1.2. Save

Saves the Rules configuration to the preliminary configuration. Rule numbers are changed if necessary so that the rules end up in the right order and each rule receives a unique number.

### 8.1.3. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 8.2. Relays

A relay in the unit listens for traffic directed to a port on a specific IP address of the unit itself. Packets arriving on this address and port are forwarded by the unit to a server or other computer. The sender of the original packet doesn't know that the packet is forwarded.

Relays are mainly used to transfer traffic to servers located on a NAT:ed (masqueraded) network, where the IP addresses on the NAT:ed network cannot be accessed from the outside. When you use an IP address that is for local use only, you must use NAT and relays because these IP addresses cannot be accessed in any other way. Relays can also be used for non-NAT:ed networks. Relays in the unit do not save any information locally; they only transfer traffic to a server.

Relays contain access control, which makes it possible to restrict the relays to certain IP addresses and time intervals.

One example is a web server on a NAT:ed internal network. The only computer that is visible from the outside is the unit, so WWW traffic must go through it. In this case, you want to relay the outside traffic to the web server. Another example is an organization with its own name server on a NAT:ed network. For outsiders to search for names or IP addresses on the organization's servers, DNS (Domain Name System) traffic must be relayed in to the name server, which requires a UDP relay.

Relays are sorted by the name of the unit IP address and port number.

### 8.2.1. Relays

Relays (Help)												
Edit	Listen To ...		Relay To ...			Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class	Log Class	Delete
	IP Address	Port	DNS Name or IP Address	IP Address	Port		Network	IPsec Peer				
<input type="checkbox"/>	Outside (193.12.253.115)	53	172.16.0.3	172.16.0.3	53	UDP relay	Internet	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	Outside (193.12.253.115)	444	172.16.0.7	172.16.0.7	3847	TLS/SSL decryption	Internet	-	main cert	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	Outside (193.12.253.115)	35000-36000	172.16.0.7	172.16.0.7		TCP port forwarding	Internet	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	mail (193.12.253.114)	25	172.16.0.4	172.16.0.4	25	TCP relay	Internet	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	mail (193.12.253.114)	25	172.16.0.5	172.16.0.5	25	TCP relay	Internet	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	www (193.12.253.113)	80	172.16.0.18	172.16.0.18	80	Semi-transparent TCP port forwarding	All	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	www (193.12.253.113)	443	172.16.0.18	172.16.0.18	443	Semi-transparent TCP port forwarding	All	-	-	24/7	Local	<input type="checkbox"/>

Add new rows  rows.

### Listen To ...

Specify here the address and port to which others should send the packets which are to be forwarded to the unit you enter under **Relay to**.

### IP Address

Select one of the names or aliases defined on the interface pages under **Network**.

### Port

The port number for this relay on the outside. This is the port on which this relay listens for traffic.

You can enter an interval here, which will make this relay listen to all ports in that interval. This only works for the port forwarding relay types.

### Relay To ...

This is the server to which the traffic should be forwarded.

If you want to add a backup server, add another row with the same IP address and port under **Listen To**. Enter a different IP (and port) here. The unit will use the server with the lowest IP address until it stops responding, and then switch to the other server.

### DNS Name or IP Address

The name/address of the server to which traffic should be forwarded.

### IP Address

This field shows the IP address of the server. The field is updated when you click on **Look up all IP addresses again** or change the **DNS Name or IP Address** field.

## Port

The port number of the server to which traffic should be forwarded.

If a port interval was entered under **Listen To**, this field must be left empty. The incoming traffic will be forwarded to the same port as it was received on.

## Relay Type

Select which relay type you want to use.

A **TCP relay** is a simple kind of forwarding. A relay listens to a port on a certain IP address in the unit and forwards all traffic to the specified server. A TCP relay only processes TCP traffic. Examples of services that can be processed by a TCP relay include Telnet (terminal connections), SMTP (email), POP (email), NNTP (news), and HTTP (www). From the client, the relay works as a server, and from the server, the relay works as a client program.

A relay is slightly more secure than port forwarding, as it rewrites the entire packet instead of just the sender address. The drawback is that the relay consumes more computer resources in the unit. The TCP relay is limited to maximum 512 sessions for each combination of IP address and port it listens to.

A standard **TCP relay** listens to a port on a certain IP address in the unit and intercepts all TCP packets. It generates a new TCP packet puts the unit's IP address as the sender, keeps all other information and forwards the new packet to the specified server.

**TCP port forwarding** is a simple kind of forwarding. It listens to a port on a certain IP address in the unit and forwards all TCP traffic to the specified server after rewriting the sender address to the unit's IP address.

**Semi-transparent TCP port forwarding** does the same as the TCP port forwarding, except that it doesn't rewrite the sender address. This means that the server will know which computer originally made the connection. The client still only sees the unit.

A **UDP relay** is a simple way of forwarding UDP traffic. A relay listens to a port at a certain IP address in the unit and forwards all traffic to the specified server. A UDP relay only processes UDP traffic. Examples of services that can be processed by a UDP relay are DNS (name/IP address queries) and SNMP (network monitoring).

A relay is slightly more secure than port forwarding, as it rewrites the entire packet instead of just the sender address. The drawback is that the relay consumes more computer resources in the unit.

A standard **UDP relay** listens to a port on a certain IP address in the unit and intercepts all UDP packets. It generates a new UDP packet puts the unit's IP address as the sender, keeps all other information and forwards the new packet to the specified server.

**UDP port forwarding** is a simple kind of forwarding. It listens to a port on a certain IP address in the unit and forwards all UDP traffic to the specified server after rewriting the sender address to the unit's IP address.

**Semi-transparent UDP port forwarding** does the same as the UDP port forwarding, except that it

doesn't rewrite the sender address. This means that the server will know which computer originally made the connection. The client still only sees the unit.

The FTP service is different because it uses one channel for commands and another to send data, so it needs a special relay.

The **FTP relay** receives attempts to connect from a network and tries to contact the FTP server. From the client, the relay works as an FTP server, and from the server, the relay works as a client program. The FTP relay can handle active and passive FTP (see [IP Firewall](#), for details).

The **FTP relay** assumes for active FTP that FTP data is available at the port number under the one for FTP commands. Usually, the server uses port 21 for FTP commands and 20 for FTP data.

The **TLS/SSL decryption relays** works in approximately the same way as a TCP relay, except that they decrypts incoming TLS/SSL packets to normal TCP when forwarding to the IP address you set under **Relay To**.

A **TLSv1.x decryption relay** receives encrypted packets on a TLS connection, and forwards the decrypted TCP packets to the destination entered under **Relay To**.

A **TLSv1.x/SSLv3.0 decryption relay** receives encrypted packets on a TLS/SSL connection, and forwards the decrypted TCP packets to the destination entered under **Relay To**.

### Allow Access From ...

#### Network

Here, you select a network group, defined on the **Networks and Computers** page under **Network**. Only the computers in the chosen group can use the relay.

#### IPsec Peer

Here, you can select an **IPsec peer**, defined on the IPsec Peers page. If an IPsec peer is selected, only encrypted traffic from this peer will be relayed. The **Local side** of the IPsec tunnel for this peer must contain the IP address in **Listen to IP Address**.

#### Time Class

The **Time Class** given defines when the relay is active. Inactive relays are ignored when handling arriving packets. You define time classes on the **Time Classes** page under **Rules and Relays**. See also [Time Classes](#) for more information.

#### Log Class

Here, you define which **Log Class** should be used to log the traffic through this relay. Log classes are defined on the Log Classes page under Logging and Tools. See also [Log Classes](#) in [Logging and Tools](#), for more information.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP**

addresses again.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 8.2.2. Save

Saves the Relays configuration to the preliminary configuration.

### 8.2.3. Undo

Clears and resets all fields in new rows and reset changes in old rows.

### 8.2.4. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 8.3. DHCP Relay

You can enable relaying of DHCP requests to a server on a different network. The DHCP relay only forwards DHCP requests between the server and the clients. In some DHCP implementations, when a client has received an IP address from the DHCP server, it needs to communicate with the server regularly to keep the leased address. This communication is not sent via the relay, which means that you have to define a firewall rule for this traffic. This is done on the **Rules** page.

Many DHCP servers and clients try to send ping requests to the IP address that is allocated. Then a rule is needed to allow ping requests from the server network to the client network.

Many DHCP servers also want to look up the IP address to be leased in the DNS. In that case, that traffic too must be allowed from the DHCP server to the DNS server.

If you don't know what kind of traffic the server will send, you can create rules for all the alternatives stated above. If the server doesn't need them, nothing else will happen. You could also check the log to see if they are used.

### 8.3.1. DHCP Relay

Rules Relays **DHCP Relay** Services Protocols Time Classes

**DHCP Relay** (Help)

Enable DHCP relay  
 Disable DHCP relay

The relay port number for sending and receiving (normally 67):

Clients are directly connected to interface/VLAN:

### DHCP relay function

Here, you select whether the DHCP relay should be On or Off.

### The relay port number for sending and receiving

Here, you enter which port number the DHCP relay should listen and send to. Usually, DHCP uses port 67.

### Clients are directly connected to interface/VLAN

The computers making DHCP requests are called clients. The DHCP relay can only relay requests from one of the unit's interfaces/VLANs. Here, you select the unit interface/VLAN to which the clients are connected.

## 8.3.2. DHCP Server

The DHCP server can be connected to any of the unit's interfaces. As the unit knows which IP addresses are connected to each interface, you don't have to select an interface here.

**DHCP Server**

Enter the DHCP server to which DHCP requests should be forwarded.

DNS Name or IP Address	IP Address
<input type="text" value="10.47.7.22"/>	10.47.7.22

Enter the DNS name or the IP address of the DHCP server.

### 8.3.3. Save

Saves the DHCP Relay configuration to the preliminary configuration.

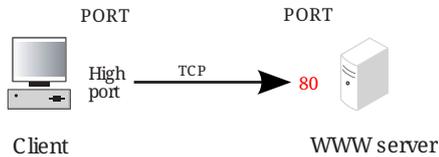
### 8.3.4. Undo

Reverts all of the above fields to their previous configuration.

## 8.4. Services

A service is defined as an IP protocol and, where it is applicable, sender and receiver ports (TCP, UDP) or types (ICMP).

Usually, a service consists of port numbers for the client and server sides and a protocol. The WWW service may look like this:



A connection is made from a client to a server where a standard protocol is used. The client machine uses an available port whose number is over 1023. The standard port for the service is used on the server. The WWW service usually uses port 80 on the server.

A large number of protocols can be used on IP. Common protocols are TCP, UDP and ICMP. Most services use the connection-oriented protocol, TCP. See [Definitions of terms](#), for more details on the common protocols. In [Common services](#), you can find examples on how to configure the unit for a lot of services.

UDP is usually used for mounting file systems over the network with NFS, name and IP address queries to a DNS server, or the SNMP network monitoring protocol.

ICMP is used to send error messages, for example, that the network or computer is not accessible, but is also used for other messages about the network. Remember that ICMP does not connect; it simply sends a short message in one direction. This is why you must turn on ICMP for the direction - from the inside out or from the outside in - in which you want to send ICMP messages.

When a connection is active, the server sends replies to the client. For this to work correctly, the unit creates a shadow rule applying to the reply traffic. The shadow rule, which only allows reply traffic, could be a fixed rule always existing and allowing reply traffic from all server ports to all client ports of all client computers, or it could be a dynamic rule, which is created when a connection is established and disappear at disconnection, and which is constrained to the server and client ports used by the established connection.

Select **Packet filter** for fixed shadow rules and **Dynamic session management** for dynamic shadow rules.

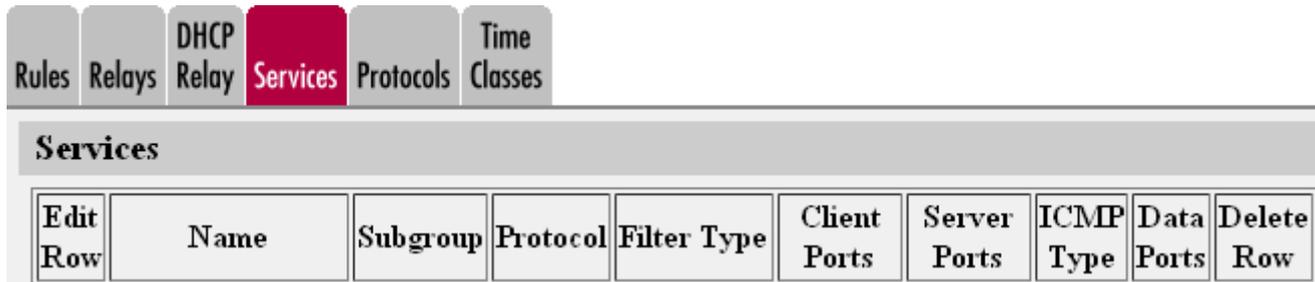
A special type, called **Dynamic FTP management**, exists for handling FTP traffic. This rule will create dynamic shadow rules when an FTP connection is established. It will also automatically create shadow rules for the data traffic, monitoring the traffic and deciding whether to make a shadow rule for active or passive FTP. When using Dynamic FTP management, no rule for the FTP data traffic is needed.

Another special type is called **Dynamic PPTP management** and is used to get PPTP traffic through the NATing unit.

When NAT is used, all shadow rules are dynamic.

## 8.4.1. Services

Here, the services used on the **Rules** page are defined. The same services can also be used for QoS, if the unit has that extension module. Most common services are predefined.



Services									
Edit Row	Name	Subgroup	Protocol	Filter Type	Client Ports	Server Ports	ICMP Type	Data Ports	Delete Row

### Name

Enter a name for the service. You can use this name when you change the rule configuration. The rows are sorted in alphabetical order, except that all upper case letters are sorted before lower case letters (B is sorted before a).

### Subgroup

You can create a group of services, consisting of several services. This can be useful when you want groups of services to be treated the same by the unit. You name the group under **Name**, and then use already defined services, or define new ones. If you want to use a defined service, select its name under **Subgroup**. The other fields in that row should be left empty.

When defining new services in a group, do exactly as when defining a single service (see the "all" service in the image).

### Protocol

**Protocol** is the protocol that is used by the defined service. Protocols are defined on the **Protocols** page.

When defining services based on TCP or UDP, the fields **Client ports** and **Server ports** should be filled in. When defining services based on ICMP the field **ICMP type** should be filled in. When defining services based on other protocols these fields should be left empty.

See [Common services](#), for more information on services and protocols.

### Filter Type

Select **Packet filter** to get a fixed shadow rule and **Dynamic session management** to get a dynamic shadow rule. When NAT is used, all shadow rules are dynamic and this column will be ignored.

Some services require a special set of rules, which is handled by special firewall types. **Dynamic FTP management** creates dynamic FTP shadow rules for control as well as data traffic. **Dynamic TFTP management** creates dynamic TFTP shadow rules for control as well as data traffic. Dynamic RTSP management creates dynamic RTSP shadow rules for control as well as media traffic. **Dynamic PPTP management** creates shadow rules for the PPTP negotiation and the encrypted PPTP traffic, which uses the GRE protocol.

## Client Ports

Client ports are the ports that are used by the client computer. You can enter any number of ports or ranges of ports, or a combination of ports and port ranges. Separate the ports and ranges with commas. The value for a port must be a number between 0 and 65535 (inclusive). A range may lie somewhere between 0 and 65535, written as number-number. For client computers, the range is often 1024-65535. Client ports are used by TCP and UDP based services.

## Server Ports

Server ports are the ports to which the client computer can connect on the server computer. You can enter any number of ports or ranges of ports, or a combination of ports and port ranges. Separate the ports and ranges with commas. The value for a port must be a number between 0 and 65535 (inclusive). A range may lie somewhere between 0 and 65535, written as number-number. Server ports are used by TCP and UDP based services.

## ICMP Type

When defining services based on ICMP, enter the ICMP type here. It should be a number between 0 and 255 (inclusive). You can also enter a range of ICMP types. A range may lie somewhere between 0 and 255, written as number-number.

## Data Ports

This column is used to specify what ranges the FTP server can use as source address when connecting the data port. When no data ports are entered the old behavior is kept, i.e. data port = control port - 1.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

### 8.4.2. Save

Saves the Services configuration to the preliminary configuration.

### 8.4.3. Undo

Clears and resets all fields in new rows and reset changes in old rows.

## 8.5. Protocols

On the **Protocols** page, the protocols are defined. These consist of one or more of the existing Internet protocols.

## 8.5.1. Protocols

Edit row	Name	Protocol	Delete row
<input type="checkbox"/>	AH	51	<input type="checkbox"/>
<input type="checkbox"/>	ESP	50	<input type="checkbox"/>
<input type="checkbox"/>	GRE	47	<input type="checkbox"/>
<input type="checkbox"/>	ICMP	1	<input type="checkbox"/>
<input type="checkbox"/>	IGMP	2	<input type="checkbox"/>
<input type="checkbox"/>	IPv6	41	<input type="checkbox"/>
<input type="checkbox"/>	TCP	6	<input type="checkbox"/>
<input type="checkbox"/>	UDP	17	<input type="checkbox"/>

Add new rows  rows.

### Name

Name is a name for the defined protocol.

### Protocol

In the **Protocol** field, enter the number(s) of the Internet protocol(s) that the **Name** protocol will consist of. The value entered must be a number between 1 and 255 (inclusive). You can enter a single number, a range of numbers, written as number-number, a series of numbers separated by commas, or a combination of these alternatives.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 8.5.2. Save

Saves the Protocols configuration to the preliminary configuration.

## 8.5.3. Undo

Clears and resets all fields in new rows and reset changes in old rows.

## 8.6. Time Classes

When defining **Rules**, you can select in what periods they should be active. The periods are defined by named time classes. A time class can be defined using several rows consisting of different time intervals. A day begins at 00:00 and ends at 24:00.

If a row in the table contains more than one weekday, e. g., from Monday to Friday, the time interval **From time** - **To time** will be interpreted as several intervals, one for each day.

Note that every time a time interval of a time class in use starts or ends, settings are applied.

Example: **From weekday** Monday **To weekday** Wednesday, **From time** 08:00 **To time** 15:00 is the same as Mondays 08:00-15:00, Tuesdays 08:00-15:00 and Wednesdays 08:00-15:00.

### 8.6.1. Time Classes

Edit Row	Name	From Weekday	To Weekday	From Time	To Time	Delete Row
<input type="checkbox"/>	+ 24/7	Monday	Sunday	00:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>	+ off-duty hours	Monday	Friday	00:00	07:00	<input type="checkbox"/>
<input type="checkbox"/>		Monday	Friday	18:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>		Saturday	Sunday	00:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>	+ office hours	Monday	Friday	07:00	18:00	<input type="checkbox"/>

Add new rows  groups with  rows per group.

#### Name

Name is the name of the time class. By clicking on the plus sign you get more rows where you can define time intervals for this time class.

#### From Weekday

The day of the week when the time class starts.

#### To Weekday

The day of the week when the time class ends.

#### From Time

Starting time for the time class. Time is written as hours:minutes, where both hours and minutes are given with two digits. Hours are in the interval 00-24 and minutes in the interval 00-59. The day starts at 00:00.

### **To Time**

Ending time for the time class. Time is written as hours:minutes, where both hours and minutes are given with two digits. Hours are in the interval 00-24 and minutes in the interval 00-59. The day ends at 24:00.

### **Delete**

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### **Add new rows**

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

### **8.6.2. Save**

Saves the Time Classes configuration to the preliminary configuration.

### **8.6.3. Undo**

Clears and resets all fields in new rows and reset changes in old rows.

# Chapter 9. SIP Services

SIP (Session Initiation Protocol) is a protocol for creating and terminating various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP takes care of the initiation, modification and termination of a session with one or more participants. The protocol makes it possible for the participants to agree on what media types they should share. You can find more information about SIP in [More About SIP](#), and in RFC 3261.

Find examples on how to configure your unit for SIP in [Part IV. How To Guides](#).

The SIP module in the unit handles SIP requests for users who have registered on the unit itself or a machine connected to the unit (see also [Local Registrar](#)). The module forwards the request through the unit, which enables users behind different network interfaces to make contact. The SIP module controls the firewall rules to temporarily let through the media streams that the users agree on, on their assigned ports.

You must enter a **DNS server** and a **Default gateway** on the **Basic Configuration** page to make the SIP module work satisfactorily.

There are two SIP license types in the unit - SIP User Registration licenses and SIP Session licenses.

**SIP User Registration licenses** are used when the unit is the registrar for a domain. Each user registered on the unit consumes a license. When the user unregisters, the license is released.

**SIP Session licenses** are used when SIP media is forwarded by the unit. For each such call, one license is consumed. When the call is ended, the license is released.

To enable the SIP function of the unit, you must at least configure on the **Basic page**.

If the unit should act as SIP server or proxy for devices on the other side of a VPN tunnel, you must add the unit's outside IP address to the local side of the IPsec Tunnels of the VPN connection.

These SIP functions are configured in the **SIP Services** section:

- SIP module on/off
- SIP logging
- Encryption of SIP signaling and media
- Port range for SIP media
- Interoperability settings
- SIP timeouts
- Remote SIP Connectivity (requires a Remote SIP Connectivity Module)
- VoIP Survival (requires a VoIP Survival Module)

## 9.1. Basic

Here, you make basic settings for the unit SIP management.

### 9.1.1. SIP Module

<b>Basic</b>	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
<b>SIP Module</b> <a href="#">(Help)</a>							
<input checked="" type="radio"/> Enable SIP module							
<input type="radio"/> Disable SIP module							

Here, select whether the SIP module should be enabled or disabled. If you select to **Disable SIP module**, no other SIP settings will have any effect.

### 9.1.2. SIP Signaling Access Control

Specify the networks and computers from which the unit accepts SIP Signaling.

<b>SIP Signaling Access Control</b> <a href="#">(Help)</a>
Specify the networks and computers from which the firewall accepts SIP Signaling.
lan ▼

If specified, only SIP signaling originating from any of the specified **Networks and Computers** will be accepted by the unit. Packets that are not accepted will either be "discarded" or "rejected" depending on the setting **IP Policy** specified under **Basic Configuration**. In the default setting ("-") the unit will accept SIP signaling from any client.

### 9.1.3. SIP Media Port Range

State a port interval which the unit should use for SIP media streams. You can use any high ports except 4500 (reserved for NAT-T), 57000-58023 (reserved for FTP relays), 61000-65096 (reserved for NAT), and 65097-65200 (reserved for RADIUS).

#### NOTE

A change in the port interval will make the SIP module restart when the configuration change is applied. When the SIP module is restarted, all active SIP sessions (SIP calls, video conferences etc) will be torn down and all SIP user registrations will be removed.

<b>SIP Media Port Range</b> <a href="#">(Help)</a>
Ports: <input type="text" value="58024"/> - <input type="text" value="60999"/>

Enter the lower and upper limit of the port range that the unit should use for media streams. The upper limit must be at least as high as the lower limit.

### 9.1.4. SIP Signaling Ports

Enter the ports the unit should listen for signaling on and select for each port which transports it should accept. Enable **Intercept** to intercept signaling addressed through the unit.

It is recommended to listen on the standard signaling ports which is 5060 for SIP and 5061 for TLS/SIPS, and to enable **Intercept** on these ports.

Selecting **Intercept** for TLS/WSS will discard packets not destined for the unit.

Active	Port	Transport	Intercept	Comment	Delete Row
Yes ▾	5060	UDP and TCP ▾	Yes ▾	Standard SIP port	<input type="checkbox"/>
No ▾	5061	TLS ▾	Yes ▾	Standard TLS port	<input type="checkbox"/>

Add new rows  rows.

#### Active

Select if the signaling port should be active or not.

#### Port

Enter a port on which the unit should listen for SIP signaling. The unit will then receive SIP signaling on this port for all its IP addresses.

SIP signaling over TLS cannot be received on a unit port which is used for something else, like configuration of the unit.

#### Transport

Select which SIP signaling transports should be allowed on this port.

#### Intercept

Intercept signaling not destined for the unit. Selecting **Intercept** for TLS/WSS will discard packets not destined for the unit.

#### Comment

Enter a comment to remind yourself why you added the port.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.1.5. SIP Media Port Range

State the range of ports that the firewall should use for SIP media streams.

Note that if you change this range, the SIP module will restart when the configuration is applied. When you restart the SIP module, all active SIP sessions are torn down and all SIP registrations are removed.

<b>SIP Media Port Range</b> <a href="#">(Help)</a>	
Ports:	<input type="text" value="58024"/> - <input type="text" value="60999"/>

### 9.1.6. Public IP address for NATed firewall

Sometimes, the unit is located behind a NAT box that is not SIP-aware. This will make signaling go awry, with the result that in many cases there will be voice in only one direction.

This can be corrected by entering the public IP address that the unit will appear to have. When sending SIP signaling towards its default gateway, the unit will use that IP address instead of its private one, which will get media to the right place.

Note that the NATing device must also be configured to forward SIP signaling on that IP address to the unit.

If nothing is entered here, the unit will use its own IP addresses.

This setting is not supported for the Standalone configuration.

<b>Public IP Address for NATed firewall</b> <a href="#">(Help)</a>	
This setting is not supported for the Standalone configuration.	
<b>DNS Name or IP Address</b>	<b>IP Address</b>
<input type="text"/>	

### 9.1.7. SIP Logging

The same settings can also be found on the **Logging Configuration** page under **Logging and Tools**.

<b>SIP Logging</b> <a href="#">(Help)</a>	
Log class for SIP signaling:	Log class for SIP packets:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP license messages:	Log class for SIP errors:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP media messages:	Log class for SIP debug messages:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP IDS/IPS:	
<input type="text" value="Local"/>	
Hide sensitive data: <input checked="" type="radio"/> Yes <input type="radio"/> No	

### **Log class for SIP signaling**

For each SIP packet, the unit generates a message, containing the sender and receiver of the packet and what type of packet it is. Select a log class for these log messages.

### **Log class for SIP packets**

The unit logs all SIP packets (one SIP packet is many lines). Select a log class for the SIP packets.

### **Log class for SIP license messages**

The unit logs license messages. Select a log class for these messages.

### **Log class for SIP errors**

The unit sends a message if there are any SIP errors. Select a log class for these log messages.

### **Log class for SIP media messages**

The unit creates log messages about when media streams are set up and torn down. Select a log class for these messages.

### **Log class for SIP debug messages**

The unit logs a lot of status messages, for example the SIP initiation phase of a reboot. Select a log class for these messages.

### **Log class for SIP IDS/IPS**

The unit logs messages regarding IDS/IPS actions and events. Select a log class for these messages.

## Hide sensitive data

Hides sensitive information in the log messages. E.g. encryption keys.

## 9.1.8. SIP Servers To Monitor

Your unit can monitor SIP servers, to check that they are alive. The information is used by the unit when SIP signaling should be passed on to the server in question. This is useful when a domain resolves to several individual hosts; the unit will know immediately if one of them is down, which will speed up the call connection.

The monitoring is done by that the unit sends SIP OPTIONS packets to the SIP server and the SIP server responds to them. In case the SIP server responds with an ICMP type 3 packet (Destination unreachable message) or when the other SIP server does not respond at all to previous SIP signaling, the unit will blacklist the SIP server. For the latter event, you can avoid the blacklisting by setting the **SIP blacklist interval** on the **Sessions and Media** page to zero(0). If the interval is set to zero (0) neither blacklisting nor monitoring will be done.

The monitoring interval (same as blacklist interval) can be set with the **SIP blacklist interval** option on the **SIP Services > Sessions and Media** page.

Edit row	Server	Port	Transport	Delete row
<input type="checkbox"/>	10.47.2.246	5060	-	<input type="checkbox"/>
<input type="checkbox"/>	10.47.2.248	5060	-	<input type="checkbox"/>
<input type="checkbox"/>	10.47.2.250	5060	-	<input type="checkbox"/>

Add new rows  rows.

### Server

Enter the host name, domain name, or IP address of the server to be monitored.

### Port

Enter the port to be monitored on that host. This should be the port to use for SIP signaling.

### Transport

Select the transport to be monitored on that host. This should be the transport to use for SIP signaling.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.1.9. SIP Server Signature

Here you can set the signature used in the Server and User-Agent headers in locally generated messages from the unit.

%product and %version are special variables that will be translated into the product's name and version respectively.

The signature is made up of a product part and an optional product version separated by a slash sign /. E.g. sipserver/1.0. The allowed set of characters are specified by the rule *token* in Section 25.1 in RFC 3261.

If this field is left empty no Server or User-Agent header will be added to locally generated messages from the unit.



The screenshot shows a configuration interface for the SIP Server Signature. At the top, there is a header bar with the text "SIP Server Signature" and a "(Help)" link. Below this is a text input field containing the value "%product/%version".

### 9.1.10. Save

Saves the Basic configuration to the preliminary configuration.

### 9.1.11. Undo

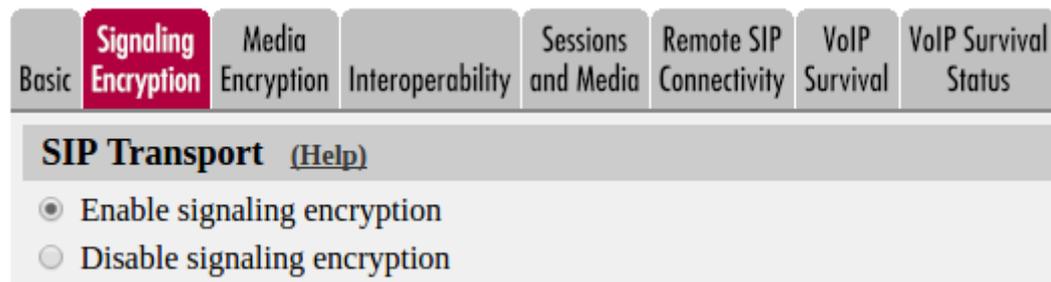
Clears and resets all fields in new rows and resets changes in old rows.

## 9.2. Signaling Encryption

To increase security, you can require that SIP users use TLS, which encrypts the connection. This makes it hard for eavesdroppers to read the SIP signaling.

### 9.2.1. SIP Transport

To make sure that no one can eavesdrop on the SIP signaling between your Ingate unit and its SIP peers, you can use encrypted SIP connections. This is managed by the TLS transport protocol (RFC 2246).

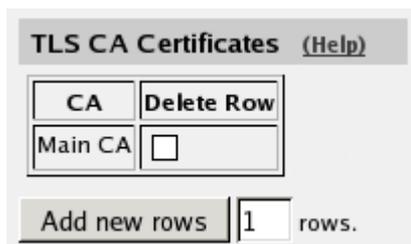


The screenshot shows a configuration page for SIP Transport. At the top, there is a navigation bar with several tabs: "Basic", "Signaling Encryption" (which is highlighted in red), "Media Encryption", "Interoperability", "Sessions and Media", "Remote SIP Connectivity", "VoIP Survival", and "VoIP Survival Status". Below the navigation bar is a header bar with the text "SIP Transport" and a "(Help)" link. Underneath, there are two radio button options: "Enable signaling encryption" (which is selected) and "Disable signaling encryption".

### 9.2.2. TLS CA Certificates

To authenticate peers for TLS connections, the unit needs certificates for the CAs used for signing

the peer certificates.



The screenshot shows a table titled "TLS CA Certificates" with a "(Help)" link. The table has two columns: "CA" and "Delete Row". The first row contains "Main CA" and an empty checkbox. Below the table is a button labeled "Add new rows" followed by a text input field containing "1" and the text "rows."

## CA

Select a CA from which the unit should accept connections. The CA certificates are imported on the **Certificates** page.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.2.3. Check server domain match

Usually, the unit only checks that the server certificate is signed by a CA listed in the **TLS CA Certificates** table. This setting makes the unit also check that the domain presented in the certificate matches the domain which the unit tried to contact.



The screenshot shows a section titled "Check Server Domain Match" with a "(Help)" link. Below the title is the text "Check if the server domain matches the certificate:". There are two radio buttons: "Yes" (unselected) and "No" (selected).

### 9.2.4. TLS Connections On Different IP Addresses

To receive TLS signaling, the unit must have an X.509 certificate, which works as an ID card, identifying the unit to your SIP peer. This will ensure that they are really communicating with your unit and not somebody else's computer. TLS uses an encryption method using two keys, one secret and one public. The secret key is kept in the unit and the public key is used in the certificate. If any of the keys are changed, the TLS connection won't work.

The unit can use different certificates to identify itself depending on which IP address the peer connected to. This is necessary when using TLS on more than one interface, as the certificate must match the used IP address. The selected certificate will be used for TLS on that IP address, for unit-initiated connections as well as connections initiated by a peer. The unit is identified by entering the interface hostname or IP address within the Common Name (CN) field of the certificate when it is created.

You can require that the connecting peer also identifies itself with a certificate (MTLS, mutual TLS). If you do that, the CA for the peer certificate must be uploaded in the **TLS CA Certificates** table.

You also select which TLS settings the unit should use when acting as server. TLS settings are defined on page [TLS](#).

TLS Connections On Different IP Addresses <a href="#">(Help)</a>					
IP Address	Own Certificate	Use CN FQDN	Require Client Cert	TLS	Delete Row
eth0 (10.48.28.61) ▼	MyCert ▼	Yes ▼	Yes ▼	TLSv1.x ▼	<input type="checkbox"/>

Add new rows  rows.

### IP Address

Select an IP address on which the unit should be able to receive SIP signaling over TLS. You can select from the unit IP addresses configured on the **Interface** pages under **Network**.

### Own Certificate

Select the certificate to use when the unit initiates or receives TLS connections using the selected IP address. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

### Use CN FQDN

Use certificate's CN (Common Name) as FQDN (Fully Qualified Domain Name) in SIP URI headers like Contact and Record-Route instead of IP address.

### Require Client Cert

Select if clients connecting to the unit on this IP address should be required to present a certificate for identification. If you turn this on, you must have uploaded the X.509 certificate for the CA that signed the client certificates. This is done in the **TLS CA Certificates** table.

### TLS

Select which methods the unit should accept when acting as server. TLS settings are defined on page [TLS](#).

## 9.2.5. Making TLS Connections

To make TLS connections where the connecting part (the client) is required to authenticate, the unit must have a certificate. The certificate is a kind of ID card, that the unit uses to identify itself. This is to make sure that the SIP peers really are talking to your unit, and not someone else's computer.

Making TLS Connections <a href="#">(Help)</a>	
Default own certificate:	Use TLS:
MyCert ▼	TLSv1.x ▼

## Default own certificate

Select the certificate to use when the unit initiates TLS connections, using an IP address which is not listed in the **TLS Connections On Different IP Addresses** table. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

## Use TLS

Select which method to use for the encrypted signaling. The unit can suggest one or more protocol versions for the signaling, and the peer will select one or reject the connection. TLS settings are defined on page [TLS](#).

### 9.2.6. Save

Saves the Signaling Encryption configuration to the preliminary configuration.

### 9.2.7. Undo

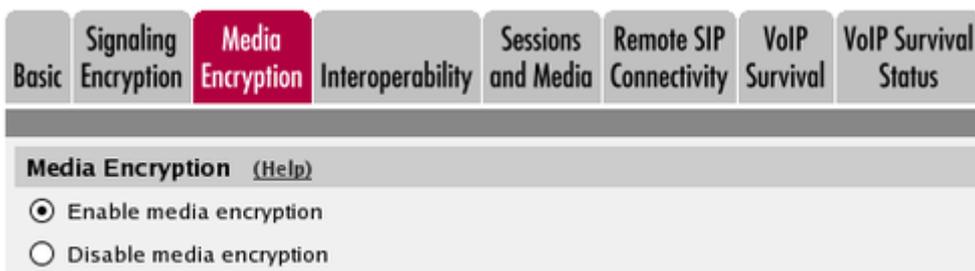
Clears and resets all fields in new rows and resets changes in old rows.

## 9.3. Media Encryption

You can select to not only encrypt the SIP signaling, but SIP media as well. This requires that the SIP device in the other end can decrypt the encrypted media streams.

If you select to encrypt media, mind that you also encrypt the SIP signaling (using TLS), or your encryption keys will be sent unencrypted over the network.

### 9.3.1. Media Encryption



Select if media encryption should be enabled or disabled. When disabled, no other media encryption settings will have effect.

### 9.3.2. SIP Media Encryption Policy

For each interface or VLAN, you can select which crypto suites are allowed. This means that negotiations about media sent to and from this interface/VLAN will only contain these crypto offers. You also select whether transcoding is allowed or not, i.e. whether the unit is allowed to change the crypto offers in the SDP or not.

Traffic for interfaces/VLANs not entered in this table will be processed according to the defined **Default Encryption Policy**.

SIP Media Encryption Policy <a href="#">(Help)</a>				
Edit Row	Media Via Interface/VLAN	Suite Requirements	Allow Transcoding	Delete Row
<input type="checkbox"/>	Internal (eth0 untagged)	-	No	<input type="checkbox"/>
<input type="checkbox"/>	External (eth1 untagged)	All encrypted	Yes	<input type="checkbox"/>

Add new rows  rows.

### Media Via Interface/VLAN

Select the interface or VLAN for media according to this policy.

### Suite Requirements

Select which crypto suites are required for the selected interface/VLAN. Select from the groups defined in the Crypto Suite Groups table.

### Allow Transcoding

Select if the unit should be allowed to rewrite the crypto offers in the SIP packet to ensure that the allowed crypto suites are used. If transcoding is not allowed, and the incoming packet does not offer any of the allowed suites, the call will be denied and a SIP packet with error code will be returned.

If the SIP packet will be sent out from another interface/VLAN than the one which received it, the unit will check this setting for both interfaces/VLANs. If at least one of them allows transcoding, it will be allowed for the packet.

Transcoding can only be done for encryption algorithms which the unit can handle, as it needs to be able to encrypt and decrypt the media streams.

If this column is missing, it is a good indication that the license for **Enhanced security** is not installed on your unit. Please contact Support at Ingate to get the **Enhanced security** License.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 9.3.3. Default Encryption Policy

Packets that do not match any of the rows in the **SIP Media Encryption Policy** table are treated according to the Default Encryption Policy.

Default Encryption Policy <a href="#">(Help)</a>	
Suite requirements:	Allow transcoding:
<input type="text" value="Encrypted"/>	<input checked="" type="radio"/> Yes <input type="radio"/> No

## Suite requirements

Select which crypto suites are required for other interfaces/VLANs. Select from the groups defined in the **Crypto Suite Groups** table.

## Allow transcoding

Select if the unit should be allowed to rewrite the crypto offers in the SIP packet to ensure that the allowed crypto suites are used. If transcoding is not allowed, and the incoming packet does not offer any of the allowed suites, the call will be denied and a SIP packet with error code will be returned.

### 9.3.4. Require TLS

To support mixed configuration where devices contacted on TLS get mcrypto and devices on other protocols get cleartext. Or just ensure no crypto keys are sent in clear.

**Require TLS** [\(Help\)](#)

Require TLS for all cryptos but cleartext

Do not require TLS

### 9.3.5. RTP Profile

SRTP (Secure RTP), when set up with sdescriptions, uses a different RTP profile (RTP/SAVP) compared to normal RTP (RTP/AVP). When the unit sends an SDP offer it can only use a single profile in the SDP.

**RTP Profile** [\(Help\)](#)

Prefer RTP/SAVP (sdescriptions)

Prefer RTP/AVP (cleartext and legacy encryptions)

Prefer RTP/AVP (together with sdescriptions)

If the selected policy only allows sdescriptions, the RTP/SAVP profile will be used. If sdescriptions are not allowed, the RTP/AVP profile will be used. If both are allowed in the selected policy, this setting will tell which profile to use.

Some clients can't understand the "RTP/SAVP" notation. In these cases, you might want to offer them as "RTP/AVP" together with the sdescription attributes (RTP/AVP (together with sdescriptions)). This violates the standard, but makes the offer compatible with clients unaware of sdescriptions.

### 9.3.6. Multi Profile

A nonstandard RTP profile negotiation method sometimes required for interoperability. When enabled the unit will send multiple m= lines in a SDP offer. One with a RTP/SAVP profile and one with a RTP/AVP profile. It will also handle SDPs containing such multi profiles.

Multi profiles will only work on networks that handle both cleartext and sdescriptions. E.g. networks that use the pre-defined suite "Any (transcodable)". The first m= line will always be

RTP/SAVP so the above RTP Profile setting doesn't have any effect when Multi Profile is enabled.

**Multi Profile** [\(Help\)](#)

Enable Multi Profile

Disable Multi Profile

### 9.3.7. DTLS-SRTP

**DTLS-SRTP** [\(Help\)](#)

Certificate: DTLS to use:

Ignore invalid dates in the client's certificate:  Yes  No

#### Certificate

The certificate to use when setting up the DTLS session. A certificate is required if this unit should transcode DTLS-SRTP. This is usually a self-signed certificate with an arbitrary common name.

#### DTLS to use

Which DTLS protocol to use.

#### Ignore invalid dates in the client's certificate

If the client's and server's clocks are not synchronized the date validation part of the DTLS handshake can go wrong. Enable this option to ignore invalid dates in the client's certificate.

### 9.3.8. Keep Established Crypto Within a Dialog

When generating an offer within a dialog (e.g. hold using re-INVITE) the same policy and profile apply as if it was the initial offer. This can cause problems with some clients in some media crypto scenarios where a call leg allows multiple crypto suites. Both cleartext and sdescriptions for instance. The profile will then be determined by the above RTP Profile setting. Which might not correspond to the previously established profile.

Setting this parameter to yes will keep the established crypto method within the SIP dialog.

**Keep Established Crypto Within a Dialog** [\(Help\)](#)

Keep established crypto within a dialog:  Yes  No

### 9.3.9. Add Cryptos in the B2BUA

This is an interoperability setting that defaults to yes.

If you experience problems with media encryption together with the B2BUA you can try to toggle this setting.

## Add Cryptos in the B2BUA [\(Help\)](#)

Add cryptos in the B2BUA:  Yes  No

### 9.3.10. Crypto Suite Groups

Define the crypto suite groups to be used in the encryption policies. Select from the crypto suites that the unit can suggest, terminate and/or let through.

Note that one group can contain one or more suites. When a group with several suites is selected, the unit will allow any of the suites included in the group.

Crypto Suite Groups <a href="#">(Help)</a>			
Edit Row	Name	Suite	Delete Row
<input type="checkbox"/>	+ All encrypted	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-f8 128, SHA1 80)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP SNOM (AES-CM 128, unknown)	<input type="checkbox"/>
<input type="checkbox"/>		Unknown k parameter (unknown)	<input type="checkbox"/>
<input type="checkbox"/>	+ Cleartext	Cleartext (no encryption)	<input type="checkbox"/>
<input type="checkbox"/>	+ Encrypted	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>

Add new rows  groups with  rows per group.

#### Name

A name for this combination of crypto suites. The name is only used internally in the unit.

#### Suite

Select from the suites the unit can recognize. The options are:

**Cleartext (no encryption):** No encryption.

**SRTP sdesc. (AES-CM 128, SHA1 80):** This is SRTP (Secure RTP) as specified by RFC 3711. It uses sdescriptions for key exchange, the AES-CM algorithm with a 128 bit key for media encryption, and the HMAC-SHA1 algorithm with an 80 bit tag for authentication. The unit can terminate this type of encryption, which means that you can require it on one side (like the outside) and require cleartext on another side (like the inside).

**SRTP sdesc. (AES-CM 128, SHA1 32):** This is SRTP (Secure RTP) as specified by RFC 3711. It uses sdescriptions for key exchange, the AES-CM algorithm with a 128 bit key for media encryption, and the HMAC-SHA1 algorithm with a 32 bit tag for authentication. The unit can terminate this type of encryption, which means that you can require it on one side (like the outside) and require cleartext on another side (like the inside).

**SRTP sdesc. (AES-f8 128, SHA1 80):** This is SRTP (Secure RTP) as specified by RFC 3711. It uses

sdescriptions for key exchange, the AES-f8 algorithm with a 128 bit key for media encryption, and the HMAC-SHA1 algorithm with an 80 bit tag for authentication. The unit cannot terminate this type of encryption, but can distinguish it in negotiations. This means that you can require this type on one side as long as you do not forbid it on another.

**SRTP SNOM (AES-CM 128, unknown):** This is SNOM's legacy encryption suite. It uses SRTP with the AES-CM encryption algorithm and a 128 bit key. The unit cannot terminate this type of encryption, but can distinguish it in negotiations. This means that you can require this type on one side as long as you do not forbid it on another.

**Unknown k parameter (unknown):** This means all other encryption offers using the k parameter that could be presented by a client. You can require this type on one side as long as you do not forbid it on another.

**Unknown sdescription (unknown):** This means all other encryption offers using sdescriptions that could be presented by a client. You can require this type on one side as long as you do not forbid it on another.

### 9.3.11. Save

Saves the Media Encryption configuration to the preliminary configuration.

### 9.3.12. Undo

Clears and resets all fields in new rows and resets changes in old rows.

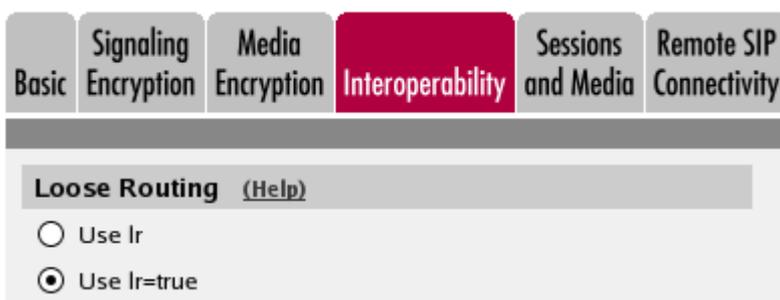
## 9.4. Interoperability

The SIP standard is still young and under considerable development. As an effect, several implementations of the standard omits parts of it, or makes guesses as to what will be accepted.

The unit adheres rather well to the standard (RFC 3261) per default, but you can also adjust the configuration to make more allowing for known issues in various SIP implementations.

### 9.4.1. Loose Routing

The unit uses the parameter "lr" in its SIP signaling to announce to other SIP devices that it uses loose routing. Some other SIP implementations incorrectly expect the lr parameter to be followed by a value, i.e. "lr=true". If you select that the unit should add this value to its SIP signaling, it will work with these implementations, too. This could affect its interaction with other SIP devices that conform to the SIP standard very strictly.



The screenshot shows a configuration interface with a horizontal menu at the top containing five tabs: "Basic", "Signaling Encryption", "Media Encryption", "Interoperability", "Sessions and Media", and "Remote SIP Connectivity". The "Interoperability" tab is highlighted in red. Below the menu, the "Loose Routing" section is visible, featuring a title bar with "Loose Routing" and a "(Help)" link. Underneath, there are two radio button options: "Use lr" and "Use lr=true". The "Use lr=true" option is selected, indicated by a filled circle.

Select to use **lr** or **lr=true**.

### 9.4.2. Relaxed Refer-To

The SIP standard requires that a Refer-To header with a question mark in it must be contained within angle brackets. Some clients do not honor this.

**VoIP Survival** **VoIP Survival Status**

**Relaxed Refer-To** [\(Help\)](#)

Recommended setting: Only allow Refer-To "?" with angle brackets

Only allow Refer-To "?" with angle brackets

Allow Refer-To "?" without angle brackets

Select whether the unit should accept Refer-To headers without angle brackets, but containing question marks. The recommended setting is **Only allow Refer-To "?" with angle brackets**.

### 9.4.3. Remove Via Headers

Some servers refuse to accept requests with more than one Via header. List those servers in this table. Enable the checkbox to remove all but our own Via header for signaling destined to any SIP server.

When a request to a listed server is sent - or if the checkbox is checked - all Via headers except the one added by the unit will be removed. When a response from the server is received they will be re-inserted.

**Remove Via Headers** [\(Help\)](#)

SIP Server			
DNS Name or IP Address	IP Address	Delete Row	

ROWS.

Remove Via Headers for all SIP servers

#### SIP Server

Enter the DNS name or IP address for the SIP servers that won't accept more than one Via header.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.4.4. Translation Exceptions

Usually, the unit rewrites IP addresses in the SIP signaling to hide it for the receiver. For some reasons, you might want to except certain IP addresses from being rewritten. Enter those IP addresses in the table.

Translation Exceptions <a href="#">(Help)</a>			
Edit Row	Except This From Translation		Delete Row
	DNS Name or IP Address	IP Address	
<input type="checkbox"/>	1.2.3.4	1.2.3.4	<input type="checkbox"/>

rows.

#### Except this from translation

Enter the DNS name or IP address to be excepted from IP address translation. If you enter a DNS name, the corresponding IP address will be excepted from translation.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.4.5. Expires Header

Some SIP clients don't understand the expires: parameter in the Contact header. To set the expiration time for those clients, you can make the unit add to REGISTER request replies an Expires header with the expires value in it.

Expires Header <a href="#">(Help)</a>
<input checked="" type="radio"/> Never add Expires header
<input type="radio"/> Add Expires header if the request contained one
<input type="radio"/> Always add Expires header

Select to **Always add Expires header**, **Never add Expires header**, or **Add Expires header if the request contained one**. The last means that the unit will add an Expires header to the response if the request from the client contained one.

## 9.4.6. Force Translation

Normally, the unit does not translate domain names in Contact and Via headers, but lets them through without modification. However, there are situations when domains should be translated. Enter domain names that should be translated in this table.

Force Translation <a href="#">(Help)</a>		
Edit Row	Always Translate This	Delete Row
<input type="checkbox"/>	vega.ingate.com	<input type="checkbox"/>

Add new rows  rows.

## 9.4.7. Always Translate This

Enter the domain that should always be translated. Wherever this domain is present in the Contact and Via header URIs, it will be replaced with the unit's own IP address.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 9.4.8. URI Encoding

When registering a SIP client on one side of the unit to a SIP server on the other side, the Contact header is normally encrypted and rewritten. By doing this, we make it possible for the SIP server to track when the same user is sending requests from different places. It is possible to turn encryption and rewriting off, and to shorten the encrypted URI in Contact headers passing through the unit.

URI Encoding <a href="#">(Help)</a>
Recommended setting: Always encrypt URIs
<input checked="" type="radio"/> Always encrypt URIs
<input type="radio"/> Use shorter, encrypted URIs
<input type="radio"/> Escape URIs
<input type="radio"/> Keep username in URIs
<input type="radio"/> Self-made GRUUs
<input type="radio"/> Use registration

Select what to do with Contact headers.

**Always encrypt URIs** will make the unit encrypt the entire Contact header URI.

**Use shorter, encrypted URIs** will make the unit generate a random string for the incoming Contact

URI. This will then be used as the username part of the outgoing Contact header URI.

When you select this, the unit makes no checks of incoming SIP URIs. It becomes possible in theory to trick the unit to send SIP packets anywhere, so security is drastically reduced.

**Escape URIs** will make the unit escape the entire original URI and use that as the username part of the outgoing Contact.

The encryption of a Contact URI is changed when the Call-ID changes, when the client gets a new IP address, or when the user changes its Contact URI.

When you select this, the unit makes no checks of incoming SIP URIs. It becomes possible in theory to trick the unit to send SIP packets anywhere, so security is drastically reduced.

**Keep username in URIs** will make the unit keep the original username part of the Contact URI, and only replace the domain part.

When you select this, it will be impossible for the remote SIP server to tell if requests for a certain user belong to one or several clients, as it has no means of telling the client registrations for a user apart. This means that if a user registers from two clients, and then unregisters from one of them, the SIP server will remove its only registration record for that user.

The unit also makes no checks of incoming SIP URIs. It becomes possible in theory to trick the unit to send SIP packets anywhere, so security is drastically reduced.

**Self-made GRUUs** (Globally Routable UA URI, see RFC 5627) will be created to replace URIs that are not globally routable. This setting hides network topology information by encryption. The advantage with this setting is that it hides only the information needed for routing, numbers and other parameters are in clear text and can be interpreted by other systems.

**Use registration** No encoding, modifies the URI to the URI registered by the user. This will make the URI even shorter and hides network topology, but is also a setting for compatibility with system not accepting encoded URI:s. This setting requires that the caller is registered with same identity as used when calling.

#### 9.4.9. Signaling Order of Re-INVITES

When the unit acts as a B2BUA (e.g. almost always when performing SIP Trunking), it normally handles re-INVITES by forwarding them and waiting for a response, just as for the original INVITE.

With some SIP devices, this can cause problems. For these situations, the unit can instead handle the re-INVITES hop by hop, meaning that it sends a "200 OK" response back before forwarding the INVITE to the next SIP device.

The consequence will be that the unit will re-use the old SDP from the other end when sending the 200. For dialogs where the re-INVITE is used to change codec or some other RTP parameter, the recommended way is to send re-INVITES all the way directly.

#### Signaling Order of Re-INVITES [\(Help\)](#)

Recommended setting: Send re-INVITES all the way directly

- Send re-INVITES all the way directly
- Send response before re-INVITES are forwarded

Select if the INVITES should be sent all the way, or be processed hop by hop.

### 9.4.10. Loose Username Check

Normally, the unit checks that the authentication username equals the username in the From header. Some clients use their whole address as authentication username (ie: `user@host.com`), which means that the username "user" in the From header is compared with the authentication username "`user@host.com`". This authentication will fail. With this function, "@host.com" is stripped from the authentication username.

#### Loose Username Check [\(Help\)](#)

- Use the username as authentication name
- Use the entire address as authentication name

Select if the entire SIP address or only the username should be used as the authentication name.

### 9.4.11. User Matching

Here, you can select to match on username only or username as well as domain.

If you match on username only, users with the same username will be treated as the same, even when they are under different domains.

#### User Matching [\(Help\)](#)

- Match only on username
- Match on username and domain

### 9.4.12. Force Record-Route for Outbound Requests

Here, you select if the unit should add a Record-Route header to all requests received by the unit, but whose Request-URI does not contain one of its **Local SIP Domains**.

The Record-Route header makes all subsequent SIP signaling for this session to be routed via the unit even if it is not the shortest route.

#### Force Record-Route For Outbound Requests [\(Help\)](#)

Recommended setting: No

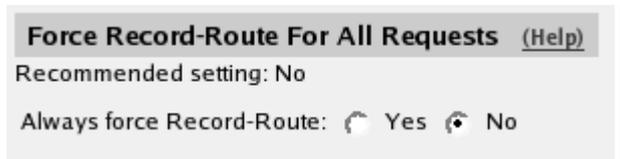
Force Record-Route for outbound requests:  Yes  No

Here, you select to add Record-Route headers for outbound requests or not.

### 9.4.13. Force Record-Route for All Requests

Here, you select if the unit should add a Record-Route header to all requests received by the unit, which should be passed on to another client/server.

The Record-Route header makes all subsequent SIP signaling for this session to be routed via the unit even if it is not the shortest route.



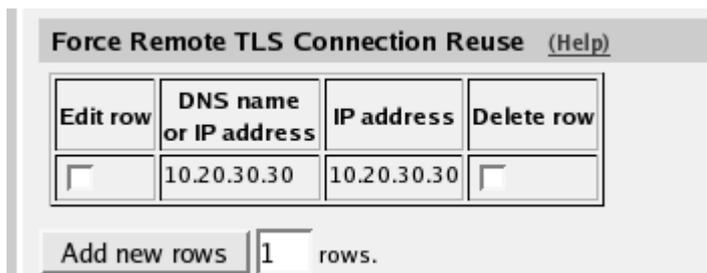
**Force Record-Route For All Requests** (Help)  
Recommended setting: No  
Always force Record-Route:  Yes  No

Here, you select to add Record-Route headers for all requests or not.

### 9.4.14. Force Remote TLS Connection Reuse

Enter SIP servers to which the unit connects using TLS. For the listed servers, the unit will use the actual source port for the TLS connection instead of port 5061.

This is useful in the SIP signaling, where port numbers are used in Via and Route headers.



**Force Remote TLS Connection Reuse** (Help)

Edit row	DNS name or IP address	IP address	Delete row
<input type="checkbox"/>	10.20.30.30	10.20.30.30	<input type="checkbox"/>

Add new rows  rows.

#### DNS Name or IP Address

Enter the DNS name or IP address for a SIP server for which the unit should reuse TLS ports.

#### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.4.15. Accept TCP Marked As TLS

When a TLS accelerator is used, SIP packets can be sent to the unit via TCP, but the packet content will look as if TLS was used.

#### Accept TCP Marked As TLS [\(Help\)](#)

Recommended setting: Only accept TLS transport for TLS marked signaling

- Only accept TLS transport for TLS marked signaling
- Accept TCP marked as TLS

Select if TCP packets with TLS content should be accepted. The recommended setting is not to accept them.

### 9.4.16. Allow Large UDP Packets

Sometimes, the SIP signaling UDP packets get larger than the standard (RFC 3261) allows. There are two ways to handle this; either send large UDP packets, which may become fragmented into several packets, or use TCP.

Some SIP devices may not be able to receive TCP packets, which is a violation of RFC 3261. This means that you have to allow large UDP packets (larger than 1300 byte), but to do this violates section 18.1.1 in RFC 3261.

Note that there also may be SIP devices that cannot handle fragmented UDP packets, even though this also violates RFC 3261.

This setting only affects SIP signaling packets.

#### Allow Large UDP Packets [\(Help\)](#)

Recommended setting: Use TCP for large packets

- Use TCP for large packets
- Allow large UDP packets

Select if large UDP packets should be allowed. The recommended setting is to use TCP when the packets become too large.

### 9.4.17. Remove Headers in 180 Responses

Some SIP servers require that the Contact and Record-Route headers are removed from 180 responses.

#### Remove Headers in 180 Responses [\(Help\)](#)

Recommended setting: Keep Record-Route and Contact headers in 180 responses

- Keep Record-Route and Contact headers in 180 responses
- Remove Record-Route and Contact headers in 180 responses

Select if the unit should remove these headers in 180 responses. The recommended setting is to keep the headers.

## 9.4.18. Forward CANCEL Body

Normally, a CANCEL request does not contain a body. There are some systems which put a body in these requests. As every SIP proxy generates a new CANCEL instead of just forwarding the incoming request, any body in the incoming request is usually dropped. Select here if the unit should forward any CANCEL body when the CANCEL itself is forwarded.

**Forward CANCEL Body** [\(Help\)](#)  
Recommended setting: Send CANCEL without body  
 Send CANCEL without body  
 Forward CANCEL body

## 9.4.19. Use CANCEL Body In ACK

Normally, a CANCEL request does not contain a body. There are some systems which put a body in these requests. As every SIP proxy generates a new CANCEL instead of just forwarding the incoming request, any body in the incoming request is usually dropped.

For INVITE requests, an ACK is always required. Some systems require that the body from the CANCEL should also be used in the ACK. Select here if the unit should use the CANCEL body in the ACK.

**Use CANCEL Body in ACK** [\(Help\)](#)  
Recommended setting: Send ACK without CANCEL body  
 Send ACK without CANCEL body  
 Use CANCEL body in ACK

## 9.4.20. Preserve RFC 2543 Hold

sendonly streams are defined differently in RFC 2543 and RFC 3264. The unit uses the RFC 3264 way, and converts SDPs when the old behaviour is seen. In particular, the c= line is modified, as was not defined in RFC 2543. Some clients aren't updated to RFC 3264 yet and will not understand what happens.

**Preserve RFC 2543 Hold** [\(Help\)](#)  
Recommended setting: Use RFC 3264 Hold for all SDPs  
 Use RFC 3264 Hold for all SDPs  
 Preserve RFC 2543 Hold

When Use RFC 3264 Hold is selected, the c= line with address 0.0.0.0 will be rewritten. When Use RFC 2543 Hold is selected, the c= line with address 0.0.0.0 will be left unmodified.

## 9.4.21. Force RFC 3264 Hold Compliance

A media stream may be of four different types: sendonly, recvonly, inactive or sendrecv (the default). When putting a call on hold the SIP user agent normally changes the type from sendrecv to sendonly or inactive. RFC 3264 specifies which stream types the peer may use in its answer. If the

offer for example contains "inactive", then the answer must be "inactive". Select "Force RFC 3264 hold compliance" when you want the unit to change the stream type to an allowed value if the received answer isn't allowed by RFC 3264. This setting has no effect when **Inhibit hold** is enabled.

**Force RFC 3264 Hold Compliance** [\(Help\)](#)  
Recommended setting: Preserve RFC 3264 hold type

- Preserve RFC 3264 hold type
- Force RFC 3264 hold compliance

Recommended setting: Preserve RFC 3264 hold type.

### 9.4.22. Inhibit Hold

This setting controls if the unit should remove requests for on-hold from SDP offers before forwarding them. When **Inhibit hold** is used, the stream(s) in SDP offers will be converted from sendonly, recvonly or inactive to sendrecv before being forwarded by the unit. Forwarded SDP answers will only reflect the stream mode (sendonly, recvonly etc.) requested in the offer, and will not depend on the received SDP answer.

**Only inhibit hold for clients behind remote NAT:** As **Inhibit hold** but only for clients detected as being behind a NAT device - WAN and local LAN clients are thus unaffected. See [Remote SIP Connectivity](#). Introduced in v6.0.

**Inhibit Hold** [\(Help\)](#)  
Recommended setting: Allow hold

- Allow hold
- Inhibit hold
- Only inhibit hold for clients behind remote NAT

Recommended setting: Allow hold.

### 9.4.23. Force Inactive Hold

When a SDP for putting a call on-hold is processed, this setting will change any "recvonly" and "sendonly" attributes to "inactive".

**Force Inactive Hold** [\(Help\)](#)  
Recommended setting: No

Force "inactive" attribute for "on-hold" SDP:  Yes  No

Recommended setting: No

### 9.4.24. Convert Escaped Whitespaces in URIs

Sometimes, whitespaces in incoming URIs are escaped, which make them look like "%20". This is

most common in URIs in the Refer-To header used by the REFER method. As some other SIP devices cannot properly decrypt these escaped whitespaces, the unit can be made to convert them back to normal whitespaces.

#### **Convert Escaped Whitespaces in URIs** [\(Help\)](#)

- Preserve "%20" in URIs
- Convert "%20" into whitespace in URIs

Select if "%20" should be converted into a whitespace or preserved in URIs.

### **9.4.25. Strip ICE Attributes**

Some SIP clients, like Microsoft Communicator 2007, seem to prefer ICE "a=candidate" attributes in SDP over other information, and it doesn't perform STUN tests as it is supposed to in order to verify the connection. This may sometimes result in no media.

A way to avoid this is to make the unit remove these attributes for all requests.

#### **Strip ICE Attributes** [\(Help\)](#)

- Keep ICE attributes in SDPs
- Strip ICE attributes in SDPs

### **9.4.26. Add Ingate SIParator/Firewall as ICE Candidate**

Some SIP clients require ICE and expect a list of ICE candidates. This setting can rewrite the SDP connection information and add the required relay candidates so that media will be sent to the unit instead.

#### **Add Ingate SIParator/Firewall as ICE Candidate** [\(Help\)](#)

- Do not add Ingate SIParator/Firewall as ICE candidate
- Add Ingate SIParator/Firewall as ICE candidate

### **9.4.27. Ports and the maddr Attribute**

The maddr attribute is used to point to a specific IP address, regardless of what the domain/IP address in the main URI should point to. This attribute only applies to the domain/IP address part according to RFC 3261, and other parameters in the original URI (like the port and transport) will still be used. However, some user agents expect that the maddr attribute will reset other URI parameters.

#### **Ports and the maddr Attribute** [\(Help\)](#)

- Use original URI port when using the maddr attribute
- Ignore original URI port when using the maddr attribute

Select if the unit should use the original URI parameters (as is defined in RFC 3261) or if the port stated in the original URI should be ignored.

### 9.4.28. Remove SDP from 1xx Provisional Responses

Enable this setting if you want to remove the SDP from 1xx provisional responses. Solves scenarios when we get different SDPs in 1xx and 200 responses in the same dialog.

#### **Remove SDP from 1xx Provisional Responses** [\(Help\)](#)

Recommended setting: No

Remove SDP from 1xx Responses:  Yes  No

Introduced in: v6.0.

Recommended setting: No

### 9.4.29. Match also port in Request-URI in Dial Plan

When matching on Request-URI in the Dial Plan using Reg Expr, append incoming port to the Request-URI used for the operation if the Request-URI contains the incoming IP address and the incoming port is not 5060. E.g. if additional **SIP Signaling Ports** have been added these can be matched in the Reg Expr field by appending :port to the IP address.

#### **Match also port in Request-URI in Dial Plan** [\(Help\)](#)

Recommended setting: No

Match also port in Request-URI:  Yes  No

Introduced in: v6.0.

Recommended setting: No

### 9.4.30. Use session identifier when comparing endpoint SDPs

Support SDPs differing only on the session identifier (sess-id).

#### **Use session identifier when comparing endpoint SDPs** [\(Help\)](#)

Recommended setting: No

Use session identifier when comparing endpoint SDPs:  Yes  No

Introduced in: v6.0.

Recommended setting: No

### 9.4.31. Accept Late Media Source Change for RSC

Accept remaining media from pre-transfer source address while awaiting media from post-transfer source address after SIP REFER of Remote SIP Clients.

Only effective together with the setting **SIP Services** → **Sessions and Media** → **Lock IP address and port to first sender**.

Only one of the clients can be a Remote SIP Client.

### **Accept Late Media Source Change for RSC** [\(Help\)](#)

Recommended setting: No

Accept Late Media Source Change for RSC:  Yes  No

Introduced in: v6.0.

Recommended setting: No

## **9.4.32. Update Username Mapping on Refer-To**

When using the URI Encoding: **Keep username in URIs**, update the username location mapping based on the Refer-To header in call transfer scenarios.

### **Update Username Mapping on Refer-To** [\(Help\)](#)

Recommended setting: No

Update Username Mapping on Refer-To:  Yes  No

Introduced in: v6.0.

Recommended setting: No

## **9.4.33. Translate Refer-To**

The Refer-To header is translated to be able to stay in the route and to hide topology. Here you can disable translation of the Refer-To header.

### **Translate Refer-To** [\(Help\)](#)

Recommended setting: Yes

Translate Refer-To:  Yes  No

Introduced in: v6.0.

Recommended setting: Yes

## **9.4.34. Convert 5xx Responses to 503**

Convert all 5xx response codes to 503 in sent SIP messages.

### **Convert 5xx Responses to 503** [\(Help\)](#)

Recommended setting: No

Convert 5xx Responses to 503:  Yes  No

Introduced in: v6.0.

Recommended setting: No

### 9.4.35. Allow RTP before answer SDP

Allow RTP before we have received the answer SDP. Requires an empty 183 response. Requires the B2BUA or SIP Trunk to handle re-negotiation when the answer SDP is received.

**Allow RTP before answer SDP** [\(Help\)](#)

Recommended setting: No

Allow RTP before answer SDP:  Yes  No

Introduced in: v6.0.

Recommended setting: No

### 9.4.36. Keep User-Agent Header When Acting as B2BUA

Usually, when the unit acts as a back to back user agent (B2BUA), it replaces the original User-Agent header with its own. This might cause problems if the other endpoint chooses what to do based on the User-Agent field and what is known about different user agent capabilities.

**Keep User-Agent Header When Acting as B2BUA** [\(Help\)](#)

Use Ingate Firewall as User-Agent header

Keep existing User-Agent header

Select if the unit should rewrite the User-Agent field or not.

### 9.4.37. SDP Offer in re-INVITE

Some SIP servers sometimes send re-INVITEs without an SDP (session description), offer when they are performing a call transfer. This is allowed according to the SIP RFC (RFC 3261).

Some service providers, or other SIP servers, might not be able to handle INVITEs without an SDP offer, which means that the call cannot be set up/transferred.

To avoid this, the unit always adds an offer to the empty re-INVITE. Select here if it should re-use an old answer (which usually only contains one codec) as the new offer, or if it should add more common codecs to the new offer to provide more choices for the new SIP client.

**SDP Offer in re-INVITE** [\(Help\)](#)

Re-use old answer for SDP offer in re-INVITE

Add codecs to new SDP offer in re-INVITE

Select if the unit should forward empty INVITEs, or add its own dummy SDP to the INVITE before forwarding it.

The dummy SDP will look something like this (addresses, ports and origin line will be changed and codecs may be removed by codec filtering functionality):

```
v=0
o=- 0 0 IN IP4 127.0.0.1
s=-
c=IN IP4 127.0.0.1
t=0 0
m=audio 9 RTP/AVP 0 18 96
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
a=sendrecv
```

### 9.4.38. Use RTCP Attribute in SDP

Some SIP devices support the RTCP attribute (RFC 3605), where you state a port on which to receive the RTCP packets. Normally, these are sent to the port next higher to the RTP port.

You can make the unit use this attribute when negotiating, and subsequently receive the RTCP stream on a port quite different to the media port. The drawback is that if the SIP peer does not support the RTCP attribute, it will instead send the RTCP packets to the normal port, and thus RTCP won't work for the call.

#### Use RTCP Attribute in SDP [\(Help\)](#)

- Always receive RTCP one port number above RTP media
- Use RTCP attribute in SDP

Select if the unit should always receive RTCP on the port adjacent to the media port, or if the RTCP attribute should be used.

### 9.4.39. Keep To Header in Forwarded Requests

When the unit back-to-back user agent (B2BUA) forwards requests, it usually changes the To header into the new target. If this target (a SIP operator or a PBX) makes decisions based on the To header, this can be an unwanted behaviour.

#### Keep To Header in Forwarded Requests [\(Help\)](#)

- Change To header into the forwarding target
- Keep the To header when forwarding requests

Select to make the unit keep the original To header when forwarding requests via the B2BUA, or to rewrite it.

### 9.4.40. Media Stream Reuse Time

When the unit closes a media stream, for example when a call is put on hold, it normally forgets

about the stream. When the call is resumed, a new media stream is set up. This new stream may use different ports than the original stream. Some faulty SIP devices don't accept that.

#### **Media Stream Reuse Time** [\(Help\)](#)

Recommended setting: 0

Remember media streams after use:

seconds

You can make the unit remember the streams, so that they can later be reused (and reopened). If they are remembered too long, the local ports may be exhausted. On the other hand, they must be remembered as long as the longest expected hold time.

### **9.4.41. Wildcard Server Domain Certificate Match**

Certificates containing wildcard domain names are normally not used with SIP.

#### **Wildcard Server Domain Certificate Match** [\(Help\)](#)

Recommended setting: Don't allow wildcard in server certificates

- Don't allow wildcard in server certificates
- Allow wildcard in server certificates

Recommended setting: Don't allow wildcard in server certificates.

### **9.4.42. DNS Override When Redirecting on 3xx**

When following 3xx redirects, DNS override may be used when processing the new target(s).

#### **DNS Override When Redirecting on 3xx** [\(Help\)](#)

Recommended setting: Use DNS Override

- Use DNS Override
- Skip DNS Override

Recommended setting: Use DNS Override.

### **9.4.43. Open Port 6891 For File Transfer**

Messenger clients do not always use the ports that are negotiated in the SIP signaling. In particular, the File Transfer function always uses the same port, regardless of what is negotiated. To make File Transfer work through the unit you must open port 6891, the Messenger File Transfer port.

You only need to do this if File Transfers are made between clients on different networks; if transfers are always only made between clients on the same network, no extra ports need to be opened.

Note: If more than one Messenger client performs file transfer through the unit at the same time, they could end up sending to each other's peers instead of their own. An attacker could possibly use this to intercept transferred files; don't use this mechanism to transfer sensitive data.

#### Open Port 6891 for File Transfer [\(Help\)](#)

Recommended setting: Do not open port 6891 unless negotiated

- Do not open port 6891 unless negotiated
- Open port 6891 at File transfer

Here, you select to open port 6891 automatically or not. The recommended setting is not to open it unless negotiated.

#### 9.4.44. Allow RFC 2069 Authentication

Some SIP units can't handle Digest authentication as described in RFC 2617, but they still do authentication. The unit can allow the simpler form of authentication described in RFC 2069 to be able to interoperate with these units.

To allow this can decrease security. Use it only if units in your system need it.

#### Allow RFC 2069 Authentication [\(Help\)](#)

Recommended setting: No

Allow RFC 2069 Digest authentication:  Yes  No

Select if authentication according to RFC 2069 should be allowed (**On**) or not (**Off**). It is recommended to keep this setting off.

#### 9.4.45. Match Refer-To in Attended Transfers

Enable this setting if an external registrar requires the username of the Contact header, i.e. the address the registrar should send incoming calls to, to be equal to the To header, i.e. the user's SIP address.

#### Match Refer-To in attended transfers [\(Help\)](#)

Recommended setting: Match on Call-ID in Replaces overriding routing information

- Match on Call-ID in Replaces overriding routing information
- Use routing information

Recommended setting: Match on Call-ID in Replaces overriding routing information

#### 9.4.46. Pretend to Support "privacy" Option Tag in Proxy

Enable this setting if you want the unit to pretend it supports the "privacy" option tag without any real support.

#### Pretend to Support "privacy" Option Tag in Proxy [\(Help\)](#)

Recommended setting: Don't pretend to support "privacy" option tag

- Don't pretend to support "privacy" option tag
- Pretend to support "privacy" option tag

Recommended setting: Don't pretend to support "privacy" option tag.

#### 9.4.47. Force Username in Registered Contact

Enable this setting if an external registrar requires the username of the Contact header, i.e. the address the registrar should send incoming calls to, to be equal to the To header, i.e. the user's SIP address.

##### **Force username in registered Contact** [\(Help\)](#)

Recommended setting: No

Force use of To header username in Contact header of REGISTER requests:  Yes  No

Recommended setting: No

#### 9.4.48. Fix BYE Route set

Enable this setting to remove the topmost *Route:* entry of a BYE request before processing it. It should be used when the received BYE contains the ITSP IP/F.Q.D.N. as first entry of the *Route:* header.

##### **Fix BYE Route set** [\(Help\)](#)

Recommended setting: No

Force remove of topmost Route set entry in BYE requests:  Yes  No

Recommended setting: No

#### 9.4.49. Fix Bad Route set

When enabled the B2BUA will ignore the routes if a dialog request matches a UA call. In proxy mode, the topmost routes not pointing to the unit are removed.

##### **Fix Bad Route set** [\(Help\)](#)

Recommended setting: No

Repair a bad route set:  Yes  No

Recommended setting: No

#### 9.4.50. Detect unchanged session version in B2BUA

A B2BUA call has its own session version counter which is usually increased when forwarding a SDP. Enable this option to avoid increasing the session version if it's unchanged in the received SDP.

### Detect unchanged session version in B2BUA [\(Help\)](#)

Recommended setting: Always increase session version

- Always increase session version
- Detect unchanged session version

Recommended setting: Always increase session version

### 9.4.51. B2BUA Receive PRACK

When enabled the B2BUA will send all 1xx responses reliably by resending them until a matching PRACK is received. See RFC 3262.

#### B2BUA Receive PRACK [\(Help\)](#)

Recommended setting: Yes

Receive PRACK in B2BUA:  Yes  No

Recommended setting: Yes

### 9.4.52. B2BUA Send PRACK

When activated the B2BUA will announce support for RFC 3262 so that the recipient of a SIP INVITE can send 1xx responses reliably.

#### B2BUA Send PRACK [\(Help\)](#)

Recommended setting: Yes

Send PRACK in B2BUA:  Yes  No

Recommended setting: Yes

### 9.4.53. Hide our Record-Route header

Some SIP servers won't accept requests with a Record-Route header. In order to be able to communicate with these servers, you can select to hide our Record-Route header in requests to those servers. The Record-Route header is restored when the reply passes the unit.

Here, list servers for which we need to hide our Record-Route header. Enable the checkbox if you want to hide our Record-Route header for all SIP servers.

#### Hide our Record-Route header [\(Help\)](#)

SIP Server		Delete Row
DNS Name or IP Address	IP Address	

Add new rows  ROWS.

Hide our Record-Route header for all SIP servers

## SIP Server

Enter the DNS name or IP address of the SIP servers for which we need to hide our Record-Route header.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.4.54. Tear Down Media State on re-INVITE

Enable this setting to tear down the old media state (friendships) before the new one is setup when receiving a re-INVITE to a different RTP endpoint (i.e. call transfer).

**Tear Down Media State on re-INVITE** [\(Help\)](#)  
Recommended setting: No  
Tear down media state when handling re-INVITES:  Yes  No

Recommended setting: No

### 9.4.55. Disable re-INVITES

Some devices does not support re-INVITES, by setting this setting to yes, you disable re-INVITES.

**Disable re-INVITES** [\(Help\)](#)  
Recommended setting: No  
Disable re-INVITES:  Yes  No

Recommended setting: No

### 9.4.56. Disable Supported Header in B2BUA

Use **Don't add Supported Header in B2BUA** to instruct the B2BUA to not add a Supported Header.

**Disable Supported Header in B2BUA** [\(Help\)](#)  
Recommended setting: Add Supported Header in B2BUA  
 Add Supported Header in B2BUA  
 Don't add Supported Header in B2BUA

Recommended setting: Add Supported Header in B2BUA

### 9.4.57. Force RTP Packetization Time

Rewrite the RTP Packetization Time (ptime) value found in the SDP. This setting should only be used in very special cases.

#### **Force RTP Packetization Time** [\(Help\)](#)

Recommended setting: Unspecified (default SDP value)

Packetization Time (ms):

Recommended setting: Unspecified (default SDP value)

### 9.4.58. Sequential Register Delay

Add a delay between sequential registers. If the unit sees multiple register attempts with different call id within the specified time delay period, they will be dropped.

#### **Sequential Register Delay** [\(Help\)](#)

Recommended setting: Unspecified (no delay)

Delay (s):

Recommended setting: Unspecified (no delay)

### 9.4.59. Resolve public GRUU locally

Enable Globally Routable UA URI (GRUU) passthrough if a user-agent uses GRUU and the server doesn't rewrite the request URI (as mandated in RFC 5627).

#### **Resolve public GRUU locally** [\(Help\)](#)

Recommended setting: No

Enable GRUU passthrough:  Yes  No

Recommended setting: No

### 9.4.60. Always add Path Header in REGISTERS

Always add the Path Extension Header Field in REGISTER requests. Please refer to RFC 3327 for more information.

#### **Always add Path Header in REGISTERS** [\(Help\)](#)

Recommended setting: No

Add Path Header in REGISTER requests:  Yes  No

Recommended setting: No

### 9.4.61. Terminate Transferor on 183 session progress

Enable this setting if you want the B2BUA to terminate the call to transferor if it sees a 183 session progress from transfer target.

**Terminate Transferor on 183** [\(Help\)](#)  
Recommended setting: No  
Terminate transferor on 183:  Yes  No

Recommended setting: No

### 9.4.62. Forward headers in 3xx responses in the B2BUA

Add headers which should be forward in 3xx responses by the B2BUA to this table.

**Forward headers in 3xx responses in the B2BUA** [\(Help\)](#)

Header name	Delete Row
-------------	------------

Add new rows  rows.

#### SIP header

Enter the name of the SIP header that you want to forward in SIP 3XX responses.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 9.4.63. B2BUA Offer in INVITE

Enable this setting to always send B2BUA offer in INVITE, by translating a re-INVITE without SDP offer to a re-INVITE with a SDP offer.

**B2BUA Offer in INVITE** [\(Help\)](#)  
Recommended setting: No  
Always send B2BUA offer in INVITE:  Yes  No

Recommended setting: No

### 9.4.64. Save

Saves the Interoperability configuration to the preliminary configuration.

### 9.4.65. Undo

Reverts all of the above fields to their previous configuration.

### 9.4.66. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

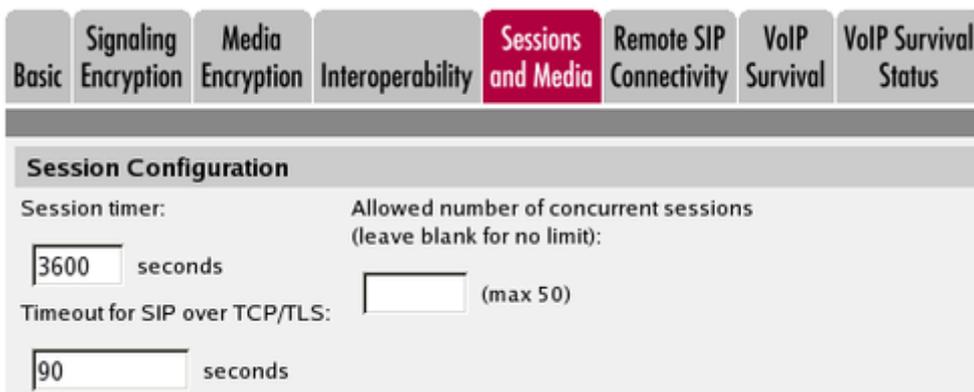
This button will only be visible if a DNS server has been configured.

## 9.5. Sessions and Media

Here, settings are made for the SIP timeouts and sessions negotiated via the unit.

Note that no DTMF settings are needed in the unit.

### 9.5.1. Session Configuration



Basic	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
<b>Session Configuration</b>							
Session timer:		Allowed number of concurrent sessions (leave blank for no limit):					
<input type="text" value="3600"/> seconds		<input type="text" value="50"/> (max 50)					
Timeout for SIP over TCP/TLS:							
<input type="text" value="90"/> seconds							

#### Session timer

Enter the maximum time for a SIP initiated connection. When the timeout is reached, the unit discards the media streams. The clients won't notice, as the connection is still active, but you won't hear anything as no media streams are let through. To avoid this, clients can regularly ask for new timeouts.

The Session timer must be at least 90 seconds to comply with the Min-SE requirement (RFC 4028).

The Session timer can be at most 24 hours within the GUI.

#### Timeout for SIP over TCP/TLS

The **Timeout for SIP over TCP/TLS** decides how long a SIP connection over TCP with the unit may

exist without having received a complete SIP request.

"0" or an empty field means that SIP over TCP or TLS cannot be used to the unit.

### Allowed number of concurrent sessions

Enter the amount of concurrent SIP sessions which the unit should handle.

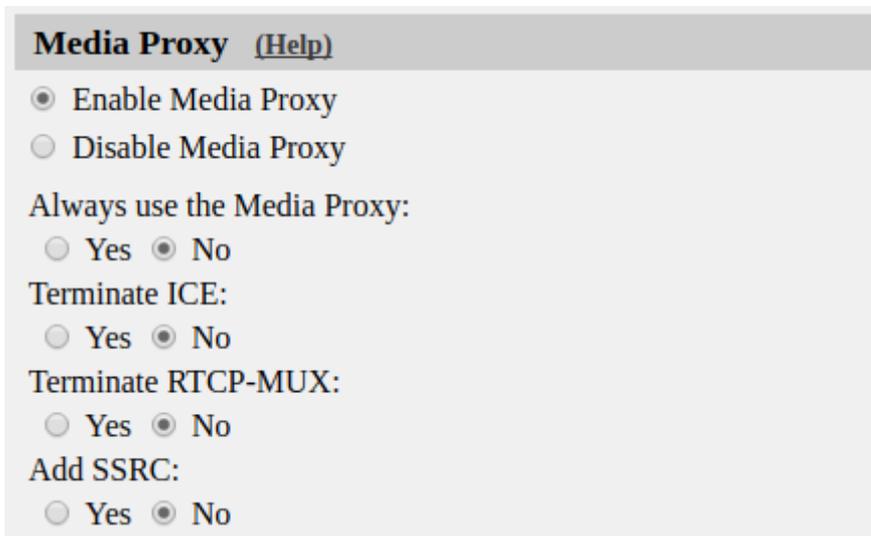
Leave the field empty to allow as many sessions as there are SIP Session licenses on the unit (number displayed inside parantheses). You can purchase additional SIP Session licenses from your retailer.

## 9.5.2. Media Proxy

Here you can enable or disable the media proxy.

The media proxy is required for:

- IP version conversion.
- DTLS-SRTP termination.
- ICE termination.
- RTCP-MUX termination.
- Adding SSRC.



**Media Proxy** [\(Help\)](#)

Enable Media Proxy  
 Disable Media Proxy

Always use the Media Proxy:  
 Yes  No

Terminate ICE:  
 Yes  No

Terminate RTCP-MUX:  
 Yes  No

Add SSRC:  
 Yes  No

### Always use the Media Proxy

Usually the media proxy will only be used when required. Here you can select to always use the media proxy when media is passed through the unit.

### ICE termination

The unit can act as an ICE-lite agent against a full ICE agent. This is needed for interoperability between clients that require ICE and clients that doesn't support ICE.

## RTCP-MUX termination

The unit can multiplex RTP and RTCP on a single port against clients that support it. Eases NAT traversal.

## Add SSRC

The unit can add SSRC to the SDP if none exists and rewrite the corresponding RTP/RTCP packets.

**NOTE** | The media proxy only supports UDP.

## 9.5.3. Media Configuration

The unit supports UDP and TCP media streams.

Set limitations for the media streams through the unit.

### Media Configuration [\(Help\)](#)

Limitation of sender of media streams:	Timeout for one-way media streams:
<input checked="" type="radio"/> Lock IP address and port to first sender	<input type="text"/> seconds
<input type="radio"/> Only allow receiving IP address, but multiple ports	
<input type="radio"/> Allow multiple sender IP addresses and ports	Tear down media streams at RTP/RTCP timeouts:
	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allowed number of senders:	Timeout for RTP streams:
<input type="text" value="10"/>	<input type="text"/> seconds
Allowed amount of media streams per SIP session:	Timeout for RTCP streams:
<input type="text" value="6"/>	<input type="text"/> seconds
Support forked media streams:	
<input type="radio"/> Yes <input checked="" type="radio"/> No	

### Limitation of sender of media streams

This setting allows you to define who can send media in a SIP call. This is never negotiated in the SIP signaling, and can theoretically be a completely different unit from the one receiving the media.

The unit usually locks a media stream to the first sender IP address and port (for security reasons). Some SIP clients change ports during the first media stream packets, which will block the media stream from being let through the unit. There are also scenarios where the media stream sender is changed to an entirely new sender.

You can select for the unit to **Lock IP address and port to first sender**, which will render the behaviour described above. **Only allow receiving IP address, but multiple ports** will allow media only from the IP address which will receive the media stream in the opposite direction, but allow for port changes on that IP address. **Allow multiple sender IP addresses and ports** lets the media stream through even if ports and/or IP addresses change.

## Allowed number of media streams per SIP session

Enter the amount of media streams a single SIP session can handle. This restriction is primarily made for preventing DOS attacks.

## Support forked media streams

If Support forked media streams is set to "yes", this allows setting up media streams for multiple endpoints where forked calls being answered simultaneously by multiple callees is supported by the endpoint.

## Timeout for one-way media streams

This setting is used by the unit to detect when media is only sent in one direction. If no media packets are received in one direction during the configured amount of seconds, the unit creates a log message about this.

## Tear down media streams at RTP/RTCP timeout

Here, you select if the unit should tear down media streams when the **Timeout for RTP streams** and **Timeout for RTCP streams** have been reached.

When the media streams are torn down, the session is still not terminated by the unit. This means that there will be no SIP messages sent out (like a BYE) to indicate that the streams were torn down.

## Timeout for RTP streams

This setting is used by the unit to detect a closed media session, even when no signaling for this was made. If no RTP packets are received during the configured amount of seconds, the unit creates a log message about this. If **Tear down media streams at timeout** was selected, the unit will also tear down the session when the RTP and RTCP timeouts have been reached.

## Timeout for RTCP streams

This setting is used by the unit to detect a closed media session, even when no signaling for this was made. If no RTCP packets are received during the configured amount of seconds, the unit creates a log message about this. If **Tear down media streams at timeout** was selected, the unit will also tear down the session when the RTP and RTCP timeouts have been reached.

### 9.5.4. Always Relay Media

#### **Always Relay Media** [\(Help\)](#)

Always relay media:  Yes  No

Here you can select to always relay media through the unit. The default setting is "No".

### 9.5.5. Reuse Port Numbers When Changing Media

### Reuse Port Numbers When Changing Media [\(Help\)](#)

Reuse port numbers when changing media (e.g. T.38 FAX):

- Don't reuse port numbers
- Reuse port numbers

You can select to reuse the media port numbers after changes in media type and number of ports. This is needed for T.38 FAX with some service providers.

### 9.5.6. Reuse Port Numbers Within Same Session

#### Reuse Port Numbers Within Same Session [\(Help\)](#)

Reuse port numbers within same session:

- Don't reuse port numbers
- Reuse port numbers
- Reuse port numbers even when IP has changed

You can select to always reuse the media port numbers within the same session.

The option to **Reuse the port even when IP has changed** should only be used together with the B2BUA or the SIP Trunk page and it only works for addresses that belong to the same network.

### 9.5.7. Detect codec changes

#### Detect codec changes [\(Help\)](#)

Detect codec changes in mid call answers in the B2BUA:

- Detect only changes to the first payload type listed
- Detect changes to all payload types (except dynamic)
- Do not detect changes to payload types in mid call answers

Enabling this setting will make the b2bua detect payload type changes in the SDP of answers to re-invite initiated by the unit and send a re-invite to the other end if something changed.

### 9.5.8. Third Party Call Control Codecs

#### Third Party Call Control Codecs [\(Help\)](#)

No.	Name	Payload Type	Rate	Channels	Parameters	Delete Row
1	PCMU					<input type="checkbox"/>
2	G729				annexb=yes	<input type="checkbox"/>
3	telephone-event	96	8000		0-15	<input type="checkbox"/>

Add new rows  rows.

These codecs are used when forwarding an initial INVITE without SDP, which are common in third party call control (3pcc) scenarios.

Some codecs have static payload types. They are defined in <http://www.iana.org/assignments/rtp-parameters>. Other codecs have dynamic payload types, which are negotiated with the peer. Both types of codecs are allowed in this table.

Enter the clock rate (Hz) in the Rate column, often 8000 Hz. Both Payload Type and Rate columns need to be specified for all codecs with dynamic payload types. The Channels and Parameters (fmt) columns are optional for all codecs.

The factory configuration contains three codecs: PCMU, G729 and telephone-event. PCMU and G729 with static payload types (0 and 18), and telephone-event with dynamic payload type 96.

### 9.5.9. Limitation of RTP Codecs

You might want to limit the use of some media codecs. There can be several reasons for this: some endpoints do not support the codecs, too many codec offers make the SIP request packet too large (which causes it to be fragmented), they consume too much bandwidth, or you want to allow only codecs with good enough voice quality.

**Limitation of RTP Codecs** [\(Help\)](#)

Allow all codecs  
 Limit codecs as configured

Codecs					
Edit Row	Type	Name	Allowed	Add	Delete Row
<input type="checkbox"/>	audio	g723	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-16	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-24	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-32	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	g726-40	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	g729	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	g729a	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	gsm	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	ilbc	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	pcma	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	pcmu	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	speex	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	audio	*	No	No	<input type="checkbox"/>
<input type="checkbox"/>	video	*	No	No	<input type="checkbox"/>

rows.

Select if all codecs should be allowed, or just the codecs that are listed as allowed in the **Codecs** table.

Codec matching is performed by its type, and not by its IANA assigned number. Matching PCMA will remove all codecs with the name PCMA, both type 8, and any other types which share the name PCMA.

## Codecs

If you selected to only allow some codecs, enter the allowed codecs in the table.

Codecs that are not allowed can also be listed here, as long as you select "Off" under This Codec Is Allowed.

## Type

Select the codec type. The "-" option will make this row match all media types where the codec name is defined.

## Name

Enter the name of the codec to be allowed. The codec name should be entered as it appears in the SDP (like PCMA or G723).

## Allowed

Select **On** to allow the codec and **Off** to block it.

## Add

You can also choose to add codecs to the SDP before forwarding it. This can be useful if you have a RTP Media Transcoder device which can transcode it to another codec supported by the endpoint.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 9.5.10. Allowed Media Ports

Here you specify which media ports are allowed in the SDP. Port 0 is always allowed. The port is always allowed if the address is 0.0.0.0 or :: or if the address belongs to this unit.

By default ports from 1024 are allowed for both UDP and TCP.

### NOTE

This check is only performed when the unit process the SDP, e.g. when media is relayed by the unit.

**Allowed Media Ports** [\(Help\)](#)

Transport	Ports		Delete Row
	Lower	Upper	
UDP ▾	1024	65535	<input type="checkbox"/>
TCP ▾	1024	65535	<input type="checkbox"/>

Add new rows  rows.

### Transport

The media transport protocol (UDP/TCP).

### Ports Lower

The start of the allowed port range for the given transport.

### Ports Upper

The end of the allowed port range for the given transport.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 9.5.11. Strip SDP Lines

Here you specify which lines to remove from the SDP by the unit.

**Strip SDP Lines** [\(Help\)](#)

Reg Expr	Case	Delete Row
b=.*	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add new rows  rows.

### Reg Expr

A regular expression to use when matching lines in the SDP (e.g. *b=.\**).

### Case

The **Case** setting governs whether or not to perform case-sensitive matching.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 9.5.12. Local Ringback

When a call is transferred by the unit, the calling person normally does not hear any new ring tone. For various purposes, you might want the unit itself to play a ring tone for call transfers.

**Local Ringback** [\(Help\)](#)

<b>Local Ringback Played at Call Transfer</b>	<b>Ring Tone for Local Ringback</b>
<input type="radio"/> Never play local ringback	<input checked="" type="radio"/> US ring tone
<input checked="" type="radio"/> Play local ringback when transferer hangs up	<input type="radio"/> UK ring tone
<input type="radio"/> Play local ringback when new target rings	
<input type="radio"/> Play local ringback when new target rings or makes progress	

### Local Ringback Played at Call Transfer

Select to never play local ringback, to play it when the new target phone rings, or to play it when the transferer hangs up, or to play it when the target rings or makes progress.

### Ring Tone for Local Ringback

Select the ring tone to be used when the unit plays ringback at call transfers.

## 9.5.13. Music on Hold Redirection

When a call is put on hold, the phone is sometimes not redirected to a Music on Hold server by the phone putting it on hold. When this happens, the unit can redirect the phone on hold to an external Music on Hold server instead.

**Music on Hold Redirection** [\(Help\)](#)

<input checked="" type="radio"/> Redirect calls on hold to Music on Hold server
<input type="radio"/> Leave calls on hold as they are

**Music on Hold Server**

SIP Address	Port	Transport
<input type="text" value="moh@10.47.10."/>	<input type="text" value="5090"/>	<input type="text" value="UDP"/> ▾

Select if the unit should redirect calls on Hold to a Music on Hold server, or if the calls should be left as they are.

## 9.5.14. Music on Hold Server

Enter the address and port of the Music on Hold server.

In the **SIP Address** field, enter the SIP domain/IP address of the Music on Hold server, and possibly also a username/extension for Music on Hold. This could look like moh@10.47.10.17.

You can also select to direct the request to a specific port, and select which transport should be used for the Music on Hold request. If no port is given, the unit will use the port from the DNS lookup (if a domain is given) or the standard SIP ports (5060 for UDP/TCP, 5061 for TLS).

## 9.5.15. Resolve domain names in the SDP

A session description can contain domain names in various attributes that need to be resolved for media to pass the firewall. If you want to support SDPs that contain domain names you need to enable this setting.

### Resolve domain names in the SDP [\(Help\)](#)

- Resolve domain names in the SDP
- Don't resolve domain names in the SDP

## 9.5.16. Requests

You can configure timeouts for the different functions of the unit's SIP module here. It is not recommended to change from the default values unless you really know what you're doing.

### Requests [\(Help\)](#)

Default timeout for INVITE requests:	Base retransmission timeout for SIP requests:
<input type="text" value="180"/> seconds	<input type="text" value="0.5"/> seconds
Maximum timeout for INVITE requests:	Maximum amount of retransmissions for INVITE requests:
<input type="text" value="300"/> seconds	<input type="text" value="6"/>
SIP blacklist interval:	Maximum amount of retransmissions for non-INVITE requests:
<input type="text" value="41"/> seconds	<input type="text" value="10"/>
B2BUA request pending timeout:	Limit Max-Forwards:
<input type="text" value="0"/> seconds	<input type="text" value="70"/>
	Maximum SIP packet size:
	<input type="text" value="131072"/> bytes

### Default timeout for INVITE requests

When sending an INVITE request you can specify a timeout, telling how long you can wait before getting an answer.

If no timeout is given when an INVITE request is sent, the unit sends the default timeout entered here.

## Maximum timeout for INVITE requests

Here, enter the maximum timeout to allow for an INVITE request. If a higher timeout is given, the unit changes it to the value entered here.

## SIP blacklist interval

The **SIP blacklist interval** setting is used by the unit when it keeps track of bad SIP servers (servers not responding to SIP signaling). The blacklist interval is the time during which no new SIP packets are sent to the server because it didn't respond to previous SIP signaling. The blacklisting means that no new SIP requests will be sent to the unit, even if requests that should be routed to this unit is received by the unit. After that time, the unit will try the server again, in case it didn't respond due to some temporary problem. This time is also the interval between successive monitoring attempts.

If the SIP request which caused the blacklisting, or a subsequent SIP request for that unit, can be routed to another device instead, the unit will keep on sending those requests to the next known IP address for the domain/user in question. When the blacklist ends, the unit will go back to sending requests to the previously blacklisted unit again. If the interval is set to zero (0) neither blacklisting nor monitoring will be done.

The SIP Servers To Monitor are set on the **SIP Services > Basic** page.

## Base retransmission timeout for SIP requests

When the unit sends out a SIP request, it will expect a reply within a certain time. If no reply has been received within the **Base retransmission timeout**, the unit will start resending the request.

## B2BUA request pending timeout

The B2BUA request pending timeout setting configures the time to wait before responding 491 if an outgoing Re-INVITE has been sent on the other call leg. Allowing the pending request to complete. If the value is zero (0) the 491 response is sent immediately.

## Maximum number of retransmissions for INVITE requests

When the unit sends out an INVITE request, it will wait for a reply until the **Base retransmission timeout** and then start to retransmit the request. The time intervals between retransmissions will double for each new retransmission.

Example: If the **Base retransmission timeout** is 0.5 seconds and the **Maximum number of retransmissions** is 6, the INVITE requests will be sent with intervals of 0.5 s, 1 s, 2 s, 4 s, 8 s, and 16 s.

## Maximum number of retransmissions for non-INVITE requests

When the unit sends out a request which is not an INVITE request, it will wait for a reply until the **Base retransmission timeout** and then start to retransmit the request. The time intervals between retransmissions will double for each new retransmission until the interval reaches 4 seconds. After that, retransmissions will be made with a 4-second interval.

Example: If the **Base retransmission timeout** is 0.5 seconds and the **Maximum number of retransmissions** is 7, the requests will be sent with intervals of 0.5 s, 1 s, 2 s, 4 s, 4 s, 4 s, and 4 s.

### **Limit Max-Forwards**

The **Limit Max-Forwards** setting configures the limit of the Max-Forwards header value in a SIP Request. If a message that is being forwarded has a value larger than this limit it will be reset to the configured value.

### **Maximum SIP packet size**

This setting allows you to set a limit to the size of SIP packets. A high value will increase performance, but use more memory. A low value will decrease performance, but use less memory.

## **9.5.17. Save**

Saves the Sessions and Media configuration to the preliminary configuration.

## **9.5.18. Undo**

Reverts all of the above fields to their previous configuration.

# **9.6. Remote SIP Connectivity**

If you are at a hotel or somewhere else where you find yourself behind a NAT-ing device that does not understand SIP, you will have use of the SIP Remote Connectivity. This will help your client to traverse the NAT, even if the device doing the NAT does not understand SIP.

If you have a STUN-capable SIP client, you need just turn on the STUN server of the unit to make the client work behind NAT. If you have a SIP client that does not do STUN (or if the STUN-capable client is located behind a Symmetric NAT device), you have to use the Remote NAT Traversal feature. This is easier for the client, but generates more network traffic for the unit.

### **9.6.1. STUN Server**

Use the STUN server if you have STUN-aware SIP clients. You will need at least two public IP addresses to make it work with all client implementations of STUN.

STUN will not work properly if the NAT device uses Symmetric NAT (where the client's private IP/port pair translates to different public IP/port pairs depending on destination, and where computers other than the destination host are not allowed to reply on that IP/port pair).

The client also needs extra configuring for this; it must know which IP addresses and ports the STUN server has.

Basic	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
-------	----------------------	------------------	------------------	--------------------	-------------------------	---------------	----------------------

---

**STUN Server** [\(Help\)](#)

Enable STUN server  
 Disable STUN server

STUN server IP addresses:      STUN server ports:

## 9.6.2. STUN server

Select if the STUN server should be switched **On** or **Off**.

### STUN server IP addresses

When activated, the STUN server requires two IP addresses, and a pair of ports on these two IP addresses, on the unit. STUN clients will then send test packets to these ports.

Select two IP addresses out of the ones assigned to the unit under **Directly Connected Networks** and **Alias** on the interface pages.

Note: for the STUN server to work properly, you need to select IP addresses which the clients can reach. In normal circumstances, this means that only public IP addresses can be used.

### STUN server ports

Enter the ports to use for the STUN server. These ports, on the IP addresses selected, will not be available for anything else.

## 9.6.3. Remote NAT Traversal

If your SIP client is not STUN-capable, you can use the built-in Remote NAT traversal feature of the unit. The client must register on the unit (or through it).

The SIP client needs to re-REGISTER, or respond to OPTIONS packets, rather often for this to work. The exact period for this depends on the NAT-ing device, but 20 seconds should be enough to get across most NAT boxes.

**Remote NAT Traversal** [\(Help\)](#)

Enable Remote NAT Traversal  
 Disable Remote NAT Traversal

IP address for remote clients: 
                                         
 Forward signaling from IP address:

IP port for remote clients:

NAT keepalive method:
 

- Use OPTIONS
- Use short registration times
- Use both OPTIONS and short registration times
- Use neither OPTIONS or short registration times

Media Route:
 

- Route media directly between clients behind the same NAT
- Always route media through the firewall

NAT timeout for UDP:  seconds

NAT timeout for TCP:  seconds

**Remote NAT traversal**

Switch this function on or off.

**Remote Clients Signaling Forwarding**

Many SIP servers need to separate signaling to and from remote clients from signaling to and from the SIP Trunk. For this purpose, you can specify which IP address and port the remote clients will connect to. This can't be the same IP address and port as what the SIP provider uses!

You also specify which IP address the unit will use when it forwards this SIP signaling to the server on the LAN. In this way, the trunk signaling and remote client signaling will be separated for the PBX.

**IP Address for Remote Clients**

Select which IP address remote clients connect to. This can be the same IP address as is used by the SIP provider, but then you need to select a different signaling port below.

**IP Port for Remote Clients**

Enter the signaling port to which remote SIP clients should connect. The unit will listen for SIP signaling on this port only for the IP address selected above.

If you select an alias IP address as the address to where remote clients should connect, you can't enter a port, but must use port 5060 (5061 for TLS connections). If you select an IP address that was entered in the **Directly Connected Networks** table, you must specify a port.

You cannot select a port that is already in use for something else, or specified in the **SIP Signaling Ports** table.

### **Forward Signaling from IP Address**

Select which IP address the unit should use as the sender IP address when forwarding signaling from remote clients.

As all other SIP signaling will be forwarded using the IP address entered in the **Directly Connected Networks**, you must select an **Alias** IP address here.

### **NAT keepalive method**

Clients using this function will have to send SIP packets very often, to keep the IP/port NAT binding. Select which method to use to force the clients to send packets frequently.

**OPTIONS** are sent from the unit to the client, and the client is required to respond to these **OPTIONS** packets to keep the NAT binding.

With **short registration times**, the unit tells the client to register with shorter intervals than it normally should have used, to keep the NAT binding. This will load the SIP registrar as well (if the unit is not the registrar), but is a method supported by all SIP clients.

If you use **Neither OPTIONS or short registration times** it's up to the clients behind the NAT box to keep the NAT hole open. One technique which is supported by the unit is CRLF Keep-Alive. This technique is described in RFC 5626.

### **NAT timeout for UDP**

Enter the timeout the NAT box uses for UDP connections. The unit uses this information when deciding the intervals with which to send **OPTIONS** or tell the client to re-register.

### **NAT timeout for TCP**

Enter the timeout the NAT box uses for TCP connections. The unit uses this information when deciding the intervals with which to send **OPTIONS** or tell the client to re-register.

### **Media Route**

Usually, media is always sent via the unit when the Remote NAT Traversal feature is used. For clients behind the same NAT, media can be made to go directly between the clients, to lower the unit and network load.

## **9.6.4. Unconditional NAT Traversal**

In the standard Remote NAT Traversal, the unit looks into the SIP signaling to discover that a SIP device is NATed. With some NAT boxes, the SIP signaling will be partly changed to make it

impossible to detect the NATing, but still impossible to get media through to the device.

For this, you can use the Unconditional NAT Traversal feature, which will perform NAT traversal for all requests on the given interface regardless of what the signaling looks like.

**Unconditional NAT Traversal** [\(Help\)](#)

Always use Remote NAT Traversal  
 Only use Remote NAT Traversal when client looks NATed

**Unconditional NAT Interfaces**

Edit Row	Interface/VLAN	Delete Row
<input type="checkbox"/>	External (eth1 untagged)	<input type="checkbox"/>

Add new rows  rows.

**Unconditional NAT Exceptions**

Edit Row	Exclude Network	Delete Row
<input type="checkbox"/>	SIP Operator	<input type="checkbox"/>

Add new rows  rows.

### Always use NAT traversal

Select if Remote NAT Traversal should always be performed on the selected interfaces.

### Unconditional NAT Interfaces

Select for which interfaces NAT traversal should always be used.

#### Interface/VLAN

SIP traffic coming in to this interface/VLAN will always be regarded as if the sending SIP device is located behind a SIP-unaware NAT box.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### Unconditional NAT Exceptions

If there are SIP devices on the selected interface that are known not to be located behind NAT boxes (like your ITSP or other Ingate units), you should list them here. Select from the networks you defined on the **Networks and Computers** page under **Network**.

You only need to list IP addresses on the selected interface.

## Exclude Network

Traffic from the IP address(es) listed here will not be handled as NATed SIP devices.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 9.6.5. Save

Saves the Remote SIP Connectivity configuration to the preliminary configuration.

## 9.6.6. Undo

Reverts all of the above fields to their previous configuration.

# 9.7. VoIP Survival

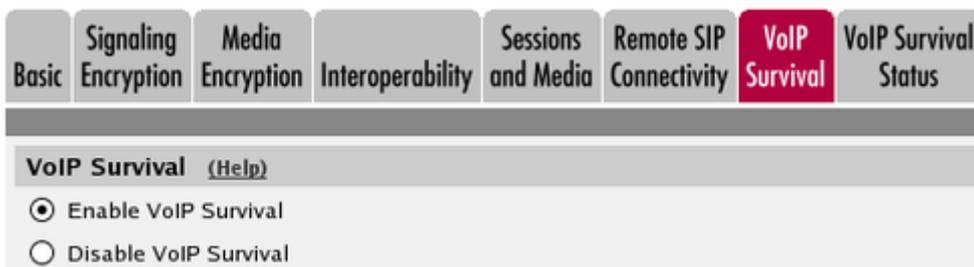
The unit can be made to monitor SIP domains to ensure that the servers managing the domains really are reachable. If a SIP domain server is unreachable, the unit will enter Survival mode, when it acts as a local registrar for the domain. This could be useful when you have a local office with a unit and all users register on a server at the main office.

When in Survival mode, the unit acts as a SIP registrar for the domain. It can also redirect SIP calls to a PSTN gateway, if the callee looks like a phone number (that is, if the URI user part contains nothing but digits, +, -, # and \*).

## 9.7.1. VoIP Survival

Here, the VoIP Survival module is switched on and off.

Note that the unit SIP module must be turned on for VoIP Survival to work.



## 9.7.2. Server Check Interval

Enter here the interval for the unit to check on the SIP servers managing the SIP domains. The interval must be shorter than the **SIP blacklist interval** on the **Sessions and Media** page.

**Server Check Interval**

seconds

### 9.7.3. Domains To Monitor

Here, you enter the SIP domains which the unit should monitor.

The unit must be able to query the monitored domains in DNS or find them in the **DNS Override For SIP Requests** table.

**Domains To Monitor**

Edit Row	Domain Name	Method	Delete Row
<input type="checkbox"/>	uk.ingate.com	Generic	<input type="checkbox"/>

Add new rows  rows.

#### Domain Name

Enter the SIP domain name which the unit should monitor. The domain name must not be a locally handled domain for this unit.

#### Method

Select which method the unit should use to obtain subscriber data for the users registering on the domain via the unit. The unit includes a request for the data in the REGISTER request to the server, and gets the information in the response.

### 9.7.4. Registrations

Here, you make settings for the registrations handled by the unit in survival mode.

**Registrations**

Re-REGISTER interval during survival mode: Time to store subscriber data:

seconds  days

#### Re-REGISTER interval during survival mode

When the unit works in survival mode, the clients should register more often than when the main server is accessible. This is to make the clients register on the main server very soon after it has become reachable again.

Here, you set the registration interval for the survival mode.

#### Time to store subscriber data

The unit stores the data sent from the main SIP server to be able to act as backup domain server. Enter the time interval after which the data will be discarded.

## 9.7.5. PSTN Settings

Here, settings are made which the unit uses for sending calls to a local PSTN gateway.

First, the Request-URI is compared to the contents of the **Survival Subscribers** list. If the Request-URI is found there, the request will be sent directly to the user, even if the URI looks like a phone number.

If a PSTN gateway is entered in the table below, other SIP requests are sent there if the Request-URI looks like a phone number (that is, if the URI user part contains nothing but digits, +, -, # and \*).

PSTN Gateways <a href="#">(Help)</a>		
Edit row	Domain/IP address	Delete row
<input type="checkbox"/>	10.47.3.162	<input type="checkbox"/>

Add new rows  rows.

PSTN Numbers <a href="#">(Help)</a>	
Local area code:	<input type="text" value="013"/>
Maximum length of local phone numbers (not including area code):	<input type="text" value="7"/> digits

## 9.7.6. PSTN Gateways

Enter a domain name or IP address for the PSTN gateway to use when the unit encounters a phone number in a SIP request. Note that the PSTN gateway should preferably not be located where the SIP server is that usually manages the SIP domain.

## 9.7.7. PSTN Numbers

Here, you enter some information about the local PSTN numbers. This information is used by the unit when calls are redirected to the PSTN gateway.

### Local area code

Enter the local area code for where the PSTN gateway is located.

### Maximum length of local phone numbers

Enter the maximum length of local phone numbers, area code not included.

If the phone number in the request is not longer than the Maximum length of local phone numbers, the area code is added to the Request-URI before it is compared to the survival database and before it is sent on to the PSTN gateway.

## 9.7.8. Save

Saves the VoIP Survival configuration to the preliminary configuration.

## 9.7.9. Undo

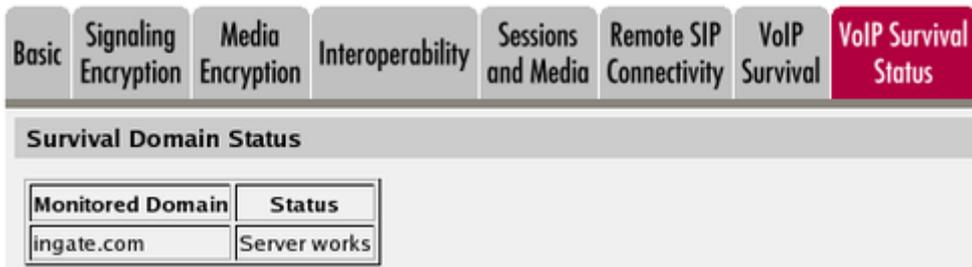
Reverts all of the above fields to their previous configuration.

## 9.8. VoIP Survival Status

Here, status is shown for the monitored domains and for users under those domains.

### 9.8.1. Survival Domain Status

Here, status is shown for all domains monitored using VoIP Survival.



Monitored Domain	Status
ingate.com	Server works

#### Monitored Domain

The name of the domain being monitored by the unit.

#### Status

The status for the domain. **Server works** means that the unit can contact the SIP server for this domain. **Survival - local server** means that the unit can't contact the SIP server and hence has taken over the domain locally.

### 9.8.2. Survival Subscribers

Here, users are shown that register on a monitored domain via the unit, and if the server sends extra information about the users.



User	Survival aliases
lisa@ingate.com	1375
henry@ingate.com	1728
jane@ingate.com	1199
mike@ingate.com	1349

#### User

This is the username of a registered user in a monitored domain. All users in monitored domains who register via the unit should appear in this table if the server sends information about them.

#### Survival aliases

Here, aliases for the user are shown. These aliases are communicated from the server using the method selected on the **VoIP Survival** page.

# Chapter 10. SIP Traffic

SIP (Session Initiation Protocol) is a protocol for creating and terminating various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP takes care of the initiation, modification and termination of a session with one or more participants. The protocol makes it possible for the participants to agree on what media types they should share. You can find more information about SIP in [More About SIP](#), and in RFC 3261.

Find examples on how to configure your unit for SIP in [Part IV. How To Guides](#).

The SIP module in the unit handles SIP requests for users who have registered on the unit itself or a machine connected to the unit (see also [Local Registrar](#)). The module forwards the request through the unit, which enables users behind different network interfaces to make contact. The SIP module controls the firewall rules to temporarily let through the media streams that the users agree on, on their assigned ports.

You must enter a DNS server and a Default gateway on the Basic Configuration page to make the SIP module work satisfactorily.

There are two SIP license types in the unit - SIP User Registration licenses and SIP Session licenses.

SIP User Registration licenses are used when the unit is the registrar for a domain. Each user registered on the unit consumes a license. When the user unregisters, the license is released.

SIP Session licenses are used when SIP media is forwarded by the unit. For each such call, one license is consumed. When the call is ended, the license is released.

These SIP functions are configured in the SIP Traffic section:

- Allowed SIP methods
- Filtering of SIP signaling
- Local SIP domains
- SIP users
- SIP user authentication
- RADIUS accounting for SIP
- Routing of outgoing SIP requests
- Routing of incoming SIP requests
- SIP IDS/IPS

## 10.1. SIP Methods

### 10.1.1. SIP Methods

Enter the SIP methods you want to allow and/or authenticate. Methods that are not listed here will be blocked by the unit.

Common methods are predefined (from RFC 3261). Note that the standard methods **ACK** and **CANCEL** cannot be authenticated.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	No	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

#### Method

Enter the name of the SIP method. This should be the name used in RFC 3261.

#### Traffic To

Here, you select the direction of the traffic. **Local domains** means that traffic to **Local SIP Domains** of this unit is affected by this row. **Other domains** means that traffic to all domains which are not **Local SIP Domains** of this unit is affected by this row. **Both** means that this row affects all traffic for the method, regardless of where the traffic is bound.

#### Allow

Select if the method in this direction should be allowed or not. For methods that are not allowed, the unit sends a 403 (Forbidden) response.

## Auth

Select if the method in this direction should be authenticated or not. Note that SIP authentication must be turned on (on the **Authentication and Accounting** page), or authentication will not be performed.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.1.2. Save

Saves the SIP Methods configuration to the preliminary configuration.

### 10.1.3. Undo

Clears and resets all fields in new rows and reset changes in old rows.

## 10.2. Filtering

Under Filtering, you can filter out SIP requests based on various criteria. Filter based on sender IP address (Sender IP Filter Rules), sending and receiving SIP user (Header Filter Rules), or content type (Content Types).

### 10.2.1. Sender IP Filter Rules

Here, you set all the rules for SIP requests from different networks. Requests that do not match any rule are handled according to the **Default Policy For SIP Requests**.

## No.

The **No.** field determines the order of the rules. Rules are used in the order in which they are displayed in the table; rule number 1 is first. The order is important if you used networks which partly contain the same IP addresses. To change order for a rule, enter the new number in the field

and press **Save**.

### From Network

The network name that the SIP request originates from. You can select between the networks defined on the **Networks and Computers** page under **Network**.

### Action

Under **Action**, you select what to do with a SIP request from the selected network. The choices are **Process all**, which handles all requests regardless of destination, **Local only**, which only handles requests to **Local SIP Domains** (entered on the **Local Registrar** page), and **Reject all**, which doesn't handle any requests at all.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### Default Policy For SIP Requests

Select what to do with SIP requests that do not match any of the **Proxy Rules**. The choices are **Process all**, which handles all requests regardless of destination, **Local only**, which only handles requests to **Local SIP Domains** (entered on the Local Registrar page), and **Reject all**, which doesn't handle any requests at all.

## 10.2.2. Preloaded Route Rules

A preloaded route is a set of route headers in an initial request. Usually you want to control how requests are routed and not allow a predefined path in the incoming request.

By default the unit rejects preloaded routes that do not point to itself. However, certain scenarios require a preloaded route set.

Here, you set all the rules for SIP requests from different networks. Requests that do not match any rule are handled according to the **Default Policy For Preloaded Routes**.

### Preloaded Route Rules [\(Help\)](#)

No.	From Network	Action	Delete Row
1	LAN ▼	Allow ▼	<input type="checkbox"/>

rows.

### Default Policy For Preloaded Routes

- Reject
- Authenticate
- Remove
- Allow

## No.

The **No.** field determines the order of the rules. Rules are used in the order in which they are displayed in the table; rule number 1 is first. The order is important if you used networks which partly contain the same IP addresses. To change order for a rule, enter the new number in the field and press **Save**.

## From Network

The network name that the SIP request originates from. You can select between the networks defined on the **Networks and Computers** page under **Network**.

## Action

Under **Action**, you select what to do with a SIP request from the selected network. The following actions are defined:

Action	Description
Reject	Respond with 403 Forbidden
Authenticate	Respond with 407 Proxy Authentication Required
Remove	Remove the preloaded routes from the request
Allow	Allow requests with preloaded routes

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.2.3. Allowed Origins for SIP over WebSocket

The Origin header can be used to mitigate against Cross-Site Request Forgery (CSRF) vulnerabilities.

Here you can specify the scheme://host[:port] that are allowed in the WebSocket handshake's Origin header. If the table is empty all origins are allowed.

For example, if your JavaScript SIP client is hosted at www.example.com you can enter that into the Host field.

If the handshake's Origin header contain an origin that is not included in this table the unit will respond with 400 Bad Request and log "Origin mismatch".

**Allowed Origins for SIP over WebSocket** [\(Help\)](#)

Scheme	Host	Port	Delete Row
https ▾	www.example.com		<input type="checkbox"/>

rows.

**Scheme**

The origin scheme - http or https.

**Host**

The origin host.

**Port**

An optional port for the origin.

**Delete**

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

**Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

**10.2.4. Block SIP Traffic to NATed Networks**

SIP devices on a NATed network are usually hidden by the unit when sending out SIP traffic; the SIP devices on the outside will just see the IP address of the unit.

By various means, someone on the outside may still have guessed the IP addresses on the NATed network, and might try to send SIP traffic directly to these IP addresses instead of addressing the unit - but sending it to the unit which is the known gateway.

You might want to block this type of SIP traffic addressed directly to a NATed network, as it is probably only malicious traffic.

**Block SIP Traffic to NATed Networks** [\(Help\)](#)

Allow SIP traffic directly to NATed networks

Block SIP traffic directly to NATed Networks

Select if the unit should allow or block traffic directly addressed to a NATed network.

**10.2.5. Policy for Signaling and Media on different Networks**

It is recommended to reject SIP Signaling, from one network, that contains media (SDP) that belongs to another network. Otherwise a malicious user could try to spoof media addresses.

This setting doesn't affect Remote SIP Connectivity as it doesn't use the media addresses from the SDP.

If the unit is set to DMZ this setting can be set to reject and additional negotiators can be configured on **Network** → **Topology** → **Surroundings**.

### Policy for Signaling and Media on different Networks [\(Help\)](#)

- Allow Signaling and Media on different Networks
- Reject Signaling and Media on different Networks

## 10.2.6. Content Type Filter Rules

The SIP packets present information in different ways, using content types (MIME types). Enter here which types the SIP proxy should accept. The most common MIME types are predefined and you only have to activate them.

The content types *application/sdp* (used for SIP requests), *application/xpidf+xml* (used for Presence) and *text/x-msmsgsinvite* (used by Messenger) are always accepted - you don't have to enter them into the table. You can find a complete list of MIME types at <https://www.iana.org/assignments/media-types/>.

#### Content Type Filter Rules [\(Help\)](#)

Edit Row	Content Type	Allowed	Delete Row
<input type="checkbox"/>	image/jpg	Yes	<input type="checkbox"/>
<input type="checkbox"/>	message/sipfrag	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/lpidf	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Yes	<input type="checkbox"/>

Add new rows  rows.

### Content Type

Enter the content type (only one in each row). The format is *category/type*, e.g. **text/plain**. You can also allow all content types by entering *\*/\** in a row and allow it.

### Allowed

Select if the unit should allow (**On**) or reject (**Off**) this content type in SIP signaling.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.2.7. Header Filter Rules

Header Filter Rules lets you filter out SIP requests based on the contents of the To and From headers. This could be useful if you want to prevent groups of users to make calls through the unit.

Wild cards can be used: \* for any number (zero or more) characters, ? for exactly one character.

Requests that do not match any rule are handled according to the **Default header filter policy** set beside the table.

<b>To/From Header Filter Rules</b> <a href="#">(Help)</a>				
No.	From Header	To Header	Action	Delete Row
<b>Default Header Filter Policy</b>				
<input checked="" type="radio"/> Process				
<input type="radio"/> Reject				
Add new rows <input type="text" value="1"/> rows.				

**No.**

The No. field determines the order of the rules. Rules are used in the order in which they are displayed in the table; rule number 1 is first. To change order for a rule, enter the new number in the field and press **Save**.

**From Header**

Enter an expression which the From header should match. If this rule should match all From headers, enter \*.

**To Header**

Enter an expression which the To header should match. If this rule should match all To headers, enter \*.

**Action**

Select if this rule should make the unit **Process** or **Reject** the matching requests. Rejected requests get a code 403 packet in reply.

**Delete**

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

**Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

**Default Header Filter Policy**

Select what to do with SIP requests that do not match any of the **Header Filter Rules**. The choices are **Process** and **Reject**. Rejected requests get a code 403 packet in reply.

## 10.2.8. Save

Saves the Filtering configuration to the preliminary configuration.

## 10.2.9. Undo

Reverts all of the above fields to their previous configuration.

# 10.3. Local Registrar

The SIP registrar keeps track of where a user is right now. The registrar receives registrations from the SIP user clients and discards them when they become obsolete. A user can register from several computers.

Here, you enter the SIP domains the unit should manage and set up the SIP user database. If authentication should be used, you also need to do some settings on the **Authentication and Accounting** page, and select which SIP methods should be authenticated on the **SIP Methods** page.

If you want to use a RADIUS server for SIP users instead of a local database, you select that on the **Authentication and Accounting** page.

### 10.3.1. Local SIP Domains

Here, you enter the domains that the SIP registrar should handle. Only users in these domains can register on the unit.

Note that you should only list domains for which the users are expected to register on the unit itself. SIP requests for other domains will be forwarded by the unit to the server managing the domain in question.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status
Local SIP Domains <a href="#">(Help)</a>									
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	10.47.2.243	<input type="checkbox"/>							
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>							
Add new rows		<input type="text" value="1"/>	rows.						

#### Domain

Enter the name of the domain, such as **ingate.com**. Sometimes you have to use an IP address (of the unit) as the domain as well, when the SIP client substitutes the domain for the IP address noted in DNS.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.3.2. Registrar Limits



The image shows a configuration form titled "Registrar Limits". It contains three input fields: "Timeout for registrations:" with a value of "3600" and the unit "seconds"; "Allowed number of users:" with an empty field and "(max 50)" in parentheses; and "Allowed number of registrations per user:" with a value of "5".

#### Timeout for registrations

Enter the timeout (in seconds) before a registration becomes obsolete. When the timeout is reached, the registrar discards the registration. This setting affects REGISTER messages both (proxied) through and to the unit.

#### Allowed amount of users

Enter the maximum amount of users allowed to register in the SIP registrar.

Leave the field empty to allow as many registrations as there are SIP Registrar User licenses on the unit (amount displayed inside parentheses). You can purchase additional SIP Registrar Users from your retailer.

#### Allowed amount of registrations per user

Enter the allowed amount of concurrent registrations for a user. A registration looks like user@computer, which means that if you re-register from the same computer, this won't count as another registration, but just an update to the existing one.

### 10.3.3. Local SIP User Database

You can restrict which users are allowed to use SIP. Here, you enter the users allowed, select a network from where the SIP traffic is allowed and give the password they should use for authentication.

If the authentication is **Off**, this list should consist of the users allowed to register on the unit. SIP authentication is turned on and off on the **Authentication and Accounting** page.

If you want to use a RADIUS server for SIP users instead of a local database, you select that on the **Authentication and Accounting** page.

Local SIP User Database (Help)						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	ingate.com	markj384		All	<input type="checkbox"/>
<input type="checkbox"/>	support	ingate.com			Office network	<input type="checkbox"/>
<input type="checkbox"/>	test	ingate.com			All	<input type="checkbox"/>

Add new rows  rows.

## Username

Enter the name of a user allowed to use SIP. Note that only the user name should be entered. Enter "\*" to state that all SIP users in this domain should have the same limitations. The user name is used when contacting the user.

If **SIP authentication** is On, every user must be entered on a separate line.

## Domain

Enter the domain that the user belongs to. An example of a domain is **ingate.com**. Enter "\*" to allow all SIP domains.

## Authentication Name

If the user should use a different name than its user name for authentication purposes, please enter the authentication name here. It is only used for authentication.

## Password

If authentication is required for some methods, press the button to enter the password.

## Register From

Here, you can restrict from where this user's SIP traffic can come when he registers. Select a computer/group of computers. The available alternatives are the networks you defined on the **Networks and Computers** page under **Network**.

This restriction is only for the REGISTER method. Other SIP methods are not checked for originator according to this setting.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.3.4. Save

Saves the Local Registrar configuration to the preliminary configuration

### 10.3.5. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 10.4. Authentication and Accounting

You can require authentication from SIP users when they perform various SIP functions (register a user, start a call, hang up a call, send a message etc). Here you configure if the unit should require authentication, and which database should be used to authenticate the user.

To require authentication for registration is a good way of ensuring that no one claims to be another user. However, you should not always use authentication; if you do, people from outside can't call you or send messages via SIP without knowing the password.

You also have the possibility to send Account ticks to a RADIUS server, to enable billing of SIP calls.

### 10.4.1. Authentication settings

SIP Methods	Filtering	Local Registrar	<b>Authentication and Accounting</b>	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status
-------------	-----------	-----------------	--------------------------------------	--------------	-----------	---------	------------	---------	----------------	----------	-----------------

#### Brute Force Authentication Protection [\(Help\)](#)

Maximum amount of attempts:

Time interval:  seconds

Stop responding after interval:  seconds

Max number of clients:

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication (enabled below).

#### SIP Authentication

Enable SIP authentication  
 Disable SIP authentication

#### SIP Realm

### 10.4.2. Brute Force Authentication Protection

Enter a **Time interval** (in seconds) in which consecutive unsuccessful authentication attempts are counted. The **Maximum amount of attempts** field specifies the amount of failed attempts that should be allowed within the Time interval. If the threshold value is reached, login to the account

will be disabled for the given Time interval. In order to disable this protection mechanism, leave the fields Time interval and Maximum amount of attempts empty. The **Stop responding after interval** field specifies the interval in seconds after the threshold is reached when no more response should be sent. If this field is empty a response will always be sent. In order to disable this protection mechanism, leave the fields empty.

The **Max number of clients** field specifies how many clients (IP addresses) to keep track of. When the limit is reached all authentication attempts will be blocked.

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication.

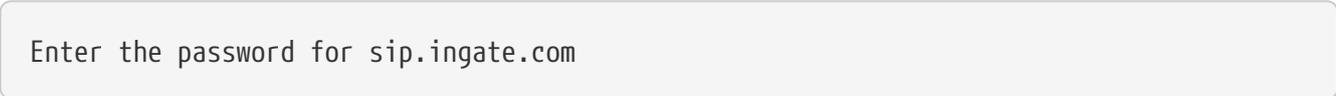
Pass-through authentication protection only works when requests are handled in a transaction stateful way. E.g. when the client and the server are on different directly connected networks.

### 10.4.3. SIP Authentication

Decide whether SIP authentication should be **On** or **Off**. If **Off**, the unit will not ask clients for authentication for any SIP method, regardless of what settings are made in the **SIP Methods** table.

### 10.4.4. SIP Realm

When authentication is required for a method, the SIP client will ask for a password. The **Realm** is what the client will present on your screen when asking for a password. If you, for example, use **sip.ingate.com** as your **Realm**, the client will ask for password with a text which looks like this:



Enter the password for sip.ingate.com

### 10.4.5. SIP User Database



### 10.4.6. Select SIP User Database

You can either enter SIP users on the **Local Registrar** page to allow them to use SIP, or use an external RADIUS database to which the unit connects to verify users. You can only use a RADIUS database if the SIP authentication is turned on.

Select if the unit should use a local SIP user database (entered on the **Local Registrar** page) or an external RADIUS database.

If a RADIUS database is used, at least one RADIUS server must be entered on the **RADIUS** page under **Basic Configuration**.

Note that when a RADIUS database is used, the RADIUS server has no means of distinguishing different SIP domains, but will authenticate only the username. As a consequence, you can't have

users on different domains with the same username.

### 10.4.7. RADIUS Database Settings

If RADIUS is used for SIP user authentication, all SIP users get the same privileges. Select the network from which they can register. Select from the networks defined on the **Networks and Computers** page under **Network**.

When RADIUS is used, you must also enter a RADIUS server on the **RADIUS** page under **Basic Configuration**.

More information about how to configure the RADIUS server to authenticate SIP users can be found in the [RADIUS](#) section.

### 10.4.8. P-Asserted-Identity

When the P-Asserted-Identity header is used, this header is added to all outgoing requests for which the unit has performed authentication. For incoming requests from untrusted domains, where this header is present, the header will be removed before the request is processed.

More information about the P-Asserted-Identity header can be found in RFC 3325.

**P-Asserted-Identity** [\(Help\)](#)

Enable P-Asserted-Identity  
 Disable P-Asserted-Identity

Trusted Domains				
Network	Transport	Certificates	Group	Delete Row
ITSP_NET	TLS	TestCA	Authenticated	<input type="checkbox"/>

Add new rows  rows.

**Use From address in P-Asserted-Identity without authentication**

Yes  
 No

#### Use P-Asserted-Identity

Select here if the unit should use the P-Asserted-Identity header or not. If it is not used, the **Trusted Domains** setting will have no effect.

#### Trusted Domains

You can also list the trusted domains for this function. Servers within the trusted domain can add a P-Asserted-Identity header, just as the unit itself can. When such a request is received by the unit, it will not perform authentication itself, but consider the user already authenticated.

#### Network

Select a network. All IP addresses in this domain will be regarded as trusted servers, which means that if any of them add a P-Asserted-Identity header, the unit will trust it. The available alternatives are the networks you defined on the **Networks and Computers** page under **Network**.

## Transport

Select a transport for the request from a trusted server.

## Certificates

If TLS is used and a certificate is found that signed the peers certificate or the peers certificate itself is found, the peer is trusted. You can add several trusted certificates for the same Network by adding multiple rows.

## Groups

Users in trusted domains can be assigned one of two predefined groups, Authenticated and Friendly. Authenticated users are allowed to make both incoming and outgoing calls, friendly Users are allowed to make incoming calls.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

Use From address in P-Asserted-Identity without authentication

Select if the SIP URI and any display name in the From header of incoming requests is to be added in a P-Asserted-Identity header without authenticating the request.

## 10.4.9. RADIUS Accounting

**RADIUS Accounting** [\(Help\)](#)  
 Enable RADIUS accounting  
 Disable RADIUS accounting  
Include media statistics:  Yes  No  
Include Remote-Party-Id:  Yes  No  
Include P-Asserted-Identity:  Yes  No  
Include Diversion:  Yes  No

RADIUS Accounting can be used to keep track of user calls. This enables billing users for SIP calls. It can also be used to get information about the quality of user calls, by gathering statistical information from the media streams involved.

When RADIUS Accounting is turned on, the unit sends account ticks to notify the configured RADIUS server about when calls start and stop. RADIUS Accounting is defined in RFC 2866.

When RADIUS Accounting is used, you must also enter a RADIUS server on the **RADIUS** page under **Basic Configuration**.

## 10.4.10. Save

Saves the Authentication and Accounting configuration to the preliminary configuration.

## 10.4.11. Undo

Reverts all of the above fields to their previous configuration.

# 10.5. SIP Accounts

The unit can register and autenticate to other SIP servers. Enter here the accounts to be used.

## 10.5.1. Registration Parameters

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	<b>SIP Accounts</b>	Dial Plan	Routing	SIP Status	SIP Test	SIP Test Status
<b>Registration Parameters</b> <a href="#">(Help)</a>									
Registration interval:		<input type="text" value="3600"/>		seconds					
Retry registration after:		<input type="text" value="300"/>		seconds					
Use exponential backoff timer on retry:		<input type="radio"/> Yes <input checked="" type="radio"/> No							

### Registration interval

When the unit registers to another SIP server, it will suggest how long the registration should last before a re-registration is necessary. The server can accept this or suggest a different interval.

Enter the registration interval to suggest here.

### Retry registration after

If the unit for some reason fails to register to the remote server, it will try again after the time interval entered here.

### Use exponential backoff timer on retry

When **Use exponential backoff timer on retry** is enabled the algorithms for retrying a failed REGISTER as specified in SIP Connect 1.1, section 15.4.1 are used. Exponential backoff timer and reconnecting with a new TCP connection in case the old was broken.

## 10.5.2. SIP Accounts

In this table, the accounts to be used for registration and authentication are entered. You can use more than one account for one server.

The accounts are used in the **Forward To** and **User Routing** tables.

SIP Accounts (Help)							
Username	Domain	Authentication Name	Display Name	P-Asserted-Identity	Password	Account Type	Delete Row
123456	operator.com		+123456		Change Password	XF/Register	<input type="checkbox"/>
123457	operator.com		+123457		Change Password	XF/Register	<input type="checkbox"/>
voicemail	sp.ingate.com	tr3849225			Change Password	Register	<input type="checkbox"/>
1034	test.ingate.com				Change Password	Domain	<input type="checkbox"/>

Add new rows  rows.

## Username

Enter the user name of a SIP account. Note that only the user name should be entered.

## Domain

Enter the domain that the account belongs to. An example of a domain is **ingate.com**. This is the domain to which the unit should register.

## Authentication Name

If the unit should use a different name than its user name for authentication purposes, please enter the authentication name here. It is only used for authentication.

## Display Name

If the unit should display a different name than the username (like a phone number or a complete name) to the callee, enter that name here.

## P-Asserted-Identity

This is a SIP URI sent in a P-Asserted-Identity header in requests forwarded to the SIP server associated with the domain. This setting is optional.

## Password

Press the button to enter the password.

## Account Type

Select an account type for this username. The options are:

**Register:** Register on behalf of a client. When this account type is selected, the unit registers the entered username at the SIP server managing that domain.

**XF:** Rewrite From header. With this Account type, the unit replaces the From header with the username and domain of this user. The request is then forwarded to the SIP server associated with the domain.

**XF/Register:** With this Account type, the unit replaces the From header as described above, then registers as described under Register above.

**Domain:** For incoming requests for this domain, the unit requires authentication before passing them on. The request is sent to the SIP server associated with the domain or specified as the

Forward to address in the **User Routing** table.

**B2BUAWM:** With this Account type, the unit replaces the From header as described under XF. It also changes the SDPs to the effect that media is always sent via the unit.

**B2BUAWM/Register:** With this Account type, the unit acts as described under B2BUAWM above. It also registers the user as described under Register above.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.5.3. Save

Saves the SIP Accounts configuration to the preliminary configuration

### 10.5.4. Undo

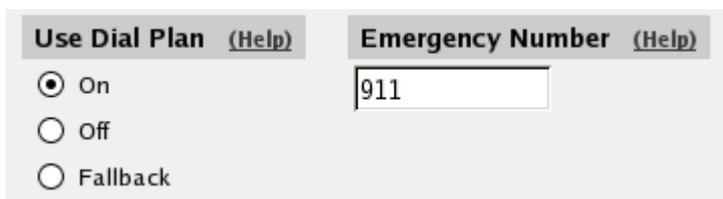
Clears and resets all fields in new rows and resets changes in old rows.

## 10.6. Dial Plan

The Dial Plan lets you route incoming SIP calls based on the incoming From header and Request-URI.

When neither the *Advanced SIP Routing* nor the *SIP Trunking module* has been installed, this page presents only limited functionality.

### 10.6.1. General



The screenshot shows two configuration sections. The first section, 'Use Dial Plan (Help)', contains three radio button options: 'On' (which is selected), 'Off', and 'Fallback'. The second section, 'Emergency Number (Help)', contains a text input field with the value '911'.

### 10.6.2. Use Dial Plan

The Dial Plan can be turned On, Off or used in Fallback mode. In fallback mode, the Dial Plan is inactive unless a particular SIP server to be routed to is out of order. As a backup, the Dial Plan then becomes active.

### 10.6.3. Emergency Number

Enter the emergency phone number for your country (like 112 or 911). Calls to this number will be allowed even if all SIP Session licenses are used up. If you have multiple emergency numbers, you

can add each additional number separated by a space character.

### 10.6.4. Matching From Header

Here you create criterias for the From header of the SIP messages. This is used when matching requests in the **Dial Plan** table. For a request to match, all criterias must be fulfilled.

You can enter a username and domain or create a regular expression (reg exp) to match the From header.

Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	Ingate	*	ingate.com		Any	-	<input type="checkbox"/>
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

Add new rows  rows.

#### Name

Enter a Name for this From header pattern. The name is used in the **Dial Plan** table.

#### Username

Enter the username that the From header should contain. You can enter "\*" to match all usernames.

#### Domain

Enter the domain that the From header should contain. You can enter "\*" to match all domains.

#### Reg Expr

Instead of entering a username and domain, you can create regular expressions to match the From header.

Read about regular expressions at <http://www.regular-expressions.info/>. The unit supports Extended Regular Expressions.

#### Transport

Select which transport protocol or protocols this should match.

#### Network

Select from which network the SIP traffic should be sent. Select from the networks created on the **Networks and Computers** page under **Network**.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.6.5. Matching Request-URI

Here you create criterias for the Request-URI of the SIP messages. This is used when matching requests in the **Dial Plan** table. For a request to match, all criterias must be fulfilled.

You can either enter the username parts and the domain, or create a regular expression to match the Request-URI.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	555 pstn		555	0..9, +, -, #, *		*local		<input type="checkbox"/>
<input type="checkbox"/>	Any number			0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Swedish	011	46	0..9, +, -, #, *		*local		<input type="checkbox"/>

Add new rows  rows.

#### Name

Enter a **Name** for this Request-URI pattern. The name is used in the **Dial Plan** table.

#### Prefix

The **Prefix** part of the username is the first part of the username. You enter zero or more characters, where there should be an exact match. The characters entered in this column are stripped before the request is forwarded.

#### Head

The **Head** part of the username is the first part of the username when the **Prefix** has been stripped. Here, too, there should be an exact match. The characters entered in this column are kept when the request is forwarded.

#### Tail

The **Tail** part of the username is what is left after the **Prefix** and **Head** parts have been removed. Select here allowed characters in the Tail. The Tail is kept when the request is forwarded.

The "anything" option means that any character and any number of characters are allowed in the Tail. The "nothing" option means that the Tail must not contain any character, which means that the username consists only of the Prefix and Head parts.

If you use a Reg Exp, select "-" as the Tail.

When neither the Advanced SIP Routing or the SIP Trunking module has been installed, this column only offers a limited number of options.

## Min. Tail

Enter the minimum number of characters in the **Tail**.

## Domain

Enter the domain that the From header should contain. You can enter "\*" to match all domains, or "\*local" to match all **Local SIP Domains**.

## Reg Expr

Instead of entering a username and domain, you can create regular expressions to match the incoming Request-URI.

In this expression, you can also make subexpressions, which can be used in the **Forward To** table. Subexpressions are made by putting the expression inside parantheses. In the expression **(sip:(.+))@ingate.com**, which matches any Request-URI like sip:user@ingate.com, there are two referable subexpressions: sip:user and user. You can create up to 9 subexpressions per row.

Read about regular expressions at <http://www.regular-expressions.info/>. The unit supports *Extended Regular Expressions*.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.6.6. Forward To

Here you may enter expressions for the Dial Plan, used to define where and how the unit should forward the request using the Dial Plan. Expressions can be defined either by selecting a non-User-account from the **Local SIP User Database** table, or by defining a replacement URI, port and transport.

Forward To <a href="#">(Help)</a>									
Name	No.	Use This	... Or This			... Or This	... Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
Add new rows <input type="text" value="1"/> groups with <input type="text" value="1"/> rows per group.									

## Name

This is the name for this destination. The name is used in the **Dial Plan** table.

## Subno.

This field is used to sort rows within this destination group. The rows are used in the displayed order.

If the first receiver does not respond, or if the unit receives a 5xx response, the request is sent to the receiver on the next row.

## Account

Select an account from the **User Routing** table to where the request should be sent.

## Replacement URI

Instead of routing the request to a defined user, you can enter a new Request-URI for the request. Enter the new URI here.

With this setting, you can only change the domain part of the Request-URI, not the user part.

## Port

Enter the port to where the request should be sent.

## Transport

Select which transport should be used to send the request.

## Reg Expr

Instead of routing the request to a defined user, or entering a fixed Request-URI, you can create an expression which forms a new Request-URI. The expression is built from subexpressions from the **Matching Request-URI** table. To use this, regular expressions must be used on the corresponding row in the **Matching Request-URI** table.

Subexpressions are numbered in the order of their starting parenthesis and referred to as \$number. In the expression **(sip:(.+))@ingate.com**, which matches any Request-URI like sip:user@ingate.com, there are two referable subexpressions: sip:user, which is referred to as \$1, and user, which is referred to as \$2. You can always refer to the entire Request-URI with \$0.

By adding the parameter ";b2bua" at the end of the expression, you force the request to the unit back-to-back user agent, which will make it stateful for all requests. This can be useful if you want the unit to send RADIUS accounting tickets for all calls.

If you just want to forward specific SIP methods, use the Forward To Reg Expr field and append a ";methods=" parameter. E.g. ;methods="NOTIFY" will disable the forward if the request is not a NOTIFY request. The methods parameter can contain several methods comma separated, e.g. ;methods="INVITE, ACK, CANCEL,BYE"

If you just want to rewrite the From header, use the **Forward To Reg Expr** field and append a ";from=" parameter as described below.

The from parameter value may contain references to **Reg Expr** sub-strings. It may reference both sub-strings in the **Matching From Header**, and the **Matching Request-URI Reg Expr** fields. Sub-strings of the From header are referenced as \$fx (where x is an integer, 0 or greater). And Request-URI sub-strings are referenced as \$rx.

The variables below can be used in the from parameter or when using generic header manipulation, the variables available are:

- **cfg.user** (The user part of the account matched (if any) by a request)
- **cfg.host** (The host part of the account matched (if any) by a request)
- **ruri.user** (The username in the incoming Request-URI)
- **ruri.host** (The domain in the incoming Request-URI)
- **ruri.uriparams** (URI parameters from Request-URI)
- **header\_name.user** (User of header "header\_name" e.g. to.user)
- **header\_name.host** (Host of header "header\_name" e.g. contact.host)
- **header\_name.dname** (Display name of header "header\_name" e.g. from.dname)
- **header\_name.uqdtype** (Unquoted display name of header "header\_name" e.g. from.uqdtype)
- **header\_name.params** (Header parameters of header "header\_name" e.g. contact.params)
- **header\_name.uriparams** (URI parameters of header "header\_name" e.g. contact.uriparams)
- **header\_name.telnum** (Tel-URI telephone number of header "header\_name" e.g. from.telnum)
- **header\_name.uri** (Complete URI of header "header\_name" e.g. contact.uri)
- **hdr.header\_name** (The complete header value of header "header\_name")
- **rawhdr.header\_name** (The complete header value of header "header\_name" (not escaped))
- **ip.interface\_name** (The IP address of network interface "interface\_name", e.g. "ip.eth1")

### Examples:

from="sip:\$(from.user)@\$(ip.eth1)" Replaces the From domain with the first IP address of interface eth1.

from="sip:\$(from.user)@example.com" Replaces the From domain with "example.com".

from="sip:\$f1@example.com" Replaces the From domain with "example.com" when matching on From Header Reg Expr "(.\*)@.\*".

If you are using SIP accounts and want to rewrite the from header you can specify the SIP account name as Reg Exp expression in the format:username@domain and use the variables shown above, the from header will be changed before the request is forwarded using your SIP account.

### Trunk

Select an Trunk from the SIP Trunks page to where the request should be sent.

## Use Alias IP

Normally, SIP traffic is sent out from the main IP address (defined in the **Directly Connected Networks** table) of the interface closest to the destination.

With **Use Alias IP** you can select a different source address to use when forwarding the request.

This requires **Aliases** defined on the interface closest to the destination.

Introduced in: v6.0.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 10.6.7. Dial Plan

Here, you create the actual Dial Plan. For each line, select a From entry and Request-URI to match. Then select an Action and, optionally, a Forward to entry to define how the matching requests should be handled by the unit.

You may define lines without a Forward to definition. This is useful if you for example are forwarding by ENUM.

Dial Plan <small>(Help)</small>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	Ingate	Swedish	Auth & Forward	Swedish operator			-	-	Redirect calls for Sweden	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	Any number	Forward	Local PSTN			-	-	Forward calls from Office	<input type="checkbox"/>
<input type="checkbox"/>	3	-	Any number	Auth & Forward	Local PSTN			-	-	Auth if not from Office	<input type="checkbox"/>

Add new rows  rows.

## No.

This is a number that is used to identify each individual Dial Plan rule. Rules are sorted in numerical order. To move a rule to a certain row, enter the number on the row to which you want to move it. You need only renumber rules that you want to move; other rules are renumbered automatically. When you click on **Save** or add a new row, the rules are re-sorted. The order of the rules is important. Rules are used in the order in which they are displayed in the table; rule number 1 is first.

## From Header

Select a matching From header pattern, created in the **Matching From Header** table;

Selecting "-" means that no restrictions are made on the From header or sending IP address.

### **Request-URI**

Select a matching Request-URI pattern, created in the **Matching Request-URI** table;

### **Action**

Select actions for this request. The unit can do the following:

**Forward:** The request is sent to the destination selected under Forward To.

**Auth:** The unit asks the requestor for authentication.

**ENUM:** The unit performs an ENUM lookup to get the new destination.

**Allow:** The Forward To column is ignored and the request is processed according to the unit settings outside the **Dial Plan** table.

**Reject:** The request is rejected. The unit sends a 403 (Forbidden) response.

A lot of combinations of the above actions are available in the drop-down menu.

When neither the *Advanced SIP Routing* or the *SIP Trunking module* has been installed, this column only offers a limited number of options.

### **Forward To**

Select a Forward To pattern, created in the **Forward To** table;

### **Add Prefix**

Sometimes, you might want to add something to a Request-URI when sending the request on to certain servers. Under **Forward**, you can enter a prefix which will be added to the Request-URI when the Forward action is performed. Under **ENUM**, you can enter a prefix which will be added to the Request-URI when the ENUM action is performed.

### **ENUM Root**

If ENUM should be performed for this request, you must select an **ENUM Root**. Select from the roots created in the ENUM Root table.

### **Time Class**

For each rule you select a **Time class**, which regulate on what days and at what time of a day the rule will be active. Inactive rules are ignored when deciding what should be done with the incoming SIP signaling. You define the different time classes on the **Time Classes** page under **Rules and Relays**.

### **Comment**

Enter a comment to remind yourself what this row is meant to do.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.6.8. Methods in Dial Plan

In this table, enumerate which SIP methods the **Dial Plan** should handle.

The ACK, PRACK, CANCEL, BYE, UPDATE and INFO methods can't be handled by the **Dial Plan**. These methods are routed in other ways according to the session they belong to.

### Methods in Dial Plan [\(Help\)](#)

The ACK, PRACK, CANCEL, BYE, UPDATE and INFO methods cannot be handled by the Dial Plan.

Method	Delete Row
INVITE	<input type="checkbox"/>
OPTIONS	<input type="checkbox"/>
SUBSCRIBE	<input type="checkbox"/>
MESSAGE	<input type="checkbox"/>
REFER	<input type="checkbox"/>
NOTIFY	<input type="checkbox"/>

Add new rows  rows.

### REGISTER in Dial Plan [\(Help\)](#)

- Keep To headers for REGISTER requests passed through the Dial Plan
- Rewrite To headers for REGISTER requests passed through the Dial Plan
- Keep From headers for REGISTER requests passed through the Dial Plan
- Rewrite From headers for REGISTER requests passed through the Dial Plan

## Method

Enter the method name. Standard SIP methods can be found in RFC 3261.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.6.9. REGISTER in Dial Plan

REGISTER requests can be handled by the Dial Plan, but require some special processing.

The REGISTER request is the standard method to connect a SIP username to an IP address. For this, the To header is used to convey the SIP username, and the Request-URI is used to tell the server to which the request should be sent. For this reason, To headers in REGISTER requests forwarded through the Dial Plan may no longer match the server to which they are sent.

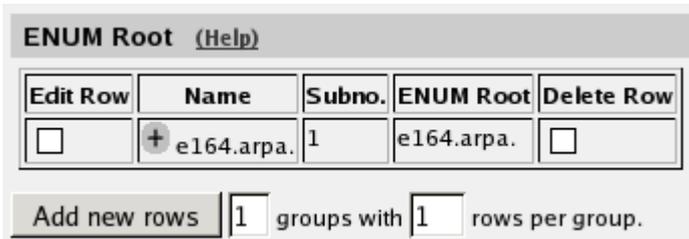
When **Rewrite To headers for REGISTER requests passed through the Dial Plan** is selected, the domain part of the To header is rewritten to match the new Request-URI.

When **Rewrite From headers for REGISTER requests passed through the Dial Plan** is selected, the domain part of the From header is rewritten to match the new Request-URI.

### 10.6.10. ENUM Root

In this table, ENUM roots can be listed. The ENUM root is something like a DNS top domain.

Normally, only the standard ENUM root e164.arpa. is used, but other roots can be added, e.g. for test purposes. Read more on ENUM in RFC 3824



Edit Row	Name	Subno.	ENUM Root	Delete Row
<input type="checkbox"/>	+ e164.arpa.	1	e164.arpa.	<input type="checkbox"/>

Add new rows  groups with  rows per group.

#### Name

Enter a name for this combination of ENUM roots.

#### Subno.

This field is used to sort rows within this ENUM root group. The rows are used in the displayed order; if the first server does not respond, the request is sent to the next one.

#### ENUM Root

The ENUM root to use.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

#### Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

### 10.6.11. Save

Saves the Dial Plan configuration to the preliminary configuration.

### 10.6.12. Undo

Reverts all of the above fields to their previous configuration.

## 10.7. Routing

Here, you configure routing of the SIP signaling received by the unit. The options are: to forward all

SIP requests to a server, regardless of what they concern (**Outbound Proxy**), to forward requests to a specific user to other users as well (**Static Registrations**), and to forward all requests addressed to a specific SIP domain to a SIP server (**DNS Override For SIP Requests**).

You can also configure how incoming calls for local SIP users should be processed. You can restrict allowed callers and send the calls on to a voice mail server.

You can also select to process class 3xx messages in the unit or pass them on to the client.

When the Advanced SIP Routing module is not installed, this page presents only limited functionality.

### 10.7.1. DNS Override For SIP Requests

Here, you can register SIP domains to which the unit should be able to forward requests, but which for some reason cannot be resolved in DNS. Enter an IP address and port to which the requests should be forwarded. You can also select to use a specific protocol.

The unit uses the Request-URI of the incoming SIP packet to match for the domains in this table. When it matches a domain, the packet will be forwarded to the IP address entered here. Note that the Request-URI will not be rewritten!

You can also enter subdomains to **Local SIP Domains**, if you want the subdomain to be handled by a separate SIP proxy. This table has a higher priority than Local SIP Domains, which means that if you register a subdomain to a domain registered under **Local SIP Domains**, the unit will forward SIP requests to the subdomain instead of processing them itself.

You can enter more than one IP address or host name for a domain, and set weights and priorities for these.

DNS Override For SIP Requests <a href="#">(Help)</a>									
Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
<input type="button" value="Add new rows"/> <input type="text" value="1"/> groups with <input type="text" value="1"/> rows per group.									

#### Domain

Enter the domain name of the SIP domain. This domain is compared to the domain in the Request-URI of the incoming SIP packet.

You can't enter a domain that was entered in the **Local SIP Domains** table.

#### Relay To

## DNS Name or IP Address

Enter the IP address for the SIP server handling the domain. You can also enter a DNS name for the SIP server, if it has a DNS-resolvable host name, even if the SIP domain is not possible to look up in DNS.

## IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

## Port

Here, enter the port on which the SIP server listens for SIP traffic. The standard port is 5060 (5061 for TLS).

## Transport

You can select which transport protocol to use between the unit and the SIP server. Under **Transport**, select from UDP, TCP and TLS.

## Priority

If you entered more than one IP address/host name for the same domain, you should also assign them **Priority** and **Weight**. A low **Priority** value means that the unit should have a high priority.

## Weight

If more than one unit has the same **Priority**, the signaling sent to them is distributed between them according to their **Weight**. If two units have the same priority, and Unit 1 has weight 4, and Unit 2 has weight 9, 4/13 of the signaling will be sent to Unit 1, and 9/13 will be sent to Unit 2.

## Auth

The unit asks the requestor for authentication.

## Modify RURI

Modify RURI means the Request-URI of the SIP request will be rewritten with the new destination before it is forwarded.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

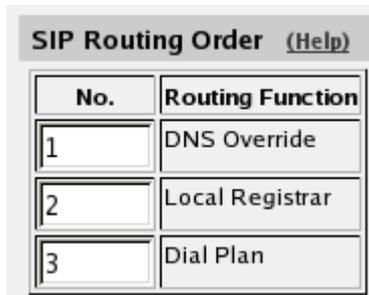
## Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 10.7.2. SIP Routing Order

You can configure the order between some SIP routing functions.

For most standard setups this is not needed, but special complicated scenarios may require a change of order.



No.	Routing Function
1	DNS Override
2	Local Registrar
3	Dial Plan

No.

The order of the function. You change order of the functions by giving them new order numbers.

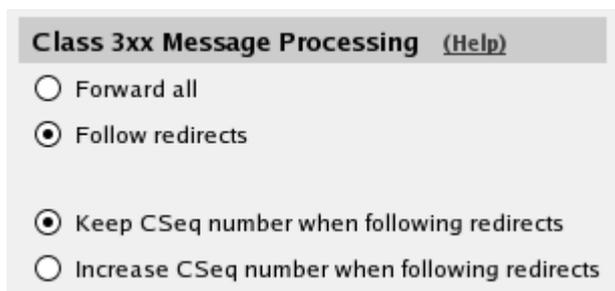
### Routing Function

These are the functions to be ordered. **DNS Override** means the **DNS Override For SIP Requests** table. **Local Registrar** means all locally registered users (but not registration requests) and the **Static Registrations** table. **Dial Plan** means the **Dial Plan** table.

## 10.7.3. Class 3xx Message Processing

Sometimes during negotiation for a connection, status messages about this process will be sent. Here you select whether to forward these to the client or process them in the unit.

A class 3xx message from a server means that the connection attempt was terminated, but no connection was established, e.g. due to use of the wrong address or service. The unit as well as some clients can use this information to make new attempts which might have a better chance to succeed.



**Class 3xx Message Processing (Help)**

Forward all

Follow redirects

Keep CSeq number when following redirects

Increase CSeq number when following redirects

The choices are **Forward all**, which forwards all class 3xx messages to the client (which might be able to use this information), and **Follow redirects**, which means that the unit itself uses the information and might make new connection attempts. In this case, it will only inform the client when the connection finally is established or the attempt has failed totally.

Normally, the CSeq number of the request is kept when SIP devices follow redirects. In some situations, other SIP equipment might require the CSeq number to increase when the unit follows

redirects. Select here if it should do so.

## 10.7.4. Static Registrations

You can specify that calls to a certain user address should also be redirected to another address, or that calls to a non-person user name (like *support@company.com*) should be redirected to one or more other addresses.

Static registrations only affect SIP requests addressed to **Local SIP Domains**.

Even if a call should be forwarded, the unit will try to put it through to the original addressee.

Note that this table should not be used for your own XF or XF/Register accounts. Use the **User Routing** table to forward calls for these accounts instead.

Edit row	Requests to user	Also forward to			Delete row
		User	sip/sips	Transport	
<input type="checkbox"/>	+ ronald@sip.ingate.com	ronald@home.ingate.com	sip	UDP	<input type="checkbox"/>
<input type="checkbox"/>	+ support@sip.ingate.com	charlie@ingate.com	sip	-	<input type="checkbox"/>
<input type="checkbox"/>		emmie@ingate.com	sips	TLS	<input type="checkbox"/>

Add new rows | 1 groups with 1 rows per group.

### Requests To User

Enter the user address. Calls to this user are sent to the user, but also forwarded to users listed under **Also forward to**. The address should be entered on the form *user@domain*.

### Also Forward To

#### User

Enter the address to which the calls should be forwarded. The address should be entered on the form *user@domain*. You can forward to more than one address by creating several rows for the same **Request to user** name.

You can add parameters to the destination address to limit what is sent to that user. Parameters are added after the address, separated by semicolon. The following parameters exist:

**methods=**: Enumerate the SIP methods that should be sent on to this user. If this parameter is not used, all requests are forwarded regardless of which method is used.

**audio**: Audio calls are forwarded to the user. Audio calls are defined as requests with an SDP where a "m=audio" line is present.

**video**: Video calls are forwarded to the user. Video calls are defined as requests with an SDP where a "m=video" line is present.

**+sip.message**: Requests are forwarded to the user if the body contains a line with "m=message" in it.

Example: If audio calls should be forwarded to *adam@sip.ingate.com*, enter *adam@sip.ingate.com;audio*. If only the NOTIFY and SUBSCRIBE methods should be forwarded to *emmie@sip.ingate.com*, enter *emmie@sip.ingate.com;methods=NOTIFY,SUBSCRIBE*.

### sip/sips

Select if the request to this address should be sent by SIP or SIPS (SIP Secure). With SIPS, you require that the request is sent over TLS all the way to the addressee.

### Transport

Select the protocol to use when sending the request.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 10.7.5. Local REFER Handling

Some SIP clients and servers are unable to handle the REFER method, which is used when transferring calls between users. You can make the unit handle the REFERs locally instead of forwarding them to the inept client.

Check boxes for the REFER requests that the unit should handle locally. If no boxes are checked, all REFER requests are forwarded to the destination indicated in the request.

**Local REFER Handling** (Help)

Always handle REFER locally     For clients not supporting REFER

For clients not supporting replaces

For dialogs with specified From URI

For dialogs with specified User-Agent

**From URIs For Which REFER is Handled Locally**

Edit Row	URI	Delete Row
<input type="checkbox"/>	*@testingate.com	<input type="checkbox"/>
<input type="checkbox"/>	martin@ingate.com	<input type="checkbox"/>

**User-Agent Headers For Which REFER is Handled Locally**

Edit Row	User-Agent	Delete Row
<input type="checkbox"/>	RTC/1.*	<input type="checkbox"/>

Add new rows  rows.

Add new rows  rows.

### Always handle REFER locally

With this option, all REFER requests through the unit will be intercepted and handled by the unit instead of the intended destination.

### **For clients not supporting REFER**

When SIP clients start a dialog, they provide a list of supported SIP methods. With this option, the unit will intercept REFER requests bound to client that did not list REFER as a supported method.

### **For clients not supporting replaces**

When SIP clients start a dialog, they provide a list of supported SIP methods and parameters. With this option, the unit will intercept REFER requests bound to client that did not list "replaces" as a supported parameter.

### **For dialogs with specified From URI**

With this option, all REFER requests with a From header matching a URI listed in the **From URIs For Which REFER is Handled Locally** table will be handled locally by the unit.

### **For dialogs with specified User-Agent header**

Some clients or servers may have a limited or erroneous handling of REFER requests. With this option, all REFER requests bound to a client with a User-Agent header matching one listed in the **User-Agent headers for which REFER is handled locally** table will be handled locally by the unit.

### **From URIs For Which REFER is Handled Locally**

Here, URIs are listed that should match From headers for which the unit should handle REFER requests locally.

If the **For dialogs with specified From URI** check box is not checked, this table will be ignored.

#### **URI**

Enter the SIP URI here. The "\*" wildcard can be used for the entire or part of the URI, like *\*@ingate.com*.

#### **Delete**

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### **Add new rows**

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### **User-Agent headers for which REFER is handled locally**

Here, User-Agent names are listed for which the unit should handle REFER requests locally.

If the **For dialogs with specified User-Agent header** check box is not checked, this table will be ignored.

## User-Agent

Enter the User-Agent name here. The "\*" wildcard can be used for the entire or part of the name, like *snom\**.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.7.6. User Routing

This table makes it possible to allow advanced routing options to be enabled per user. You may enter aliases that are used to match incoming request to a specific user. Additionally you may define that the request should be forwarded to other users, and also set up connections to voice mail.

User Routing <small>(Help)</small>									
Edit Row	User	Alias	Restrict Incoming Callers	Forward		Send To Voice Mail	Time Class	Comment	Delete Row
				Action	To				
<input type="checkbox"/>	arthur@ingate.com	1324	No	-		Busy or 15 s	-		<input type="checkbox"/>
<input type="checkbox"/>	harry@ingate.com	1733,harry.smith	No	-		When Busy	-		<input type="checkbox"/>
<input type="checkbox"/>	helen@ingate.com	1294,helen.younger	No	-		After 15 s	-		<input type="checkbox"/>
<input type="checkbox"/>	mark@ingate.com	1387	Yes	Forward	mark.jones@uk.ingate.com	-	-	Moved	<input type="checkbox"/>

Add new rows | 1 rows.

## User

Select a user here from the users defined in the **Local SIP User Database** table.

When you have selected to use a RADIUS database for authentication purposes, there will be a special option here called "\*local domain users". This selection goes for all users on the domain, even when they are not registered. This means that all usernames, even those not configured in the RADIUS database, will be included in this selection, as the unit has no access to the entire user list.

## Alias

Enter aliases for the user, such as short extensions or optional SIP call names.

## Restrict Incoming Callers

You can select to restrict which external users are allowed to make calls. If you turn Restrict Incoming Callers **On**, only locally defined users (in the **Local SIP User Database** table) and users in the **Allow Calls From Unauthenticated Users** table are allowed to call this user.

## Forward

You can send the request to other users. Select here how and whom it should be sent.

## Action

One of the following actions can be selected:

**Reject:** The call is rejected. Nothing is forwarded.

**Forward:** The call will only be forwarded to the users under **To**; if there are any registrations for the user selected under **User**, they will not receive the call.

**Parallel:** The call is forwarded to all users under **To** and all local registrations for the user selected under **User**. Requests for all these users are sent in parallel.

**Sequence:** The call is forwarded to all users under **To** and all local registrations for the user selected under **User**. First, the request is sent to all local registrations. If there is no final response after 25 seconds, the request is sent on to the first user in the To list. After another 25 seconds, the request is sent to the second user in the To list.

**Random:** The call is forwarded to all users under **To** and all local registrations for the user selected under **User**. First, the request is sent to a randomly chosen user in the list. If there is no final response after 25 seconds, the request is sent on to another user in the list.

This can be useful for support centres.

## To

Enter a comma-separated list of the users to forward the request to.

## Send To Voice Mail

Select when to send the SIP request on to a Voice Mail server.

## Time Class

For each rule you select a **Time class**, which regulate on what days and at what time of a day the rule will be active. Inactive rules are ignored when deciding what should be done with the incoming SIP signaling. You define the different time classes on the **Time Classes** page under **Rules and Relays**.

## Comment

Enter a comment to remind yourself what this row is meant to do.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.7.7. Allow Calls From Unauthenticated Users

If Restrict Incoming Callers was turned on for a user in the **User Routing** table, only local users are allowed to make calls to that user. You can enter external users in this table who should also be allowed to make calls for that user.

Allow Calls From Unauthenticated Users <a href="#">(Help)</a>		
Edit row	SIP URL	Delete row
<input type="checkbox"/>	mary.jones@exsiple.com	<input type="checkbox"/>
<input type="checkbox"/>	sales@stockholm.net	<input type="checkbox"/>

Add new rows  rows.

#### SIP URL

Enter allowed SIP URLs. A SIP URL can look like this: *sip:lisa@ingate.com*.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 10.7.8. Voice Mail Server

Here you configure which voice mail server to use for the users in the **User Routing** table. You can also enter the Request-URI to use when connecting to the voice mail server. The Request-URI must start with a sip: or sips:, and can contain references to various usernames and domains.

Voice Mail Server <a href="#">(Help)</a>			
Edit row	No.	Request-URI	Delete row
<input type="checkbox"/>	1	sip:\$(to.user)@\$(to.host);maddr=vmail.ingate.com	<input type="checkbox"/>

Add new rows  rows.

#### No.

The Voice Mail servers are used in the order they are presented in the table. To move a server to a certain row, enter the number on the row to which you want to move it. You need only renumber servers that you want to move; other servers are renumbered automatically. When you click on **Save**, the servers are re-sorted.

## Request-URI

Enter a fixed Request-URI or one containing references to the current call. The following references are available:

**cfg.user:** The username from the current line in the User Routing table.

**cfg.host:** The domain from the current line in the User Routing table.

**ruri.user:** The username in the incoming Request-URI.

**ruri.host:** The domain in the incoming Request-URI.

**to.user:** The username in the incoming To header.

**to.host:** The domain in the incoming To header.

**from.user:** The username in the incoming From header.

**from.host:** The domain in the incoming From header.

When you want to reference one of the above entities, you put them in  $\$( )$ .

If you want to use the username from the current line in the **User Routing** table, and send it to this user at *vmserver.com*, it should look like this:

```
sip:$(cfg.user)@vmserver.com
```

If you want to use the username and domain from the incoming Request-URI and just send the request on to *vmserver.com*, it should look like this.

```
sip:$(ruri.user)@$(ruri.host);maddr=vmserver.com
```

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.7.9. Sender IP Address Per Destination

Normally, SIP traffic is sent out from the main IP address (defined in the **Directly Connected Networks** table) of the interface closest to the destination.

With **Send From IP Address** you can select a different source address to use when forwarding the request.

This requires **Aliases** defined on the interface closest to the destination.

Sender IP Address Per Destination <a href="#">(Help)</a>				
Edit Row	SIP Destination		Send From IP Address	Delete Row
	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	10.47.4.3	10.47.4.3	SIP-2	<input type="checkbox"/>
<input type="checkbox"/>	10.47.4.22	10.47.4.22	SIP-1	<input type="checkbox"/>

Add new rows  rows.

### SIP Destination

Enter the DNS name or IP address of the unit to which SIP signaling should be sent.

### Send From IP Address

Select which IP address to use as the sender address when sending SIP signaling to this unit. Select from the IP addresses defined in the **Alias** table.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.7.10. SIP Default Gateway

Normally, SIP traffic is sent out via the **Main Default Gateways**. If you want SIP traffic sent out via a different default gateway, you can define **Additional Default Gateways** and select one of them here.

This can be useful if you use a managed line to connect to your SIP Trunk operator.

SIP Default Gateway <a href="#">(Help)</a>	
SIP default gateway:	<input type="text" value="SIP operator"/>

Select a SIP default gateway. If you select "-", the unit will use the **Main Default Gateways** configuration for SIP traffic.

## 10.7.11. Outbound Proxy

Here, you can enter one or more external SIP proxies to which all or part of the SIP requests should be sent. This could be useful e.g. if the unit separates two local departments of a company, and all SIP requests should be processed by the *main firewall* connected to the Internet.

This setting should only be used when the unit should not try to re-route requests, as it will only be able to send to the outbound proxy entered here.

You can direct requests to different SIP proxies based on the sender and receiver domain of the request.

<b>Outbound Proxy</b> <a href="#">(Help)</a>						
<b>From Domain</b>	<b>Request-URI Domain</b>	<b>Domain or IP Address</b>	<b>Port</b>	<b>Gateway</b>	<b>Sender IP Address</b>	<b>Delete Row</b>
<input type="button" value="Add new rows"/> <input type="text" value="1"/> rows.						

### From Domain

Enter a SIP domain here. When an incoming SIP request originates from a user in this domain (the domain is in the From field), the unit will send it on to the SIP proxy entered on this row.

You can send all requests to the same external SIP proxy. Enter "\*" here to match all SIP domains.

### Request-URI Domain

Enter a SIP domain here. When an incoming SIP request is bound to a user in this domain (the domain is in the Request-URI), the unit will send it on to the SIP proxy entered on this row.

You can send all requests to the same external SIP proxy. Enter "\*" here to match all SIP domains.

### Domain or IP Address

Enter the domain name or IP address of the external SIP proxy. If you want to use a SIP proxy assigned by DHCP (option 120 for IPv4 and option 22 for IPv6), use the following syntax in the **Domain or IP Address** field: num.name.\_sip-servers, where *num* is the index of available sip-servers and *name* is the name of a DHCP enabled Directly Connected Network. E.g. 0.eth0\_dhcp6.\_sip-servers will use the first available SIP server from the DHCP enabled network eth0\_dhcp6.

### Port

Enter the port number of the external SIP proxy.

If no port number is entered, the unit will make a DNS query for an SRV record. If a port number is entered, it will query for an A record.

### Gateway

Enter the gateway for the external SIP proxy.

You can select which default gateway should be used for requests sent to this SIP proxy. If you select "-", the requests will be sent to the SIP Default Gateway.

## Sender IP Address

You can select which IP address to use when sending the requests to this SIP proxy. If you select "-", the primary IP address will be used.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

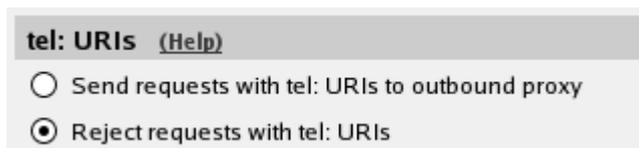
## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.7.12. tel: URIs

tel: URIs is a different URI scheme than the *user@domain* scheme, where the URIs contain only the phone number itself, and the SIP server is expected to know what to do with them.

The unit has no built-in support for tel: URIs itself, but if your outbound proxy can resolve them, you can have the unit send them there.



You can select to **Send requests with tel: URIs to outbound proxy**. If you entered a SIP server to receive requests from all domains in the **Outbound Proxy** table, this is also where all tel: URI requests will be sent. You must ensure that this SIP server will know how to handle these requests.

If you have no access to a SIP server which handles tel: URIs, you can instead select to **Reject requests with tel: URIs**. In this case, when the unit receives a request with a tel: URI, it will respond with the code 416.

## 10.7.13. Refer-To Replacement Domain

This setting applies to REFER requests for transfers with Refer-To headers containing a domain (for which this unit is responsible) or an IP address configured on one of its interfaces. This can for example be used to ensure that the user name is left unchanged in REFERs where the PBX needs to match the user name in its dial plan. Choose the transfer type and enter the domain, host name or IP address of the PBX here.

**Refer-To Replacement Domain** [\(Help\)](#)

Replace Refer-To Domain:

Never

In blind transfers

In blind and attended transfers

Refer-To replacement domain:

### 10.7.14. Automatic assignment of Sender IP address

You can select to assign sender IP address based on the From header of the SIP request. The address is chosen from the primary address or any alias.

**Automatic assignment of sender IP address** [\(Help\)](#)

Don't assign sender IP address automatically

Assign sender IP address based on From header

You can select between two different algorithms for distributing the sender IP address among available addresses. The first algorithm doesn't make any assumptions of the username format. The second algorithm assumes that usernames are selected from consecutive telephone numbers.

### 10.7.15. Save

Saves the Routing configuration to the preliminary configuration.

### 10.7.16. Undo

Reverts all of the above fields to their previous configuration.

### 10.7.17. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 10.8. SIP Status

### 10.8.1. SIP Status

You can monitor the current SIP activity. The tables are updated when you select the page or reload it.

Active Sessions

Here the currently active sessions are listed.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	Status
<b>Active Sessions (2 sessions)</b>									
Start	Caller	Callee	State	Call ID / Media Type					
2008-11-03 13:14:24	<sip:+4613143558@88.131.158.218	<sip:con2@ingate.com>	Established	1066bd00-490eeb2066462-1553f863@sipgt-33a70b2a					
	127.0.0.1:59590 -- (193.180.23.15:59050)			UDP Audio					
2008-11-03 13:11:35	<sip:+4613143558@88.131.158.218	<sip:con2@ingate.com>	Established	3d796090-490eea77c0f1a-2a0513f5@sipgt-33a70b2a					
	127.0.0.1:59586 -- (193.180.23.15:59048)			UDP Audio					

### Start

The time when the call started.

### Caller

The SIP and IP addresses of the calling user.

### Callee

The SIP and IP addresses of the called user.

### State

Shows if the call is established or under negotiation.

### Call ID/Media Type

Each SIP session has a unique ID, which is shown here. You can also see what media type is used in the call.

## 10.8.2. Monitored SIP Servers

Here, status is shown for all domains monitored according to the **SIP Servers To Monitor** table.

<b>Monitored SIP Servers</b>			
Server	Port	Transport	Status
ingate.com		UDP	Online

### Server

The name of the SIP server being monitored by the unit.

### Port

The port of the SIP server being monitored by the unit.

## Transport

The transport being monitored by the unit for this SIP server.

## Status

The status for the monitored SIP server. **Online** means that the unit can contact the SIP server. **Offline** means that the unit can't contact the SIP server.

### 10.8.3. Registered Users

Here the currently registered users are listed.

Registered Users (6 registrations)		
User	Registered From	Survival Aliases
arthur@ingate.com	62.181.235.250	-
harry@ingate.com	10.47.2.227:5060	-
harry@ingate.com	10.47.2.232:5060	-
helen@ingate.com	10.47.2.201:2051	-
helen@ingate.com	10.47.2.123:5060	-
mark@ingate.com	10.47.2.111:5060	-

## User

The SIP address of the registered user. The address looks like *name@domain*, where *name* is a user name or a telephone number, and *domain* is a domain name or the IP address of the SIP registrar (the unit).

## Registered from

The IP address of the computer from which the user registered.

## Survival aliases

If the VoIP Survival module is installed, aliases for this user is shown here. The aliases shown are the ones configured for the user on the main server.

## 10.9. SIP IDS/IPS

SIP IDS/IPS allows you to detect intrusions and DOS attacks aimed at your SIP infrastructure, and to block malicious SIP signaling packets designed to attack certain SIP clients or servers.

You write your own rules which define what should be regarded as an attack.

### 10.9.1. SIP IDS/IPS

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status
-------------	-----------	-----------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------

**SIP IDS/IPS** [\(Help\)](#)

Enable SIP IDS/IPS

Disable SIP IDS/IPS

Select to turn the SIP IDS/IPS module on or off.

### 10.9.2. Packet Match Definition

Here you specify criteria to match SIP signaling packets. For a packet to match, all criteria must be fulfilled. Note: Sub-rows in a rule specify additional match criteria - that is to say: the rows are additive, and not successive, and all sub-rows must match for the rule to match. In other words, if one sub-row does not match, yet two other sub-rows do match, the whole rule will not match.

The default option "-" means "match everything".

**Packet Match Definition** [\(Help\)](#)

Name	Neg	Network	Transport	Message	Part	Reg Expr	Case	Delete Row
+ Scanners	<input type="checkbox"/>	-	-	Request	Header	User-Agent:(friendly-scanner sundayddr sipvicious sipcli)	<input type="checkbox"/>	<input type="checkbox"/>

Add new rows  groups with  rows per group.

#### Name

Name for this packet match.

#### Neg

Logical negation operator (NOT match).

#### Network

The IP source of the SIP packet.

#### Transport

The transport protocol of the SIP packet. TLS/WS/WSS use TCP.

#### Message

The message type (Request/Response).

#### Part

The part of the SIP message to match against using the regular expression (**Reg Expr**). If "-" is selected it will match on the whole message.

- **Start-line:** The first line of the SIP message.

- **Method:** The method of a SIP request, e.g. INVITE or REGISTER.
- **Request-URI:** The Request-URI of a SIP request.
- **Header:** A specific header of the SIP message.
- **Body:** The body of the SIP message, e.g. the SDP.

If the **Header** message part is selected, the regular expression must start with the header name followed by a colon (e.g. "From:" ). After the colon follows the regular expression to match against the header value.

The header name can not be a regular expression and it can only appear once at the start of the regular expression.

Header names that have a compact form will match both versions. For example if you write "From:" it will match both "From" and "f" headers.

Example: **Part** is set to *Header* and **Reg Expr** is "User-Agent:.\*friendly.\*". This will match all SIP messages with a User-Agent header that contains "friendly".

### Reg Expr

Regular expression to match against the whole message or only a part of it.

### Case

Whether or not to perform case-sensitive matching.

### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.9.3. Packet Rate Thresholds

Here, you define thresholds which the unit should regard as intrusion/DOS attacks.

Select a **Match** or leave blank ("-") to match everything. Then supply a **Window** value and the amount of **Hits** during this window that should constitute an undesirable threshold. Hits are counted per origin. An origin is a client/source IP address and transport protocol (UDP/TCP).

If you enter a value in the **Blacklist** field, the origin which reaches a defined rate threshold will be blacklisted for this duration. While they are blacklisted, all SIP signaling from an origin will be discarded.

If ("-") is selected, any SIP packet will be counted as a hit; Requests, responses and even malformed packets.

If **Auto** is enabled, SIP packets are subjected to an "automatic hits" configuration. The true value is not shown on the web page but is calculated based on the unit's performance and session licenses. The shown value (500) is used as a normative constant only and may be in/decreased to tune the calculated threshold value up or down. In case you do not want this "automatic hits" setting, but still want all SIP packets counted, then disable **Auto** and enter your own **Hits** value.

### Capturing group hits counting (CC)

By default hits counting is based on the source IP address, but it is also possible to count based on the message's content. This is done using regular expression capturing groups.

Example: **CC** is checked and **Match** refers to a definition where **Part** is set to *Header* and **Reg Expr** is *User-Agent:(.\*)*. This will count hits based on the captured string between the parentheses.

If multiple capturing groups are used their results will be concatenated.

Note, **CC** requires the message to match the definition and the definition must contain a **Reg Expr** with at least one capturing group. The definition can not use the logical negation operator **Neg** together with the **Reg Expr** capturing groups. If the capturing groups results in an empty string it will also be counted which can be an indication that something is wrong with the capturing groups.

Packet Rate Thresholds <small>(Help)</small>								
Name	Active	Match	Window (s)	Hits	Auto	Blacklist (s)	CC	Delete Row
Default auto	Yes ▾	- ▾	10	500	<input checked="" type="checkbox"/>	300	<input type="checkbox"/>	<input type="checkbox"/>
Default not auto	No ▾	- ▾	10	500	<input type="checkbox"/>	300	<input type="checkbox"/>	<input type="checkbox"/>

Add new rows  rows.

#### Name

The name of the packet rate threshold rule.

#### Active

If the rule is active or not.

#### Match

A reference to the [Packet Match Definition](#) table or "-" to match everything.

#### Window

The time frame used when counting packets (measured in seconds).

#### Hits

The amount of hits during the specified time window.

#### Auto

Automatic hits configuration.

## Blacklist

The blacklist interval in seconds.

## CC

Count based on Reg Expr capturing groups instead of IP address.

## Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 10.9.4. Packet Filter Rules

Here you can match on SIP packets and select how they should be handled.

Rules are evaluated in an ordinal fashion where 1 is first. If a match is found for a packet the evaluation stops and the specified **Action** is taken.

Packet Filter Rules <small>(Help)</small>					
No.	Name	Active	Match	Action	Delete Row
1	Scanners	Yes ▾	Scanners ▾	Discard ▾	<input type="checkbox"/>

Add new rows  rows.

### No.

The order of the rule in relation to other rules.

### Name

The name of the packet filter rule.

### Active

Whether or not the rule is active.

### Match

A reference to a [Packet Match Definition](#). "-" matches everything.

### Action

The action to perform when a matching packet arrives.

- **Discard:** The packet is dropped and no response is sent.
- **Reject:** The packet is blocked and a SIP "403 Forbidden" response is sent.

- **Allow:** The packet is allowed.

## 10.9.5. SIP System Limits

Here you define limits for the SIP subsystem.

**SIP System Limits** [\(Help\)](#)  
Max SIP system load:  %

### Max SIP system load

The max allowed load of the SIP subsystem. The value can be within 0 and 100 percent. If the limit is reached new SIP connections will be discarded.

## 10.9.6. Save

Saves the SIP IDS/IPS configuration to the preliminary configuration.

## 10.9.7. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 10.10. SIP IDS/IPS Status

You can monitor the activities of the SIP IDS/IPS module. The tables are updated when you select the page or reload it.

### 10.10.1. Packet Rate Thresholds

Here you can view the Packet Rate Thresholds hit counters.

Packet Rate Thresholds	
Name	Hits
Default auto	0

#### Name

This is the name of the Packet Rate Threshold.

#### Hits

The number of hits for this rule.

### 10.10.2. Packet Filter Rules

Here you can view the Packet Filter Rules hit counters.

## Packet Filter Rules

No.	Name	Hits
1	Scanners	0

### No.

The order of the rule.

### Name

This is the name of the Packet Filter Rule.

### Hits

The number of hits for this rule.

## 10.10.3. Blacklistings

Here you can view the current blacklistings.

## Blacklistings

Transport	IP Address/CC	Time Left (s)
-----------	---------------	---------------

### Transport

The transport protocol of the SIP packet. TCP/UDP.

### IP Address/CC

The IP address or a CC (Capturing group hits counting).

### Time Left (s)

The time span (in seconds) left of the blacklisting period.

# Chapter 11. SIP Trunks

## 11.1. SIP Trunks

A more extensive description is found in the separate: [How To SIP Trunking Using the SIP Trunk Page](#).

Using the SIP Trunk page will always invoke the B2BUA for the connection of the PBX to the service provider's SIP Trunk and offers the following advantages:

- The IP-PBX only talks to the Ingate
- Wider separation between the PBX and the Trunk Service
- The SIP Trunking Service Credentials (User IDs and Passwords) are stored only in the Ingate
- More SIP normalization possibilities
- Individual or main CallerID (number) presented to the called party
- If a new SIP Trunking Service platform is introduced, only the Ingate has to be reconfigured

There can be up to nine SIP Trunk pages with individual PBXs, trunks and interoperability settings.

When using the SIP Trunk page, there will be a clear demarcation point for the SIP Trunking service hand off.

Using the SIP Trunk page improves the previous way of configuring the Ingate. It offers simplicity, additional functionality and a wider support of various PBXs and Trunk Services. (It is still possible to configure SIP Trunking the previous way, just leaving this SIP Trunking page empty.)

Both the PBX with its Phones and Other SIP Clients Can Use the SIP Trunk.

The SIP Trunk page also offers a simple way to allow SIP clients (SIP phones and Soft SIP clients for PCs) to register to the Ingate and use the SIP Trunk. This is done in addition to supporting the PBX and its extension phones.

### 11.1.1. Licenses/Modules Required for the SIP Trunk Page

You can have up to nine SIP Trunk pages for different PBXs and or SIP Trunk Services, but usually only one is required. The SIP Trunking Module license is required to use SIP Trunk pages and one page is included with that license. To get more SIP Trunk pages, you buy Additional Trunk Group licenses.

### 11.1.2. Steps to Configure SIP Trunking

There are four steps to connect the PBX to the SIP Trunking service. Each of these steps is simple and straightforward:

- Define on the Dial Plan page which outgoing calls to send to the SIP Trunk
- Enter the SIP Service parameters (at the top of the SIP Trunk page)

- Enter the PBX parameters (at the bottom of the SIP Trunk page)
- Define the registration and authentication towards the Trunk Service and the number routing between the Trunk Service and the PBX (in the middle of the SIP Trunk page)

Note that there are help texts available in the Ingate for each setting . just press the .Help. links on the SIP Trunking page.

The Ingate Startup Tool TG, will use the SIP Trunk page when configuring SIP Trunking. (Use the previous Ingate Startup Tool - without the .TG. postfix - if you want to configure the previous way, without using the SIP Trunk page.)

For more details, see the separate: "How To SIP Trunking Using the SIP Trunk Page" found under the Account Login on <https://www.ingate.com>.

## 11.2. Setting up SIP Trunking

### 11.2.1. Defining Outgoing Call Handling in the Dial Plan

Outgoing calls are processed through the Dial Plan, which must be On. At a minimum, the fields exemplified below must be entered. The actual Dial Plan table is searched line by line from the top for a match from the PBX of the dialed number where after it is forwarded to the SIP Trunk page.

1. Calls from the PBX connected to network "ShoreTel".
2. ...with a any dialed number send sent to this unit (regular expression (.\*)@10.100.0.13).
3. ...will be forward for further processing to "Gamma Trunk".
4. ...which is defined on SIP Trunk page 1.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts **Dial Plan** Routing Time Classes SIP Status IDS/IPS SIP Status SIP Test SIP Test Status

**Use Dial Plan** (Help) **Emergency Number** (Help)

On  Off  Fallback

911

**Matching From Header** (Help)

Name	Use This ...		... Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
1) PBX	*	*		UDP	ShoreTel	<input type="checkbox"/>
WAN	*	*		Any	WAN	<input type="checkbox"/>

Add new rows 1 rows.

**Matching Request-URI** (Help)

Name	Use This ...				... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Reg Expr	
2) Callout			-		sip(.*)@10.100.0.13	<input type="checkbox"/>

Add new rows 1 rows.

**Forward To** (Help)

Name	Subno.	Use This ...		... Or This		... Or This	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	
4) Gamma Trunk	1	-			-	SIP Trunk 1: Gamma:Shoretel	<input type="checkbox"/>

Add new rows 1 groups with 1 rows per group.

**Dial Plan** (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
3) 1	PBX	Callout	Forward	Gamma Trunk			-	-		<input type="checkbox"/>
2	WAN	-	Reject	-			-	-		<input type="checkbox"/>

### 11.2.2. The SIP Trunk Page

The SIP Trunk pages are found under SIP Trunks. Several SIP Trunk pages may be defined if you have several PBXs or Trunk Services. You need to purchase Additional Trunk Group licenses to get more than one SIP Trunk page.

**SIP Trunks** Trunk 1

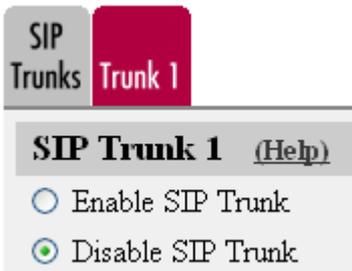
View trunk: SIP Trunk 1

#### View trunk

Click to open the list of available Trunks.

#### Goto SIP Trunk page

Click to view the specified Trunk page.



### Enable the SIP Trunk

Details and examples are found in the separate: "How To SIP Trunking Using the SIP Trunk Page" under the Account Login on <https://www.ingate.com>.

## 11.3. Field Descriptions for the SIP Trunking Page

These descriptions are also found in the Ingate product GUI help texts.

### 11.3.1. SIP Trunking Service

This section contains settings for the interface towards the ITSP, the SIP Trunk.

## SIP Trunking Service [\(Help\)](#)

1)	<input type="radio"/> Use parameters from other SIP trunk <input checked="" type="radio"/> Define SIP trunk parameters	
2)	Service name:	TService <i>(Descriptive name)</i>
3)	Service Provider Domain:	tservice.com <i>(FQDN or IP address)</i>
4)	Restrict to calls from:	- <i>( '-' = No restriction)</i>
5)	Outbound Proxy:	<input type="text"/> <i>(FQDN or IP address)</i>
6)	Use alias IP address:	- <i>(Forces this source address from our side)</i>
7)	Outbound Gateway:	- <i>( '-' = Use Default Gateway)</i>
8)	Signaling Transport:	- <i>( '-' = Automatic)</i>
9)	Port number:	<input type="text"/>
10)	From header domain:	<input checked="" type="radio"/> Provider domain <input type="radio"/> Enterprise domain <input type="radio"/> External IP address <input type="radio"/> as entered:
11)	Host name in Request-URI of incoming calls:	<input type="text"/> <i>(Trunk ID - Domain name)</i>
12)	Remote Trunk Group Parameters (RFC 4904):	<input type="text"/>
	Used as:	- <i>( '-' = Don't use TGP)</i>
12)	Local Trunk Group Parameters (RFC 4904):	<input type="text"/>
	Used as:	- <i>( '-' = Don't use TGP)</i>
13)	Preserve Max-Forwards:	No
14)	Relay media for remote users:	No
15)	Exactly one Via header:	No
16)	'gin' registration (RFC 6140):	No
17)	Hide Record-Route:	No
18)	Show only one To tag:	No
19)	SIP 3xx redirection to provider domain:	No
20)	SIP 3xx redirection to caller domain:	No
21)	Route incoming based on:	Request-URI
22)	Service Provider domain is trusted:	No <i>(For P-Asserted-Identity)</i>
23)	Use P-Preferred-Identity:	No <i>(Instead of P-Asserted-Identity)</i>
24)	Max simultaneous calls:	<input type="text"/> <i>(Call Admission Control)</i>
25)	Max simultaneous calls per Trunk Line:	<input type="text"/>

1. **Use parameters from other SIP trunk / Define SIP trunk parameters** - Determines whether the settings for the SIP Trunking Service should be taken from this page or another SIP Trunk page.
2. **Service Name** - Define a name for the service on this trunk.
3. **Service Provider Domain** - The FQDN or IP address of the ITSP SIP server. This domain name will be used in the Request-URI and To header field for outgoing SIP requests. If there are two redundant SIP Servers, you should enter both here, separated by comma. (Do not enter both SIP Servers, if these instead are addressed by DNS SRV records for the Outbound Proxy.) If the first SIP Server is out of service, the second will be tried. You should also add these SIP Servers to the

table "SIP Services" > Basic > "SIP Servers To Monitor" to speed up failover. You can also specify URI parameters by appending a semicolon followed by the URI parameter, for example ;user=phone multiple parameters can be appended separated by semicolons.

4. **Restrict to calls from** - If specified, only calls originating from any of the specified networks will be handled as an incoming call to this SIP Trunk page. If not specified, a call may origin from anywhere as long as the called number matches any numbers configured here.
5. **Outbound Proxy** - Optional. Outbound SIP proxy for this trunk.
6. **Use alias IP address** - If IP aliases have been configured, you can select one of them for usage when communicating on the SIP Trunk.
7. **Outbound Gateway** - If an extra WAN interface has been configured for specific SIP traffic, you can select to use this WAN interface when communicating over this SIP trunk.
8. **Signaling transport** - The transport protocol for SIP messages on the SIP trunk. Automatic means the transport protocol is determined by automatic means as defined in RFC 3263 based on "Outbound Proxy" or "Service Provider Domain" settings.
9. **Port number** - The port number for SIP messages on the SIP trunk.
10. **From header domain** - This setting selects the domain name to use in the From header field for outgoing SIP requests on the SIP Trunk. You can also specify URI parameters by appending a semicolon followed by the URI parameter, for example ;user=phone multiple parameters can be appended separated by semicolons.
  - Provider domain = Use domain name from "Service Provider Domain" setting.
  - Enterprise domain = The domain name is kept as received from the caller.
  - External IP address = The IP address of the network interface on which the request is sent.
  - As entered = Use the manually entered "From domain" name.
11. **Host name in Request-URI of incoming calls** - The host part of Request-URI is usually one of this units IP addresses and this setting should then not be used. However, if the SIP Trunk Provider uses the host name as a "trunk ID", this setting has to be set to the trunk ID you get from your provider.
12. **Local/Remote Trunk Group Parameters (RFC 4904)** - Optional, with this setting you enable support for trunk group parameters (TGP) according to RFC 4904. Enter ";tgrp=the\_trunk\_group;trunk-context=the\_trunk\_context" (replace the\_trunk\_group and the\_trunk\_context with whatever you have got from the SIP Trunk Provider). Remote TGP refers to parameters placed in R-URI of egress calls to service provider and parameters received in Contact of ingress calls from service provider. Local TGP is the opposite, parameters found in R-URI of ingress calls from service provider and parameters placed in Contact of egress calls to service provider.

**Used as** - This selection lets you choose how to use the Trunk Group Parameters:

- Originating Trunk Group Parameters = The TGP will be used for matching incoming calls from the provider. If they match, the call will be forwarded using any matching line or the main trunk line. If the incoming call contains TGP that don't match the call will not be considered for forwarding by any line on this page.
- Destination Trunk Group Parameters = The TGP will be used to signal the destination trunk

group and trunk context for outgoing calls to the trunk provider.

- Originating and Destination T.G.P = The TGP will be used for both of the above.

Reading TGP found in ingress calls means that the TGP found is matched to the configured values here. If they match the call will be forwarded using any matching line or the main trunk line. If the incoming call contains TGP that don't match the call will not be considered for forwarding by any line on this page.

13. **Preserve Max-Forwards** - Don't decrease Max-Forwards value of the SIP message as it passes through this trunk interface. Recommended setting is No as Max-Forwards helps detecting message loops resulting from bad configuration. But for interoperability with trunks using a very low Max-Forwards, this setting is required. If your calls fail with a "483 Too many hops" message and you don't think there is a message loop, this setting may help.
14. **Relay media for remote users** - Makes this unit relay the media so that the ITSP gets it from this unit, although the media endpoint may be located anywhere on the Internet. Solves interoperability problems with some ITSPs. Try this if you have problems with media (one or no way audio) when users are connected to your LAN from a remote location or calls are transferred externally.
15. **Exactly one Via header** - This unit has a built-in SIP proxy that adds a Via header to SIP requests. Some ITSP's do not expect the SIP request to have been routed by a SIP proxy and this setting is intended to solve such interoperability problems.
16. **"gin" registration (RFC 6140)** - Enables support for gin, see draft-ietf-martini-gin. The registration will then contain bulk number contact URI's and require that intermediate proxies and the registrar supports gin.
17. **Hide Record-Route** - For the same reasons as for the Via header, the Record-Route is a SIP proxy header field that can be hidden.
18. **Show only one To tag** - In case the SIP request is sent to a proxy that forks the call to multiple targets, this setting makes sure the caller becomes unaware of that several phones are ringing for the same call. This is also an interop setting for systems not expecting a SIP proxy in call path.
19. **SIP 3xx redirection to provider domain** - If domain in Contact header of 3xx responses should be modified to the domain of service provider.
20. **SIP 3xx redirection to caller domain** - If domain in Contact header of 3xx responses should be modified to the domain of the caller (From URI).
21. **Route incoming based on** - Defines where to look for the called number for matching an incoming call in the tables below. Request-URI is the default but some ITSPs put this information in To or P-Called-Party-ID headers.
22. **Service Provider domain is trusted** - Select this to enable usage of P-Asserted-Identity header field on the SIP Trunk as defined in RFC 3325. See setting for Identity in the tables below. Some trunks may use this field as caller-ID.
23. **Use P-Preferred-Identity** - Puts the identity found in the table below into a P-Preferred-Identity field instead of P-Asserted-Identity for outgoing calls.
24. **Max simultaneous calls** - Optional CAC (Call Admission Control). Amount of calls supported on the SIP Trunk. If the limit is reached, new calls will not be tried, instead a busy response is sent

back to the caller.

- 25. **Max simultaneous calls per Trunk Line** - Optional. This defines how many calls each line supports before it should be regarded as busy.

### 11.3.2. Number Routing, Registration and Authentication

**Outgoing Calls** to the trunk are sent to a specific SIP Trunking page via **Forward To** in the **Dial Plan**. The from header in an outgoing call is searched for a match in the **From**-columns.

**Incoming Calls** from the trunk are first scanned through the **Incoming Trunk Match** columns and only sent to the **Dial Plan** if no match is found.

### 11.3.3. Main Trunk Line

Used as the default if no match or an empty field is encountered in the tables below. This line should be configured for the main telephone number, and should contain the User ID and Password for the service if only one set is given. Registration shall be enabled on this line (only) if the service uses "implicit registration".

1)	2)	3)	4)	5)	6)	7)	8)	9)	10)
<b>Main Trunk Line</b> <small>(Help)</small>									
<b>No.</b>	<b>Reg</b>	<b>Outgoing Calls</b>			<b>Authentication</b>		<b>Incoming Calls</b>		
		<b>Display Name</b>	<b>User Name</b>	<b>Identity</b>	<b>User ID</b>	<b>Password</b>	<b>Incoming Trunk Match</b>	<b>Forward to</b>	
1	Yes	LEAVE EMPTY!		1305670700	1305670700@tservice.c	305670700	Change Password		

**NOTE** The From-field for outgoing calls must be empty on this line. The columns for incoming calls may be left empty on this line.

### 11.3.4. PBX Lines

This table is used for DID numbers that are mapped to the PBX.

1)	2)	3)	4)	5)	6)	7)	8)	9)	10)
<b>PBX Lines</b> <small>(Help)</small>									
<b>No.</b>	<b>Reg</b>	<b>Outgoing Calls</b>			<b>Authentication</b>		<b>Incoming Calls</b>		
		<b>From PBX Number/User</b>	<b>Display Name</b>	<b>User Name</b>	<b>Identity</b>	<b>User ID</b>	<b>Password</b>	<b>Incoming Trunk Match</b>	<b>Forward to PBX Account</b>
1	No	13056707([0-8])[0-9]	13056707\$1	13056707\$1			Change Password	0(13056707[0-8])[0-9]	\$1
2	No	anonymous		anonymous@anonymous			Change Password		

### 11.3.5. SIP Lines

This table is used for DID numbers that are directly mapped to SIP clients registered to (or through) this device, i.e. not to phones that are connected to the PBX.

1)	2)	3)	4)	5)	6)	7)	8)	9)	10)
<b>SIP Lines</b> <small>(Help)</small>									
<b>No.</b>	<b>Reg</b>	<b>Outgoing Calls</b>			<b>Authentication</b>		<b>Incoming Calls</b>		
		<b>From SIP Number/User</b>	<b>Display Name</b>	<b>User Name</b>	<b>Identity</b>	<b>User ID</b>	<b>Password</b>	<b>Incoming Trunk Match</b>	<b>Forward to SIP Account</b>
1	No	steven	Steven Brown	01305670790			Change Password	01305670790	steven
2	No	+1305670799	Fax	01305670799			Change Password	01305670799	+1305670799
3	No	pda[9(0-9)]		13056707\$1			Change Password	013056707(9(0-9))	pda\$1

1. **No.** - Line number used for sorting the rows. Change numbers if you want to change the order of rows.
2. **Reg** - Set to Yes if this account should be registered at the ITSP SIP Server, e.g if implicit registration (or registration for all DID numbers) is used.
3. **From Number/User** - Can contain a number/name or regular expression. For outgoing calls, this field is matched to the calling user's user name in the From SIP URI (often a number but can also be a name). If there is a match, this line is selected for usage for the outgoing call. This field does not exist for Main Trunk Line as it is defined as the line to use if there is no match on any individual line.
4. **Display Name** - Optional SIP display name to use for outgoing calls, intended for presentation to the called party as a human readable string. In this field you can use the result of a subexpression from a match in a regular expression defined in the **From Number/User** field on the same row. E.g. dialing from 1306770713 having 1306(7707[0-9]{2}) in **From Number/User** with 0\$1 in **Display Name**, will show 0770713 to the called party.
5. **User Name** - The SIP user name to use in the From SIP URI for outgoing calls and registrations. This is usually the telephone number of the ITSP SIP account and usually the number displayed as caller ID on the PSTN. In this field you can use the result of a subexpression from a match in a regular expression defined in the **From Number/User** field on the same row. E.g. dialing from 1306770713 having 1306(7707[0-9]{2}) in **From Number/User** with +\$0 in **User Name**, will result in +1306770713 in the From header to the ITSP. Generic Header Manipulation can be used in this field. See "How To use Generic Header Manipulation" under the Account Login on <https://www.ingate.com>.
6. **Identity** - Optional value to use in P-Asserted-Identity or P-Preferred-Identity for outgoing calls. See "Use P-Preferred-Identity" above. The ITSP may take this as the caller ID to use on the PSTN. In this field you can use the result of a subexpression from a match in a regular expression defined in the **From Number/User** field on the same row. E.g. dialing from 1306770713 having 1306(7707[0-9]{2}) in **From Number/User** with +\$0@goodservice.com in **Identity**, will result in +1306770713@goodservice.com in the P-Asserted- or P-Preferred-Identity header to the ITSP.
7. **User ID** - Optional digest authentication user id if the trunk requires authentication. The Main Line settings will be used if empty in a matching line.
8. **Password** - Optional digest authentication password if the trunk requires authentication. The Main Line settings will be used if empty in a matching line.
9. **Incoming Trunk Match** - The number or regular expression entered here has to match an incoming call to enable forwarding as specified in the **Forward to.** field.
10. **Forward to** - For PBX Lines, this is the number an incoming call will be forwarded to on the PBX. For SIP Lines, this is the SIP address (complete SIP URI or a SIP user name/number on this unit's SIP Server) an incoming call will be forwarded to. In this field you can use the result of a subexpression from a match in a regular expression defined in the **Incoming Trunk Match** field on the same row. E.g. an incoming call to +1306770713 having \+1306(7707[0-9]{2}) in **Incoming Trunk Match** with 0\$1 in **Forward to...** will result in forwarding to the PBX number 0770713. Generic Header Manipulation can be used in this field. See "How To use Generic Header Manipulation" under the Account Login on <https://www.ingate.com>.

See "How To use Regular Expressions" under the Account Login on <https://www.ingate.com> for

information and help regarding Regular Expressions.

### 11.3.6. Setup for the PBX

This section contains settings for the interface towards the PBX.

**Setup for the PBX** [\(Help\)](#)

1)  Use PBX from other SIP trunk  
 Define PBX settings

2) PBX Name:  (Descriptive name)

3) Use alias IP address:  (Forces this source address from our side)

4)	PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
		User ID	Password	DNS Name or IP Address	IP Address	
	<input type="text"/>	<input type="text"/>	<input type="text" value="Change Password"/>	<input type="text" value="10.10.10.150"/>	<input type="text" value="10.10.10.150"/>	<input type="text"/>

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

5) PBX Network:

6) Signaling transport:  (-' = Automatic)

7) Port number:

8) Match From Number/User in field:

9) To header field:  Same as Request-URI  
 Copy from Trunk  
 Initial Request-URI  
 as entered:

10) Remote Trunk Group Parameters usage:  (-' = Don't use TGP)  
Local Trunk Group Parameters usage:  (-' = Don't use TGP)

1. **Use PBX from other SIP Trunk / Define PBX settings** - Determines whether the settings for the PBX should be taken from this page or from another SIP Trunk page.
2. **PBX Name** - Defines a name for the PBX on this page.
3. **Use alias IP address** - Optional. If IP aliases have been configured, you can select one of them for usage when communicating with the PBX.
4. **PBX account**
  - a. **PBX Registration SIP Address** - Optional. If the PBX registers on this unit, this defines the SIP account (address-of-record) it registers to.
  - b. **Authentication User ID and Password** - Will be used for digest authentication of registration by the PBX, if entered. Will also be used for Digest Authentication of invites for outgoing calls, if enforced by the Dial Plan.
  - c. **PBX IP address** - The IP address of the PBX. Recommended to always enter if fixed.
  - d. **PBX Domain Name** - Optional SIP domain name of the PBX in case the PBX wants incoming calls be addressed to *sip:number@domain* instead of *sip:number@ip-address*. You shall also use this field if you have two redundant PBXs. Then add the IP address or FQDN of both PBXs in this field, separated by comma. (Do not fill in the PBX IP Address field then.) If the first PBX is out of service, the second will be tried. You should also enter these PBXs for

monitoring at the **SIP Services > VoIP Survival** page to speed up failover. You can also specify URI parameters by appending a semicolon followed by the URI parameter, for example `;user=phone` multiple parameters can be appended separated by semicolons.

5. **PBX Network** - Specifies which "Network and Computers" the PBX is connected to.
6. **Signaling transport** - The transport protocol (optional) for SIP messages sent to the PBX. Automatic means the transport protocol is determined automatically by applying the rules of RFC 3263 on the SIP URI sent to PBX.
7. **Port number** - The port number (optional) for SIP messages sent to the PBX.
8. **Match From Number/User in field** - Sets which field in the SIP message that will be used as the caller's number when matching the **From Number/User** column in the table specifications above.
9. **To header field** - Set the To header field to use for incoming calls to the PBX:
  - Same as Request-URI = The To header field is set to the same value as the Request-URI.
  - Copy from Trunk = Copies the To URI from the incoming call on the Trunk interface.
  - Initial Request-URI = Set to equal the Request-URI as it looks initially before passing internal SIP proxy.
  - As entered = Enter the URI to use in To header manually in the box to the right. Variable substitution as described above is available in this box.
10. **Local/Remote Trunk Group Parameters usage** - Optional setting for using the Trunk Group Parameters defined above also on the PBX interface.
  - Originating Trunk Group Parameters = The TGP will be used for signaling originating TGP when forwarding calls to the PBX.
  - Destination Trunk Group Parameters = The TGP will be used for matching destination TGP on outgoing calls. If they match, the configuration in this page will be used regardless of what is written in Dial Plan. If there is no match, nothing happens.
  - Originating and Destination T.G.P = The TGP will be used for both of the above.

# Chapter 12. Failover

The failover function makes it possible to have a hot standby unit which always has the current configuration and which automatically takes over when the active unit goes down. The two units become a failover team.

This function requires that one interface on the unit is dedicated for failover and can't be used for anything else.

## 12.1. Introduction

This is a short description of what Ingate Failover can do and what is required to make it work.

### 12.1.1. Requirements

Failover requires two units - each of which MUST;

- have at least three interfaces
- run the same software version
- have the same expansion modules i.e. licenses.

The units must be located in a way so as to connect them with a cross-over network cable. You must also connect all other interfaces on the standby unit to the same Layer 2 network segments (i.e. routers/switches) as the active unit.

### 12.1.2. Features

The Failover function allows you to create failover teams out of two units, where one unit is active and the other a standby unit. The standby stays in constant contact with the active unit to check if it is working and to get new configuration whenever the configuration is changed on the active unit. When the active unit fails, the standby takes over, with the same configuration (including IP addresses). It's possible to encrypt the communication (including configuration transfers) between the active and the standby unit. Configuration transfers occur on the dedicated failover interface. Note, the encryption setting (including the passphrase) cannot be changed after the team is created.

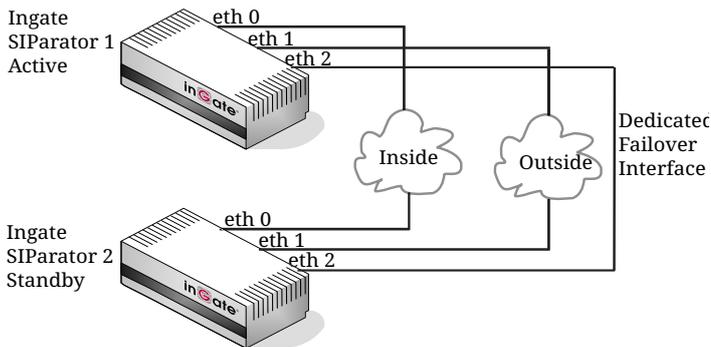
If either of the units stops working, or if the active unit can't connect to the standby unit via the cross-over cable, the unit won't accept new changes to the configuration. This is because there is no way for the active unit to transfer the changes to the standby unit. If this should happen, and there is no way to reestablish the connection between the two units, the mode of the active unit must be changed to a standalone unit (which breaks the failover team) to allow changes in the configuration.

Update interval	30 s
Maximum failover time	7 s + time to apply configuration
SIP registrations kept after failover	Yes
SIP calls kept after failover	No

To improve fault detection within the failover team, reference hosts are used to help to diagnose failure of the interfaces. It is recommended to configure 2 reference hosts per interface. At least one reference host is required per interface. All networks in the units in a failover team send out heartbeat packets. This provides monitoring to detect failure of single interfaces as well as noticing complete service failures in any of the team members.

### 12.1.3. Example

Unit 1 and unit 2 are a failover pair. Eth2 is the dedicated interface. eth0-1 of both unit 1 & 2 connect to the same network equipment, as required for normal failover operation.



If the dedicated interface, i.e. eth2 on unit 1 & 2 were to be severed, this simply means that unit 1 & 2 are no longer able to exchange configuration changes and updates between each-other. The two units will continue to exchange heartbeat messages with each-other over the remaining, active interfaces, i.e. eth0-1. When the dedicated interface ceases normal operation, a GUI message will be displayed to the effect that the configuration can no longer be modified, and configuration changes in the GUI are no longer permitted. The units will both remain operational, in their active/standby modes as long as they continue to exchange heartbeat messages on eth0-1.

If one of the remaining interfaces over which the heartbeat messages are exchanged were to fail on the active unit, the failover standby unit will take over, i.e. fail over. This is where failover reference hosts are useful: they confirm the detection of this type of fault. If all of the remaining interfaces on the active unit were to fail, OR, if eth0-1 on unit 1 cannot establish heartbeat contact with eth0-1 on unit 2 (e.g. VLANs were to prevent such contact), the standby unit becomes active, based on the assumption that the active unit has failed totally. Normal state resumes when heartbeat contact is (re)established and/or when the dedicated interface is (re)connected. Heartbeats are also sent over the dedicated interface.

Unit 1 and unit 2 should have direct layer2 contact with each other on interfaces eth0-1 respectively i.e. unit 1 eth0 → unit 2 eth0, unit 1 eth1 → unit 2 eth1, and so on. Where layer 2 contact is not available or possible, reference hosts must be used per interface to enable detection of interface failure.

Summary: if heartbeat and dedicated connections all fail, unit 1 & 2 fail over.

## 12.2. Failover Setup

For the failover function to work properly, you must configure the units in the right way, and connect them correctly. Here is a short guide on how to do this.

## 12.2.1. Create a new failover team

To create a new failover team, you must initiate the two units in different ways. The first unit is made team master via web interface configuration, the second is added to the team via either web interface configuration or by connecting to it via the serial cable.

### Unit 1

The following procedure will produce a correctly configured team master:

- On the **Failover Settings** page, select the interface which should be directly connected to the other unit as **Dedicated Interface** to use.
- Check the default **Dedicated Interface Network** to see that it doesn't clash with any of your internal networks.
- To enable encryption of communication between the active and the standby unit, set **Enable encryption** to *yes* and press the **Change Passphrase** button to enter a *passphrase*.
- To be able to access the standby unit's web interface you must set up a relay from the active unit. This can be done below **Standby Unit Access Relay**.

#### WARNING

If you enable encryption, you need to enable encryption and enter the same *passphrase* when joining unit 2 (the standby unit). Otherwise, the communication won't work and the failover team will be broken.

- Press the **Become master** button to create a new failover team with this unit as its first member. This will cause the unit to reboot.

### Unit 2

To make unit 2 (the standby unit) slave member of the failover team, you can either configure it using the web interface or connect to it using the serial cable. See [Installation](#), for a thorough description on how to do this.

#### Either Web Interface

- Go to the **Failover Settings** page and select the same interface that was selected as **Dedicated Interface** for unit 1.
- The **Dedicated Interface Network** should also match the network used on unit 1.
- If you enabled encryption of communication when you created the team on unit 1 you must enable encryption with the **same** *passphrase* that was entered on unit 1.
- Press the **Become slave** button to join an existing failover team as the slave.

#### Or Serial Console

- Log on from your terminal as *admin* and select **3. Join a failover team and become slave**.
- Select the same interface that was selected as **Dedicated Interface** for unit 1.
- The **IP network address** and **IP netmask** must also match the **Dedicated Interface Network**

used on unit 1.

- If you enabled encryption of communication when you created the team on unit 1 you must enable encryption with the **same passphrase** that was entered on unit 1.

#### WARNING

If there is a configuration mismatch on the encryption setting, the communication won't work and the failover team will be broken. In this case you need to re-join unit 2 with a matching configuration (i.e. same *passphrase*).

All existing configuration will be removed and the unit will reboot. It will then obtain its configuration from unit 1.

### 12.2.2. Connecting the units

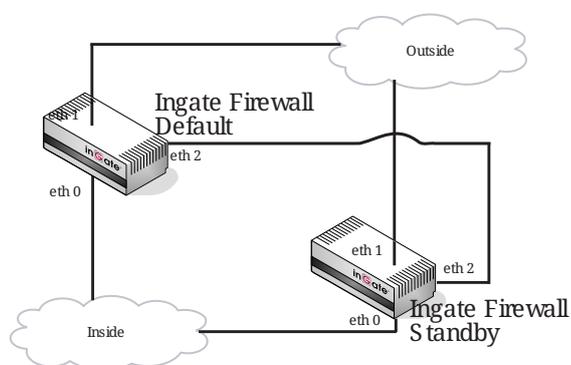
After installing the units, you must also connect them properly.

The **Dedicated Interface** on unit 1 which was reserved for failover must be connected to the corresponding interface on unit 2. If you for example selected eth2 as the **Dedicated Interface** to use, you must connect eth2 on unit 1 with eth2 on unit 2.

The other interfaces must be connected in parallel to the networks on which the unit should operate. If you configured eth0 to be on the Inside and eth1 on the Outside, both eth0 interfaces should be connected to the local network and both eth1 interfaces to the Internet network.

#### WARNING

You can't have a router between any pair of interfaces; they must be located on the same logical IP network, i.e. on the same Layer 2 segment.



### 12.2.3. Leaving a failover team

If you for some reason want to quit using failover and use the units as standalone units, you must do things in the right order to release the team which uses a direct cable connection:

1. The **Standby** unit must be taken away first using one of these methods:
  - a. Log in to the standby unit's web interface using the **Standby Unit Access Relay**, go to the **Failover Settings** page and press the **Become standalone** button.
  - b. Log on as **admin** via the serial cable and select **4. Leave the failover team and become standalone**.
2. Change type of the **Active** unit on the **Failover Settings** page by pressing the **Become**

**standalone** button.

**NOTE**

The standby unit will keep the configuration after leaving the team. Thus if both units are kept running after the standby unit becomes standalone they will have the same IP addresses and you will get an IP address conflict. Disconnecting all interfaces except the Dedicated Interface prevents this.

### 12.2.4. Replacing a unit in the failover team

You might want to replace a unit if it breaks or for other maintenance reasons.

If you want to replace a unit in the failover team, you must first split the team and then make a new one.

**NOTE**

Be careful to check which one of the team members that is Active, so that you don't disconnect it instead of the faulty one. Check this on the **Failover Status** page.

- See [Leaving a failover team](#) for how to split the team.
- See [Create a new failover team](#) for how to create a new team with the new replacement unit.

### 12.2.5. Upgrading a failover team

Both units in a team must use the same software version.

1. Go to the **Failover Status** page to see the serial numbers of the units in the team.
2. Download the upgrade file from <https://account.ingate.com/>.
3. Use the **Standby Unit Access Relay** and log in to the standby unit's web interface.
4. Follow the instructions to [Upgrade](#) the standby unit.
5. Make sure you can access the standby unit's web interface using the **Standby Unit Access Relay** and check that it is upgraded.
6. Follow the instructions to [Upgrade](#) the active unit.
7. When the active unit reboots a failover will happen. The current standby unit will become active and when the previous active unit has rebooted it will become the standby unit.
8. Make sure you can access the *new* standby unit's web interface using the **Standby Unit Access Relay** and check that it is upgraded. You must accept the upgrade by pressing **Accept upgrade**.

Now both units should have the same software version.

## 12.3. Failover Settings

Here, you configure the unit to enable it to communicate with the other unit of the failover team. Here is also where you change type between a standalone unit and one which is a team member.

To ensure that the two units will successfully operate as a failover team both the units should adhere to the identifier shown in the **Failover Settings** tab. If the identifier doesn't match please

compare the information found on the **About** page.

**NOTE** | The identifier **437c94d0** shown in the picture below is just an example.

### 12.3.1. Failover Dedicated Interface

To synchronize settings between two units in a failover team, each unit needs an interface dedicated to synchronization. This interface cannot be used for any other traffic.

Note, this setting cannot be changed after the team is created.

**Failover Settings** | Reference Hosts | Failover Status

To minimize the downtime in case the firewall hardware breaks down it is possible to designate two units to the same services. Here, settings are made for this.

To ensure that the two units will successfully operate as a failover team both the units should adhere to the identifier **437c94d0**. If the identifier doesn't match please compare the information found on the About page.

**Failover Dedicated Interface** ([Help](#))

The dedicated interface to use:

#### The dedicated interface to use

Select the interface to be used for communication with the other unit of the team. This interface must be connected to the corresponding interface of the other unit.

### 12.3.2. Failover Dedicated Interface Network

A small network must be reserved for use over the dedicated interface. This is used for communication within the failover team and cannot be used for anything else.

This network must contain at least four addresses (one for each unit, one network address and one broadcast address). You can dedicate a larger network if you like, but since the interfaces will be directly connected to each other, no more than four addresses will be used.

Note, this setting cannot be changed after the team is created.

**Failover Dedicated Interface Network** ([Help](#))

DNS Name or Network Address	Network Address	Netmask / Bits	Range
<input type="text" value="10.120.121.64"/>	<input type="text" value="10.120.121.64"/>	<input type="text" value="255.255.255.252"/>	<input type="text" value="10.120.121.64 - 10.120.121.67"/>

#### DNS Name or Network Address

Enter the DNS name or IP address of the dedicated network.

## Network Address

Shows the IP address of the **DNS Name or Network Address** you entered in the previous field.

## Netmask/Bits

**Netmask/Bits** is the netmask that will be used to specify the size of the dedicated network. You must use an IPv4 netmask of maximum 30 (255.255.255.252). See [Configuring](#), for instructions on writing the netmask.

## Range

The **Range** shows all IP addresses of the dedicated network. The range is calculated from the configuration under **DNS Name or Network Address** and **Netmask/Bits**. Check that the correct information was entered in these fields.

### 12.3.3. Encryption of Communication

Enable this setting if you want to encrypt the communication (including configuration transfers) between the active and the standby unit. Configuration transfers occur via the **Failover Dedicated Interface**. Enter a passphrase that will be used when encrypting the communication (the **same** passphrase must be used when joining the slave). Note, this setting cannot be changed after the team is created.

#### Encryption of Communication [\(Help\)](#)

Enable this setting if you want to encrypt the communication (including configuration transfers) between the active and the standby unit. Enter a passphrase that will be used when encrypting the communication (the **same** passphrase must be used when joining the slave).

Enable encryption:  Yes  No

[Change Passphrase](#)

### 12.3.4. Standby Unit Access Relay

Here you can set up a relay to the standby unit's web interface. This allows you to log in to the standby unit and perform administrative tasks such as applying an upgrade or license, displaying the log and rebooting the unit.

The team must be operational before you can access the standby unit.

You can not access the standby using the relay if one unit leaves the team.

No configuration changes can be made on the standby unit.

This setting can be set up or changed after the team is created.

**Standby Unit Access Relay** [\(Help\)](#)

Protocol	IP Address	Port	Cert	TLS	Allow	Delete Row
HTTP ▼	eth0 (192.168.1.1) ▼	8080	- ▼	- ▼	LAN ▼	<input type="checkbox"/>

Add new rows  rows.

**Protocol**

The protocol to use (HTTP/HTTPS).

**IP Address**

The IP address to listen on.

**Port**

The port to listen on.

**Cert**

Select the certificate to use for HTTPS.

If HTTPS is used it is terminated on the standby unit, thus the traffic between the browser and the standby unit will be encrypted.

**TLS**

The TLS protocol to use.

**Allow**

Here, you select a network group, defined on the Networks and Computers page. Only the computers in the chosen group can use the relay.

**Delete**

If you select this box, the row is deleted when you choose **Add new rows** or **Save**.

**Add new rows**

Enter the amount of new rows you want to add to the table, and then choose **Add new rows**.

The standby unit shows an information bar at the header of each page.

No configuration changes can be made on the standby unit.

STANDBY UNIT

- No action taken as you do not have sufficient access rights.

Save/Load Configuration Show Configuration User Administration Upgrade Table Look Date and Time Restart Change Language

**Test Run and Apply Conf** (Help) **Show Message About Unapplied Changes**

Duration of limited test mode:

30 seconds

Apply configuration

On every page  
 On the Save/Load Configuration page  
 Never

### 12.3.5. Create, Join or Leave a Failover Team

The unit can work as **Standalone** or as a **Master/Slave**. In Standalone mode, it works as a standard unit. As a **Master/Slave**, it still performs the usual functionality, but in addition, it communicates with the other team member to transfer configuration when changed. The team members constantly check whether the other unit is alive.

Here you change failover type for the unit from **Standalone** to **Master/Slave** or from **Master/Slave** to **Standalone**. When you change type, the unit will reboot.

**Create a new Team** (Help)  
The change will be immediate and cause a reboot.  
Become master

**Join an existing Team** (Help)  
The change will be immediate and cause a reboot.  
Become slave

**Leave Team** (Help)  
The change will be immediate and cause a reboot.  
Become standalone

#### Create a new Team

Press **Become master** to create a new failover team, with this unit as master.

If the unit was standalone, it will reboot and then listen for its team partner on the dedicated interface, to transfer its configuration.

#### Join an existing Team

Press **Become slave** to join an existing failover team as the slave. The change will be immediate, cause a reset of the configuration and a reboot.

## Leave Team

Disconnect the other unit in the team (or turn off the power) and press **Become standalone** to make the unit standalone again.

The change will be immediate and cause a reboot.

### NOTE

The standby unit will keep the configuration after leaving the team. Thus if both units are kept running after the standby unit becomes standalone they will have the same IP addresses and you will get an IP address conflict. Disconnecting all interfaces except the Dedicated Interface prevents this.

## 12.3.6. Save

Saves all Failover Settings configuration to the preliminary configuration.

## 12.3.7. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 12.3.8. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 12.4. Reference Hosts

The standby unit in the failover pair can become active if a network interface on the active unit is faulty. For the unit to detect a faulty interface, it needs to be aware of some reference hosts which it should be able to contact. Requirements for reference hosts are that they sit on the same logical IP segment, i.e. Layer 2 as the chosen interface IP. Reference hosts on any WAN segment must sit within the same gateway.

Each interface in use (except for the dedicated interface) must have one or two reference hosts. The replies from them are used to determine which interface in the active or the standby unit is broken. Without reference hosts, should a situation arise in which there are no heartbeats flowing in one or both directions between two interfaces, there is no way to know whether the TX on one unit is broken or if RX on the other unit is broken or if there is a combination of errors. Replies from reference hosts can decisively break the tie. When performing shape comparison, each interface's RX and TX are looked at separately.

The shape of RX and TX for a particular interface, for example eth1 on both units is calculated, then a decision is made as to which unit is in better shape with regards to that particular interface. Sometimes it's clear that one of the interfaces is broken and that that unit is in worse shape than the other with regards to that interface.

Comparisons are made for each interface in use of a unit, except for the dedicated interface, and for

each error detected its shape deteriorates. For each error, a log message is also generated telling what is broken on which unit. After comparison, the units determine if they are in equal shape or if one unit is in better shape than the other. If it is determined that the active unit is in worse shape than the standby unit, a failover is initiated. If the standby unit is in worse shape, an alert log message is generated and the active unit continues to run as before.

On this page, enter IP addresses of reference hosts that will reply to ping from the unit. As faulty reference hosts will cause the failover pair to repeatedly change the active unit, you should select the reference hosts with care. It is recommended that you enter two hosts for each interface.

Failover Settings
Reference Hosts
Failover Status

**Failover Reference Hosts** [\(Help\)](#)

Edit Row	Interface	Reference Host			Delete Row
		Dynamic	DNS Name or IP Address	IP Address	
<input type="checkbox"/>	Internal (eth0)	-	10.47.2.1	10.47.2.1	<input type="checkbox"/>
<input type="checkbox"/>	External (eth1)	-	193.12.253.118	193.12.253.118	<input type="checkbox"/>
<input type="checkbox"/>	External2 (eth2)	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

### 12.4.1. Interface

Select the interface to be tested. The reference host entered on this line must be reachable via this interface, i.e. not located behind another interface of the unit.

### 12.4.2. Reference Host

#### Dynamic

If an interface will receive its IP address from a DHCP server, the unit can use its default gateway as a reference host for that interface. In this case, select the corresponding IP address here and leave the other fields empty.

#### DNS Name or IP Address

The name/IP address of the reference host used to test this interface.

#### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

### 12.4.3. Delete

If you select this box, the row is deleted when you choose **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### 12.4.4. Add new rows

Enter the amount of new rows you want to add to the table, and then choose **Add new rows**.

#### 12.4.5. Save

Saves all Reference Hosts configuration to the preliminary configuration.

#### 12.4.6. Undo

Clears and resets all fields in new rows and resets changes in old rows.

#### 12.4.7. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

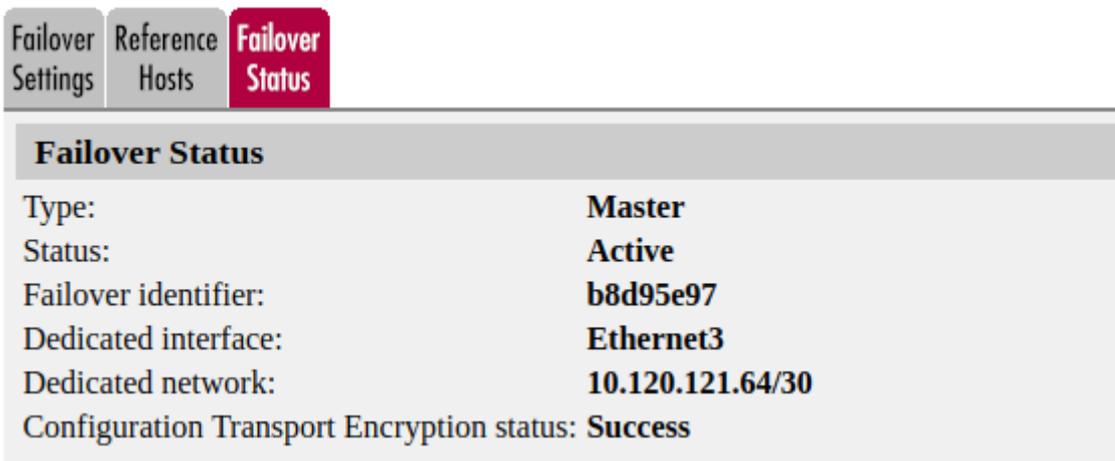
This button will only be visible if a DNS server has been configured.

### 12.5. Failover Status

Here the configuration used by the failover team is shown. Here, you can also view the status of the units in the team.

#### 12.5.1. Failover Status

Here are the settings used by the unit for failover communication.



Failover Settings	Reference Hosts	<b>Failover Status</b>
<b>Failover Status</b>		
Type:	<b>Master</b>	
Status:	<b>Active</b>	
Failover identifier:	<b>b8d95e97</b>	
Dedicated interface:	<b>Ethernet3</b>	
Dedicated network:	<b>10.120.121.64/30</b>	
Configuration Transport Encryption status:	<b>Success</b>	

#### Type

A unit can be **Standalone**, **Master** or **Slave**.

#### Status

The unit's failover status. It can be **Active** or **Standby**.

## Failover identifier

To ensure that the two units will successfully operate as a failover team both the units must adhere to this identifier. If the identifier doesn't match please compare the information found on the **About** page.

## Dedicated interface

If the unit is a member of a failover team, the interface used for failover communication is shown here.

## Dedicated network

If the unit is a member of a failover team, the network used for failover communication is shown here.

## Configuration Transport Encryption status

The status of the configuration transport encryption.

- N/A if encryption of failover communication is disabled.
- **Success**
- **Failure (please check the encryption passphrase)**

## 12.5.2. Failover Team

Here, you can see a list of the members of this failover team and their status.

### Failover Team

A failover team consists of two units connected in parallel. Technically, a team can consist of just one unit, but then no failover is possible, of course. The unit that is currently running the show is in active mode.

This failover team consists of:

Serial Number	Status
IG-200-627-1020-7	Active
IG-200-627-1021-5	Standby

### Serial number

The serial number of each team member.

### Status

A team member can have one of the following statuses. Switching between them is done automatically.

## Active

A team of failover units can only have one unit active. This is the unit that owns the configuration that is currently in use. The unit that is in active mode may not necessarily be completely functional. If both the active and standby units have malfunctions, the best choice is used.

## Standby

A team of failover units can have only one unit in standby mode. The unit in standby mode is ready to take over, in case of a failure of the active one. It continuously gets all configuration changes from the unit in active mode.

## Unavailable

Unavailable indicates that the team member is inaccessible, that is, it may be turned off, could be failing for some reason or all cables could have been disconnected.

# 12.6. Fault messages

If either of the units stops working, or if the active unit can't connect to the standby unit via the cross-over cable, the unit won't accept new changes to the configuration. This is because there is no way for the active unit to transfer the changes to the standby unit. If this should happen, and there is no way to reestablish the connection between the two units, the mode of the active unit must be changed to a standalone unit (which breaks the failover team) to allow changes in the configuration.

In top of the GUI the reason for the fault that has occurred is displayed. Repair actions can be different depending on the reason for the fault. Following are examples of what is presented in the GUI.

### 12.6.1. No contact over the dedicated interface!



**No contact over the dedicated interface!** You can display all pages, but you cannot make any changes until the other member becomes online or this unit is changed to standalone operation.

Warnings exist: [Go to warning 1](#)

Check the cabling for the dedicated interface before changing to standalone mode.

### 12.6.2. No contact with failover standby unit!



**No contact with failover standby unit!** You can display all pages, but you cannot make any changes until the other member becomes online or this unit is changed to standalone operation.

Warnings exist: [Go to warning 1](#)

Wait for a while to see if the faulty unit comes back into service, if not it needs to be repaired. For each error, log messages are also generated telling what is broken on which unit, check those for better diagnosis for what should be repaired.

Example log messages regarding heartbeats - each interface sends heartbeats to its respective partner interface to determine their shape - that is functioning or broken:

```
--- Warning: heartbeatd:      Interface eth3 error[9/1]. No contact between RX of
this unit
and TX of other unit.
Other unit IG-000-000-0000-0:
0 lost beats, 0 unsolicited RX
This unit IG-111-111-1111-1:
3 lost beats, 0 unsolicited RX

--- Warning: heartbeatd:      Interface eth3 error[1/9]. TX of other unit is broken.
Other unit IG-000-000-0000-0:
0 lost beats, 1 unsolicited RX
This unit IG-111-111-1111-1:
3 lost beats, 1 unsolicited RX
```

TX = Transmit / RX = Receive

"3 lost beats" = the number of heart-beats I have not received from the *Other unit*

"1 unsolicited RX" = I received something, which means my Receive is working.

### 12.6.3. Standby unit has lower version than active unit



**Standby unit has lower version than active unit!** You can display all pages, but you cannot make any changes until the standby unit is upgraded or this unit is changed to standalone operation.

The members of a team must have the same software version.

Upgrade the standby unit to the same version as the active unit using the **Standby Unit Access Relay** feature.

# Chapter 13. Virtual Private Networks

VPN (Virtual Private Network) is a method of creating a secure private network via an insecure network such as Internet.

Assume that a company with several offices that are geographically distributed - for example, one office in Washington D.C. and one in Atlantic City - wants to connect its local networks to a company network. One relatively inexpensive way of doing this is through Internet. The firewalls in the offices create encrypted connections, tunnels, between the different offices. The users do not need to manage the encryption or set a new configuration. This kind of VPN is called Branch Office VPN.

VPN is also used when a single computer on an insecure network wants to connect to the office network through Internet. The client computer, also called a Road Warrior, must have special VPN software compatible with the unit VPN software. The client connects to the Internet and creates an encrypted connection to the office firewall.

In [More About VPN](#), you find more information about the configuration of VPN clients.

You can find examples on how to configure VPN in [Part IV. How To Guides](#).

## 13.1. Specification of Ingate VPN

This is a short description of what Ingate VPN can do and what is required of other devices to be able to set up a VPN connection with the unit.

### *Features*

- Supports connections to other IPSec compliant gateways and to IPSec clients (with or without a NAT:ed IP address)
- Supports connections to PPTP clients
- No user licenses
- Key negotiation protocol (IPSec peers): IKEv1 and IKEv2
- Connection negotiation protocol: IPSec
- Encryption algorithm (IPSec peers): AES or 3DES
- Authentication algorithm (IPSec peers): SHA-1, SHA2-256, SHA2-512 or MD5
- Diffie-Hellman groups 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 23 and 24 are supported.
- Authentication (IPSec peers): Shared secret, X.509 certificates or XAUTH+PSK
- Customizable key lifetimes (maximum 172800 s for IKE keys, 86400 s for IPSec keys)
- Dead Peer Detection
- IKE Mode Configuration (MODECFG)
- Authentication (PPTP peers): Password

You can have several networks behind one VPN peer, provided that they are proper subnets.

If you have defined **Alias** for the interface closest to the VPN peer, you can select which unit address to use when connecting to a peer.

IPSec clients connections can be configured to require user authentication using a RADIUS server.

You must define firewall rules for VPN traffic. You can group peers that should have the same privileges.

#### *Requirements for IPSec peers*

- Key negotiation protocol: IKEv1 and IKEv2
- Connection negotiation protocol: IPSec
- Encryption algorithm: AES or 3DES
- Authentication algorithm: SHA-1, SHA2-256, SHA2-512 or MD5
- Authentication: Shared secret (VPN gateways only), X.509 certificates or XAUTH+PSK
- Preferably support PFS (Perfect Forward Secrecy) group 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 23 or 24
- Support Main mode (phase 1)
- Support Tunnel mode (phase 2)

## 13.2. Ingate VPN technology

Ingate VPN supports IPSec and IKE, which are standards developed by IETF (Internet Engineering Task Force). More and more software developers base their products on these protocols.

Ingate VPN also supports PPTP connections, another protocol for making private connections over insecure networks.

You can read more about IPSec, IKE, and PPTP in [More About VPN](#).

### 13.2.1. Network security

*Authentication* is the process of making sure that the message you receive really originates from the right sender, and that it hasn't been corrupted during transmission. Authentication also protects against resending of packets, but not against eavesdropping.

*Encryption* is the process of distorting data so that only the desired receiver can read the message.

Different methods of authentication and encryption exist. Ingate VPN supports the authentication algorithms MD5 and SHA-1, and the encryption algorithms 3DES (triple DES) with a key length of 168 bits, and AES with a key length of 128 bits.

## 13.3. IPsec Peers

Here, all parts communicating with the unit via IPsec are defined. The machines you define here are the units and road warriors which set up the encrypted IPsec tunnel to the unit. The networks using the **IPsec tunnels** are defined on the IPsec Tunnels page.

These settings are called *Phase 1 settings* in some other IPsec products.

IPsec Peers (Help)									
These settings are called "Phase 1 settings" in some other IPsec products.									
Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Atlantic City	-	Yes	Outside (193.12.253.115)	198.122.30.2	No	198.122.30.2	No	
<input type="checkbox"/>	+ Boston	-	Yes	Outside (193.12.253.115)	13.73.22	No	13.73.22	No	
<input type="checkbox"/>	+ Chicago	-	Yes	Outside (193.12.253.115)	chicago.ingate.com	Yes	chicago.ingate.com	No	
<input type="checkbox"/>	+ Juliet	-	Yes	Outside (193.12.253.115)	*	No	*	No	
<input type="checkbox"/>	+ Offices	-	Yes	Outside (193.12.253.115)	19735.2.2	No	19735.2.2	No	
<input type="checkbox"/>		Atlantic City	-	-		No		-	
<input type="checkbox"/>		Chicago	-	-		No		-	

Add new rows | 1 groups with 1 rows per group.

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: C9:97:87:1F:9E:BF:7C:38:BE:25:85:D6:04:84:2F:F6	<input type="checkbox"/>
3600	Yes	AES/3DES	X.509 certificate	Subject: /C=US/O=Ingate Systems/CN=chicago.ingate.se Issuer: /C=US/O=Ingate Systems/CN=chicago.ingate.se MD5 Fingerprint: 81:0C:01:C2:63:09:B1:23:F0:E3:25:EE:D7:DE:D4:09 Valid to: 2008-07-16 15:43:05	<input type="checkbox"/>
3600	Yes	AES/3DES	Trusted CA	Main CA	<input type="checkbox"/>
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>
	-	-	-		<input type="checkbox"/>
	-	-	-		<input type="checkbox"/>

You can create a group consisting of several peers by defining them directly in the group row (see first row in the **Offices** group) or by defining them separately and adding them to the group (see second row in the **Offices** group). Defining them in the group will give all peers in the group the name of the group when appearing in the logs, which could be inconvenient. Subgroups defined separately will be logged as their own names.

In the example above, the key negotiations with **Atlantic City** will appear as **Atlantic City** negotiations in the log, regardless of the negotiations coming through the **Atlantic City** or the **Offices** alternative. Negotiations with the unnamed subgroup will appear as **Offices** negotiations in the log.

### 13.3.1. Name

Enter a name for the IPsec peer. **Name** is only used internally in the unit.

### 13.3.2. Subgroup

Here, you can select an already defined IPsec peer in order to form a group of several peers. Assign more than one row to a name by clicking the plus sign to the left of the name, or by creating a group with several rows.

If you select a subgroup here, the rest of the fields in the row should be left empty.

### 13.3.3. Status

Select whether this tunnel should be active or not. If **Off** is selected, no IPsec connection will be established with this IPsec peer. If you selected a peer under **Subgroup**, select "-" here.

### 13.3.4. Local Side

Select the unit IP address which should manage the IPsec traffic. This is the IP address to which the IPsec peer connects.

You must select an IP address from the logical network closest to the IPsec peer. Usually this means an IP address on the outside of the unit on the network with your **Default gateway**. If more than one **Directly connected networks** are defined, an IP address on the network directed to the IPsec peer must be selected, i.e. the direction in which the IPsec packets will be sent.

### 13.3.5. Remote Side

#### DNS Name or IP Address

Here, enter the host name or IP address of the IPsec peer. If the peer is a road warrior, having no fixed IP address, you enter "\*" here.

If the peer IP address changes, but it keeps the same host name, you can enter the host name here, and select to do runtime DNS lookups of the name (see **Dynamic**).

The information in this field is used by the unit as the peer IP address as well as the peer ID. This could cause problems when the peer is NATed. If you have a peer where the ID can be set manually, it should be set to the public IP which the peer appears to have. The public IP address is also what should be entered here.

If the peer is a NATed unit, you cannot enter an IP address here, but must use the "\*", even if the public and the private IP addresses of the unit are known. This also means that you cannot use a preshared secret for this peer, but must use X.509 certificates.

#### Dynamic

Check the box here if the IP address of this peer should be looked up every time the unit wants to use it. If the box is not checked, the unit will only perform a DNS lookup for this address at configuration and when you click on **Look up all IP addresses** again.

This feature can only be used when the peers authenticate with X.509 certificates. You can't use this if you want to use a Preshared secret.

## IP Address

Here the IP address of the computer, entered in **DNS Name or IP Address**, is shown. If the peer is a road warrior, only "\*" is shown here. This field is only updated when you click on **Save** or **Look up all IP addresses again**.

### 13.3.6. RADIUS

Select for road warriors whether RADIUS authentication is required for a successful connection. If you want to use RADIUS, you must also configure a RADIUS server on the **RADIUS** page under **Basic Configuration**, and an authentication server on the **Authentication Server** page. If you selected a peer under **Subgroup**, select "-" here.

### 13.3.7. Blacklist

Blacklisting means that if a IPsec connection to a road warrior (marked with "\*" in the **IP address** field) is broken, the unit will block unencrypted traffic to this IP address for a certain time period; the IP address is blacklisted.

The encrypted IPsec connection is established between the road warrior and the unit, though usually the computer you want to connect to isn't the unit, but another computer on a network behind the unit. This computer does not detect the IPsec tunnel, but sends data unencrypted to the road warrior as in any open connection. If the IPsec tunnel is disconnected, the computer on the internal network will not detect this, and keep on sending unencrypted data to the IP address of the road warrior. As the IPsec tunnel no longer exist, the data will be sent unencrypted to the insecure network. Blacklisting prevents this by blocking all packets for a certain time period.

When blacklisting of a connection is possible, an asterisk ("\*") will appear in the **Blacklist** field. The time interval for blacklisting is set on the **IPsec Settings** page.

Blacklisting can produce unwanted effects if a computer allows access from both IPsec clients and unencrypted clients, and where the clients share the same IP address. The effect is that the unencrypted clients can't reach the computer for the blacklisting interval. The chance that this occurs is small, and it is no security threat.

### 13.3.8. ISAKMP Key Lifetime

Here, the lifetime for encryption keys is set. A common value for this parameter is 1 hour (3600 seconds) and the maximum value is 48 hours (172,800 seconds). The time interval must be the same on both computers creating the VPN tunnel.

The length of this time interval is a balance between security and fast data flow. The longer time the same key is used, the more vulnerable the system is for cracking of this key. On the other hand, if the time interval is very short, a high rate of the data traffic is used for negotiating new encryption keys.

Some implementations of IPsec name this parameter **IKE key lifetime**.

### 13.3.9. Initiate Re-keying

Sometimes, an IPsec peer might want to always start the key renegotiation. Some types of IPsec clients do not support that the peer initiates a renegotiation, but must always initiate themselves. Normally, you cannot predict which end of the IPsec connection will start, as the timeout for when to start the renegotiation has an element of randomness included.

If **Initiate Re-keying** is On, the unit will start renegotiate whenever the keys are getting obsolete.

If **Initiate Re-keying** is Off, the unit will never start renegotiate keys if it was the responder in the initial negotiation (like when it is connected to a Road Warrior), but only wait for the peer to start. If it was the initiator, it will start renegotiate if there has been traffic sent through the IPsec connection recently. If there has been no recent traffic, it will wait for the peer to start.

### 13.3.10. IKEv2

This setting specifies how the IKE protocol version 2 is handled. Select **Allow** if you want to allow IKEv1 but use IKEv2 if the other end wants to use it. **Suggest** will allow IKEv2 and use it as default over IKEv1. Use **Force** to allow IKEv2 but not IKEv1. **Disallow** will allow IKEv1 but not allow IKEv2.

### 13.3.11. Encryption

Select which encryption algorithms the unit should propose or accept in phase 1. Select from the definitions made on the **IPsec Cryptos** page.

### 13.3.12. Authentication

#### Type

You can select **Preshared secret**, **X.509 certificate**, **Trusted CA, with DN**, **Trusted CA** or **XAUTH+PSK** as the **Authentication type**. All except Preshared secret and XAUTH+PSK are different ways of using X.509 certificates. Road warriors, and peers whose IP addresses are looked up dynamically, must not use **Preshared secret**. If you selected a **Subgroup**, you should select "-" here.

If X.509 certificates are used, the unit must also have a certificate of its own. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

**Preshared secret** is like a password which the IPsec peer and the unit use to recognize each other.

**XAUTH+PSK** is Extended Authentication and a preshared secret. Users will authenticate with a preshared secret, a username and a password.

**X.509 certificate** is an ordered list of details about the computer, digitally signed to ensure the authenticity of the information.

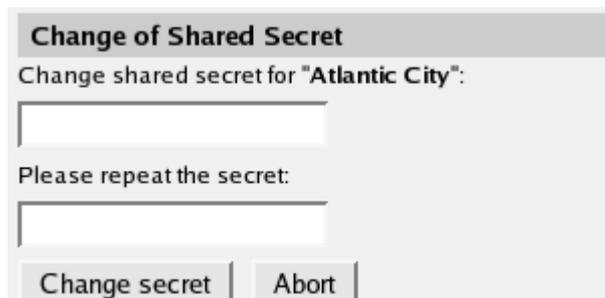
If **Trusted CA, with DN** was selected, the client is expected to authenticate using an X.509 certificate signed by a CA of which the unit knows (the CA certificate should be uploaded on the **Certificates** page and listed on the **IPsec Certificates** page). You must also enter the client's Distinguished Name (DN) here.

If **Trusted CA** was selected, the client is expected to authenticate using an X.509 certificate signed by a CA of which the unit knows (the CA certificate should be uploaded on the **Certificates** page). On the **IPsec Certificates** page, all certificates for trusted VPN CA should be listed.

## Info

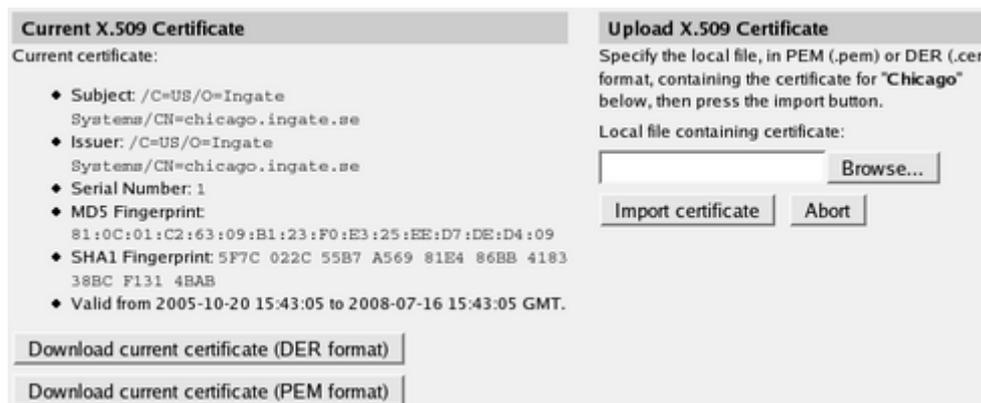
Here, you enter the information the unit should use to identify the IPsec peer. Press the **Change/view** button to insert the information. The look of the form appearing when you press the button depends on which **Authentication type** you selected.

If you selected **Preshared secret** or XAUTH+PSK, you will see a simple form where you enter the secret twice. As the secret is like a password or an encryption key, it is important that it is kept a secret. If an eavesdropper gets your secret, he can easily decrypt all your traffic encrypted with the help of this secret.



As the secret is saved unencrypted in the unit configuration, you should be careful with where you store the configuration.

If you selected **X.509 certificate**, you will see a form where you upload the public certificate of the IPsec peer. If the peer is another Ingate unit, you get its public certificate by downloading it on the **IPsec Certificates** page for that unit.



If you selected **Trusted CA, with DN**, you will see a form where you enter the Distinguished Name (DN) in LDAP format of the client certificate. You can use the wildcard "\*" for one or more RDNs.

You must enter all RDNs of the client certificate which are supported by the unit. The following RDNs are supported:

C	Country code
CN	Common Name

D	Description
DC	Domain Component
E	E-mail
GN	Given name
I	Initials
ID	X.500 Unique Identifier
L	Locality or town
N	Name
O	Organisation
OU	Organisational Unit
SN	Surname
SERIALNUMBER	Serial Number
ST	State or province
T	Personal title
UID	User ID

**Enter Distinguished Name**

Specify the Distinguished Name of the peer certificate(s) for "Juliet" below, in LDAP format, then press the Change button.

Distinguished Name:

If you selected **Trusted CA**, select one of the CAs whose certificates were imported on the **Certificates** page. You can also select "-", which means that the client certificate could be signed by any of the trusted CAs.

Authentication	
Type	Info
Trusted CA ▼	Main CA ▼

### 13.3.13. Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

### 13.3.14. Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 13.3.15. Save

Saves the IPsec Peers configuration to the preliminary configuration.

### 13.3.16. Undo

Clears and resets all fields in new rows and resets changes in old rows.

### 13.3.17. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 13.4. IPsec Tunnels

Here, you specify which networks and computers should use the IPsec connection. Several networks can use the same IPsec connection.

You must enter the networks here, even if you just configure the unit for a road warrior. See also **Remote network**.

These settings are called *Phase 2 settings* in some other IPsec products.

If you want to use the SIP functions in the unit through an IPsec connection, you must add a line with Local side address (the one entered as the **Local Side** on the **IPsec Peers** page) as the **Local Network** for each of the remote networks for this IPsec connection (IPsec peer).

### 13.4.1. IPsec Tunnels

Here, you enter the remote networks which are allowed to use an IPsec connection, and which local networks they can access via the connection.

IPsec Peers **IPsec Tunnels** IPsec Cryptos IPsec Certificates IPsec Settings Authentication Server IPsec Status PPTP Status

**IPsec Tunnels** [\(Help\)](#)  
 These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Atlantic City	Network	DMZ network	-	Network	Atlantic network	1800	AES,3DES	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>		Network	Home network	-	Network	Atlantic network	1800	AES,3DES	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>	+ Boston	Network	Home network	Outside (193.12.253.115)	Network	Boston side		AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>	+ Juliet	Network	Home network	-	Remote/private address	-	300	AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>	+ Offices	Network	Home network	-	Network	Chicago network	1800	AES,3DES	Off	<input type="checkbox"/>
<input type="checkbox"/>		Network	Home network	-	Network	Chicago network	1800	AES,3DES	Off	<input type="checkbox"/>

Add new rows | 1 groups with 1 rows per group.

## Peer

Select an IPsec tunnel from the list of defined **IPsec Peers**.

If you want several networks to share the same IPsec tunnel, you add new rows by clicking the plus sign to the left of the network name.

## Local Network

### *Address Type*

Here, you select if the IPsec tunnel to this peer should be used by the unit itself, or by a network behind it. **Local side address** means that the IP address selected under **Local side** on the **IPsec Peers** page is the only local address that can be reached through this tunnel. If **Network** is selected, a network behind the unit can use the tunnel.

### *Network*

If **Network** was selected in the previous field, you must also select a network here. Select from the networks defined in the **IPsec Networks** table below.

### *NAT as*

If the network behind the other VPN gateway is the same as the local network, you will need to perform NAT for traffic between these networks. Select here which IP address to use when NATting the traffic.

If no IP address is selected, NAT is not performed for this traffic.

## Remote Network

### *Address Type*

Here, you select the type of network that is found on the other side of this IPsec tunnel. This is the network that can be reached through the tunnel, and which can reach the Local network.

The following options exist:

- **Network.** Behind the IPsec peer there is a network which is supposed to use the IPsec tunnel. This could be an office network behind a firewall.

For this choice, you must also select a network in the next field.

- **Network, allow subset.** Behind the IPsec peer there is an IPsec client using a dynamic IP address, and the network of this IP address is known to you. Allow subset means that the unit will accept IPsec negotiations for the entire given network or parts of it.

This is also what to select if you have a NATed IPsec client which is always located on the same IP network.

For this choice, you must also select a network in the next field.

- **Remote side address.** The IPsec peer itself will use the tunnel, but there is no network behind it allowed to access the tunnel. This could be a road warrior which always has a public IP address.

- **Any private address.** The IPsec peer is a NATed road warrior. Note: this option only works when the peer client is NATed, and its IP is a private address. If it is sometimes not NATed, **Remote/private address** should be used instead. If the NATed address is not in one of the private IP address spans, **Network, allow subset** should be used.
- **Remote/private address.** The IPsec peer is a road warrior which sometimes has a public IP address and sometimes a NATed private IP address.

## Network

If **Network** or **Network, allow subset** was selected in the previous field, you must also select a network here. Select from the networks defined in the **IPsec Networks** table below.

If the traffic is NATed, the Remote network must be an IP address of the remote gateway - not the remote network that is the same as the local network.

## IPsec Key Lifetime

The time interval between IPsec key expirations. This field can be empty. Recommended values are 5 minutes for road warriors and 8 hours for networks with fixed IP addresses. If you have many road warriors (a hundred or more), the key lifetime should be increased. Usually, moderately small values should be used for road warriors, making it easier for the unit to detect a broken connection.

The time interval must be the same on both computers creating the IPsec tunnel.

## Encryption

Select which encryptions to use for the data traffic through the IPsec tunnel. The recommended action is to encrypt the traffic. The key negotiations are encrypted regardless of what is selected here.

The encryption options are defined on the **IPsec Cryptos** page.

## PFS Group

Select if PFS should be proposed in the negotiations, and if so, which PFS group to use.

Regardless of this setting, the unit will always accept PFS proposals (for group 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 23 or 24) from the IPsec peer.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 13.4.2. IPsec Networks

If you selected Network anywhere above, you have to define networks here. These networks are what the unit negotiates when the IPsec connection is made.

IPsec Networks <a href="#">(Help)</a>					
Edit Row	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
<input type="checkbox"/>	Atlantic network	10.20.30.0	10.20.30.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Boston side	13.7.3.22	13.7.3.22	32	<input type="checkbox"/>
<input type="checkbox"/>	Chicago network	192.168.10.0	192.168.10.0	24	<input type="checkbox"/>
<input type="checkbox"/>	DMZ network	172.16.0.0	172.16.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>

Add new rows  rows.

### Name

Give the network a name. The name could be anything, like Our office or 10.0.0.0/23. The name is only used internally in the unit.

### DNS Name or Network Address

Enter the DNS name or network address for the network which will use the IPsec tunnel.

### Network Address

Shows the IP address of the **DNS Name or Network Address** you entered in the previous field.

### Netmask/Bits

Netmask/Bits is the mask that will be used to specify this network.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 13.4.3. Save

Saves the IPsec Tunnels configuration to the preliminary configuration.

## 13.4.4. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 13.4.5. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 13.5. IPsec Advanced

Here you can define advanced settings related to IPsec.

### 13.5.1. IPsec Peers

Here you find advanced settings for **IPsec Peers**.

Peer	NAT Traversal	Dead Peer Detection				Mode Configuration	Local ID		Remote ID		IKEv2 ESN	Delete Row
		Enabled	Delay	Timeout	Action		Type	Value	Type	Value		
igtest	Auto	No	30	120	Hold	IP Address	10.48.28.230	-		No	<input type="checkbox"/>	

Add new rows  rows.

#### Peer

The peer for which the advanced settings applies. An IPsec peer is defined on the **IPsec Peers** page.

#### NAT Traversal

Select *Auto* to detect if NAT-T should be used. Select *Force* to force NAT-T (ESP encapsulated in UDP).

#### Dead Peer Detection

Setting	Description
Enabled	Enable/Disable Dead Peer Detection.
Delay	Delay (in seconds) between DPD keepalives.
Timeout	Timeout (in seconds) before the peer is considered dead.
Action	Action to take when the peer is considered dead.  <i>Hold</i> : Try to re-negotiate the connection if matching traffic arrives. <i>Clear</i> : The connection is closed and no re-negotiation will happen. <i>Restart</i> : The connection will be re-negotiated.

#### Mode Configuration

Select the mode configuration that should apply to clients connecting to the Peer. A Mode

Configuration is created in the table [IKE Mode Configuration \(MODECFG\)](#).

### Local ID

The local id that should be sent when using preshared secret authentication.

Setting	Description
Type	The type of local id. <i>IP Address: An IP address.</i>
Value	The value of the local id. E.g. an IP address.

### Remote ID

The remote id that should be expected when using preshared secret authentication.

Setting	Description
Type	The type of remote id. <i>IP Address: An IP address.</i>
Value	The value of the remote id. E.g. an IP address.

### IKEv2 ESN

If you want to enable IKEv2 Extended Sequence Number (ESN) transforms select *Yes* or *Either*. If either is selected, as an initiator, the responder will make the decision. As a responder, no will be chosen.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

### 13.5.2. Save

Saves the IPsec Advanced configuration to the preliminary configuration.

### 13.5.3. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 13.6. IPsec Cryptos

On this page you define the IPsec crypto options to be selected on the **IPsec Peers** and **IPsec**

Tunnels pages.

### 13.6.1. IKE/ISAKMP (Phase 1) Encryption Proposals

In this table the IPsec proposals for Phase 1 are defined.

IPsec Peers
IPsec Tunnels
IPsec Advanced
IPsec Cryptos
IPsec Certificates
IPsec Settings
Authentication Server
IPsec Status
PPTP
PPTP Status

**IKE/ISAKMP (Phase 1) Encryption Proposals** [\(Help\)](#)

Edit Row	Name	Subno.	Encryption/Authentication	Diffie-Hellman Group	Delete Row
<input type="checkbox"/>	+ AES	1	AES256-SHA256 ▾	MODP2048 (Group 14) ▾	<input type="checkbox"/>
<input type="checkbox"/>		2	AES256-SHA512	MODP2048 (Group 14)	<input type="checkbox"/>
<input type="checkbox"/>		3	AES128-SHA256	MODP2048 (Group 14)	<input type="checkbox"/>
<input type="checkbox"/>		4	AES128-SHA512	MODP2048 (Group 14)	<input type="checkbox"/>
<input type="checkbox"/>	+ AES/3DES	1	AES128-SHA256	MODP2048 (Group 14)	<input type="checkbox"/>
<input type="checkbox"/>		2	AES128-SHA256	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		3	AES128-SHA256	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>		4	AES128-SHA1	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		5	AES128-SHA1	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>		6	AES128-MD5	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		7	AES128-MD5	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>		8	3DES-SHA256	MODP2048 (Group 14)	<input type="checkbox"/>
<input type="checkbox"/>		9	3DES-SHA256	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		10	3DES-SHA256	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>		11	3DES-SHA1	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		12	3DES-SHA1	MODP1024 (Group 2)	<input type="checkbox"/>
<input type="checkbox"/>		13	3DES-MD5	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		14	3DES-MD5	MODP1024 (Group 2)	<input type="checkbox"/>

Add new rows  groups with  rows per group.

**Name**

The name of this encryption option. This name is only used internally in the unit.

**Subno.**

The order of the proposed encryption/authentication algorithms is important, as this shows which preferences the unit has, and should have impact on which option the peer selects.

This field is used to sort rows within the encryption proposal group. The rows are used in the displayed order.

**Encryption/Authentication**

Select an encryption/authentication combination from the ones defined in the **Crypto Definitions**

table.

### Diffie-Hellman Group

Select which Diffie-Hellman group to use for this proposal. Group 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 23 or 24 are supported.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 13.6.2. ESP/IPsec (Phase 2) Encryption Proposals

In this table the IPsec proposals for Phase 2 are defined.

ESP/IPsec (Phase 2) Encryption Proposals <a href="#">(Help)</a>				
Edit Row	Name	Subno.	Encryption/Authentication	Delete Row
<input type="checkbox"/>	+ AES	1	AES128-SHA256	<input type="checkbox"/>
<input type="checkbox"/>		2	AES128-SHA512	<input type="checkbox"/>
<input type="checkbox"/>		3	AES256-SHA256	<input type="checkbox"/>
<input type="checkbox"/>		4	AES256-SHA512	<input type="checkbox"/>
<input type="checkbox"/>	+ AES/3DES	1	AES128-SHA256	<input type="checkbox"/>
<input type="checkbox"/>		2	AES128-SHA1	<input type="checkbox"/>
<input type="checkbox"/>		3	AES128-MD5	<input type="checkbox"/>
<input type="checkbox"/>		4	3DES-SHA256	<input type="checkbox"/>
<input type="checkbox"/>		5	3DES-SHA1	<input type="checkbox"/>
<input type="checkbox"/>		6	3DES-MD5	<input type="checkbox"/>

Add new rows  groups with  rows per group.

### Name

The name of this encryption option. This name is only used internally in the unit.

### Subno.

The order of the proposed encryption/authentication algorithms is important, as this shows which preferences the unit has, and should have impact on which option the peer selects.

This field is used to sort rows within the encryption proposal group. The rows are used in the displayed order.

## Encryption/Authentication

Select an encryption/authentication combination from the ones defined in the **Crypto Definitions** table.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

## 13.6.3. Crypto Definitions

In this table the encryption/authentication combinations to be used in the **IKE/ISAKMP (Phase 1) Encryption Proposals** and **ESP/IPsec (Phase 2) Encryption Proposals** tables are defined.

<b>Crypto Definitions</b> <a href="#">(Help)</a>				
Edit Row	Name	Encryption	Authentication Hash	Delete Row
<input type="checkbox"/>	3DES-MD5	3DES	MD5	<input type="checkbox"/>
<input type="checkbox"/>	3DES-SHA1	3DES	SHA1	<input type="checkbox"/>
<input type="checkbox"/>	3DES-SHA256	3DES	SHA2(256)	<input type="checkbox"/>
<input type="checkbox"/>	3DES-SHA512	3DES	SHA2(512)	<input type="checkbox"/>
<input type="checkbox"/>	AES128-MD5	AES(128)	MD5	<input type="checkbox"/>
<input type="checkbox"/>	AES128-SHA1	AES(128)	SHA1	<input type="checkbox"/>
<input type="checkbox"/>	AES128-SHA256	AES(128)	SHA2(256)	<input type="checkbox"/>
<input type="checkbox"/>	AES128-SHA512	AES(128)	SHA2(512)	<input type="checkbox"/>
<input type="checkbox"/>	AES192-MD5	AES(192)	MD5	<input type="checkbox"/>
<input type="checkbox"/>	AES192-SHA1	AES(192)	SHA1	<input type="checkbox"/>
<input type="checkbox"/>	AES192-SHA256	AES(192)	SHA2(256)	<input type="checkbox"/>
<input type="checkbox"/>	AES192-SHA512	AES(192)	SHA2(512)	<input type="checkbox"/>
<input type="checkbox"/>	AES256-MD5	AES(256)	MD5	<input type="checkbox"/>
<input type="checkbox"/>	AES256-SHA1	AES(256)	SHA1	<input type="checkbox"/>
<input type="checkbox"/>	AES256-SHA256	AES(256)	SHA2(256)	<input type="checkbox"/>
<input type="checkbox"/>	AES256-SHA512	AES(256)	SHA2(512)	<input type="checkbox"/>

Add new rows  rows.

### Name

The name of this combination.

## Encryption

Select an encryption algorithm.

## Authentication Hash

Select an authentication algorithm. Currently, SHA-1, SHA2-256, SHA2-512 and MD5 are supported.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new groups and rows you want to add to the table, and then click on **Add new rows**.

### 13.6.4. Save

Saves the IPsec Cryptos configuration to the preliminary configuration.

### 13.6.5. Undo

Clears and resets all fields in new rows and resets changes in old rows.

### 13.6.6. Look up all IP addresses again

Looks up the IP addresses for all DNS names on this page in the DNS servers you entered on the **Basic Configuration** page.

This button will only be visible if a DNS server has been configured.

## 13.7. IPsec Certificates

When X.509 certificates are used to establish the identity of a remote IPsec peer, the unit must also have an X.509 certificate itself. The same certificate is used for all peers. Here you select what certificate to use. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

IPsec Peers	IPsec Tunnels	IPsec Cryptos	<b>IPsec Certificates</b>	IPsec Settings	Authentication Server	IPsec Status	PPTP	PPTP Status
-------------	---------------	---------------	---------------------------	----------------	-----------------------	--------------	------	-------------

<b>Local X.509 Certificate</b> <a href="#">(Help)</a>	<b>IPsec CA Certificates</b> <a href="#">(Help)</a>						
Use this certificate for IPsec:							
<input type="text" value="VPN cert"/>	<table border="1"><tr><td><b>Edit Row</b></td><td><b>CA</b></td><td><b>Delete Row</b></td></tr><tr><td><input type="checkbox"/></td><td>Main CA</td><td><input type="checkbox"/></td></tr></table>	<b>Edit Row</b>	<b>CA</b>	<b>Delete Row</b>	<input type="checkbox"/>	Main CA	<input type="checkbox"/>
<b>Edit Row</b>	<b>CA</b>	<b>Delete Row</b>					
<input type="checkbox"/>	Main CA	<input type="checkbox"/>					
<b>Add new rows</b>	<input type="text" value="1"/> rows.						

### 13.7.1. Local X.509 Certificate

Select which of the unit certificates to use for IPsec authentication. The same certificate is used for all peers.

### 13.7.2. CA Certificates

You can select to trust peer certificates signed by trusted CA servers. List the trusted CAs here. This is required if you want to use Trusted CA or Trusted CA, with DN as authentication types.

#### CA

Select a CA from which the unit should accept connections. The CA certificates are imported on the **Certificates** page.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 13.7.3. Save

Saves all IPsec Certificates configuration to the preliminary configuration.

### 13.7.4. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 13.8. IPsec Settings

When IPsec VPN is used, additional settings are needed. You can make settings for the blacklist function, NAT-T and various log events.

### 13.8.1. Local Extended Authentication Database

Here you add local users available for extended authentication (XAUTH).

**Local Extended Authentication Database** [\(Help\)](#)

Here you add local users available for extended authentication (XAUTH).

Username	Password	Peer	Enabled	Delete Row
alice	<a href="#">Change Password</a>	RemoteWorkers ▼	Yes ▼	<input type="checkbox"/>
john	<a href="#">Change Password</a>	RemoteWorkers ▼	Yes ▼	<input type="checkbox"/>

[Add new rows](#)  rows.

## Username

The authentication name for the user.

## Password

The password for the user.

## Peer

The IPsec peer that the user should be available for. If "-" is chosen the user will be available to all peers configured for extended authentication.

## Enabled

Select if the user should be able to log in or not.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 13.8.2. IKE Mode Configuration (MODECFG)

Here you add settings for client configuration via IKE Mode Configuration.

IKE Mode Configuration (MODECFG) <a href="#">(Help)</a>								
Here you add settings for client configuration via IKE Mode Configuration.								
Name	IP Range	DNS 1		DNS 2		Domain	Banner	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address			
RemoteConfig	RemotePool ▾	10.10.10.5	10.10.10.5					<input type="checkbox"/>

Add new rows  rows.

## Name

The name for the setting. The name is referenced in the table **IPsec Peers** in the tab [IPsec Advanced](#).

## IP Range

The address pool from which the clients are assigned addresses. A range is created on the page [Networks and Computers](#).

## DNS 1

The first DNS server that should be assigned to clients.

## DNS 2

The second DNS server that should be assigned to clients.

## Domain

The domain that should be assigned to clients.

## Banner

The banner that should be shown to clients.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

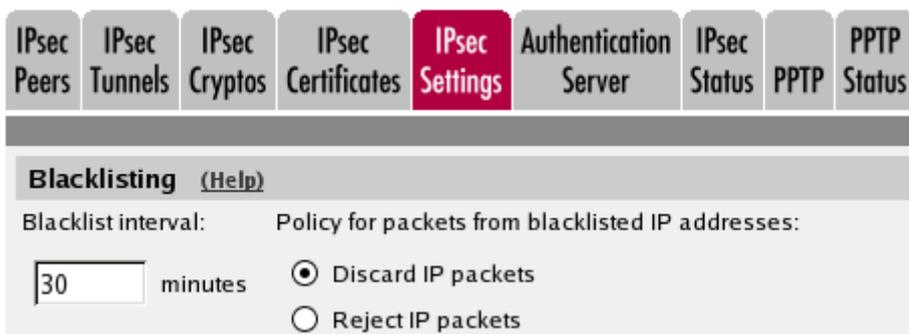
## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 13.8.3. Blacklisting

When a road warrior disconnects, its IP address will be blacklisted for a while. Here, you specify the time interval for the blacklisting and what to do with the blocked packets.

You can read more about blacklisting in the [IPsec Peers](#) section.



The screenshot shows a navigation bar with tabs: IPsec Peers, IPsec Tunnels, IPsec Cryptos, IPsec Certificates, IPsec Settings (selected), Authentication Server, IPsec Status, PPTP, and PPTP Status. Below the navigation bar is a section titled "Blacklisting (Help)". Under "Blacklist interval:", there is a text input field containing "30" followed by "minutes". Under "Policy for packets from blacklisted IP addresses:", there are two radio button options: "Discard IP packets" (which is selected) and "Reject IP packets".

#### Blacklist interval

Specify the time interval (in minutes) for the blacklisting of an IP address.

#### Policy for packets from blacklisted IP addresses

When an IP address is blacklisted, all packets to and from this address (except for new tunnel negotiations) are blocked. Here, you specify whether they should be rejected or discarded. **Discard IP packets** means that the unit ignores the IP packets without replying that the packet did not arrive. **Reject IP** packets makes the unit reply with an ICMP packet telling that the packet did not arrive.

### 13.8.4. NAT Traversal (NAT-T)

The unit supports IPsec NAT-T as defined in the Internet-Drafts [ietf-ipsec-nat-t-ike](#) and [ietf-ipsec-](#)

udp-encaps.

NAT-T means that IPsec uses UDP ports 500 and 4500, instead of UDP port 500 and the ESP protocol. This makes it possible for NAT-T capable IPsec peers to connect to the unit even if they are located behind a non-IPsec-aware NAT device. It also makes it possible for the unit to connect to NAT-T capable peers if it is itself located behind such a NAT device. This also means that the unit's UDP ports 500 and 4500 are blocked from other use.

When the unit is located behind a NAT device, it sends keep alive packets to maintain the connection. You can also force it to send keep alive packets for all NAT-T connections.

**NAT Traversal (NAT-T) [\(Help\)](#)**

Keep alive interval:

seconds

### Keep alive interval

Enter the time interval (in seconds) the unit should use when sending keep alive packets.

### Interoperability

Enable Preshared secret authentication for Road Warriors in order to authenticate multiple IPsec clients with the same secret. Notice that the use of this setting incorporates security risks, and its use should be avoided.

**Interoperability [\(Help\)](#)**

Enable Preshared secret authentication for Road Warriors:

Yes  No

### 13.8.5. Logging

The unit generates log messages for different events and for the traffic that arrives at the unit. By selecting proper log classes, you can instruct the unit how it should handle these messages.

The same settings can also be found on the **Logging Configuration** page under **Logging and Tools**.

**Logging [\(Help\)](#)**

Log class for IPsec key negotiations:	Log class for IKE and NAT-T packets:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for IPsec key negotiation debug messages:	Log class for IPsec user authentications:
<input type="text" value="-"/>	<input type="text" value="Local"/>
Log class for ESP packets:	Log class for blacklisting events:
<input type="text" value="-"/>	<input type="text" value="Local"/>
Log class for packets to and from blacklisted IP addresses:	
<input type="text" value="Local"/>	

### **Log class for IPsec key negotiations**

Here, you set the log class for new negotiations of IPsec connection keys.

### **Log class for IPsec key negotiation debug messages**

Here, you set the log class for debug information about negotiations of IPsec connection keys.

### **Log class for ESP packets**

Specify what log class the unit should use for encrypted packets (ESP packets to the unit). Logging of encrypted packets will generate a lot of log events.

### **Log class for packets to and from blacklisted IP addresses**

Here, you set the log class for the packets that are rejected or discarded according to the blacklisting policy selected above.

### **Log class for IKE and NAT-T packets**

Here, you set the log class for the packets used for IKE key negotiations and for NAT-T packets. As they both use the same port on the unit, it will log both using the same log class.

### **Log class for IPsec user authentications**

Here, you set the log class for unit messages about road warrior authentications via RADIUS and their disconnections.

### **Log class for blacklisting events**

Here, you specify how the unit should report beginnings and ends of blacklisting events.

## **13.8.6. Save**

Saves the IPsec Settings configuration to the preliminary configuration.

## **13.8.7. Undo**

Reverts all of the above fields to their previous configuration.

# **13.9. Authentication Server**

When a Road Warrior IPsec client that requires RADIUS authentication establishes an IPsec tunnel to the unit, it only gets access to an authentication server in the unit. The user must connect to it (using a web browser) and authenticate himself. Once that is done, rules and relays are set up properly.

This means that there must be a row in the **IPsec Tunnels** table containing the authentication server on the **Local side**, or the RADIUS authentication won't work.

When you want to disconnect, you should log out from the authentication server using the web browser. This will create a blacklisting of this IP address, which means that you will not be able to contact the unit during the blacklist period. A result of the blacklist is that you will not receive any **Logout succeeded** message when the **Log out** button is pressed, since the unit is blocking all traffic to the client.

If you do not log out, only disconnect, the unit eventually will detect that the IPsec client is unreachable. The user is then logged off. This is done when the unit tries to negotiate a new IPsec key. The IPsec key lifetime should be rather short because of this.

IP Address	Port	Cert	TLS	Delete Row
eth0 (10.48.28.61) ▾	443	MyCert ▾	TLSv1.x ▾	<input type="checkbox"/>

Add new rows  rows.

### 13.9.1. Authentication Server

Select the IP address and port that the IPsec users should use to identify themselves for the RADIUS server. You cannot select the same combination of IP address and port as is used for configuring the unit.

#### IP Address

The IP address to listen on.

#### Port

The port to listen on.

#### Cert

The authentication server is contacted via HTTPS (HTTP over TLS). To use TLS, the server must have an X.509 certificate, which works as an ID card, identifying the server to your web browser. This will ensure that you are really communicating with your server and not somebody else's computer. TLS uses an encryption method using two keys, one secret and one public. The secret key is kept in the server and the public key is used in the certificate. If any of the keys are changed, the TLS connection won't work.

Select which of the unit certificates to use for road warrior RADIUS authentication. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

#### TLS

The TLS protocol to use.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 13.9.2. Save

Saves the Authentication Server configuration to the preliminary configuration.

## 13.9.3. Undo

Reverts all of the above fields to their previous configuration.

# 13.10. IPsec Status

Here, status for the IPsec connections is shown. The unit shows active blacklistings and the status for configured IPsec tunnels.

## 13.10.1. Current Blacklistings

IPsec Peers	IPsec Tunnels	IPsec Cryptos	IPsec Certificates	IPsec Settings	Authentication Server	IPsec Status	PPTP	PPTP Status
<b>Current Blacklistings</b>								
No IP addresses are blacklisted at the moment.								

Here a list of current blacklistings is shown. You can select to end a blacklisting by selecting the button **Remove** in the **Remove blacklisting** column.

## 13.10.2. IPsec Tunnel Status

Here, the IPsec tunnels configured for this unit are shown. You can see the status for the tunnels or renegotiate tunnels for a peer.

The unit considers the tunnel down if no SA has been negotiated, if the SA expired without successful renegotiation, or if one of the tunnel endpoints requested that the tunnel should be torn down.

IPsec Tunnel Status						
Peer Name	Peer IP Address	Renegotiate	Local Net	Remote Net	Tunnel Status	Certificate Subject
t1	3.1.1.3:500	<input type="checkbox"/>			ISAKMP is down	
			193.180.23.0/24	10.1.1.0/24	IPsec is down	
t2	3.1.1.3:500	<input type="checkbox"/>			ISAKMP is down	
			193.180.23.0/24	10.1.1.0/24	IPsec is down	

Renegotiate IPsec tunnels

### Peer name

Peer name, configured on the **IPsec Peers** page.

### Peer IP address

The IP address used by the peer when connecting to the unit.

### Renegotiate IPsec tunnels

Press this button to renegotiate all IPsec tunnels for this peer.

### Local net

The local network for this IPsec tunnel.

### Remote net

The remote network for this IPsec tunnel

### Tunnel status

Here, the status for the connection is shown. On the Peer line, status for the ISAKMP SA is shown. Each IPsec tunnel line shows status for that tunnel.

### Certificate subject

If a certificate is used for authentication, this field shows for whom it was issued.

## 13.10.3. Forbidden Private Addresses for Road Warriors

Forbidden means that they are directly connected, configured as a static route, an explicit remote IPsec network, or the dedicated failover network. If your Road Warriors cannot connect beyond Phase 1, and receive errors regarding private or virtual IPs, it is likely due to its address belonging to a range in this table.

## Forbidden Private Addresses for Road Warriors [\(Help\)](#)

Forbidden means that they are directly connected, configured as a static route, an explicit remote IPsec network, or the dedicated failover network.

Network Address	Netmask / Bits
10.48.0.0	16
192.168.100.0	24
192.168.200.0	24
2001:678:5d8:1000::	64
fec0::	64
fec3::	64

## 13.11. PPTP

PPTP (Point-to-Point Tunneling Protocol) is one way of setting up a virtual private network (VPN). It originates from the PPP protocol, which was meant to be used between two end peers, but the PPTP is constructed for connections between a road warrior and a VPN gateway.

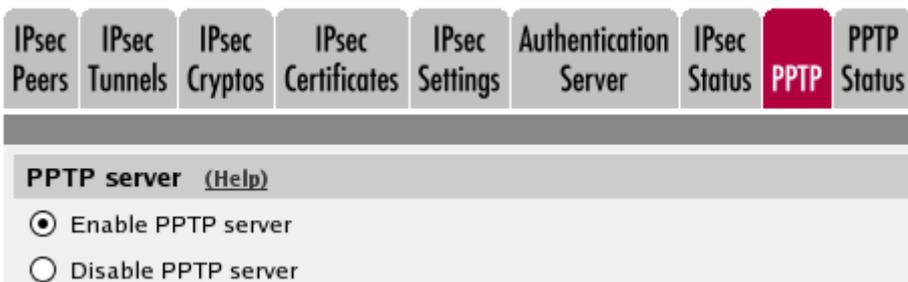
In the unit, you can accept connections over PPTP from a road warrior. To other internal computers, this traffic will appear to originate from the internal network configured below.

The unit supports:

- up to 100 simultaneous PPTP client connections
- **only** 128bit MPPE encryption
- only MSCHAPv2 authentication

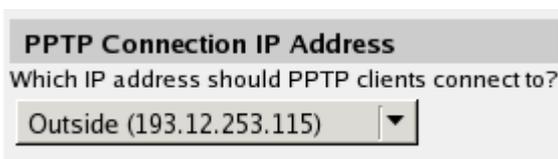
To actually permit traffic coming through the connection, into your networks you also have to create rules for the connections on the **Rules** page under **Rules and Relays**. The rules should be for the network selected under Client IP addresses.

### 13.11.1. PPTP server



Select here if the PPTP server should be **On** or **Off**. When the server is on, the unit listens for connection attempts over TCP on port 1723. This will block this port from other use.

### 13.11.2. PPTP Connection IP Address



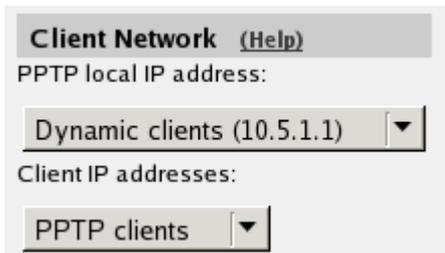
Select one of the unit's IP addresses (defined on the interface pages under **Network**. This is the IP

address to which the PPTP clients should direct their connections.

### 13.11.3. Client Network

You must assign a network to the connected PPTP clients. When a client connects, it will be assigned an IP address on the selected network. The clients must also have an endpoint to the tunnel, which is a unit IP address on the same directly connected network as the assigned PPTP network.

If all IP addresses assigned for PPTP clients are already used when yet another user tries to connect, that connection attempt will fail until an IP address is released by another user.



#### PPTP local IP address

Select one of the unit's IP addresses, which will act as an endpoint for the PPTP tunnel.

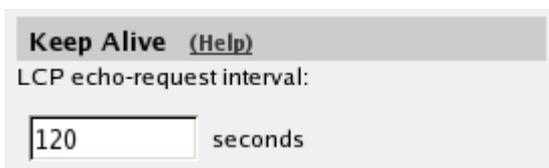
#### Client IP addresses

Select a network from which the PPTP clients will be assigned IP addresses for local usage. You select from the networks configured on the **Networks and Computers** page under **Network**. The network must not contain more than 100 IP addresses, which must be part of the same directly connected network as the **PPTP local IP** selected above.

### 13.11.4. Keep Alive

The unit can be made to send packets to the PPTP clients to check the PPTP connection. When a client has not responded to three consecutive packets, the connection is considered broken and the PPTP tunnel is removed.

The unit uses LCP echo request packets for this. If you want to disable this feature, just leave the input field blank.



#### LCP echo request interval

Enter the interval with which the unit should send LCP echo request packets to check PPTP connections. If you want to disable this feature, just leave the input field blank.

### 13.11.5. Client Parameters

You can give the connected clients information about what DNS and/or WINS servers to use when accessing computers on the local network.

DNS Servers <a href="#">(Help)</a>		WINS Servers <a href="#">(Help)</a>	
Primary DNS:		Primary WINS:	
DNS name or IP address	IP address	DNS name or IP address	IP address
<input type="text" value="10.7.0.7"/>	10.7.0.7	<input type="text" value="10.7.0.9"/>	10.7.0.9
Secondary DNS:		Secondary WINS:	
DNS name or IP address	IP address	DNS name or IP address	IP address
<input type="text"/>		<input type="text" value="10.7.0.12"/>	10.7.0.12

#### DNS Servers

One or two DNS servers can be specified, which the clients can use to look up domain names.

#### WINS Servers

One or two WINS servers can be specified, which the clients can use to access Windows computers.

### 13.11.6. PPTP Users

Specify which users can connect to the unit using PPTP.

PPTP Users <a href="#">(Help)</a>				
Edit Row	User	Password	Enabled	Delete Row
<input type="checkbox"/>	bob		Yes	<input type="checkbox"/>
<input type="checkbox"/>	cindy		Yes	<input type="checkbox"/>
<input type="checkbox"/>	fred		Yes	<input type="checkbox"/>
<input type="checkbox"/>	lucy		Yes	<input type="checkbox"/>
<input type="checkbox"/>	minnie		Yes	<input type="checkbox"/>
<input type="checkbox"/>	steve		Yes	<input type="checkbox"/>

rows.

#### User

Enter the name of the user which can connect.

#### Password

Each user must authenticate himself with a password. Press **Change** to enter the password for this user.

## Enabled

Select if PPTP connections with this user should be enabled (**On**) or not (**Off**).

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

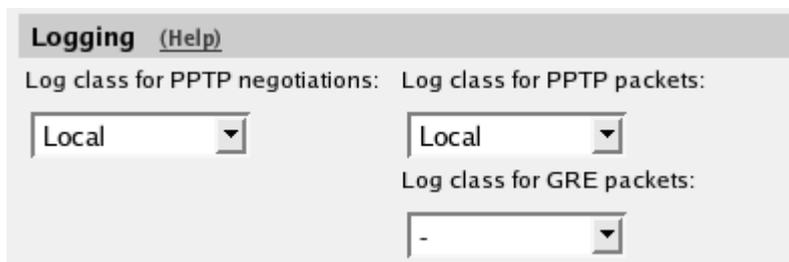
## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 13.11.7. Logging

Select here how the negotiation and tunnel traffic should be logged. Choose between the log classes configured on the **Log Classes** page under **Logging and Tools**.

The same settings can also be found on the **Logging Configuration** page under **Logging and Tools**.



The screenshot shows a configuration window titled "Logging (Help)". It contains three dropdown menus for selecting log classes. The first two are labeled "Log class for PPTP negotiations:" and "Log class for PPTP packets:", both with "Local" selected. The third is labeled "Log class for GRE packets:" with "-" selected.

### Log class for PPTP negotiations

The unit generates log messages about the progress of the PPTP negotiations. Here, you select a log class for these messages.

### Log class for PPTP packets

PPTP clients wanting to establish a VPN tunnel connects to the unit on port 1723. Here, you select a log class for these packets.

### Log class for GRE packets

The encrypted traffic through the VPN tunnel is sent as GRE packets. Here, you select a log class for these packets.

## 13.11.8. Save

Saves the PPTP configuration to the preliminary configuration.

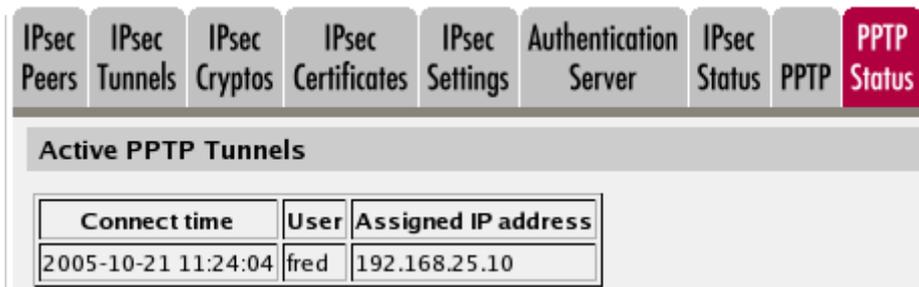
## 13.11.9. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 13.12. PPTP Status

On this page, you can view information about active PPTP connections to the unit.

### 13.12.1. Active PPTP tunnels



The screenshot shows a navigation menu with the following items: IPsec Peers, IPsec Tunnels, IPsec Cryptos, IPsec Certificates, IPsec Settings, Authentication Server, IPsec Status, PPTP, and PPTP Status (highlighted in red). Below the menu is a section titled "Active PPTP Tunnels" containing a table with the following data:

Connect time	User	Assigned IP address
2005-10-21 11:24:04	fred	192.168.25.10

#### Connect Time

The time when the user connected to the unit.

#### User

The name of the connected PPTP user.

#### Assigned IP Address

The local IP address the PPTP user was assigned.

# Chapter 14. QoS

## 14.1. Specification of Ingate QoS

The QoS (Quality of Service) extension module enables bandwidth limitation and prioritizing for different kinds of traffic through the unit. You can also set priority bits (TOS or DSCP) in the packets to force prioritisation in the receiving network equipment. For each interface you can state a guaranteed and a maximum bandwidth for the total outgoing traffic of this interface and for classes of traffic. The traffic can be classified on sender, receiver, whether it is SIP traffic or not, DSCP and TOS marking, type of service (e-mail, www, ftp etc) and packet size. You can also prioritize traffic based on the traffic classes.

Normally, DSCP bits get stripped upon traversing interfaces. SIP signalling is received by the unit. Outgoing SIP messages don't always correspond to incoming messages since SIP messages are most often handled state full. For example 100 Trying is sent hop-by-hop, and when using the B2BUA then there are two separate call legs and a reINVITE on one leg doesn't necessarily cause a reINVITE on the other leg.

A service is defined as an IP protocol and, where it is applicable, sender and receiver ports (TCP, UDP) or types (ICMP).

## 14.2. Configuration of QoS

In order to limit or prioritize the traffic, the unit must be able to classify packets. This is done using the traffic classes which you define on the **QoS Classes** page. After that, the bandwidth limitation and prioritizing for outgoing traffic is configured on the interface pages.

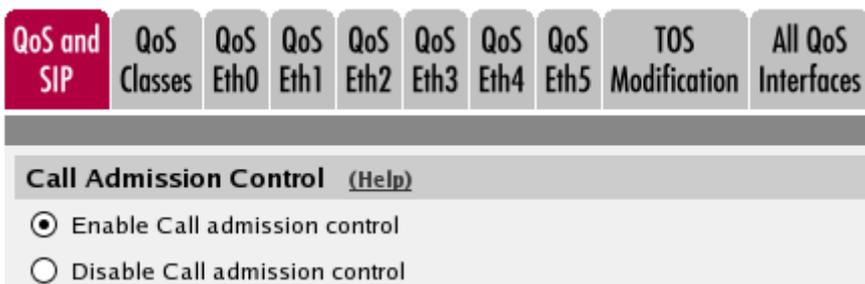
You can also set a priority which receiving network equipment can use. This is configured on the **TOS Modification** page by modifying the TOS or DSCP field of the packet.

## 14.3. QoS and SIP

On this page, you can make the unit reject SIP calls when there is not bandwidth enough to get a good audio and video quality.

If a call is rejected for this reason, the unit sends the response 486 (Busy Here) to the client.

### 14.3.1. Call Admission Control



The screenshot shows a navigation bar with the following items: **QoS and SIP** (highlighted in red), **QoS Classes**, **QoS Eth0**, **QoS Eth1**, **QoS Eth2**, **QoS Eth3**, **QoS Eth4**, **QoS Eth5**, **TOS Modification**, and **All QoS Interfaces**. Below the navigation bar, the page title is **Call Admission Control** with a [\(Help\)](#) link. There are two radio button options:  **Enable Call admission control** and  **Disable Call admission control**.

Select here to turn the call admission on and off.

### 14.3.2. Bandwidths For SIP Media

Enter here reserved bandwidths for SIP media for the different interfaces. The entered values are used when the unit determines if there is enough bandwidth left for a new SIP call.

Bandwidths For SIP Media <a href="#">(Help)</a>				
Interface	Outgoing (kbit/s)		Incoming (kbit/s)	
	Allowed for Media (kbit/s)	Allowed for Emergency (kbit/s)	Allowed for Media (kbit/s)	Allowed for Emergency (kbit/s)
Internal (eth0)	1000		1000	
External (eth1)	600	200	700	
External2 (eth2)				
DHCP clients (eth3)	1500		1500	
SIP-1 (eth4)				
SIP-2 (eth5)				

#### Interface

The interface for which bandwidth limits are set.

#### Outgoing

Enter here the bandwidth that can be used for outgoing SIP media from this interface.

#### Allowed for Media

The **Allowed** bandwidth is the guaranteed bandwidth as well as the limit for outgoing SIP media for the interface. If there is not SIP media to fill that reserve, the bandwidth can be used for other traffic.

#### Allowed for Emergency

The **Emergency** bandwidth is bandwidth that is reserved for calling the **Emergency Number** set on the **Dial Plan** page.

#### Incoming

Enter here the bandwidth that can be used for incoming SIP media to this interface.

#### Allowed for Media

The **Allowed** bandwidth is the guaranteed bandwidth as well as the limit for incoming SIP media for the interface. If there is not SIP media to fill that reserve, the bandwidth can be used for other traffic.

## Allowed for Emergency

The **Emergency** bandwidth is bandwidth that is reserved for calling the **Emergency Number** set on the **Dial Plan** page.

### 14.3.3. Codec Bandwidths

Enter bandwidths used by the various codecs. This will be used by the unit when calculating if there is enough bandwidth left for new calls.

Codec Bandwidths <a href="#">(Help)</a>					
Edit Row	Type	Codec Name	Bandwidth (kbit/s)	Allowed	Delete Row
<input type="checkbox"/>	audio	*	32	Yes	<input type="checkbox"/>
<input type="checkbox"/>	video	*	150	No	<input type="checkbox"/>

Add new rows  rows.

#### Type

Select the codec type. The "-" option will make this row match all media types where the codec name is defined.

#### Codec Name

Enter the name of the codec. The codec name should be entered as it appears in the SDP (like *PCMA* or *G723*).

#### Bandwidth

Enter the bandwidth used by this codec.

#### This Codec Is Allowed

Select **On** to allow the codec and **Off** to block it.

This setting will only be used if **Codec Filtering** is set to **Yes**.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 14.3.4. Codec Filtering

Codec Filtering <a href="#">(Help)</a>	
<input type="radio"/>	Allow all codecs
<input checked="" type="radio"/>	Filter out codecs

Select to let the unit filter certain codecs when forwarding SIP signaling.

### 14.3.5. Save

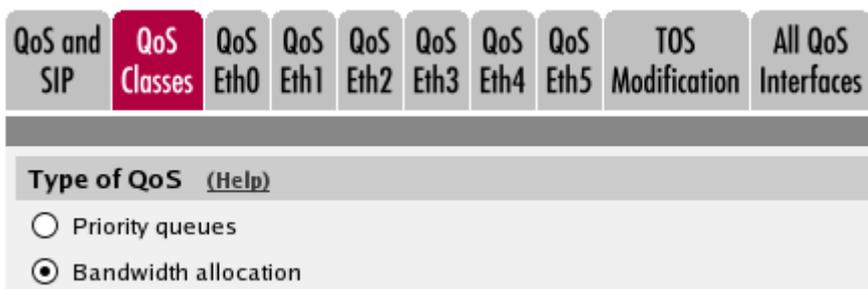
Saves the QoS and SIP configuration to the preliminary configuration.

### 14.3.6. Undo

Reverts all the above fields to their previous configuration.

## 14.4. QoS Classes

### 14.4.1. Type of QoS



Specify which type of QoS you want to use.

Using *Priority queues*, you assign different priority to different types of traffic. Lower priority traffic will be delayed when higher priority traffic fills the bandwidth.

Using *Bandwidth allocation*, you assign guaranteed bandwidth and bandwidth limits for different types of traffic.

### 14.4.2. QoS Classes

Create traffic classes for packets sent through the unit. The classes are used for prioritizing and limiting different types of traffic or traffic from different networks. The traffic can be classified on sender, receiver, type of service (e-mail, www, ftp etc) and packet size.

When determining what class a packet belongs to, the unit reads the table from the top, and uses the first match.

QoS Classes <a href="#">(Help)</a>											
Edit Row	No.	Class Name	Client	Server	Service	SIP	Packet Size (bytes)		TOS Octet		Delete Row
							Min	Max	TOS	DSCP	
<input type="checkbox"/>	1	TCP out	Office network	Internet	tcp	Non-SIP			-		<input type="checkbox"/>
<input type="checkbox"/>	2	UDP DHCP (small packets)	DHCP clients	Internet	udp	Non-SIP	20	300	MR		<input type="checkbox"/>
<input type="checkbox"/>	3	UDP SIP signaling	-	-	udp	Signaling			-		<input type="checkbox"/>

Add new rows  rows.

## No.

This is a number that is used to rank each individual class. To move a class to a certain row, enter the number on the row to which you want to move it. You need only renumber classes that you want to move; other classes are renumbered automatically. When you click on **Save**, the classes are re-sorted. The order of the classes is important. *Classes are used in the order in which they are displayed in the table*; class number 1 is always first.

## Class Name

Enter a name for this class. The name is only used internally in the unit.

## Client

Under **Client**, you can select from defined **Networks and Computers**. The class comprises the traffic from **Client** to **Server**. If you want to define traffic from a VPN tunnel, you must use a client network with the interface "-".

If you want this class to comprise all traffic regardless of origin, select "-" here. If you select SIP signaling in this class, you must select "-" here.

## Server

Under **Server**, you can select from defined **Networks and Computers**. The class comprises the traffic from **Client** to **Server**. Traffic which goes out from the unit through a VPN tunnel is classified before encryption. The encrypted packet then keeps the class which the unencrypted packet had.

If you want this class to comprise all traffic regardless of destination, select "-" here.

## Service

The network service for this class. If the class should comprise all IP traffic for this **Client** and **Server**, select "-" here.

You configure services on the **Services** page under **Rules and Relays**. Examples of services are WWW and telnet.

## SIP

Select whether this class should comprise SIP **Signaling**, SIP **Media** or **Non-SIP** traffic. If you select Signaling or Media, make sure that the **Service** comprises this type of traffic. If you don't want to restrict the services, select "-" as the **Service**.

## Packet Size

Enter the minimum and maximum packet size for this class. This can be useful if you for example want to prioritize smaller packets higher than bigger ones.

Valid values for this field are numbers between 20 and 65535.

## TOS Octet

Select if the class defined here should only match packets which have some kind of priority mark.

Here, packets are only examined to see if the TOS octet already has a certain value. To set the octet to give packets priority in subsequent network equipment, go to the **TOS Modification** page.

## TOS

Select a value for the TOS (Type of Service) field of the packet. Select between **Empty** (no TOS bit set), **MD** (Minimize Delay; the packet is forwarded as quickly as possible), **MT** (Maximize Throughput; data throughput is maximized), and **MR** (Maximize Reliability; data is forwarded as reliably as possible). If the packet should belong to this class regardless of the TOS value, select "-".

For more information about TOS, read RFC 791 & 795.

## DSCP

Enter a value for the DSCP (Differentiated Services CodePoint) field of the packet. DSCP, like TOS, is a standard for telling network equipment how the packet should be treated. The DSCP field has 6 bits, which means that only the numbers 0-63 (inclusive) are valid.

For more information about DSCP, read RFC 2474.

## Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 14.4.3. Save

Saves the QoS Classes configuration to the preliminary configuration. Class numbers are changed if necessary so that the classes end up in the right order and each class receives a unique number.

## 14.4.4. Undo

Clears and resets all fields in new rows and resets changes in old rows.

## 14.5. QoS Interfaces

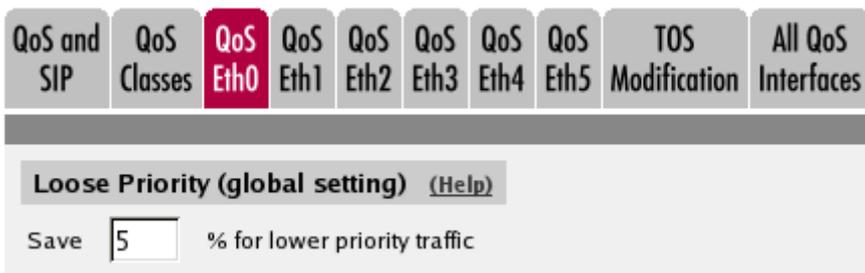
There is a page for each network interface (Eth0, Eth1, ...) on the unit. Select a page to make configuration for that interface. There is also a page where configuration for all interfaces can be viewed and changed.

Here, you make QoS settings for outbound traffic from this interface, such as maximum bandwidth for the interface and how various traffic types should be prioritized.

### 14.5.1. Loose Priority

You can enter bandwidth limits (in kbit/s) for each of the eight priority queues in the unit, where queue number 1 has the highest priority. This can be useful if you don't want to cut off low-priority traffic entirely. If no bandwidth is stated for a priority queue, traffic with lower priority will only be forwarded if there is any bandwidth left when all traffic in this queue has been forwarded.

This setting is *only available* if you selected *Priority queues* as the **Type of QoS**.



You can select to save some bandwidth for lower priority traffic.

This setting is recursive. Example: An interface has a limit of 1000 kbit/s. Traffic on this interface has been given priority levels 1, 2, and 3. If you select to save 5 % for lower priority traffic, the priority 1 traffic will always be able to use up to 95 % of the bandwidth (950 kbit/s). Priority 2 and 3 traffic then has 5 % (50 kbit/s) left to use. From these 50 kbit/s, 95 % (47.5 kbit/s) is allotted to priority 2 traffic, and 5 % (2.5 kbit/s) is left for priority 3 traffic.

This means that traffic with a low priority gets very little bandwidth, but some traffic will always be let through. When there is less higher priority traffic, the traffic with a lower priority will be able to use more bandwidth.

The same setting is used for all interfaces.

Incoming and outgoing traffic can have different QoS configuration.

### 14.5.2. General



## Outgoing/Incoming QoS

Select here to turn QoS **On** or **Off** for outbound/incoming traffic from this interface. If **Off** is selected, no other settings in this column will affect the performance of the unit.

### 14.5.3. Bandwidths

**Bandwidths** [\(Help\)](#)  
Total bandwidth limit:  kbit/s  
Reserved for SIP media: 1000 kbit/s  
Available bandwidth: 5000 kbit/s

#### Total bandwidth limit

You can enter an upper limit (in kbit/s) for the bandwidth of outbound/incoming traffic for this interface. Packets outside this bandwidth limit are discarded.

The lowest limit allowed is 12 kbit/s.

#### Reserved for SIP media

This is the bandwidth reserved on the **QoS and SIP** page.

#### Available bandwidth

This is the bandwidth available when all reserved bandwidth has been subtracted. This bandwidth can be used in the **Classification** and **Unclassified Traffic** tables.

### 14.5.4. Classification

Here you select how this interface should treat packets in different classes.

The table will contain different columns depending on your choice of **Type of QoS** on the **QoS Classes** page.

#### Priority queues

**Classification** [\(Help\)](#)

Edit Row	Class	Priority	Delete Row
<input type="checkbox"/>	UDP SIP signaling	1 (highest)	<input type="checkbox"/>
<input type="checkbox"/>	TCP out	2	<input type="checkbox"/>
<input type="checkbox"/>	UDP DHCP (small packets)	4	<input type="checkbox"/>

Add new rows  rows.

*Class*

Select a class for which to assign a priority. The classes are defined on the **QoS Classes** page.

#### Priority

Select a priority queue for this class. There are eight priority levels, where level 1 has the highest priority.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### Bandwidth allocation

Classification <a href="#">(Help)</a>						
Edit Row	Class	Bandwidth				Delete Row
		Assigned		Max		
		%	kbit/s	%	kbit/s	
<input type="checkbox"/>	UDP SIP signaling	10	220	15	450	<input type="checkbox"/>
<input type="checkbox"/>	TCP out	25	550			<input type="checkbox"/>

rows.

#### Class

Select a class for which to state bandwidth limits. The classes are defined on the **QoS Classes** page.

#### Bandwidth

Enter bandwidth limits (in % of the available bandwidth) for this class. **Guaranteed** bandwidth states a bandwidth which this class is always allowed. This field must not be left empty. The total guaranteed bandwidth for a priority queue (here and for the **Unclassified Traffic**) must not be more than 100 %.

The **Limit** for this class is an upper limit for the bandwidth utilization.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 14.5.5. Unclassified Traffic

Here you state how traffic on this interface should be treated when it is not in any of the classes stated above.

The table will contain different columns depending on your choice of **Type of QoS** on the **QoS**

Classes page.

## Priority queues

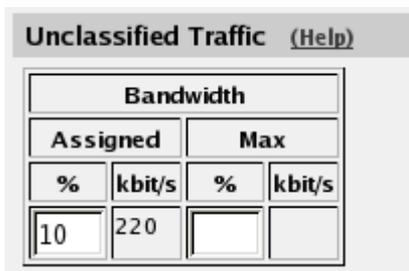


The screenshot shows a configuration window titled "Unclassified Traffic" with a "(Help)" link. Below the title is a "Priority" label above a dropdown menu. The dropdown menu is currently set to the value "2".

### Priority

Select a priority level for the unclassified traffic. There are eight priority levels, where level 1 has the highest priority.

## Bandwidth allocation



The screenshot shows a configuration window titled "Unclassified Traffic" with a "(Help)" link. Below the title is a "Bandwidth" table. The table has two main columns: "Assigned" and "Max". Each of these columns is further divided into two sub-columns: "%" and "kbit/s". The "Assigned" column has a value of "10" in the "%" sub-column and "220" in the "kbit/s" sub-column. The "Max" column has empty fields in both sub-columns.

Bandwidth			
Assigned		Max	
%	kbit/s	%	kbit/s
10	220		

### Bandwidth

Enter bandwidth limits (in % of available bandwidth) for the unclassified traffic. **Guaranteed** bandwidth states a bandwidth which the traffic is always allowed. This field must not be left empty. The total guaranteed bandwidth for a priority queue (here and under **Classification**) must not be more than 100 %.

The **Limit** for the unclassified traffic is an upper limit for the bandwidth utilization.

## 14.5.6. Save

Saves all Interface configuration to the preliminary configuration.

## 14.5.7. Undo

Clears and resets all fields in new rows and resets changes in old rows.

# 14.6. TOS Modification

On this page, you can set the TOS or DSCP value for outgoing packets in a class.

## 14.6.1. TOS/DSCP Modification

TOS (Type of Service) and DSCP (Differentiated Service CodePoint) are two ways of telling network equipment how to treat and prioritize packets. TOS and DSCP are two different standards and cannot be used simultaneously.

For more information about TOS, read RFC 791 & 795. For more information about DSCP, read RFC 2474.

### Class

Select a class for which the packets should be modified. Select from the classes defined on the **QoS Classes** page.

### TOS Octet

#### TOS

Select a new TOS value for packets in this class. Select between **Empty** (no TOS bit set), **MD** (Minimize Delay; the packet is forwarded as quickly as possible), **MT** (Maximize Throughput; data throughput is maximized), and **MR** (Maximize Reliability; data is forwarded as reliably as possible). If the packet should have a DSCP value instead, select "-" here.

#### DSCP

Enter a new DSCP value for packets in this class. The DSCP field has 6 bits, which means that only the numbers 0-63 (inclusive) are possible to set for this field.

In addition to this, only some of the numbers are valid values for the DSCP field. There is also no simple linear scale of the type "a larger value means a higher priority". Do not enter a value in this field if you do not know that the value is valid.

Note that in this field, you enter a decimal number. In most tracing applications, the DSCP value is shown as a hexadecimal number.

### Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

## 14.6.2. Save

Saves the TOS Modification configuration to the preliminary configuration.

### **14.6.3. Undo**

Clears and resets all fields in new rows and reset changes in old rows.

# Chapter 15. Logging and Tools

The unit can log different types of traffic, attempts to connect and other events. You can select to have the logs stored on the unit's local hard drive, in which case they can be queried. When the unit's hard drive gets full, it removes the oldest data to make space for saving new data.

You can also clear the logs manually by running the installation program (see [Basic Administration](#)) and select to **Reset the rest of the configuration** and **3. Revert to the factory configuration**. NB: This will clear the logs, remove all configuration on the unit and then apply the configuration set during the running of the installation program.

Ingate SIParator/Firewall S21 has no hard drive, but save the logs to the memory, which means that the log disappears at reboot.

For traffic that uses the TCP protocol, only the first packet is logged, the one that initiates the connection. For the UDP and ICMP protocols, all packets are logged, except when the UDP packets are let through using Dynamic session management, in which case only the first packet is logged. In this section, you specify what you want to log and alarm and study the logs. Logging of events is also configured under **Access Control, Rules** and **Relays**.

## 15.1. Display Log

On this page, you can view the logs. You select the type of traffic you want to study by selecting which packets should be displayed.

### 15.1.1. Search the Log

Extracts from the log can be displayed in your web browser for troubleshooting or monitoring.

Below the search form, you can also export log extracts to a file.

Display Log Packet Capture Check Network Display Load Hardware Monitoring Logging Configuration Log Classes Log Sending

**Search the Log** [\(Help\)](#)

Display log 300 rows/page (timeout 15 seconds)

Periodical search 180 seconds until next search

#### Display log

For screen display, enter the desired number of lines per page and press **Display log**.

If you enter a large number of lines, and there are only a few entries per day of the event you selected, the unit will keep on searching through the entire log. You can limit this by entering a timeout in seconds, after which the unit should stop searching regardless of progress.

## Periodical search

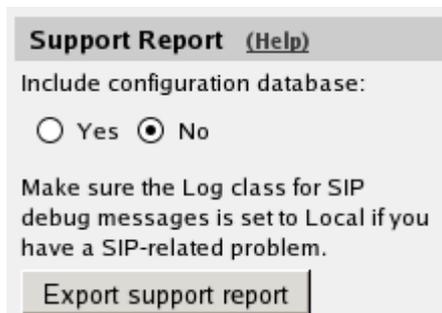
**Periodical search** will cause new events to appear automatically in the log display. You enter the time interval for updating in the **Seconds until next search** field. This will only affect log display on your screen.

### 15.1.2. Support Report

When you press Export support report, the unit will create a compressed file with a log for the time period selected, and configuration files. This is the preferred way of sending information to the Ingate support team.

If the time interval entered does not contain any log files, the unit will display an error message. Check that you entered the correct date.

Units without a hard drive rotate out the logs quickly, as there is a very limited space to keep them. This could be a reason for the Support Report not containing any logs. In this case, make the test again and download the Support Report directly after that.



The screenshot shows a dialog box titled "Support Report" with a "(Help)" link. Below the title, it asks "Include configuration database:" and provides two radio button options: "Yes" and "No", with "No" selected. Below this, there is a note: "Make sure the Log class for SIP debug messages is set to Local if you have a SIP-related problem." At the bottom of the dialog is a button labeled "Export support report".

### 15.1.3. Packet Selection

You can select packets by IP addresses, IP protocols, IP version and whether they were allowed to pass the unit or not. Only packets matching all three criteria are shown.

**Packet Type Selection**

All packets ▾

**IP Version Selection**

All Versions ▾

**IP Address Selection** [\(Help\)](#)

A:   not this address

B:   not this address

A src    A dst    A any    not this combination  
 A to B    B to A    Between A&B

**Protocol/Port Selection**

All IP protocols

TCP    All ports  
 UDP    Selected ports: [\(Help\)](#)  
A:   not this port  
B:   not this port  
 A src    A dst    A any    not this  
 A to B    B to A    Between A&B combination

ICMP  
 ICMPv6

ESP

Protocol number: [\(Help\)](#)   not

### Packet Type Selection

You can limit the selection to only allowed packets or rejected/discarded packets, or a subset of these. For example, you can select allowed, un-NAT:ed packets only.

### IP Version Selection

Select between IPv4, IPv6 or both versions.

### IP Address Selection

You can limit the selection by specifying certain IP addresses.

In these fields, enter a single IP address (e. g., 10.3.27.3), a range of IP addresses (e. g., 10.3.27.1-

10.3.28.254), an IP address followed by a netmask (e.g.,10.3.27.0/24), a combination of these, or nothing at all. If a field is empty, all IP addresses are selected.

If you want to study all traffic except the one to or from a specific computer or group of computers, enter the IP address(es) here and mark the "not this address" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the IP address in field A matches. Field B is ignored.
A dst	Packets to the IP address in field A matches. Field B is ignored.
A any	Packets to or from the IP address in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to study all packets to or from 10.3.27.18, except those to the file server 10.3.27.2, you should fill in the form like this:

**IP Address Selection**

A:   not this address

B:   not this address

A src  A dst  A any  not this combination

A to B  B to A  Between A&B

## Protocol/Port Selection

You can limit the selection by specifying certain protocols.

### *All IP protocols*

No restriction regarding protocols.

### *TCP/UDP*

When selecting TCP or UDP, you can choose all packets or packets to certain ports only.

In these fields, you can enter a single port number (32), a range of port numbers (1-1023), a list of port numbers and ranges separated by commas (53, 1024-65535) or nothing at all. If the field is empty, any port will match.

If you want to study all traffic except the one to or from a specific port or group of ports, enter the port number(s) here and mark the "not this port" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the port number in field A matches. Field B is ignored.
A dst	Packets to the port number in field A matches. Field B is ignored.
A any	Packets to or from the port number in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to search for all packets to a web server, but not packets on the "normal" client and server ports in your environment, fill in the form like this:

**Protocol/Port Selection**

TCP    All ports  
 UDP    Selected ports:

A:     not this port  
 B:     not this port

A src    A dst    A any    not this combination  
 A to B    B to A    Between A&B

### ICMP/ICMPv6

ICMP packets contain a type field and a code field. When searching for ICMP packets, you can select all packets or only those matching certain criteria.

In the type and code fields, you can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e.g., 5, 10-20) or nothing at all. If the field is empty, any type or code will match.

If you want to study all traffic except the one of a certain type/code, enter the type/code number(s) here and mark the "not" box.

### ESP

ESP is an authentication/encryption protocol. Select this if you want to search for encrypted packets.

Note that you must have selected a log class which saves to local file, for encrypted packets, to be able to display them here.

### Protocol number

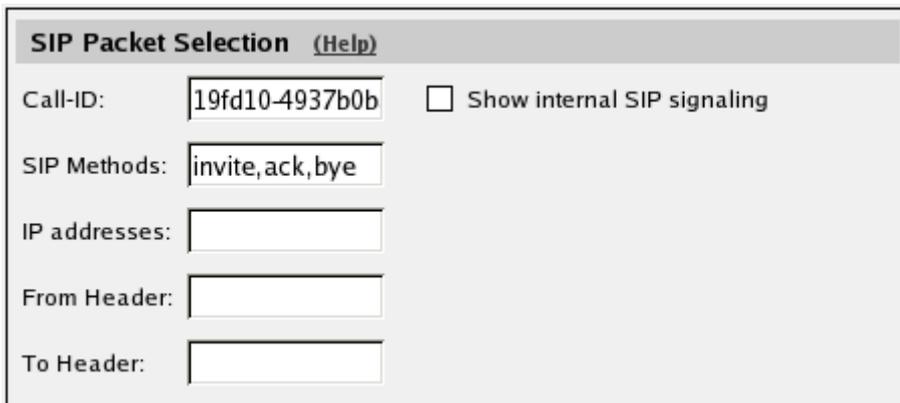
Here, you enter the number(s) of the protocols you want to search for. You can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e.g., 5, 10-20) or nothing at all. If the field is empty, any protocol will match.

If you want to study all traffic except the one over a certain protocol or protocols, enter the protocol number(s) here and mark the "not" box.

### 15.1.4. SIP Packet Selection

In this section, you can filter out certain SIP messages based on Call-ID, SIP method, sending or receiving IP address and the content of the To and From headers.

This selection will only have effect on the SIP choices **SIP signaling** and **SIP packets** under Show This.



The screenshot shows a window titled "SIP Packet Selection" with a "(Help)" link. It contains several input fields and a checkbox:

- Call-ID:** A text box containing "19fd10-4937b0b". To its right is a checkbox labeled "Show internal SIP signaling" which is currently unchecked.
- SIP Methods:** A text box containing "invite,ack,bye".
- IP addresses:** An empty text box.
- From Header:** An empty text box.
- To Header:** An empty text box.

#### Call-ID

Enter the Call-ID for the event you want to examine. Matching is done only on entire Call-IDs (no substrings).

#### SIP Methods

Enter the SIP methods that should be displayed, separated by commas. If you enter INVITE, REGISTER, the log will show all INVITE and REGISTER requests, and all responses for these requests. Note that if you want to see ACKs for a call, you have to enter that method as well as INVITE to see the entire call setup.

#### IP addresses

Enter one or more IP addresses for which you want to see SIP traffic. For the IP addresses entered, all SIP signaling received from and sent to the addresses will be shown.

#### From Header

Enter one or more URIs that appear in the From headers for the event you want to examine. The From headers typically contain usernames and domains, like [george@ingate.com](mailto:george@ingate.com).

#### To Header

Enter one or more URIs that appear in the To headers for the event you want to examine. The To headers typically contain usernames and domains, like [george@ingate.com](mailto:george@ingate.com).

## Show internal SIP signaling

The unit often loops SIP messages to itself when processing and routing SIP signaling. Normally, the looped messages are not shown, but when this checkbox is checked, the log will display all steps in the message processing.

### 15.1.5. Time Limits

On the right-hand side of the boxes, select time interval and order for the log display.

**Time Limits**

Show log from: [\(clear\)](#)

date (YYYY-MM-DD)      time (HH:MM:SS)

Show log until: [\(clear\)](#)

date (YYYY-MM-DD)      time (HH:MM:SS)

Show newest at top

#### Show log from

You can limit the selection by a time interval.

The date is written as a year with two or four digits, month (01-12) and day (01-31). The optional punctuation between year, month and day must be dash (-). Time is written as two digits for the hour, two digits for the minute and possibly two digits for the second, although the seconds can be left out. The optional punctuation between hours, minutes and seconds must be colon (:) or period (.).

You can enter a date, a time or both to set a start time for the log display. If you leave the date field blank and enter a time in the corresponding time field, today's date is used. If you leave the time field blank and enter a date in the date field, the time is set to 00:00:00. If both fields are left blank, all events back to the log start will be displayed.

#### Show log until

You can enter a date, a time or both to set an end time for the log display. If you leave the date field blank and enter a time in the corresponding time field, today's date is used. If you leave the time field blank and enter a date in the date field, the time is set to 23:59:59. If both fields are left blank, all events until the latest log event will be displayed.

#### Show newest at top

Choosing Show newest at top will display the log in reverse order, i. e., the latest log event will be displayed first.

### 15.1.6. Show This

You can select the events you want to search for. NB: You must select **IP packets as selected** to get a log display of the packets selected in the boxes.

**Show This**  
Select: [All](#), [None](#), [SIP](#).

- IP packets as selected
- Configuration server logins
- Administration and configuration
- Time-controlled reconfigurations
- Manual reconfigurations and reboots
- Time changes
- DHCP/PPPoE client
- RADIUS errors
- SNMP problems
- Hardware errors
- Mail errors
- Negotiated IPsec tunnels
- Blacklisting events
- IPsec key negotiations
- IPsec key negotiation debug messages
- IPsec user authentication
- PPTP negotiations
- SIP errors
- SIP signaling
- SIP packets
- SIP license messages
- SIP media messages
- SIP IDS/IPS
- SIP debug messages

### 15.1.7. Export the Log

Extracts from the log can be exported to a text file for processing in external tools.

**Export the Log** [\(Help\)](#)  
   MB max

You can also save the log to a file. Enter the maximum size of the log file. If you must have the latest log events, select **Show newest at top**.

You can choose between different file formats; TAB-separated file, comma-separated file and WELF (WebTrends Enhanced Log Format). These are text formats, which means that you can import the files in a text editor for analysis. TAB- and comma-separated files contain all information from the log file. WELF is an open standard used by several log analyzer tools. However, all WELF compatible syslog messages will not be exported. You can find a thorough description of the file formats in [Format Descriptions](#).

WELF uses the unit name you enter on the **Basic Configuration** page. Some WELF applications have licenses restricted to a certain number of units. This can cause trouble if you change the name of your unit.

If you export a log to WELF with **Show newest at top** selected, this may become troublesome when using some WELF applications, which cannot handle events in reverse order.

Press **Export log** and enter the file name and path to export to file.

### Clear form

Resets the form.

## 15.2. The log

The log shows every packet and event on a separate row.

The rows displaying IP packets show the date and time, type of protocol, from interface, computer and port, to interface, computer and port, ICMP type for ICMP traffic, flags, whether the packet was accepted, rejected or discarded, and the reason for this. For TCP traffic, and for UDP traffic which is session managed, only the connection packet is displayed. SIP media streams are not logged.

The unit's own IP address is displayed in the log with a purple background color. Rejected and discarded packets are displayed with a yellowish background.

Time	Protocol	From			To			Type: Code	Flags	Decision	Reason
		iface	IP address	Port	iface	IP address	Port				
2005-10-21 08:09:15.239	UDP	eth4	193.12.253.50	123	eth0	193.180.23.12	123			Rejected	IP policy
2005-10-21 08:09:14.827	TCP	eth0	193.180.23.109	55716		193.180.23.3	80		S	Accepted	Config server
2005-10-21 08:09:14.277	UDP	eth0	193.180.23.249	138		193.180.23.255	138			Rejected	IP policy
2005-10-21 08:09:13.821	UDP	eth4	193.12.253.49	20031	eth0	193.180.23.12	20031			Accepted	Rule 57
2005-10-21 08:09:13.669	TCP	eth0	193.180.23.180	1099	ipsec0	10.48.254.2	80		S	Accepted	Rule 2
2005-10-21 08:09:13.165	TCP	eth0	193.180.23.180	1099	ipsec0	10.48.254.2	80		S	Accepted	Rule 2
2005-10-21 08:09:12.734	ICMP	ipsec0	10.48.254.2		eth0	193.180.23.180		0:0		Accepted	Rule 1

The following flags are used:

S	SYN	Request for connection
A	ACK	Response to a previous packet
U	URG	Contains out-of-band data

P	PUSH	Packets that must be delivered quickly
F	FIN	Disconnect request
R	RST	Reset - response to incorrect packet

For more information on flags, see RFC 793.

When the clock is reset, the log shows this on a separate line like this:

```
2008-12-05 08:17:07.340 >>> info: fuego_run: admin [193.180.23.63] changed date and time.
```

If the unit is restarted, the log shows this on a line like this:

```
2008-12-05 08:18:10 >>> Restart
```

## 15.3. Packet Capture

The unit has a built-in packet capturer which can produce pcap trace files. This sniffer will capture all IP packets according to your selections, even those you can't see in the log (like RTP packets).

The unit capturer needs to be manually activated and deactivated. As this produces a log which usually contains a lot more packets than the standard log, it is advisable only to run the capturer for short time periods.

The capture of the packets can be downloaded and analyzed in any tool that handles pcap traces, like Ethereal/Wireshark.

### 15.3.1. Network Interface Selection

Select on which interface or VLAN the sniffer should listen for packets. You can also select to listen on all interfaces.

Some network cards have VLAN hardware support. For this type of cards, incoming VLAN tagged traffic is not logged on the main interface, but only on the VLAN interface. Outgoing VLAN tagged traffic is logged on the main interface.

Other interfaces do not have VLAN hardware support. For this type of interface, VLAN traffic is logged on the main interface.

Currently, the only network cards in Ingate products to support VLAN are the Gigabit network cards.

### 15.3.2. IP Version Selection



The screenshot shows a control box titled "IP Version Selection". Inside the box, there is a dropdown menu currently set to "All Versions".

Select between IPv4, IPv6 or both versions.

### 15.3.3. IP Address Selection

You can limit the selection by specifying certain IP addresses.

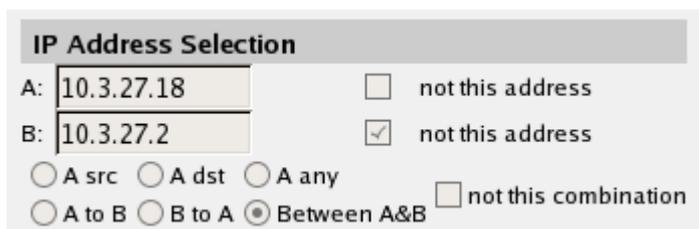
In these fields, enter a single IP address (e.g., 10.3.27.3), a range of IP addresses (e. g., 10.3.27.1-10.3.28.254), an IP address followed by a netmask (e.g.,10.3.27.0/24), a combination of these, or nothing at all. If a field is empty, all IP addresses are selected.

If you want to study all traffic except the one to or from a specific computer or group of computers, enter the IP address(es) here and mark the "not this address" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the IP address in field A matches. Field B is ignored.
A dst	Packets to the IP address in field A matches. Field B is ignored.
A any	Packets to or from the IP address in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to study all packets to or from 10.3.27.18, except those to the file server 10.3.27.2, you should fill in the form like this:



The screenshot shows the "IP Address Selection" form. It has two input fields, A and B. Field A contains "10.3.27.18" and field B contains "10.3.27.2". To the right of each field is a checkbox labeled "not this address". The checkbox for field B is checked. Below the fields are radio buttons for selection options: "A src", "A dst", "A any", "A to B", "B to A", "Between A&B", and "not this combination". The "Between A&B" option is selected.

### Protocol/Port Selection

You can limit the selection by specifying certain protocols.

## All IP protocols

No restriction regarding protocols.

## TCP/UDP

When selecting TCP or UDP, you can choose all packets or packets to certain ports only.

In these fields, you can enter a single port number (32), a range of port numbers (1-1023), a list of port numbers and ranges separated by commas (53, 1024-65535) or nothing at all. If the field is empty, any port will match.

If you want to study all traffic except the one to or from a specific port or group of ports, enter the port number(s) here and mark the "not this port" box.

The selection can be modified by the control boxes under the fields A and B:

A src	Packets from the port number in field A matches. Field B is ignored.
A dst	Packets to the port number in field A matches. Field B is ignored.
A any	Packets to or from the port number in field A matches. Field B is ignored.
A to B	Packets from A to B matches.
B to A	Packets from B to A matches.
Between A&B	Packets from A to B, or from B to A, matches.
not this combination	Packets that do not match the given combination of A and B are shown in the log.

If you, for example, want to search for all packets to a web server, but not packets on the "normal" client and server ports in your environment, fill in the form like this:

**Protocol/Port Selection**

TCP  All ports

UDP  Selected ports:

A:   not this port

B:   not this port

A src  A dst  A any  not this combination

A to B  B to A  Between A&B

## ICMP/ICMPv6

ICMP packets contain a type field and a code field. When searching for ICMP packets, you can select all packets or only those matching certain criteria.

In the type and code fields, you can enter a single number (e.g., 5), a range of numbers (e.g., 5-10), a list of numbers and ranges, separated by commas (e.g., 5, 10-20) or nothing at all. If the field is empty, any type or code will match.

If you want to study all traffic except the one of a certain type/code, enter the type/code number(s) here and mark the "not" box.

## ESP

ESP is an authentication/encryption protocol. Select this if you want to search for encrypted packets.

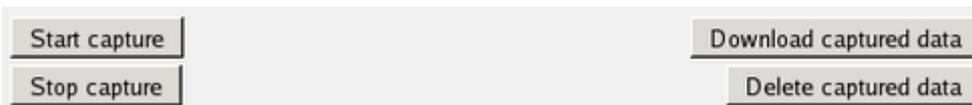
Note that you must have selected a log class which saves to local file, for encrypted packets, to be able to display them here.

## Protocol number

Here, you enter the number(s) of the protocols you want to search for. You can enter a single number (e. g., 5), a range of numbers (e. g., 5-10), a list of numbers and ranges, separated by commas (e. g., 5, 10-20) or nothing at all. If the field is empty, any protocol will match.

If you want to study all traffic except the one over a certain protocol or protocols, enter the protocol number(s) here and mark the "not" box.

### 15.3.4. Collect data



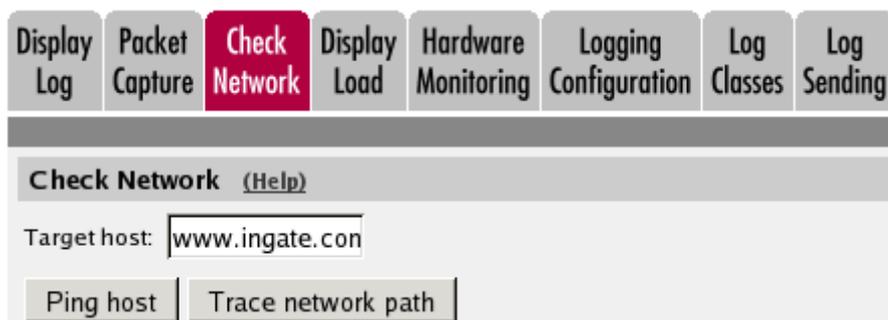
Below the selection boxes, you activate and deactivate the capture function by pressing the **Start capture** and **Stop capture** buttons.

When the capturer has been stopped, the captured log can be downloaded by pressing the **Download captured data** button. The captured data can be deleted by pressing the **Delete captured data** button.

## 15.4. Check Network

You can perform ping and trace a network path from the unit to another IP address to check that the network connection is working.

### 15.4.1. Check Network



## Target host

Enter the IP address of the computer for which you want to check the network connectivity.

## Ping host

When you press this button, the unit will send ten ping packets to the target host and register the replies from that host.

Note that the target host must be configured to respond to ping packets for this test to succeed. Most common computers do that by default, but Ingate units do not respond to ping request unless they have been configured to do so.

## Trace network path

When you press this button, the unit will send packets to the target host and register which path is used by those packets.

For this test to succeed, there must not be more than 30 network elements between the unit and the target host.

## 15.4.2. Test Results

Below the buttons, the result of the latest test run is shown. A ping test will result in the ten sent packets and their response times.

```
PING 88.131.69.225 (88.131.69.225) 56(84) bytes of data.  
64 bytes from 88.131.69.225: icmp_seq=1 ttl=63 time=1.54 ms  
64 bytes from 88.131.69.225: icmp_seq=2 ttl=63 time=1.57 ms  
64 bytes from 88.131.69.225: icmp_seq=3 ttl=63 time=1.22 ms  
64 bytes from 88.131.69.225: icmp_seq=4 ttl=63 time=1.58 ms  
64 bytes from 88.131.69.225: icmp_seq=5 ttl=63 time=0.843 ms  
64 bytes from 88.131.69.225: icmp_seq=6 ttl=63 time=0.842 ms  
64 bytes from 88.131.69.225: icmp_seq=7 ttl=63 time=0.869 ms  
64 bytes from 88.131.69.225: icmp_seq=8 ttl=63 time=1.63 ms  
64 bytes from 88.131.69.225: icmp_seq=9 ttl=63 time=0.633 ms  
64 bytes from 88.131.69.225: icmp_seq=10 ttl=63 time=0.771 ms  
  
--- 88.131.69.225 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9048ms  
rtt min/avg/max/mdev = 0.633/1.150/1.630/0.381 ms  
  
MAC address for 88.131.69.225: not local
```

A trace test will result in a list of all network elements the packets use to get to the target host.

```
traceroute to 88.131.69.225 (88.131.69.225), 30 hops max, 38 byte packets  
 1 193.180.23.3 0.563 ms 0.446 ms 0.493 ms  
 2 88.131.69.225 1.492 ms 0.721 ms 1.974 ms
```

## 15.5. Display Load

On this page, you can see statistics on the traffic load to and from the unit's interfaces and the memory and CPU load. This feature is available for all models except Ingate SIParator/Firewall S21.

Once every 10 seconds, the load on all interfaces is scanned and saved to a local file. Every file contains 240 samples and a file generation consists of 42 files and has a size of approximately 20 MB. The first generation of files contains samples for the last week (approximately). Every new file generation is created by merging two consecutive samples, enabling the storing of samples for the double time period in the same disk space. Merging the samples include calculation of the minimum, average and maximum values for the time interval covered by the samples. After ten generations (about 3 years) the samples are deleted.

### 15.5.1. Packet Load

#### Interface

You can select one or more of the unit’s interfaces or the total traffic. Selecting more than one interface will generate one graph per interface. You can also select to view only VPN traffic.

#### Direction

Select one or more of **Sent**, **Received** and **Sent+Received**. Each selection generates a separate graph in the diagram.

#### Unit

Select between displaying packets/second or bits/second. The graphs may look different, because all packets aren’t the same size.

#### Max Value

Enter the maximum value to show in the diagram. If no value is entered, the diagram automatically scales to a suitable value.

## 15.5.2. Time Period

Select a time period or enter a period of your own choice in the bottom fields. The date is written as a year with two or four digits, month (01-12) and day (01-31). The optional punctuation between year, month and day must be dash (-). Time is written as two digits for the hour, two digits for the minute and possibly two digits for the second, although the seconds can be left out. The optional punctuation between hours, minutes and seconds must be colon (:) or period (.).

**Time Period**

Last hour

Last 24 hours

Today

Yesterday

This week

Previous week

This month

Previous month

Other period:

From date (YYYY-MM-DD):

From time (HH:MM):

To date (YYYY-MM-DD):

To time (HH:MM):

## 15.5.3. Value

Select maximum, average or minimum value of each sample period. If viewing load for time periods within the last week, all three selections will result in the same graph.

**Value**

Max

Average

Min

## 15.5.4. Show This

The unit also stores load values for CPU, memory and swap usage. These values can also be shown in the diagram. Check the boxes for the values to be shown. Each selection generates a separate graph in the diagram.

**Show This**

CPU load

Memory load (RAM)

Swap usage

### 15.5.5. The Diagram

**Diagram Size**      **Diagram Heading**

600 (width) × 400 (height) pixels      Internal + Total

#### Diagram Size

Enter the desired width and height of the resulting load diagram.

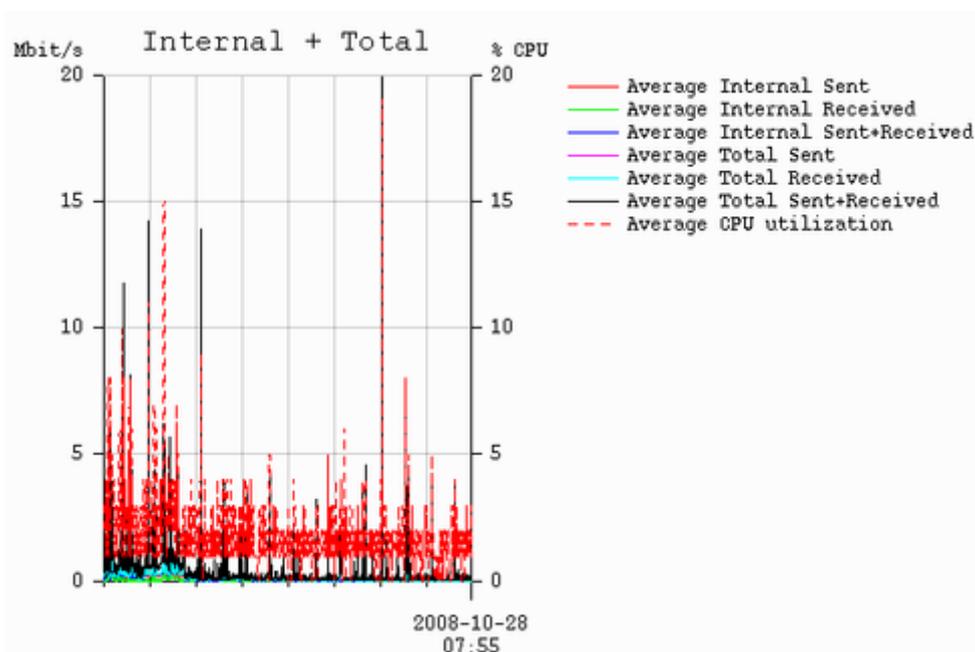
#### Diagram Heading

You can enter a heading for the load diagram. This is useful if you view several diagrams and save them.

#### View diagram

Creates a diagram at the top of the page.

For each combination of selections, a graph will be generated. Example: You selected **eth0** and **Total** as interfaces, and **Sent**, **Received** and **Sent+Received** as directions. This will generate a total of six graphs of different colours in the diagram.



## 15.6. Logging Configuration

Your unit generates log messages for various events and for the traffic to and through the unit.

Here, you select log classes to state what to do with the log messages.

When an IP packet is received by the unit, a log message is generated, containing sender and receiver IP addresses and other information such as the protocol used and if the packet was allowed, rejected or discarded. The unit then uses the log settings for Rules, Relays, Configuration Transport and Log class when no rule matches to know how to process the log message.

The unit also produces log messages for SIP-related and VPN-related events as well as administrator events (when the administrator logs on or when a setting is changed). Here, you configure what will happen to these log messages.

### 15.6.1. Traffic

#### Traffic

Log class when no rule matches:

Log class for spoofed packets:

Log class for broadcast packets:

Log class for DHCP requests:

Log class for Tunnel packets:

Log class for Neighbor Discovery packets:

Log class for Cloud information:

Log class for SNMP requests to the firewall:

Log class for packets to/from the firewall:

#### Log class when no rule matches

Here, you select a log class for packets addressed through the unit that do not match any rules and are therefore processed by the **IP policy** (discard or reject) that you selected on the **Basic Configuration** page.

#### Log class for spoofed packets

Here, you select a log class for packets with obviously spoofed addresses. A spoofed IP address can be a non-existing IP address on a network connection or packets where the sender or receiver address is an IP address in the range 127.0.0.0 - 127.255.255.255.

### **Log class for broadcast packets**

Here, you select a log class for broadcast packets. Broadcast is a method of sending packets when you don't know the actual recipient. The packets are sent to all computers on the network. See [Definitions of terms](#) for more information about broadcast.

### **Log class for DHCP requests**

Here, you select a log class for DHCP requests. DHCP is a protocol used for dynamic allocation of IP addresses. Requests are sent by broadcast from computers wanting an IP address to a DHCP server. The unit logs all DHCP related packets using the log class you select here. There are usually a lot of these packets, so we recommend using the log class "None", meaning that no packets are logged at all.

### **Log class for Tunnel packets**

Here, you select a log class for Tunnel packets. Tunnel packets are sent to and from the unit when any of the tunnel types 6in4, 6to4 or 6rd are configured and used.

### **Log class for Neighbor Discovery packets**

Here, you select a log class for Neighbor Discovery packets. The Neighbor Discovery Protocol is used in IPv6 to find hosts and routers. The following ICMPv6 messages are part of NDP:

- Router Solicitation (Type 133)
- Router Advertisement (Type 134)
- Neighbor Solicitation (Type 135)
- Neighbor Advertisement (Type 136)
- Redirect (Type 137)

### **Log class for Cloud information**

Here, you select a log class for Cloud information. Cloud information will include traffic to and from the meta-data server and additional services managing the cloud environment.

### **Log class for SNMP requests to the firewall**

Here, you select a log class for SNMP requests to the unit. SNMP is a protocol for monitoring network equipment such as firewalls and routers.

### **Log class for packets to/from the firewall**

Here, you select a log class for traffic addressed to/from the unit itself. Even if you select not to log this traffic, the configuration traffic to the unit will be logged according to the log class set on the **Access Control** page.

## **15.6.2. Warnings**

**Warnings**

Log class for hardware errors:

Log class for email errors:

Log class for RADIUS errors:

Log class for SNMP errors:

### Log class for hardware errors

Some units have hardware monitoring, and will generate log messages when the hardware fails in some way. Here, you select a log class for these messages.

### Log class for email errors

If the unit is unable to send email messages, for example, if the mail server won't reply, the unit generates a log message. Here, you select a log class for these messages.

### Log class for RADIUS errors

Radiusmux (see the [RADIUS](#) section in [Basic Configuration](#)) generates messages for incomprehensible RADIUS server responses and for denying logins on account of permissions (a user defined for road warriors is not automatically allowed to log onto the configuration server). Here, you select a log class for these messages.

### Log class for SNMP errors

The unit generates messages about SNMP errors. Here, you select a log class for these messages.

## 15.6.3. Master Log

You can select to temporarily log all traffic, regardless of the log classes selected for various rules, or not to log anything.

The master log function affects all log messages from rules, relays and configuration traffic.

**Master Log** [\(Help\)](#)

Master log mode: Log class for master logging (used if **Log all** is selected):

No logging

Log as marked

Log all

### Master log mode

Select not to log anything, to log all traffic no matter its marking, or only log for marked rules/relays

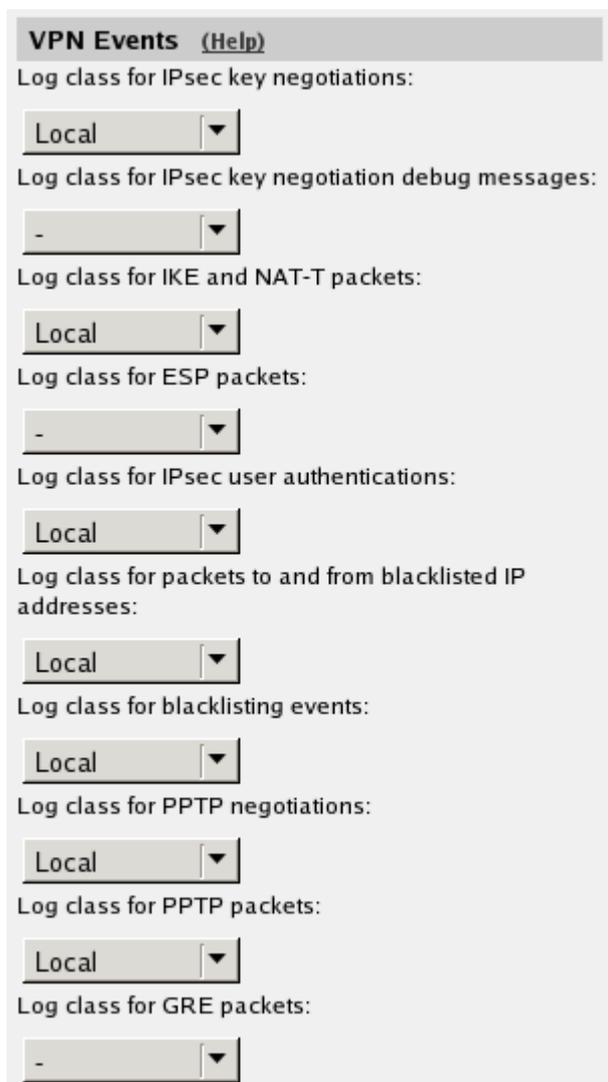
that are marked under **Log class** in **Rules**, **Relays** and **Configuration Computers** (on the **Access Control** page).

### Log class for master logging

If **Log all** is selected, you must select a log class for this logging. This log class will be used for all rules, relays and configuration server logins, instead of the separate log classes selected for those settings.

## 15.6.4. VPN Events

The same settings can also be found on the **IPsec Settings** and **PPTP** pages under **Virtual Private Networks**.



The screenshot shows the 'VPN Events' configuration page with a '(Help)' link. It contains ten settings, each with a label and a dropdown menu:

- Log class for IPsec key negotiations: Local
- Log class for IPsec key negotiation debug messages: -
- Log class for IKE and NAT-T packets: Local
- Log class for ESP packets: -
- Log class for IPsec user authentications: Local
- Log class for packets to and from blacklisted IP addresses: Local
- Log class for blacklisting events: Local
- Log class for PPTP negotiations: Local
- Log class for PPTP packets: Local
- Log class for GRE packets: -

### Log class for IPsec key negotiations

Here, you set the log class for new negotiations of IPsec connection keys.

### Log class for IPsec key negotiation debug messages

Here, you set the log class for debug information about negotiations of IPsec connection keys.

### **Log class for ESP packets**

Specify what log class the unit should use for encrypted packets (ESP packets to the unit). Logging of encrypted packets will generate a lot of log events.

### **Log class for packets to and from blacklisted IP addresses**

Here, you set the log class for the packets that are rejected or discarded according to the blacklisting policy selected above.

### **Log class for IKE and NAT-T packets**

Here, you set the log class for the packets used for IKE key negotiations and for NAT-T packets. As they both use the same port on the unit, it will log both using the same log class.

### **Log class for IPsec user authentications**

Here, you set the log class for unit messages about road warrior authentications via RADIUS and their disconnections.

### **Log class for blacklisting events**

Here, you specify how the unit should report beginnings and ends of blacklisting events.

### **Log class for packets to and from blacklisted IP addresses**

Here, you set the log class for the packets that are rejected or discarded according to the blacklisting policy selected above.

### **Log class for PPTP negotiations**

The unit generates log messages about the progress of the PPTP negotiations. Here, you select a log class for these messages.

### **Log class for PPTP packets**

PPTP clients wanting to establish a VPN tunnel connects to the unit on port 1723. Here, you select a log class for these packets.

### **Log class for GRE packets**

The encrypted traffic through the VPN tunnel is sent as GRE packets. Here, you select a log class for these packets.

## **15.6.5. SIP Events**

The same settings can also be found on the Basic page under SIP Services.

**SIP Events** (Help)

Log class for SIP signaling:  
Local ▼

Log class for SIP packets:  
Local ▼

Log class for SIP license messages:  
Local ▼

Log class for SIP errors:  
Local ▼

Log class for SIP media messages:  
Local ▼

Log class for SIP IDS/IPS:  
Local ▼

Log class for SIP debug messages:  
Local ▼

Hide sensitive data:  Yes  No

### Log class for SIP signaling

For each SIP packet, the unit generates a message, containing the sender and receiver of the packet and what type of packet it is. Select a log class for these log messages.

### Log class for SIP packets

The unit logs all SIP packets (one SIP packet is many lines). Select a log class for the SIP packets.

### Log class for SIP license messages

The unit logs license messages. Select a log class for these messages.

### Log class for SIP errors

The unit sends a message if there are any SIP errors. Select a log class for these log messages.

### Log class for SIP media messages

The unit creates log messages about when media streams are set up and torn down. Select a log class for these messages.

### Log class for SIP IDS/IPS

The unit logs messages regarding IDS/IPS actions and events. Select a log class for these messages.

### Log class for SIP debug messages

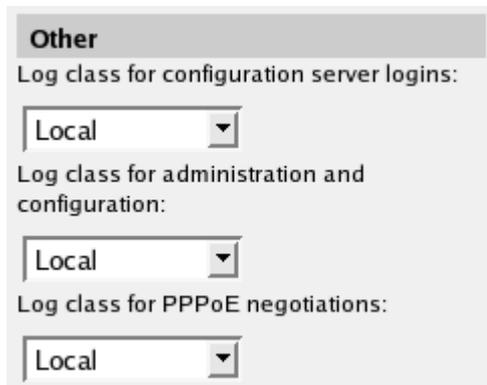
The unit logs a lot of status messages, for example the SIP initiation phase of a reboot. Select a log

class for these messages.

### Hide sensitive data

Hides sensitive information in the log messages. E.g. encryption keys.

### 15.6.6. Other



**Other**

Log class for configuration server logins:  
Local

Log class for administration and configuration:  
Local

Log class for PPPoE negotiations:  
Local

#### Log class for configuration server logins

Each time a user logs onto the unit configuration server, a message is generated, containing information about the type of login and more. Here, you select a log class for these messages.

#### Log class for administration and configuration

Each time a user logs onto the unit configuration server, a message is generated, containing information about the type of login and more. Here, you select a log class for these messages.

#### Log class for PPPoE negotiations

The unit generates log messages for its own PPPoE negotiations. Here, you select a log class for these messages.

### 15.6.7. Save

Saves the Logging Configuration configuration to the preliminary configuration.

### 15.6.8. Undo

Reverts all of the above fields to their previous configuration.

## 15.7. Log Classes

Log classes determine the handling of traffic logs, other event logs and alarms. You can select no logging, log to a local file (on the unit), send the log messages via syslog to a syslog server and send the log messages as emails. When configuring logging on all other pages, you select between the different log classes defined here.

Log Classes						
Edit Row	Name	Log Locally?	Syslog		Email Address	Delete Row
			Facility	Level		
<input type="checkbox"/>	Email	Yes	-	-	peppi@try.ingate.com	<input type="checkbox"/>
<input type="checkbox"/>	Local	Yes	-	-		<input type="checkbox"/>
<input type="checkbox"/>	Local+Syslog	Yes	Auth	Notice		<input type="checkbox"/>
<input type="checkbox"/>	Syslog	No	Auth	Notice		<input type="checkbox"/>

Add new rows  rows.

### 15.7.1. Name

Here, you give the log class a **Name**.

### 15.7.2. Local Log

Select to save log messages to a local file on the unit. Locally saved logs can be searched on the **Display Log** page. **On** will cause the log messages using this log class to be saved to file. **Off** will cause the log messages not to be saved on the unit and thus also not possible to search under **Display Log**.

### 15.7.3. Syslog

Syslog sends log messages to a syslog server. You enter the IP address of the syslog server on the **Log Sending** page. Select **Facility** and **Level** for the syslog message. See your syslog server manual for more information on facility and level. Selecting **None** for both **Facility** and **Level** turns the syslog alternative off. **None** must be selected for both or none of **Facility** and **Level**. The unit will display a red warning text until both or none of them are **None**.

### 15.7.4. Email Address

The unit may also send the log messages by email to one or more email addresses. Enter the addresses here (separated by comma). You must specify a mail server on the **Log Sending** page for the unit to send the emails properly.

### 15.7.5. Delete

If you select this box, the row is deleted when you click on **Add new rows** or **Save**.

### 15.7.6. Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

## 15.7.7. Save

Saves the Log Classes configuration to the preliminary configuration.

## 15.7.8. Undo

Clears and resets all fields in new rows and resets changes in old rows.

# 15.8. Log Sending

In the unit, there are two ways of sending log messages automatically to somewhere outside the box; to send to a syslog server and to send an email to an email address. If either method is used, the unit must know where to send this. On this page, servers for log sending are configured.

### 15.8.1. SMTP Server

Here, you set an SMTP server for the log messages that the unit generates. This server will send the email messages to the email addresses set on the **Log Classes** page. If the connection between the unit and the SMTP server isn't working, an error message will be shown on this page, and be logged according to the log class set on the **Logging Configuration** page. However, no error message will be shown here if the primary SMTP server can't connect to other mail servers. Therefore you should test if email log messages to the addresses set under **Log Classes** really reach their destination addresses.

Every log message does not create a separate email; the unit collects log messages and sends them every 5 minutes. The first message is sent within a minute.

Email sent from the unit has the From address "Ingate Firewall".

Enter the DNS name or IP address of the SMTP server.

### 15.8.2. Status for Outbound Email

A message is shown here if the unit can't connect to the mail server selected under **SMTP Server**,

or if other errors concerning email occur. To indicate this error further, the activity LEDs on the unit front go out and the ALERT LED is lit. On an Ingate SIParator/Firewall S21, only the **ALERT** LED is lit..

### 15.8.3. Syslog Servers

Here, you enter one or more syslog servers for the syslog messages that the unit generates. This is the computer which receives and stores the syslog log messages.

#### Dynamic

If an interface will receive its IP address from a DHCP server, the unit can also get information about its syslog server from that server. In this case, select the corresponding IP address here and leave the other fields empty.

#### DNS Name or IP Address

Enter the DNS name or IP address for the syslog server.

#### IP Address

Shows the IP address of the **DNS Name or IP Address** you entered in the previous field.

#### Delete

If you select this box, the row is deleted when you click on **Add new rows**, **Save**, or **Look up all IP addresses again**.

#### Add new rows

Enter the amount of new rows you want to add to the table, and then click on **Add new rows**.

### 15.8.4. Save

Saves the configuration for Log Sending to the preliminary configuration.

### 15.8.5. Undo

Reverts the fields to the previous configuration.

# Part III. Serial Console

This part contains complete descriptions of settings in the unit terminal interface.

# Chapter 16. Basic Administration

Some settings are available without having to log on the web interface, but instead connecting to the unit console via the serial cable. Here, the settings available from the console are listed.

The serial console is a text user interface which requires a terminal software on your workstation, such as Hyperterm in Windows.

## 16.1. Connecting to the serial console

Connect the unit to your workstation with the enclosed serial cable, plug in the power cord and turn the unit on. You will have to wait a few minutes while the unit boots up.

If you use a **Windows workstation**, connect like this: Start *PUTTY* (of course other terminal programs can be used, however only *PUTTY* is described here).

Check which Serial Port that is used by checking in the Device manager, for example it can be COM3.

Write in Serial line: COM3 (use the port that is in use, in this example COM3)

Select Connection Type: Serial

Among the port settings make sure that the Speed is 19200 bit/s.

Use the default values for all other settings.

Connect by clicking *Open*.

Wait for a login prompt. (In some cases you have to press Return to get the login prompt.)

If you use a **Linux workstation**, connect like this:

1. Plug in your USB serial converter.
2. Determine the tty port the converter is on.

```
dmesg | grep tty
```

You should get something like this:

```
usb 2-1.5: p12303 converter now attached to ttyUSB0
```

That means you should use `/dev/ttyUSB0`.

3. Use `minicom` to access the console.

```
minicom -8 -b 19200 -D /dev/ttyUSB0
```

You have to press Return to get the login prompt.

If you get the following error:

```
minicom: cannot open /dev/ttyUSB0: Permission denied
```

You need to make sure you have permission to access the ttyUSB0 device. Consult the manual of your particular distribution.

Log on from your workstation as the user *admin*. The first time you log on, no password is required. You set the password when you run the **1. Basic configuration** from the menu, that is presented when you have logged on.

## 16.2. Main Menu

The first thing you see after logging on as admin is the main menu. Here, you can change password, make a basic configuration of the unit, enter the unit into a failover team, save or load configuration, or remove all log messages from the e-mail queue.

```
Administration
```

```
=====
```

```
(Navigation tip: You may use Ctrl-d to skip back to this menu.)
```

1. Basic configuration
2. Download/Upload
3. Join a failover team and become slave
4. Leave the failover team and become standalone
5. Wipe email logs
6. Set password
7. Command line interface
8. Clear the log database
- a. About
- reboot. Reboot
- reset. Factory reset
- q. Exit admin

```
==>
```

### 1. Basic configuration

Basic settings for the unit, such as the IP address and the password.

This is one of two ways of giving the unit an IP address. The other way is to perform a *magic ping* (see [Installation](#)).

## 2. *Save/Load configuration*

Save or upload the configuration using the Zmodem protocol.

## 3. *Join a failover team and become slave*

Make this unit member of a failover team.

## 4. *Leave the failover team and become standalone*

Make this unit leave its failover team. Only shown if member of a failover team.

## 5. *Wipe email logs*

Remove all log messages queued to be sent by e-mail.

## 6. *Set password*

Set a new password for the admin user.

## 7. *Command line interface*

Enter the Command Line Interface (CLI). See [Command Line Reference](#), for more information about the CLI.

## 8. *Clear the log database*

Clear the log database. Note, all logs will be removed.

### *a. About*

Under **About**, you get basic information about the unit's serial number, software version, installed licenses and patches, and links to more information.

### *reboot. Reboot*

Restart the unit.

### *reset. Reset*

Perform a factory reset on the unit and reset all settings.

### *q. Exit admin*

Log out from the admin program.

## 16.3. Basic configuration

Use **Basic configuration** to give the unit a start configuration. You can assign an IP address to it (for the web GUI), enter the IP addresses of computers allowed to connect to the web GUI and change the administrator password.

Wherever you can enter a value, there will be a default one in brackets, which is the current value. Press Return to select the default value. This is an easy way to fast-forward if you only want to change one of the parameters.

### 16.3.1. IP address

Give the unit an IP address. The IP address will be added to any addresses already configured on

the unit. The IP address entered here is the one that should be used to access the web GUI.

```
Basic unit installation program version 6.1.4
```

```
Press return to keep the default value
```

```
Network configuration inside:
```

```
Physical device name[eth0]:
```

```
IP address [0.0.0.0]: 10.47.2.242
```

```
Netmask/bits [255.255.255.0]: 255.255.0.0
```

```
Deactivate other interfaces? (y/n) [n]
```

### Physical device name

Select which interface should get the IP address. The interfaces are named as on the exterior of the unit, such as eth0 and eth1.

### IP address

Enter the IP address for the unit on the interface above. If the unit didn't have an IP address before, the default address will be 0.0.0.0. Enter a different address, or the unit will be unreachable via the web GUI.

### Netmask/bits

At Netmask/bits, enter the netmask for the network to which the IP address above belongs. The netmask can be written as an IP address or a number of bits (see also [Configuring](#)).

### Deactivate other interfaces

If the unit has been used one or more interfaces are active. Select here if all interfaces but the one selected above should be deactivated. You can activate them again via the web GUI.

## 16.3.2. Configuration computers

Enter here the computers from which it is allowed to configure the unit. The computers entered here are the only ones allowed to access the web GUI.

Select between allowing a single computer or an entire network.

```
Computers from which configuration is allowed:
```

```
You can select either a single computer or a network.
```

```
Configure from a single computer? (y/n) [y]
```

## Configure from a single computer

If configuration of the unit should be allowed from a single computer only, answer **y** to the question above. Then enter the IP address of the configuration computer.

```
IP address [0.0.0.0]: 10.47.2.240
```

If the configuration computer is on the same network as the unit, these are all configuration settings needed. If the configuration computer is on a different network, the unit will ask for routing to that network.

```
Static routing:
```

```
The computer allowed to configure from is not on a network local to  
this unit. You must configure a static route to it. Give  
the IP address of the router on the network the unit is on.
```

```
The IP address of the router [0.0.0.0]: 10.47.3.1
```

```
Network address [10.47.0.0]: 10.10.0.0
```

```
Netmask [255.255.255.0]:
```

To let the unit know where traffic to the configuration computer should be sent to, you must enter the router it should use here. Enter the router which is on the same network as the unit and which is used to route traffic to the configuration computer.

You should also enter the network to which the configuration computer is connected.

## Configure from multiple computers

If configuration of the unit should be allowed from more than one computer, answer **n** to the question above. Then enter the network address of the network to which the configuration computers are connected. This will allow all computers on this network to configure the unit.

```
Network number [0.0.0.0]: 10.47.2.0
```

```
Netmask/bits [255.255.255.0]: 255.255.255.0
```

Enter the network address and netmask for the configuration computer network. If they are on the same network as the unit, these are all configuration settings needed. If the configuration computers are on a different network, the unit will ask for routing to that network.

### Static routing:

The network allowed to configure from is not on a network local to this unit. You must configure a static route to it. Give the IP address of the router on the network this unit is on.

The IP address of the router [0.0.0.0]: 10.47.3.1  
Network address [10.47.0.0]: 10.10.0.0  
Netmask [255.255.255.0]:

Enter the IP address of the router and the network to which the configuration computers are connected. This could be a bigger network than the one entered to distinguish the configuration computers.

### Password

Set a password for the unit here.

Password []:

Note that the password will be printed on the screen when entered. It will also be shown when all settings are made.

### Other

You can also select if all other configuration should be removed or not.

Other configuration  
Do you want to reset the rest of the configuration? (y/n) [n]

If you answer **n**, nothing is removed. If you answer **y**, you have three alternatives to select from:

1. Clear as little as possible. This is the alternative that is used if you answer **n** to the question above. Both the preliminary and the permanent configurations will be updated with the configuration specified above.
2. Revert to the factory configuration and then apply the configuration specified above. This will affect the permanent but not the preliminary configuration.
3. Revert to the factory configuration and empty all logs and then apply the configuration specified above. Both the preliminary and the permanent configurations will be affected.

Update mode (1-3) [1]:

When all settings are entered, they are shown on the screen to be confirmed.

Is this configuration correct (yes/no/abort)?

**yes** will make the unit reboot using the new settings.

**no** will make the unit go through the Basic configuration questions again and allow you to change settings.

**abort** will make the Basic configuration script end without changing any settings.

## 16.4. Save/Load configuration

Here, you can save your configuration to a file or load a configuration from a file. The transfer is made using the Zmodem protocol, which can be found in terminal software such as Hyperterminal.

### 16.4.1. Load preliminary configuration

The configuration file selected here will be uploaded as a preliminary configuration. The permanent configuration will not be affected.

To load the configuration, select this alternative and then start the transfer in your terminal program.

### 16.4.2. Load both configurations and apply

The configuration file selected here will be uploaded as both the preliminary and the permanent configuration. When the upload is finished, the configuration will be applied.

To load the configuration, select this alternative and then start the transfer in your terminal program.

### 16.4.3. Save preliminary configuration

Save the preliminary configuration to a file. If your terminal program starts the transfer automatically, the file will be named `config.cfg`.

### 16.4.4. Save permanent configuration

Save the permanent configuration to a file. If your terminal program starts the transfer automatically, the file will be named `config.cfg`.

### 16.4.5. Main menu

Select this alternative to return to the main menu.

## 16.5. Join a failover team and become slave

Here, you make the unit the second member of a failover team (a slave). All current configuration will be removed. The unit will receive its new configuration from the first member of the team (the master).

Dedicated network interface [eth0]:

Enter the network interface which will be directly connected to the other unit in the team. This interface will be used to synchronize the configurations and can't be used for anything else.

IP network address for eth0 [10.120.121.64]:

Enter the network address for this interface. The network address must be the same as the one entered for the first member of the failover team. If you used the default values for that unit you can do the same here.

IP netmask for eth0 [255.255.255.252]:

Enter the netmask for the network. The netmask must be big enough to comprise IP addresses for two computers, a network address and a broadcast address, i.e. at least four addresses. The default netmask (255.255.255.252) should suffice. There is no use in assigning a larger network, since the units should be connected via a crossover TP cable.

Current configuration:

Dedicated interface: eth0

Network address: 10.120.121.64

Network mask: 255.255.255.252

Is this configuration correct (yes/no/abort)?

When all settings are made they are shown.

**yes** will make the unit reboot, remove all current configuration and apply the new settings. It will then wait for configuration from the other team member.

**no** will make the unit start over again asking for new settings, starting with the dedicated interface.

**abort** will abort the failover configuration and return to the main menu without changing any settings on the unit.

## 16.6. Leave the failover team and become standalone

Here, you make the unit leave its failover team. The unit will keep the configuration from the team except the failover settings.

This will change the operation mode from being a member of a failover team to become a standalone unit.  
The unit will reboot to complete this procedure.

Do you want to proceed (yes/no)?

**yes** will make the unit leave the failover team and reboot as a standalone unit.

**no** will make you return to the main menu without changing any settings.

## 16.7. Wipe email logs

Here, you can erase all log messages queued for sending via email to one or more receivers. This could be useful if you by mistake made settings where lots of events are logged via email, which fill the queue rapidly.

This will remove all email logs that are waiting to be sent.

Do you want to proceed (yes/no)?

**yes** will remove all log messages from the email queue. These messages are not saved to file or similar before removed. If you log locally as well as via email, the local log will not be affected by this.

Note that this will only remove messages already queued up for sending. To prevent further queue jams, you must also change log classes for the events in question (see [Logging and Tools](#)).

**no** will make you return to the main menu without removing anything.

## 16.8. Clear the log database

Clear the log database, note all logs will be removed.

This will discard the log database! Note that this operation can take several minutes. Please do not interrupt.

Do you want to proceed (yes/no)?

## 16.9. Set password

Here, you can change password for the *admin* user.

Old password:  
New password:  
New password again:

As this option requires that you are logged on as *admin*, you need to know the current password in order to change into a new one. If you have forgotten the password, you must reset it using the **FD** button to set a new one.

## 16.10. Exit admin

Select **Exit admin** to log out.

# Chapter 17. Command Line Reference

This is a reference for the Command Line Interface (CLI), which can be accessed via the serial console or SSH (see [Basic Administration](#)).

## 17.1. Command Reference

Here is a list of the commands available in the Command Line Interface (CLI).

Commands are presented like this: **command** [--flag] **parameter1** | **parameter2** [**parameter3 ...**].  
An example is:

```
ping ip-address
```

**--flag means** that the flag can modify the command in some way.

**parameter1** means that the parameter1 (like "ip-address" in the example) should be replaced with a specified parameter of that type (like a real IP address, 193.180.23.23).

**parameter1 | parameter2** means that either parameter1 or parameter2 can be used.

[**parameter3**] means that this parameter is optional.

**parameter3 ...** means that this type of parameter can be used multiple times.

### 17.1.1. Help and Troubleshooting

#### **datetime**

Usage: **datetime** [--list-zones] [**date=DATE**] [**time=TIME**] [**zone=TIMEZONE**]

With this command, you set or display the current date, time and/or timezone.

If the assignment parameters **date=** or **time=** are given, the current date and/or time is changed. The assignment parameter **zone=** changes the timezone used by the unit.

When no parameters are given, the current date and time is displayed.

The **--list-zones flag**, lists all available timezones.

This flag can not be combined with any setting of time, date or timezone.

#### **exit**

Usage: **exit**

With this command, you exit from the command line interface.

## help

Usage: **help** [command ...]

When this command is given without parameters, you get a list of available commands and tips about how to exit and how to interrupt a command.

If you enter a command, you will get information about how to use that command.

## interface-status \*

Usage: **interface-status** [interface ...]

With this command, you display status information for network interfaces.

If no interface is specified, status information for all interfaces are displayed.

\* Note that **interface-status** [interface ...] is not available for Ingate Software SIParator/Firewalls.

## list-errors

Usage: **list-errors** [--verbose] [table ...]

List errors in a table. If no table name is entered, all errors in tables in the preliminary configuration are listed.

With the **--verbose** flag, a longer description of each error is displayed.

## operational-mode

Usage: **operational-mode** firewall | siparator

This command selects operational mode firewall or SIParator.

## ping

Usage: **ping** ip-address | dns-name

Check if a host is reachable using ICMP Echo Request (ping). To use DNS names, a DNS server must be configured for the unit.

## reboot

Usage: **reboot** [--now]

This command reboots the unit.

## terminal-coding

Usage: **terminal-coding** encoding

Sets the character encoding used by the terminal. Supported encodings are ascii, iso-8859-1 and utf-8.

## **terminal-speed**

Usage: **terminal-speed bits/second**

Sets the speed (in bits/second) used by the terminal. This is only effective on the serial port console. The speed will be reset to the default when you logout from the console.

## **traceroute**

Usage: **traceroute ip-address | dns-name**

Check the route for a packet to a remote host. To use DNS names, a DNS server must be configured for the unit.

## **unit-information**

Usage: **unit-information**

Shows information about this unit.

## **17.1.2. Modifying Tables**

### **add-row**

Usage: **add-row table [field=value ...]**

With this command, you add a row to a table and enter values into the listed fields for that row.

Note that this command cannot be used on tables with a fixed number of rows. These tables are marked with "Fixed" or "Single row" in the **Table Definitions** section.

### **clear-table**

Usage: **clear-table table**

Remove all rows from a table.

Note that this command cannot be used on tables with a fixed number of rows. These tables are marked with "Fixed" or "Single row" in the **Table Definitions** section.

### **delete-row**

Usage: **delete-row table rowid [rowid ...]**

With this command, you delete one or more rows from a table. You get row IDs with the **dump-table** command.

Note that this command cannot be used on tables with a fixed number of rows. These tables are marked with "Fixed" or "Single row" in the **Table Definitions** section.

## **describe-table**

Usage: **describe-table** [--all] [table ...]

Describe a table (or all tables) with its fields and field types.

## **dump-table**

Usage: **dump-table** [--all] [--single-line] [table ...]

With this command, you show the contents of one or more tables. This is done as a number of commands that will re-create the data.

For tables with a fixed number of rows, a number of **modify-row** commands will be shown. For tables with a dynamic number of rows, there will be a **clear-table** command followed by a number of **add-row** commands.

The **--all** flag will make the unit show all tables. When this flag is used, you must not enter a table name.

The **--single-line** flag formats the output to make each command a single line. Otherwise, long commands will be split over multiple lines to make them easier to read and edit manually.

## **list-tables**

Usage: **list-tables** pattern

List all tables matching the given pattern. The wildcard character "\*" can be used in the pattern.

If you would like to find all tables with the string "forward" somewhere in the name, enter this:

**list-tables \*forward\***

## **load-factory**

Usage: **load-factory** [--all]

With this command, you reset the preliminary configuration to the factory default.

The **--all** flag resets all tables to their default values. Currently this flag is mandatory.

## **modify-row**

Usage: **modify-row** table [rowid] field=value [field=value ...]

With this command, you modify the listed fields of an existing row in a table. You get row IDs with the **dump-table** command.

If the table has a single fixed row ("Single row"), no row ID is required.

## **revert-edits**

Usage: **revert-edits** [--all]

With this command, you reset the preliminary configuration to the permanent configuration.

The --all flag resets all tables to their permanent configuration. Currently this flag is mandatory.

### **17.1.3. Test Run and Apply Conf**

#### **abort-testrun**

Usage: **abort-testrun**

With this command, you abort the ongoing test run.

#### **acknowledge-event**

Usage: **acknowledge-event**

Some events need to be acknowledged before you can enter any new commands. These events include when the unit ends a time-limited test mode.

Whenever you need to acknowledge an event, you will be prompted to do so by the CLI.

#### **confirm-testrun**

Usage: **confirm-testrun**

With this command, you confirm the ongoing test run, making the preliminary configuration permanent.

#### **continue-testrun**

Usage: **continue-testrun**

With this command, you enter an unlimited test mode. This can only be done when a test run is in progress. When in the unlimited test mode, you can make the preliminary configuration permanent using the **confirm-testrun** command, or abort the test run using the **abort-testrun** command.

#### **start-testrun**

Usage: **start-testrun** [timelimit]

With this command, you enter a limited test run of the unit's preliminary configuration. The test run will be automatically aborted when the time limit has expired, unless you enter the unlimited test mode using the **continue-testrun** command, or make the configuration permanent using the **confirm-testrun** command.

The test run can also be manually aborted using the **abort-testrun** command.

The time limit is specified in seconds. If no time limit is entered, the limit set in the

`webgui.testmode` table is used.

## 17.2. Table Definitions

Here, the tables used in the Command Line Interface (CLI) are defined. For each table, the fields in the table are defined. Types and selections are defined in subsequent sections.

### 17.2.1. `db.cert.cas`

A list of CA certificates for use in the Ingate.

Field Name	Field Type	Explanation
cert	OptCACertificate	The CA certificate.
crl	OptCertCrl	A certificate revocation list.
name	Name	The reference name for this certificate.

### 17.2.2. `db.cert.own_certs`

A list of own X.509 certificates.

Field Name	Field Type	Explanation
cert	OptPrivCert	An X.509 certificate.
name	Name	The reference name for this certificate.

### 17.2.3. `db.config.allow_config`

A list of networks allowed to connect to the Ingate via HTTP or HTTPS for administration purposes.

Field Name	Field Type	Explanation
client_network	DnsIpNetwork_Filter	The network allowed to connect to the Ingate for administration purposes.
from_tunnel	OptIpsecPeerReference	Select if configuration traffic must be sent via an IPsec peer.
http	OnOffButton	Select if this row should apply to HTTP.
https	OnOffButton	Select if this row should apply to HTTPS.
logclass	LogclassReference	The logclass for this configuration traffic.
number	Integer	The rule number.
ssh	OnOffButton	Select if this row should apply to SSH.

### 17.2.4. db.config.allow\_via\_interface

Select to allow configuration traffic (HTTP, HTTPS, and SSH) via the different interfaces of the Ingate.

Field Name	Field Type	Explanation
config_on	OnOffToggle	Allow configuration via this interface.
interface	TunnelOrIfReference	An interface on the Ingate.

### 17.2.5. db.config.auth\_logclass

The log class for configuration server logins.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.6. db.config.authentication

Select how administrator logins via HTTP and HTTPS should be authenticated.

Field Name	Field Type	Explanation
auth_type	ConfigAuthSel	The authentication method to use for administrators.

### 17.2.7. db.config.authentication\_session

Settings regarding authenticated web GUI sessions.

Field Name	Field Type	Explanation
pwd_timeout	PasswordTimeout	The authentication timeout in web GUI.

### 17.2.8. db.config.mgmt\_logclass

The log class for administration and configuration.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.9. db.config.servers

The IP address, port, cert and TLS settings which should allow connections to the administrator interface,

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate to use for this IP/port combination.
ip	OptOwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.
protocol	ConfigProtoSel	The protocol to allow connection to.
tls	OptTlsReference	The TLS settings to use for this IP/port combination.

### 17.2.10. db.ems.cwmp\_acs

Settings for ACS.

Field Name	Field Type	Explanation
acs_password	cwmp_acs_password	Authentication password to use against the ACS.
acs_username	OptName	Authentication username to use against the ACS.
cacert	OptCaReference	The CA certificate to use for verifying the ACS's certificate.
path	OptString	The ACS's URI path component.
port	cwmp_port	The ACS's port.
server	OptDnsReachableHost	The ACS's IP address.
sslver	cwmp_acs_sslver	The TLS version to use against the ACS.
urischeme	cwmp_urischeme	The ACS's URI scheme.

### 17.2.11. db.ems.cwmp\_acs\_hidden

Hidden settings for ACS.

Field Name	Field Type	Explanation
parameterkey	OptString	ParameterKey.

### 17.2.12. db.ems.cwmp\_acs\_misc

Misc settings for ACS.

Field Name	Field Type	Explanation
p_enable	OnOffToggle	PeriodicInformEnable.
p_interval	PositiveSysInteger	PeriodicInformInterval.

Field Name	Field Type	Explanation
p_time	OptDateISO8601	PeriodicInformTime.

### 17.2.13. db.ems.cwmp\_cpe

Settings for CPE.

Field Name	Field Type	Explanation
cr_password	cwmp_cpe_password	Connection Request password.
cr_username	OptName	Connection Request username.
local_ip	OptOwnIpReference	IP address to listen for Connection Requests.
local_port	cwmp_port	Port to listen for Connection Requests.
privcert	OptCertReference	Private certificate to use for Connection Requests.

### 17.2.14. db.ems.cwmp\_cpe\_gui\_access

GUI Access settings for CPE.

Field Name	Field Type	Explanation
access_type	AdminTypeSel	The administrator type to use when accessing the GUI.
local_ip	OptOwnIpReference	The IP address to use for accessing the GUI.
local_port	OptPortNumber	The port to use for accessing the GUI.
urischeme	cwmp_urischeme	URI scheme to use for accessing the GUI.

### 17.2.15. db.ems.cwmp\_cpe\_gui\_access\_active

Enable/Disable GUI Access via ACS.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.16. db.ems.cwmp\_cpe\_misc

Misc settings for CPE.

Field Name	Field Type	Explanation
bkl_duration	PositiveSysInteger	Blacklist duration.

Field Name	Field Type	Explanation
bkl_interval	PositiveSysInteger	A time interval (in seconds) where connection attempts are counted.
bkl_max	NonNegativeInteger	The maximum number of connection attempts within the time interval.

### 17.2.17. db.ems.cwmp\_debug\_logclass

The log class for CWMP debug messages.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.18. db.ems.cwmp\_error\_logclass

The log class for CWMP error messages.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.19. db.ems.cwmp\_info\_logclass

The log class for CWMP informational messages.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.20. db.ems.ems\_active

Enable/Disable CWMP.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.21. db.failover.iface\_ref\_hosts

A list of reference hosts for the failover team.

Field Name	Field Type	Explanation
address	DnsDynIpOtherHost	The IP address of the reference host.
interface	InterfaceSel	The interface to which the reference host is connected.

### 17.2.22. db.failover.servers

The IP address, port, cert and TLS settings which should allow connections to the standby unit's web interface.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate to use for this IP/port combination.
ip	OwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.
protocol	StandbyAccessProtoSel	The protocol to allow connection to.
src	NetgroupReference	The source addresses which are allowed to use this relay.
tls	OptTlsReference	The TLS settings to use for this IP/port combination.

### 17.2.23. db.fent.always\_fent

Always enable SIP NAT Traversal for selected addresses.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.24. db.fent.always\_fent\_exceptions

Addresses to exclude from always activate SIP NAT Traversal.

Field Name	Field Type	Explanation
exclude_netgroup	NetgroupReference	The network to exclude.

### 17.2.25. db.fent.always\_fent\_interfaces

Interfaces and VLANs on which to always activate SIP NAT Traversal.

Field Name	Field Type	Explanation
interface	VlanIfReference	The interface or VLAN to include.

### 17.2.26. db.fent.fent

Turn the SIP NAT Traversal on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.27. db.fent.fent\_keepalive

Type of keepalive to use for fented clients.

Field Name	Field Type	Explanation
tcp_timeout	PositiveSysInteger	Timeout for TCP - adapt to the NAT used (seconds).
type	FentKeepaliveSel	Use which method to keep fented clients alive.
udp_timeout	PositiveSysInteger	Timeout for UDP - adapt to the NAT used (seconds).

### 17.2.28. db.fent.map\_signal\_address

Map signaling address for remote users.

Field Name	Field Type	Explanation
listen_ip	OptOwnIpReference	Incoming destination IP address.
listen_port	OptPortNumber	Incoming destination port.
send_ip	OptAliasIpReference	Outgoing source IP address.

### 17.2.29. db.fent.media\_release

Route media directly between clients behind the same NAT.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.30. db.fent.reset\_friend

Accept late media source change for RSC.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.31. db.fent.stun

Settings for the builtin STUN server.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turn the STUN server on or off.
port1	OptPortNumber	One port of the STUN server, used by both IP addresses.

Field Name	Field Type	Explanation
port2	OptPortNumber	Another port of the STUN server, used by both IP addresses.
server1	OptDepOwnIpReference	One IP address of the STUN server.
server2	OptDepOwnIpReference	Another IP address of the STUN server.

### 17.2.32. db.firewall.allow\_icmpv6\_rfc4890

Allow ICMPv6 types and codes specified in RFC 4890, section 4.3.1, to the firewall.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.33. db.firewall.blind\_route\_policy

This policy controls how packets from currently unused gateways should be treated.

Field Name	Field Type	Explanation
action	BlindSel	The policy to use for packets from unused gateways.

### 17.2.34. db.firewall.broadcast\_logclass

The log class for broadcast packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.35. db.firewall.cloud\_logclass

The log class for cloud information.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.36. db.firewall.default\_policy

This setting specifies how the Ingate should treat packets that do not match any other configured rule.

Field Name	Field Type	Explanation
action	PolicySel	The policy to use for packets that don't match any

### 17.2.37. db.firewall.dhcp\_logclass

The log class for DHCP packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.38. db.firewall.dhcp\_relay

Define forwarding of DHCP requests from one network to a server on a different network.

Field Name	Field Type	Explanation
enabled	OnOffToggle	The status of the DHCP relay.
interface	OptDepUsableVlanInterface	The interface on which to listen for DHCP requests.
port	PortNumber	The server port to which DHCP requests should be forwarded.
server	OptDnsReachableHost	The server IP address to which DHCP requests should be forwarded.

### 17.2.39. db.firewall.forwarding\_rules

The firewall rules allowing or blocking traffic through the Ingate.

Field Name	Field Type	Explanation
action	FunctionSel	The policy for how this type of traffic should be treated.
client_netgroup	NetgroupReference	The source network for the traffic.
comment	OptComment	A comment field for the administrator.
enabled	OnOffToggleOn	Turns this rule on or off.
from_tunnel	OptIpsecPeerReference	An optional source IPsec tunnel.
logclass	FirewallLogclassReference	How traffic matching this rule should be logged.
number	Integer	The rule number.
server_netgroup	NetgroupReference	The destination network for the traffic.
service	ServicesReference	The service to allow or block.
timeclass	TimeclassReference	When this rule is active.
to_tunnel	OptIpsecPeerReference	An optional destination IPsec tunnel.

### 17.2.40. db.firewall.master\_logclass

The master log function affects all log messages from rules, relays and configuration traffic.

Field Name	Field Type	Explanation
logclass	FirewallLogclassReference	The log class to use when <i>always</i> is selected.
override	OverrideSel	Select how much of the traffic through the firewall is logged.

### 17.2.41. db.firewall.nd\_logclass

The log class for Neighbor Discovery packets sent/received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.42. db.firewall.network\_groups

In this table all groups of computers/IP addresses are defined, to be used when configuring the rest of the Ingate.

Field Name	Field Type	Explanation
interface	OptVlanTunnelOrIfReference	The interface or VLAN of the Ingate on which this IP range is located.
lower_ip	OptDnsIpAddress	The first IP address in the range for this group.
name	GroupName	A name of the network group. It is used when referring to it from this or other tables.
subgroup	SubGroup	A reference to the <i>name</i> field. Used when building a network group from multiple other groups.
upper_ip	OptDnsIpAddress	The last IP address in the range for this group. This field can be left empty if the group is a single IP address.

### 17.2.43. db.firewall.own\_logclass

The log class for packets addressed to the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.44. db.firewall.ping\_policy

This setting specifies how the Ingate should reply to ping packets to its own IP addresses.

Field Name	Field Type	Explanation
policy	PingPolicySel	Select the policy.

### 17.2.45. db.firewall.policy\_logclass

The log class for packets that are processed according to the default policy of the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.46. db.firewall.protocols

Defines IP protocols used when building up services.

Field Name	Field Type	Explanation
name	Name	The name of this protocol. This name is used to refer to the protocol in other tables.
protocol	ProtocolRangeList	The protocol number. Should be a number between 1 and 255.

### 17.2.47. db.firewall.relays

The relays forwarding traffic received by the Ingate.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate to use, only for certain relay types.
client_netgroup	NetgroupReference	The computers which are allowed to use this relay.
from_tunnel	OptIpsecPeerReference	An IPsec peer from which the traffic should originate.
listen_ip	OwnIpReference	The IP address on which the Ingate should listen.
listen_port	PortRange	The port or port range on which the Ingate should listen.
logclass	FirewallLogclassReference	How traffic matching this relay should be logged.
relay_type	RelayTypeSel	The relay type to use when forwarding the traffic.
server_ip	DnsReachableHost	The IP address to which traffic should be forwarded.

Field Name	Field Type	Explanation
server_port	OptPortNumber	The port to which traffic should be forwarded. May be empty to preserve the original port.
timeclass	TimeclassReference	When this relay is active.
tls	OptTlsReference	The TLS settings to use, only for certain relay types.

### 17.2.48. db.firewall.services

Defines services used when building up firewall rules.

Field Name	Field Type	Explanation
client_ports	OptPortRangeList	Ports from which the traffic originates.
data_ports	OptPortRangeList	Related data_ports used by Dynamic FTP management
fwtype	FilterTypeSel	The filter type to use for this service.
ixmptype	OptIcmpRangeList	Type for ICMP packets.
name	GroupName	A name of the service. It is used to refer to this service.
protocol	OptProtocolReference	A reference to the <i>name</i> field of the <i>db.firewall.protocols</i> table.
server_ports	OptPortRangeList	Ports to which the traffic is destined.
subgroup	SubGroup	A reference to the <i>name</i> field. Used when building a service from multiple other services.

### 17.2.49. db.firewall.spoofing\_logclass

The log class for spoofed packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.50. db.firewall.timeclasses

Time classes are defined to make time-limited rules and SIP routing possible.

Field Name	Field Type	Explanation
from_day	WeekdaySel	The day when the time class starts.

Field Name	Field Type	Explanation
from_time	Time_HH_MM	The time when the time class starts.
name	GroupName	A name of the time class. It is used when referring to it from other tables.
to_day	WeekdaySel	The day when the time class ends.
to_time	Time_HH_MM	The time when the time class end.

### 17.2.51. db.firewall.tunnel\_logclass

The log class for Tunnel packets sent/received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.52. db.idsips.active

Switches the IDS/IPS module on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.53. db.idsips.limits

Table for SIP system limits.

Field Name	Field Type	Explanation
max_load	Percent	Max allowed SIP subsystem load.

### 17.2.54. db.idsips.packet\_filtering

Table for user specified IDS/IPS packet filtering rules.

Field Name	Field Type	Explanation
action	FunctionSel	The action to take for this packet filter.
enabled	OnOffToggleOn	Turns this packet filter on or off.
match	OptIDSIPSPacketMatchingReference	What to match on for this packet filter.
name	IpsRuleName	User-defined name.

Field Name	Field Type	Explanation
number	Integer	The packet filter number.

### 17.2.55. db.idsips.packet\_matching

Table for user specified IDS/IPS packet matching rules.

Field Name	Field Type	Explanation
case	OnOffButton	Make the regexp case sensitive.
message	OptSipMessageSel	The SIP message type to match on.
name	GroupName	A name of the packet matching group. It is used when referring to it from this or other tables.
neg	OnOffButton	The logical negation of the match.
part	OptSipMessagePartSel	The SIP message part to match on.
regexp	OptLongRegexp	The regexp to match on.
source	OptNetgroupReference	The source network to match on.
transport	OptTransportSel	The transport protocol to match on.

### 17.2.56. db.idsips.rate\_limiting

Table for user specified IDS/IPS rate limiting rules.

Field Name	Field Type	Explanation
auto	OnOffButton	Makes the hits number hardware agnostic.
blacklist	Blacklist	The blacklist interval (in seconds).
cc	OnOffButton	Count hits based on match with capturing groups.
enabled	OnOffToggleOn	Turns this rule on or off.
hits	Hits	The number of hits inside the given window.
match	OptIDSIPSPacketMatchingReference	What to match on.
name	IpsRuleName	User-defined name.
window	Window	Time interval (in seconds) for hits.

## 17.2.57. db.ipsec.blacklisted\_packets

Settings for IPsec blacklisted packets.

Field Name	Field Type	Explanation
action	PolicySel	Action taken for blacklisted packets.
logclass	VPNLogclassReference	Log class for blacklisted packets.

## 17.2.58. db.ipsec.blacklisting

IPsec blacklisting settings.

Field Name	Field Type	Explanation
duration	Integer	The blacklist interval (seconds).
logclass	VPNLogclassReference	Log class for IPsec blacklistings.

## 17.2.59. db.ipsec.crypto\_def

A list of IPsec crypto definitions, to be used in other tables.

Field Name	Field Type	Explanation
auth	IpsecAuthSel	The authentication algorithm to use.
encryption	IpsecEncSel	The encryption algorithm to use.
name	Name	The name of this crypto definition. This name is used to refer to the definition in other tables.

## 17.2.60. db.ipsec.esp\_proposals

A list of ESP crypto proposals.

Field Name	Field Type	Explanation
crypto	CryptoDefReference	A crypto definition.
name	GroupName	The name of this proposal. This name is used to refer to the proposal in other tables.
number	Integer	The order of cryptos in this proposal.

### 17.2.61. db.ipsec.espah\_logclass

The log class for ESP packets.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

### 17.2.62. db.ipsec.ike\_logclass

The log class for IKE and NAT-T packets.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

### 17.2.63. db.ipsec.ike\_proposals

A list of IKE crypto proposals.

Field Name	Field Type	Explanation
crypto	CryptoDefReference	A crypto definition.
group	IsakmpGroupSel	Diffie-Hellman group.
name	GroupName	The name of this proposal. This name is used to refer to the proposal in other tables.
number	Integer	The order of cryptos in this proposal.

### 17.2.64. db.ipsec.interop

Interoperability settings.

Field Name	Field Type	Explanation
enable_psk_rw	OnOffToggle	Enable PSK authentication from Road Warriors.

### 17.2.65. db.ipsec.ipsec\_nets

A list of networks which will use IPsec connections.

Field Name	Field Type	Explanation
name	Name	A name of the network. It is used to refer to this network.
network	DnsIpNetwork_Filter	The network to be tunneled through an IPsec tunnel.

## 17.2.66. db.ipsec.modecfg

A list of modecfg configurations.

Field Name	Field Type	Explanation
banner	OptString	Authorization banner text.
dns1	OptDnsIpAddress	First DNS server.
dns2	OptDnsIpAddress	Second DNS server.
domain	OptDomainName	A domain name.
iprange	NetgroupReference	The IP address range.
name	Name	The name for this modecfg configuration.

## 17.2.67. db.ipsec.nat\_t\_keepalive

NAT-T keepalive settings.

Field Name	Field Type	Explanation
interval	Integer	The interval between two keepalive packets (seconds).

## 17.2.68. db.ipsec.peers

A list of IPsec peers for the Ingate.

Field Name	Field Type	Explanation
auth_type	AuthTypeSel	The authentication type for this peer.
enabled	OptOnOffToggleOn	Activate this peer.
ikev2	Ikev2Sel	IKEv2 settings.
isakmp_sa_life	IsakmpSALife	ISAKMP key lifetime.
local_addr	OptOwnIpReference	The Ingate's IP address to which this peer must connect.
name	GroupName	A name of the peer. It is used to refer to this peer.
proposal	IkeCryptoReference	Crypto algorithms to use.
radius	OptOnOffToggle	Activate RADIUS authentication for a road warrior peer.
rekey	OptOnOffToggleOn	Re-key tunnel when it expires.
remote_addr	OptDnsAutoRuntimeNoPARPHost	The peer's IP address.
secret	AuthData	Authentication data for this peer.

Field Name	Field Type	Explanation
subgroup	SubGroup	A reference to the <i>name</i> field. Used when building a peer from multiple other peers.

### 17.2.69. db.ipsec.peers\_advanced

Advanced settings for IPsec Peers.

Field Name	Field Type	Explanation
dpd_action	DpdActionSel	Action to take when the peer is considered dead.
dpd_delay	DpdDelay	Delay (in seconds) between DPD keepalives.
dpd_enabled	OnOffToggle	Enable/Disable Dead Peer Detection.
dpd_timeout	DpdTimeout	Timeout (in seconds) before the peer is considered dead.
ikev2_esn	Ikev2EsnSel	Select support for IKEv2 ESN.
localid_type	IdTypeSel	Local ID type.
localid_value	OptString	Local ID value.
modecfg	OptIpsecModeCfgReference	Enable/Disable IKE Mode-Configuration.
nat_t	NatTraversalSel	Detect or force NAT Traversal.
peer	OptIpsecPeerReference	The peer for which the advanced settings applies to.
remoteid_type	IdTypeSel	Remote ID type.
remoteid_value	OptString	Remote ID value.

### 17.2.70. db.ipsec.pluto\_logclass

The log class for IPsec key negotiations.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

### 17.2.71. db.ipsec.plutoverbose\_logclass

The log class for verbose messages from IPsec key negotiations.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

## 17.2.72. db.ipsec.radiusauth\_server

The Ingate IP address and port to use for road warrior RADIUS authentication. A certificate must also be selected.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate to use for this IP/port combination.
ip	OptOwnIpReference	An IP address of this unit.
port	PortNumber	A port number of the IP address.
tls	TlsReference	The TLS settings to use for this IP/port combination.

## 17.2.73. db.ipsec.tunneled\_nets

Definitions of which networks can use each IPsec connection.

Field Name	Field Type	Explanation
ipsec_sa_life	IpsecSALife	IPsec key lifetime.
local_net	OptIpsecNetReference	The local network which can use the connection.
local_type	IpsecNetLocalSel	The type of IP for which the IPsec connection is negotiated and which can use the connection.
nat_as_address	OptOwnIpReference	What address traffic through this tunnel should be NAT:ed as, if set. The IPsec SA will be negotiated for this address too, instead of the specified local network.
peer	IpsecPeerGroup	The peer for which network definitions are made.
pfs	PfsGroupSel	The PFS group to use when initiating.
proposal	EspCryptoReference	Crypto algorithms we propose.
remote_net	OptIpsecNetReference	The remote network which can use the connection.
remote_type	IpsecNetRemoteSel	The type of IP for which the IPsec connection is negotiated and which can use the connection.

### 17.2.74. db.ipsec.userauth\_logclass

The log class for IPsec user authentications.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

### 17.2.75. db.ipsec.x509\_cacerts

Certificates for CAs which have signed IPsec peer certificates.

Field Name	Field Type	Explanation
ca	CaReference	A CA certificate.

### 17.2.76. db.ipsec.x509\_cert

The X.509 certificate to use for IPsec connections.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate of this unit.

### 17.2.77. db.ipsec.xauth\_users

A list of XAUTH users in the system.

Field Name	Field Type	Explanation
enabled	OnOffToggleOn	Activate the user.
password	XauthPassword	The password for this user.
peer	OptIpsecPeerReference	The peer for which the user applies to.
username	Name	The username of the XAUTH user.

### 17.2.78. db.misc.contrack\_timeouts

Timeouts for connections through the Ingate.

Field Name	Field Type	Explanation
icmp	PositiveSysInteger	Timeout for ICMP connections.
icmp6	PositiveSysInteger	Timeout for ICMPv6 connections.
tcp_established	PositiveSysInteger	Timeout for established TCP connections.
udp	PositiveSysInteger	Timeout for one-way UDP connections.

Field Name	Field Type	Explanation
udp_stream	PositiveSysInteger	Timeout for two-way UDP connections.

### 17.2.79. db.misc.default\_domain

The default domain when entering configuration.

Field Name	Field Type	Explanation
domain	OptDomainName	A domain name to use in the settings.

### 17.2.80. db.misc.dhcp\_server

Configuration for the DHCP server.

Field Name	Field Type	Explanation
gateway	OptDnsAutoIpAddress	The default gateway for DHCP clients.
interface	OptDepUsableVlanInterface	The Ingate interface to listen for DHCP requests.
lower_ip	DnsIpAddress	The first IP address in the range reserved for DHCP clients.
options	dhcp_server_options_reference	DHCP Server options.
upper_ip	DnsIpAddress	The last IP address in the range reserved for DHCP clients.

### 17.2.81. db.misc.dhcp\_server\_data\_type

Grouping DHCP data types.

Field Name	Field Type	Explanation
name	GroupName	A name of the data type.
order	Integer	The order of this row.
type	dhcp_server_data_type_sel	A data type.

### 17.2.82. db.misc.dhcp\_server\_dns\_servers

The DNS servers to give out to clients, if others than the Ingate uses itself.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
server	DnsDynIpReachableHost	A DNS server.

### 17.2.83. db.misc.dhcp\_server\_domain

The domain which the DHCP server should give out.

Field Name	Field Type	Explanation
domain	OptDomainName	The domain to use.

### 17.2.84. db.misc.dhcp\_server\_give\_ns

Controls if the DHCP server should give out DNS servers to clients.

Field Name	Field Type	Explanation
enabled	AutoConfOffSel	Select how to assign DNS servers.

### 17.2.85. db.misc.dhcp\_server\_lease\_time

Lease intervals for the DHCP server.

Field Name	Field Type	Explanation
default	DhcpLeaseTime	The default time.
max	DhcpLeaseTime	The maximum time.
min	DhcpLeaseTime	The minimum time.

### 17.2.86. db.misc.dhcp\_server\_netbios\_enabled

Enable or disable NetBIOS over TCP/IP for Microsoft clients.

Field Name	Field Type	Explanation
enabled	OptOnOffToggleOn	NetBIOS over TCP/IP setting.

### 17.2.87. db.misc.dhcp\_server\_netbios\_nodetype

The NetBIOS node type to give out to clients.

Field Name	Field Type	Explanation
type	NetbiosNodeTypeSel	The NetBIOS node type.

### 17.2.88. db.misc.dhcp\_server\_options

DHCP Server options.

Field Name	Field Type	Explanation
array_of	OnOffToggle	Allow multiple values.
group_name	GroupName	Name of the option group.

Field Name	Field Type	Explanation
opt_code	DhcpOptionCode	DHCP option code.
opt_data_type	dhcp_server_data_type_reference	DHCP data type.
opt_name	Name	Name of the option.
opt_value	LongStringListQuote	The value of the option.

### 17.2.89. db.misc.dhcp\_server\_status

Activate the built-in DHCP server.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.90. db.misc.dhcp\_server\_wins\_servers

WINS server which the DHCP server should give out.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
server	DnsReachableHost	The WINS server.

### 17.2.91. db.misc.dns\_preference

A list of DNS lookup preferences which the Ingate can use.

Field Name	Field Type	Explanation
preference	DnsPreferenceSel	A DNS lookup preference.

### 17.2.92. db.misc.dns\_servers

A list of DNS servers which the Ingate can use.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
server	DnsDynIpReachableHost	A DNS server.

### 17.2.93. db.misc.dyndns

Settings for the DynDNS service.

Field Name	Field Type	Explanation
backup	OnOffToggle	The SMTP server entered here is a backup server.

Field Name	Field Type	Explanation
ca	OptCaReference	The CA certificate used to verify the server certificate of the Dynamic DNS service.
enabled	OnOffToggle	Activate update via DynDNS.
ip	OptDepOwnIpReference	The local IP address to be referred to for the host names listed here.
mx	OptDomainName	The SMTP server for the domain(s).
offline	OnOffToggle	Use offline URL redirection.
password	DyndnsPassword	The DynDNS password.
service	DyndnsServiceSel	The DynDNS service to use.
user	OptName	The DynDNS user name.
wildcard	OnOffToggle	Use wildcard host names.

### 17.2.94. db.misc.dyndns\_name

A list of host and domain names to be updated at DynDNS.

Field Name	Field Type	Explanation
name	DomainName	A host or domain name.

### 17.2.95. db.misc.force\_nlck

Force running nlck on reboot.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.96. db.misc.fversion

Activate version control on the Ingate.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.97. db.misc.ntp\_servers

A list of NTP servers to use.

Field Name	Field Type	Explanation
server	DnsDynIpReachableHost	A server name or IP address.

## 17.2.98. db.misc.options

List advanced options.

Field Name	Field Type	Explanation
name	Identifier	The option name.
value	OptString	The option value.

## 17.2.99. db.misc.radvd\_interface\_settings

RA interface settings.

Field Name	Field Type	Explanation
def_router	OptOnOffToggleOn	Advertise as default router.
interface	UsableVlanInterface	The interface for which RA should be enabled.
managed_flag	OptOnOffToggle	Managed address configuration flag (M-bit).
name	Name	Name of the RA interface.
other_flag	OptOnOffToggle	Other configuration flag (O-bit).
rdnss	OptOnOffToggleOn	Send RDNSS (Recursive DNS Server) if available.

## 17.2.100. db.misc.radvd\_prefix\_settings

RA prefix settings.

Field Name	Field Type	Explanation
interface	radvd_interface_ref	The interface that the prefix will advertised on.
prefix	radvd_prefix_ref	The prefix to be advertised via RA.

## 17.2.101. db.misc.radvd\_prefixes

A list of prefixes which can be advertised via RA.

Field Name	Field Type	Explanation
name	Name	A name of the prefix. It is used to refer to this network.
prefix	DnsIpAddress	The prefix to be advertised via RA.

### 17.2.102. db.misc.radvd\_status

Activate the radvd daemon.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.103. db.misc.unitname

The name of this Ingate unit.

Field Name	Field Type	Explanation
unitname	OptString	The user-defined name.

### 17.2.104. db.misc.use\_ntp

Activate NTP for the Ingate system clock.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.105. db.monitor.cpubload\_level\_alarm

When to create alarm messages for high CPU load.

Field Name	Field Type	Explanation
max_cpubload	OptPercent	The load level when an alarm message should be created and the alarm state set.
ok_cpubload	OptPercent	The load level when the alarm state is reset.

### 17.2.106. db.monitor.email\_alert\_logclass

The log class for email errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.107. db.monitor.email\_server

The SMTP server to use when log messages are sent to an email address.

Field Name	Field Type	Explanation
server	OptDnsReachableHost	A server name or IP address.

### 17.2.108. db.monitor.fan\_level\_alarms

When to create alarm messages for slow-going fans.

Field Name	Field Type	Explanation
alarmby	Integer	The fan speed when an alarm message should be created and the alarm state set.
resumeby	Integer	The fan speed when the alarm state is reset.

### 17.2.109. db.monitor.hardware\_logclass

The log class for hardware errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.110. db.monitor.logclasses

A list of log classes used in the Ingate.

Field Name	Field Type	Explanation
email	OptString	Enter email address(es) which the log message should be sent to.
facility	SyslogFacilitySel	Select the syslog facility to use.
level	SyslogLevelSel	Select the syslog level to use.
local	OnOffToggle	Turn on or off logging to local disk/memory.
name	Name	The name of the log class. The name is used when referring to this log class.

### 17.2.111. db.monitor.memory\_level\_alarm

When to create alarm messages for high memory usage.

Field Name	Field Type	Explanation
max_memory	OptPercent	The memory usage level when an alarm message should be created and the alarm state set.
ok_memory	OptPercent	The memory usage level when the alarm state is reset.

### 17.2.112. db.monitor.radius\_errors\_logclass

The log class for RADIUS errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.113. db.monitor.sip\_level\_alarms

When to create alarm messages for used SIP User Registration and Session licenses.

Field Name	Field Type	Explanation
max_registered_users	OptNonNegativeInteger	The number of registered users when an alarm message should be created and the alarm state set.
max_sessions	OptNonNegativeInteger	The number of sessions when an alarm message should be created and the alarm state set.
ok_registered_users	OptNonNegativeInteger	The number of registered users when the alarm state is reset.
ok_sessions	OptNonNegativeInteger	The number of sessions when the alarm state is reset.

### 17.2.114. db.monitor.snmp\_agent\_address

The IP address of the Ingate which responds to SNMP requests.

Field Name	Field Type	Explanation
snmpagentip	OptDepOwnIpReference	The IP address to respond to SNMP requests.

### 17.2.115. db.monitor.snmp\_agent\_logclass

The log class for SNMP errors.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.116. db.monitor.snmp\_contact\_person

The contact person for this Ingate.

Field Name	Field Type	Explanation
snmp_contact_person	OptDepString	The name of the contact.

### 17.2.117. db.monitor.snmp\_management\_stations

The servers allowed to send SNMP requests to the Ingate.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	The server network.

### 17.2.118. db.monitor.snmp\_node\_location

The location of this Ingate.

Field Name	Field Type	Explanation
snmp_node_location	OptDepString	The location.

### 17.2.119. db.monitor.snmp\_packet\_logclass

The log class for SNMP requests received by the Ingate.

Field Name	Field Type	Explanation
logclass	LogclassReference	A log class.

### 17.2.120. db.monitor.snmp\_trap\_cwmp\_sending

Turn SNMP trap sending via CWMP on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.121. db.monitor.snmp\_trap\_receivers

A list of SNMP trap receivers.

Field Name	Field Type	Explanation
community	NonWhiteName	The SNMP community to use when sending traps.
server	DnsReachableHost	The server to receive traps.
version	SnmpTrapVersionSel	The SNMP version to use when sending traps.

### 17.2.122. db.monitor.snmp\_trap\_sending

Turn SNMP trap sending on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.123. db.monitor.snmp\_v1v2c\_access

Turn SNMP access using version 1 or version 2c on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.124. db.monitor.snmp\_v1v2c\_auth

Authentication for SNMP requests v1 and v2c.

Field Name	Field Type	Explanation
community	NonWhiteName	A community.

### 17.2.125. db.monitor.snmp\_v3\_access

Turn SNMP access using version 3 on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.126. db.monitor.snmp\_v3\_auth

Authentication for SNMP requests v3.

Field Name	Field Type	Explanation
authentication	SnmpV3AuthSel	Authentication algorithm used for this user.
password	SnmpPassword	The password for this user.
privacy	SnmpV3PrivacySel	Encryption algorithm used for this user.
user	NonWhiteName	A user allowed to make SNMP requests.

### 17.2.127. db.monitor.syslog\_servers

A list of syslog servers where log messages should be sent.

Field Name	Field Type	Explanation
server	DnsDynIpReachableHost	A server name or IP address.

### 17.2.128. db.monitor.watchdogs

Watchdog settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns this watchdog on or off.
service	NonWhiteName	The service monitored.

### 17.2.129. db.network.alias\_addresses

A list of extra Ingate IP addresses on the networks defined in the *db.network.local\_nets* table.

Field Name	Field Type	Explanation
address	DnsIpAddress	The IP address to use.
interface	InterfaceSel	The interface to which the network is connected.
name	Name	A name for this IP address. It is used to refer to the IP address.

### 17.2.130. db.network.discard\_weird\_fragments

Activate discarding of weird fragments, typically overlaps.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.131. db.network.extra\_default\_gateways

A list of additional default routers.

Field Name	Field Type	Explanation
gateway	DnsDynIpAddress	The router to use for this network.
interface	InterfaceSel	The interface where the router is located.
name	Name	The name of this default gateway.

### 17.2.132. db.network.interfaces

Interface settings.

Field Name	Field Type	Explanation
autoneg	AutonegSel	Set speed and duplex for the interface.
enabled	OnOffToggle	Enable the interface.
interface	InterfaceSel	The physical interface.
name	Name	A name for this interface.

### 17.2.133. db.network.local\_nets

A list of IP networks directly connected to the Ingate, and the Ingate's IP addresses on these networks.

Field Name	Field Type	Explanation
address	DnsDynIpNetwork_Interface	The IP address of the interface, and the netmask of the network.
interface	TunnelOrIfReference	The interface to which the network is connected.
name	Name	A name for this IP address. It is used to refer to the IP address.
vlanid	OptVlanId	The VLAN associated with the network.

### 17.2.134. db.network.masquerading

A list of the directions in which traffic should be NATed.

Field Name	Field Type	Explanation
destination_interface	TunnelOrIfReference	The destination computer is located behind this interface.
destination_network	OptDnsIpNetwork_Filter	The destination computer is located on this network.
nat_as_address	OptOwnIpReference	Use this IP address when this traffic is NATed.
number	Integer	The priority of this row.
source_interface	TunnelOrIfReference	The source computer is located behind this interface.
source_network	OptDnsIpNetwork_Filter	The source computer is located on this network.

### 17.2.135. db.network.port\_allocations

Local port ranges

Field Name	Field Type	Explanation
auto_lower	PortNumber	The lowest port number in the auto range.
auto_upper	PortNumber	The highest port number in the auto range.
ftp_lower	PortNumber	The lowest port number in the FTP range.

Field Name	Field Type	Explanation
ftp_upper	PortNumber	The highest port number in the FTP range.
local_lower	PortNumber	The lowest port number in the local range.
local_upper	PortNumber	The highest port number in the local range.
nat_lower	PortNumber	The lowest port number in the NAT range.
nat_upper	PortNumber	The highest port number in the NAT range.

### 17.2.136. db.network.pppoe

PPPoE settings.

Field Name	Field Type	Explanation
lcp_echo_interval	OptPositiveSysInteger	Keep alive packet interval (seconds).
logclass	FirewallLogclassReference	The log class to use for PPPoE negotiations.
password	OptPassword	The PPPoE password.
service	OptNonWhiteString	The PPPoE service.
user	OptNonWhiteString	The name of the PPPoE user.

### 17.2.137. db.network.proxy\_arp

A list of proxy ARP entries.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface where extruded addresses are located.
local_addr	OwnIp4Reference	Directly connected network to extrude addresses from.
network	DnsIp4Network_Filter	Subnet or address to extrude to another interface.
vlanid	OptVlanId	The VLAN where extruded addresses are located.

### 17.2.138. db.network.route\_test\_servers

A list of reference servers to use when determining if a default gateway is alive.

Field Name	Field Type	Explanation
server	DnsIpAddress	The reference server to use.

### 17.2.139. db.network.routes

A list of static routes for networks not directly connected to the Ingate.

Field Name	Field Type	Explanation
destination	RouteDestination	The routed network.
gateway	OptDnsDynIpAddress	The router to use for this network.
interface	TunnelOrIfReference	The interface where the router is located.
priority	RoutePriority	The priority of the gateway.

### 17.2.140. db.network.tunnels\_6in4

Tunnel settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Enable the tunnel.
local_addr	OwnIp4Reference	Local tunnel endpoint.
name	TunnelIdentifier	A name for this tunnel.
remote_addr	DnsReachableHost	Remote tunnel endpoint.

### 17.2.141. db.network.tunnels\_6rd

Tunnel settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Enable the tunnel.
ipv4_mask_len	IPv4MaskLen	The number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain.
local_addr	OwnIp4Reference	Local tunnel endpoint.
name	TunnelIdentifier	A name for this tunnel.
network	DnsIpNetwork_Filter	The IPv6 network
remote_addr	DnsReachableHost	Remote tunnel endpoint.

### 17.2.142. db.network.tunnels\_6to4

Tunnel settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Enable the tunnel.
local_addr	OwnIp4Reference	Local tunnel endpoint.
name	TunnelIdentifier	A name for this tunnel.

### 17.2.143. db.network.unreachable

A list of unreachable routes.

Field Name	Field Type	Explanation
destination	RouteDestination	The unreachable network.

### 17.2.144. db.network.vlans

A list of VLANs used on the different interfaces.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface on which the VLAN is defined.
name	Name	A name of the VLAN. It is used to refer to this VLAN.
vlanid	VlanId	The id of this VLAN.

### 17.2.145. db.pptp.gre\_logclass

The log class for GRE packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

### 17.2.146. db.pptp.pptp\_enable

Turn the PPTP function on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.147. db.pptp.pptp\_logclass

The log class for PPTP packets received by the Ingate.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

## 17.2.148. db.pptp.pptp\_nets

Settings for the built-in PPTP server.

Field Name	Field Type	Explanation
client_netgroup	OptDepNetgroupReference	The range of IP addresses for PPTP clients.
dns1	OptDnsIpAddress	The DNS server which PPTP clients should use.
dns2	OptDnsIpAddress	A second DNS server which PPTP clients should use.
lcp_echo_interval	OptPositiveSysInteger	Keep alive packet interval (seconds).
local_addr	OptDepOwnIpReference	The local gateway for PPTP clients.
wins1	OptDnsIpAddress	The WINS server which PPTP clients should use.
wins2	OptDnsIpAddress	A second WINS server which PPTP clients should use.

## 17.2.149. db.pptp.pptp\_serverip

The IP address for the PPTP server in the Ingate.

Field Name	Field Type	Explanation
ip	OptDepOwnIpReference	The server IP address.

## 17.2.150. db.pptp.pptp\_users

A list of PPTP users in the system.

Field Name	Field Type	Explanation
enabled	OnOffToggleOn	Activate the user.
password	PptpPassword	PPTP password for this user.
user	Name	The name of the PPTP user.

## 17.2.151. db.pptp.pptpneg\_logclass

The log class for PPTP negotiations to the Ingate PPTP server.

Field Name	Field Type	Explanation
logclass	VPNLogclassReference	A log class.

## 17.2.152. db.qos.bandwidths

QoS bandwidth settings per interface.

Field Name	Field Type	Explanation
egress_bandwidth	OptBandWidth	Egress bandwidth limit for the interface (kbit/s).
egress_enabled	OnOffToggle	Use egress QoS for this interface.
egress_reserve_sip_media	OptBandWidth	Bandwidth reservation for outgoing SIP media (kbit/s). Currently only applies to UDP.
egress_reserve_sip_media_emergency	OptBandWidth	Bandwidth reservation for outgoing emergency SIP media (kbit/s). Currently only applies to UDP.
ingress_bandwidth	OptBandWidth	Ingress bandwidth limit for the interface (kbit/s).
ingress_enabled	OnOffToggle	Use ingress QoS for this interface.
ingress_reserve_sip_media	OptBandWidth	Bandwidth reservation for incoming SIP media (kbit/s). Currently only applies to UDP.
ingress_reserve_sip_media_emergency	OptBandWidth	Bandwidth reservation for incoming emergency SIP media (kbit/s). Currently only applies to UDP.
interface	InterfaceSel	The interface for which QoS settings are made.

## 17.2.153. db.qos.classes

A list of QoS classes used for matching incoming traffic.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	The source network for the traffic.
dscp	OptDSCPInteger	The DSCP field of the packets.
max_packet_size	OptPacketSize	The maximum packet size for the traffic.
min_packet_size	OptPacketSize	The minimum packet size for the traffic.
name	Name	The name of this class. This name is used to refer to the class in other tables.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
server_netgroup	OptNetgroupReference	The destination network for the traffic.
service	OptServicesReference	The service matching the traffic.
sip	SipSel	The traffic type.
tos	OptTosSel	The TOS field of the packets.

### 17.2.154. db.qos.egress\_default\_queueing

Assign priority and bandwidth for traffic not listen in the *db.qos.egress\_queueing* table.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	PriorityQueueSel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

### 17.2.155. db.qos.egress\_queueing

Assign priority and bandwidth for different types of traffic.

Field Name	Field Type	Explanation
cname	QoSClassReference	The traffic for which bandwidth is assigned or limited.
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	PriorityQueueSel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

### 17.2.156. db.qos.ingress\_default\_queueing

Assign priority and bandwidth for traffic not listen in the *db.qos.ingress\_queueing* table.

Field Name	Field Type	Explanation
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	PriorityQueueSel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

### 17.2.157. db.qos.ingress\_queueing

Assign priority and bandwidth for different types of traffic.

Field Name	Field Type	Explanation
cname	QoSClassReference	The traffic for which bandwidth is assigned or limited.
interface	InterfaceSel	The interface for the outgoing traffic.
limit	OptPercentFloat	Bandwidth limit (kbit/s).
queue	PriorityQueueSel	Priority queue for the traffic.
rate	OptPercentFloat	Bandwidth assignment (kbit/s).

### 17.2.158. db.qos.sip\_cac

Call Admission Control settings.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Use Call Admission control.

### 17.2.159. db.qos.status

Global QoS settings.

Field Name	Field Type	Explanation
prio_save	Percent	Save this amount of bandwidth for lower priority traffic.
type	QoSTypeSel	Type of QoS to use.

### 17.2.160. db.qos.tagging

A list of traffic to mark up by setting the TOS or DSCP field.

Field Name	Field Type	Explanation
cname	QoSClassReference	The traffic to mark up.
dscp	OptDSCPInteger	Set the DSCP field.
tos	OptTosSel	Set the TOS field.

### 17.2.161. db.qturn.accounting

Accounting level.

Field Name	Field Type	Explanation
level	QTurnAccountingSel	Accounting level.

### 17.2.162. db.qturn.active

Turns the Q-TURN module on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.163. db.qturn.allow\_unauthenticated

Allow unauthenticated users.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	Allowed networks and computers.

### 17.2.164. db.qturn.cert

The X.509 certificate to use for Q-Turn connections.

Field Name	Field Type	Explanation
cert	OptCertReference	A certificate of this unit.

### 17.2.165. db.qturn.debug\_level

Debug level.

Field Name	Field Type	Explanation
level	QTurnDebugLevelSel	Verbosity level.

### 17.2.166. db.qturn.default\_password

.

Field Name	Field Type	Explanation
password	QTurnUserPassword	Turn user password.

### 17.2.167. db.qturn.listen

A list of additional ports for incoming Q-Turn signaling to the Ingate.

Field Name	Field Type	Explanation
comment	OptComment	A comment field for the administrator.
enabled	OnOffToggle	Enable to listen.
port	PortNumber	The port on which to listen.

Field Name	Field Type	Explanation
transport	QTurnTransportListenSel	The accepted Q-Turn transports on this port.

### 17.2.168. db.qturn.media\_ports

The port range the Ingate should use for Q-Turn.

Field Name	Field Type	Explanation
ports_lower	PortNumber	The lowest port number in the range.
ports_upper	PortNumber	The highest port number in the range.

### 17.2.169. db.qturn.relay\_device

.

Field Name	Field Type	Explanation
interface	OptUsableVlanInterface	The interface to which the network is connected.

### 17.2.170. db.qturn.signaling\_acl

Q-Turn signaling access control.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	Allowed networks and computers.

### 17.2.171. db.qturn.users

A list of Q-Turn users for this Ingate.

Field Name	Field Type	Explanation
password	QTurnUserPassword	The password for the user.
user	QTurnUserName	The name of this Q-Turn user.

### 17.2.172. db.sip.accelerated\_tls

Accept TCP marked as TLS.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.173. db.sip.active

Turns the SIP module on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.174. db.sip.add\_expire\_header

Select if an Expires header should be added to the response to a SIP REGISTER request.

Field Name	Field Type	Explanation
action	AddExpireHeaderSel	Select which action to perform.

### 17.2.175. db.sip.add\_ice\_candidates

Add ourself as an ICE candidate to the SDP.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.176. db.sip.add\_incoming\_port\_to\_ruri

Interop fix for Ingate Bug #4923.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.177. db.sip.allow\_rtp\_before\_answer\_sdp

Allow RTP before receiving the answer SDP.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.178. db.sip.allowed\_codecs

Field Name	Field Type	Explanation
add	OnOffToggle	Add this codec
allow	OnOffToggle	Allow this codec.
bandwidth	OptPositiveSysInteger	Bandwidth needed by this codec.
name	WildcardIdentifier	Name of codec.
type	OptCodecTypeSel	Type of codec.

### 17.2.179. db.sip.allowed\_media

Field Name	Field Type	Explanation
ports_lower	PortNumber	The lowest port number in the range.
ports_upper	PortNumber	The highest port number in the range.
transport	TransportSel	The transport protocol.

### 17.2.180. db.sip.allowed\_origins

Allowed WebSocket Origins.

Field Name	Field Type	Explanation
host	DomainNameOrIpStr	The origin's host.
port	OptPortNumber	The origin's port.
scheme	OriginSchemeSel	The origin's scheme.

### 17.2.181. db.sip.always\_add\_path

Interop fix for Ingate Bug #1938.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.182. db.sip.always\_relay\_media

Always relay media.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.183. db.sip.asserted\_identity

Turn use of P-Asserted-Identity on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.184. db.sip.assign\_ip\_alias\_by\_user

Automatically assign an IP alias based on From.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.185. db.sip.auth\_methods

Allow and authenticate SIP requests based on which SIP method is used.

Field Name	Field Type	Explanation
allow	OnOffToggleOn	Allow this type of SIP request.
auth	OnOffToggle	Require authentication for this type of SIP request.
method	SipMethod	The SIP method for which the settings are made.
traffic_to	SipAuthDirSel	The direction of the SIP request.

### 17.2.186. db.sip.b2bua\_answer\_pt\_changes

Setting for b2bua to detect codec changes in mid call answers.

Field Name	Field Type	Explanation
cond	PtChangesSel	When to detect pt changes.

### 17.2.187. db.sip.b2bua\_detect\_noop\_sdp

Keep session version in B2BUA when unchanged by remote endpoint.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.188. db.sip.b2bua\_fwd\_3xx\_hdrs

Forward 3xx headers in the B2BUA.

Field Name	Field Type	Explanation
header	NonemptyString	Header to forward.

### 17.2.189. db.sip.b2bua\_offer\_from\_template

The B2BUA can use a template SDP if it needs an offer and no other is available.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.190. db.sip.b2bua\_offer\_in\_invite

Should B2BUA always send offer in INVITE, also when there is no offer in the incoming INVITE.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.191. db.sip.b2bua\_send\_prack

Send PRACK in the B2BUA.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.192. db.sip.b2bua\_pending\_timeout

SIP B2bua\_pending\_timeout configuration.

Field Name	Field Type	Explanation
timeout	NonNegativeInteger	Timeout in seconds, 0 is disabled.

### 17.2.193. db.sip.b2bua\_receive\_prack

Receive PRACK in the B2BUA.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.194. db.sip.b2bua\_reinvites\_end\_to\_end

Should B2BUA wait for response from real UAS before responding to re-INVITE.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.195. db.sip.bpc\_auth

Brute force authentication protection.

Field Name	Field Type	Explanation
interval	OptPositiveSysInteger	A time interval (in seconds) where authentication attempts are counted.
max_attempts	OptPositiveSysInteger	The maximum number of authentication attempts within the time interval.
noresp	OptNonNegativeSysInteger	Do not respond with a challenge after this interval.
size	MaxBPCSize	The maximum number of IP addresses (clients) to keep track of.

### 17.2.196. db.sip.break\_friendships

When a reIVITE to a different RTP endpoint (i.e. call transfer) reaches the B2BUA the old media state (friendships) is torn down before the new one is setup.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.197. db.sip.codec\_filtering

Turn codec filtering on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.198. db.sip.convert\_5xx\_to\_503

Convert 5xx response codes to 503.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.199. db.sip.data\_interfaces

Interfaces between which data traffic should be allowed in WAN mode.

Field Name	Field Type	Explanation
interface	DepUsableVlanInterface	The interface.

### 17.2.200. db.sip.default\_gateway

Specify which default gateway should SIP should use by default.

Field Name	Field Type	Explanation
gateway	OptExtraGwReference	The additional gateway to use.

### 17.2.201. db.sip.dialing\_domains

List domain names/IP addresses that should not be rewritten when forwarded by the Ingate.

Field Name	Field Type	Explanation
ip	DnsIpAddress	The domain name.

### 17.2.202. db.sip.dns\_override\_on\_recursion

DNS Override when recusing on 3xx.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.203. db.sip.emergency

PSTN emergency number.

Field Name	Field Type	Explanation
emergency	NoCommaString	The emergency number.

### 17.2.204. db.sip.extern\_radius\_db

Settings for SIP authorization and authentication.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	The network from which RADIUS database SIP users are allowed to register.
db_type	SipRadiusSel	Which database to use for SIP authorization and authentication.

### 17.2.205. db.sip.external\_relay

Match on the domain in the Request-URI, and send the request on to a different server.

Field Name	Field Type	Explanation
auth	OnOffToggle	Require authentication.
domain	DomainGroup	Matches the domain in the Request-URI.
modify_ruri	OnOffToggle	Modify the Request-URI of the SIP request with the new destination before it is forwarded.
port	OptPortNumber	Port to forward the request to.
priority	Rfc2782Priority	Priority of this IP address. A lower number is a higher priority.
relay_to	DnsReachableHost	SIP domain or IP address to forward the request to.
transport	SipTransportSel	Transport to use when forwarding the request.

Field Name	Field Type	Explanation
weight	Rfc2782Weight	Weight of this IP address. For IP addresses of the same priority, requests are forwarded according to their weight. A higher number means more requests.

### 17.2.206. db.sip.fake\_proxy\_supported\_privacy

Fake that the proxy supports the privacy option tag.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.207. db.sip.find\_gruu\_locally

Interop fix for Ingate Bug #1263.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.208. db.sip.fix\_bad\_route\_set

Interop fix for Ingate Bug #2261.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.209. db.sip.fix\_bye\_route\_set

Interop fix for Ingate Bug #4593.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.210. db.sip.fix\_file\_transfer\_port

Always open port 6891 for file transfer.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.211. db.sip.force\_3264\_hold

Force compliance to RFC 3264 in SDP answers for hold.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.212. db.sip.force\_inactive\_hold

Interop fix for Ingate Bug #4825.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.213. db.sip.force\_modify

List domain names/IP addresses that should always be rewritten when forwarded by the Ingate.

Field Name	Field Type	Explanation
domain	WildcardDomainOrIp	The domain name.

### 17.2.214. db.sip.force\_ptime

Interop fix for Ingate Bug #4673.

Field Name	Field Type	Explanation
ptime	OptRtpPacketizationTime	Packetization time (ms)

### 17.2.215. db.sip.forward\_cancel\_body

Forward packet body from incoming CANCEL to outgoing CANCEL.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.216. db.sip.forward\_to\_header

Forward the To header through B2BUA instead of replacing it.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.217. db.sip.forward\_user\_agent

Forward the User-agent header through B2BUA instead of replacing it.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

## 17.2.218. db.sip.fw\_siparator\_nat

Enable or disable SIParator NAT in Firewall mode.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

## 17.2.219. db.sip.global\_policies

Miscellaneous SIP settings.

Field Name	Field Type	Explanation
sip_policy	SipFunctionSel	The default policy for SIP requests. Exceptions are made in the <i>db.sip.relay_rules</i> table.
sipauth_allow_rfc2069	OnOffToggle	Turn on or off support for authentication according to RFC 2069.
sipauth_enabled	OnOffToggle	Turn SIP Authentication on or off.
sipauth_realm	OptString	The SIP realm to use for authentication.

## 17.2.220. db.sip.header\_filter\_default

Default rule for processing SIP requests based on the From and To headers.

Field Name	Field Type	Explanation
action	SipFilterActionSel	The action to take for requests.

## 17.2.221. db.sip.header\_filter\_rules

Rules for processing SIP requests based on the From and To headers.

Field Name	Field Type	Explanation
action	SipFilterActionSel	The action to take for this request.
from_header	HeaderPattern	A pattern to match the From header of the request.
number	Integer	Priority of this rule. A lower number is a higher priority.
to_header	HeaderPattern	A pattern to match the To header of the request.

### 17.2.222. db.sip.hide\_rr

Peers for which we need to hide our Record-Route header.

Field Name	Field Type	Explanation
ip	DnsReachableHost	The server for which to hide Record-Route header.

### 17.2.223. db.sip.hide\_rr\_all

Hide Record-Route for all servers..

Field Name	Field Type	Explanation
enabled	OnOffButton	Hide Record-Route for all servers.

### 17.2.224. db.sip.hide\_sensitive

Hide sensitive information in sip log messages (bug 2222).

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.225. db.sip.ignore\_uri\_port\_when\_maddr

Ignore port in URI when an maddr parameter is present.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.226. db.sip.inhibit\_hold

Replace hold SDP with sendrecv.

Field Name	Field Type	Explanation
action	InhibitHoldSel	Select which action to perform.

### 17.2.227. db.sip.is\_multiple\_2xx\_media

Fix for Ingate Bug #3779.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.228. db.sip.large\_udp

Select to allow larger UDP packets than the standard allows, instead of switching to TCP signaling.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.229. db.sip.listen

A list of ports for incoming SIP signaling to the Ingate.

Field Name	Field Type	Explanation
comment	OptComment	A comment field for the administrator.
enabled	OnOffToggle	If this row is active.
port	PortNumber	The port on which to listen.
transparent	OnOffToggle	Enable transparent proxy mode using a DNAT trap.
transport	SipTransportListenSel	The accepted SIP transports on this port.

### 17.2.230. db.sip.local\_domains

The SIP domains that this Ingate should be registrar for.

Field Name	Field Type	Explanation
domain	DomainNameOrIpStr	A SIP domain.

### 17.2.231. db.sip.loose\_refer\_to

Accept Refer-To headers with ? but no angle brackets.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.232. db.sip.loose\_user\_name\_check

Only use the username, not the domain, when authenticating.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.233. db.sip.lr\_true

Select to use *lr=true* in routing headers.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.234. db.sip.media\_encryption\_dtls\_srtp

SIP media encryption DTLS-SRTP settings.

Field Name	Field Type	Explanation
cert	OptCertReference	The X.509 certificate to use for DTLS-SRTP.
dtls	TlsReference	The DTLS settings to use.
ign_cert_dates	OnOffToggle	Ignore invalid DTLS-SRTP certificate dates.

### 17.2.235. db.sip.media\_encryption\_policy

Standard encryption settings. Exceptions are made in the *db.sip.media\_encryption\_rules* table.

Field Name	Field Type	Explanation
allow_transcoding	OnOffToggle	Allow transcoding of signaling.
allowed_suites	OptMediaEncryptionSuiteReference	The crypto group allowed.

### 17.2.236. db.sip.media\_encryption\_rules

Encryption settings per networks and computers. Exceptions from the standard policy set in *db.sip.media\_encryption\_policy*.

Field Name	Field Type	Explanation
allow_transcoding	OnOffToggle	Allow transcoding of signaling for this network.
allowed_suites	OptMediaEncryptionSuiteReference	The crypto group allowed via this network.
media_netgroup	NetgroupReference	The network and computers for which encryption settings are made.
number	Integer	Rule number.

### 17.2.237. db.sip.media\_encryption\_settings

SIP media encryption settings.

Field Name	Field Type	Explanation
b2bua	OnOffToggle	Add cryptos in the b2bua.
enabled	OnOffToggle	Turn media encryption on or off.
multi_profile	OnOffToggle	Enable multi profile (SAVP/AVP) handling.

Field Name	Field Type	Explanation
prefer_rtp_savp	RtpProfileSelection	Use RTP/SAVP descriptions.
require_tls	OnOffToggle	Require TLS for all cryptos but cleartext.
use_last_computed	OnOffToggle	Keep established crypto within a dialog.

### 17.2.238. db.sip.media\_encryption\_suite

Grouping crypto methods.

Field Name	Field Type	Explanation
name	GroupName	A name of the crypto methods group.
suite	MediaEncryptionSuiteSel	An encryption method.

### 17.2.239. db.sip.media\_ports

The port range the Ingate should use for SIP media.

Field Name	Field Type	Explanation
ports_lower	PortNumber	The lowest port number in the range.
ports_upper	PortNumber	The highest port number in the range.

### 17.2.240. db.sip.media\_proxy

SIP media proxy settings.

Field Name	Field Type	Explanation
add_ssrc	OnOffToggle	Add SSRC.
enabled	OnOffToggle	Turn media proxy on or off.
force	OnOffToggle	Always use the Media Proxy.
terminate_ice	OnOffToggle	Terminate ICE.
terminate_rtcp_mux	OnOffToggle	Terminate RTCP-MUX.

### 17.2.241. db.sip.media\_restriction

Limit where SIP media can be sent from.

Field Name	Field Type	Explanation
max_senders	MaxSenders	Allowed number of senders.
medialock	MediaLockSel	Media sender limitation.

### 17.2.242. db.sip.media\_stream\_linger

Behaviour for no longer used media streams.

Field Name	Field Type	Explanation
time	NonNegativeInteger	Linger time for unreferenced media streams.

### 17.2.243. db.sip.media\_timeouts

SIP media timeouts.

Field Name	Field Type	Explanation
oneway	OptPositiveSysInteger	One-way media stream timeout (seconds).
rtcp	OptPositiveSysInteger	RTCP stream timeout (seconds).
rtp	OptPositiveSysInteger	RTP stream timeout (seconds).
tear_down	OnOffToggle	Select to tear down media streams at RTP/RTCP timeout.

### 17.2.244. db.sip.message

Set the maximum SIP message size that the Ingate should accept.

Field Name	Field Type	Explanation
limit_max_forwards	NonNegativeInteger	The limit of the Max-Forwards header value.
max_message_size	MaxMessageSizeInteger	The maximum size of SIP messages.
servername	ServerName	The value to use in our own Server and User-Agent headers.

### 17.2.245. db.sip.mfull

Select to match incoming SIP requests on username and domain instead of only on username.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.246. db.sip.mimetypes

A list of content types to allow or reject in SIP packets.

Field Name	Field Type	Explanation
allowed	OnOffToggle	Allow or reject packets with this content type.

Field Name	Field Type	Explanation
mimetype	MimeType	A content type in a SIP packet.

### 17.2.247. db.sip.modify\_referto

Interop fix for Ingate Bug #5433.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.248. db.sip.monitor\_server

Monitored SIP servers.

Field Name	Field Type	Explanation
port	OptPortNumber	The port to be monitored on the server.
server	UnresolvedReachableHost	The server to be monitored.
transport	OptSipTransportSel	The transport to be monitored on the server.

### 17.2.249. db.sip.music\_on\_hold

Play music on hold.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.250. db.sip.music\_on\_hold\_servers

The music on hold servers to use (currently no more than one).

Field Name	Field Type	Explanation
port	OptPortNumber	The port of the MOH server.
transport	OptSipTransportSel	The transport used by the MOH server.
userdomain	OptSipUri	The IP address or SIP domain of the MOH server, optionally including user.

### 17.2.251. db.sip.no\_sip\_to\_nat

Do not redirect packets to NATed addresses to sipfw, block them.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.252. db.sip.option\_timeout

SIP blacklist/monitoring interval. If the interval is set to zero (0) neither blacklisting nor monitoring will be done.

Field Name	Field Type	Explanation
timeout	OptionTimeout	Blacklist interval (seconds).

### 17.2.253. db.sip.outbound\_proxy

Where to send SIP requests. Multiple outbound proxies can be used based on the domains in the From header and request-URI of the request.

Field Name	Field Type	Explanation
from_domain	SipUserDomainDefaultAll	Matches the domain part of the From header.
gateway	OptExtraGwReference	Optional extra gateway to use instead of default one.
proxy_domain	UnresolvedReachableOrLocalHost	IP address or SIP domain to forward the request to.
proxy_port	OptPortNumber	Port to forward the request to.
ruri_domain	SipUserDomainDefaultAll	Matches the domain part of the request-URI.
send_ip	OptAliasIpReference	Optional IP alias used as sender address.

### 17.2.254. db.sip.pai\_use\_from

Copy From header to P-Asserted-Identity on or off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.255. db.sip.percent20\_to\_whitespace

Turns the conversion of %20 to a real whitespace on and off in sipfw.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.256. db.sip.preloaded\_route\_default

Default rule for processing preloaded routes.

Field Name	Field Type	Explanation
action	SipPreloadedRouteActionSel	The action to take for requests.

### 17.2.257. db.sip.preloaded\_route\_rules

Rules for processing preloaded routes based on the source network.

Field Name	Field Type	Explanation
action	SipPreloadedRouteActionSel	The action to take for the request.
number	Integer	Rule number.
source	NetgroupReference	The source network of the request.

### 17.2.258. db.sip.preserve\_2543\_hold

Perform Hold according to the old RFC2543.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.259. db.sip.public\_ip

The public IP for a NATed Ingate box. Used in SIP signaling.

Field Name	Field Type	Explanation
ip	OptDnsReachableHost	An IP address.

### 17.2.260. db.sip.radius\_acct

RADIUS accounting on the unit.

Field Name	Field Type	Explanation
diversion	OnOffToggle	Include first Diversion header in RADIUS accounting.
enabled	OnOffToggle	Turns RADIUS accounting on or off.
media	OnOffToggle	Include media statistics in RADIUS accounting.
p_asserted_identity	OnOffToggle	Include first P-Asserted-Identity header in RADIUS accounting.

Field Name	Field Type	Explanation
remote_party_id	OnOffToggle	Include first Remote-Party-Id header in RADIUS accounting.

### 17.2.261. db.sip.radius\_acct\_interfaces

In this table the interfaces available for media accounting are defined.

Field Name	Field Type	Explanation
if_enabled	OptVlanIfReference	Do account for this interface.

### 17.2.262. db.sip.recurse\_on\_3xx\_in\_b2bua

Enables recursion on 3xx in the B2BUA, instead of the proxy, if recursion is enabled in reply\_config.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.263. db.sip.redirect\_server

SIP redirect server.

Field Name	Field Type	Explanation
server	OptDnsReachableHost	A server name or IP address.

### 17.2.264. db.sip.referto\_replacement

Specify replacement domain used in Refer-To header for domains/IPs this server is responsible for.

Field Name	Field Type	Explanation
domain	OptDomainNameOrIpStr	The replacement domain name.
type	ReferToReplacementSel	One of <i>never</i> , <i>blind</i> and <i>both</i> .

### 17.2.265. db.sip.referto\_with\_b2bua\_callid

Handle INVITE with Replaces containing a Call-Id known by a B2BUA regardless if the Request URI belongs to the B2BUA or not.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.266. db.sip.register\_force\_aor\_user

Force use of To header username in Contact header of REGISTER requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.267. db.sip.register\_wait

Interop fix for Ingate Bug #4673.

Field Name	Field Type	Explanation
delay	OptRtpPacketizationTime	Delay (s)

### 17.2.268. db.sip.registrar\_limits

Limitations for the built-in SIP registrar.

Field Name	Field Type	Explanation
max_registrations	MaxReg	The allowed number of registrations per user.
max_users	OptNonNegativeInteger	The allowed number of registered users.
registration_timeout	RegTimeout	Registration timeout (seconds).

### 17.2.269. db.sip.reinvites\_disable

Interop fix for Ingate Bug #4673.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.270. db.sip.relay\_rules

Rules for processing SIP requests based on the source network.

Field Name	Field Type	Explanation
action	SipFunctionSel	The action to take for this request.
client_netgroup	NetgroupReference	The source network of the request.
number	Integer	Priority of this rule. A lower number is a higher priority.

### 17.2.271. db.sip.remove\_sdp\_from\_1xx

Interop fix for Ingate Bug #4955.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.272. db.sip.remove\_via

Remove Via headers from requests sent to the listed servers.

Field Name	Field Type	Explanation
ip	DnsReachableHost	The server for which to remove Via headers.

### 17.2.273. db.sip.remove\_via\_all

Remove Via headers from requests sent to all servers.

Field Name	Field Type	Explanation
enabled	OnOffButton	Remove Via headers for all servers.

### 17.2.274. db.sip.reply\_config

Select if 3xx messages (redirection messages) should be forwarded to the endpoint or used in the Ingate box.

Field Name	Field Type	Explanation
class3	Class3Sel	Select how to use 3xx messages.

### 17.2.275. db.sip.req\_same\_signal\_media\_grp

Reject Signaling and Media on different Networks

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.276. db.sip.resolve\_domains\_in\_sdp

Resolve domain names in the SDP

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.277. db.sip.reuse\_media\_port

Reuse media port numbers.

Field Name	Field Type	Explanation
ignore_media	OnOffToggle	when changing media (e.g. T.38 FAX)
in_session	ReuseMediaPortSel	within same session

### 17.2.278. db.sip.rewrite\_from\_for\_register\_in\_dp

Rewrite From headers for REGISTER requests passed through the Dial Plan.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.279. db.sip.rewrite\_to\_for\_register\_in\_dp

Rewrite To headers for REGISTER requests passed through the Dial Plan.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.280. db.sip.ringback

Ringback settings.

Field Name	Field Type	Explanation
action	RingbackSel	Select when ringback should be played.
tone_type	RingToneTypeSel	Type of ring tone to play (US or UK).

### 17.2.281. db.sip.route180

Make the unit remove the Record-Route and Contact headers in 180 responses to SIP requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.282. db.sip.route\_use\_sport

A list of SIP servers for which the actual source port of previous TLS connections will be reused when connecting with TLS, instead of port 5061.

Field Name	Field Type	Explanation
ip	DnsReachableHost	The IP address of the server.

### 17.2.283. db.sip.routing\_order

Prioritization of routing methods in the Ingate.

Field Name	Field Type	Explanation
function	RoutingPrioritySel	The routing method to be prioritized.
number	Integer	Priority number of the row. Must be unique.

### 17.2.284. db.sip.rroute\_always

Make the unit add a Record-Route header for all SIP requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.285. db.sip.rroute\_outbound

Make the unit add a Record-Route header for all non-local SIP requests.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.286. db.sip.session\_limits

Limitations for SIP sessions.

Field Name	Field Type	Explanation
max_sipsessions	OptNonNegativeInteger	The allowed number of concurrent sessions. If left blank, no limit is set.
max_streams_per_req	MaxStreamsPerSession	The allowed number of media streams per SIP session.
session_timeout	SessionTimeout	Session timeout (seconds).

### 17.2.287. db.sip.signaling\_acl

SIP signaling access control.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	Allowed networks and computers.

## 17.2.288. db.sip.signal\_address\_for\_destination

Select signaling address based on destination.

Field Name	Field Type	Explanation
send_ip	AliasIpReference	Outgoing source IP address.
server	DnsReachableHost	Outgoing destination IP address.

## 17.2.289. db.sip.sip\_alias

Set up forwarding of SIP requests to local SIP users.

Field Name	Field Type	Explanation
alias	SipAliasAlias	The user to which requests should be forwarded.
sips_sel	SipsSel	Select SIP/SIPS for the forwarded request.
transport	OptSipTransportSel	Select the transport to use for forwarded requests.
user	SipUriWithUserWildcardDomain	The user for which requests should be forwarded.

## 17.2.290. db.sip.sip\_errors\_logclass

The log class for SIP errors.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

## 17.2.291. db.sip.sip\_idsips\_logclass

The log class for SIP IDS/IPS messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

## 17.2.292. db.sip.sip\_license\_logclass

The log class for SIP license messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

### 17.2.293. db.sip.sip\_media\_logclass

The log class for SIP media messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

### 17.2.294. db.sip.sip\_message\_logclass

The log class for SIP packets.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

### 17.2.295. db.sip.sip\_signaling\_logclass

The log class for SIP signaling.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

### 17.2.296. db.sip.sip\_verbose\_logclass

The log class for SIP debug messages.

Field Name	Field Type	Explanation
logclass	SIPLogclassReference	A log class.

### 17.2.297. db.sip.st\_type

Sets the SIParator type.

Field Name	Field Type	Explanation
st_type	StTypeSel	The SIParator type.

### 17.2.298. db.sip.strip\_ice\_attributes

Remove ICE attributes from SDP.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.299. db.sip.strip\_sdp\_lines

Strip SDP Lines.

Field Name	Field Type	Explanation
case	OnOffButton	Make the regexp case sensitive.
regexp	LongRegexp	The regexp to match on.

### 17.2.300. db.sip.supported\_disable

Interop fix for Ingate Bug #4673.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.301. db.sip.surroundings

A list of Surroundings for a DMZ SIParator. Used to group networks which are on the same side of the connected firewall.

Field Name	Field Type	Explanation
negotiator_netgroup	OptNetgroupReference	Additional network allowed without spoofing block.
surrounding_netgroup	NetgroupReference	A Surrounding network for a DMZ SIParator.

### 17.2.302. db.sip.tcp\_timeout

Timeout for SIP connections over TCP/TLS.

Field Name	Field Type	Explanation
tcp_timeout	PositiveSysInteger	Timeout for TCP (seconds).

### 17.2.303. db.sip.tel\_to\_outbound\_proxy

Select to send all TEL URI requests to the outbound proxy.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.304. db.sip.terminate\_transferor\_on\_183

Interop fix for Ingate Bug #4762.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.305. db.sip.testua

SIP TestUA configuration.

Field Name	Field Type	Explanation
display_name	OptString	TestUA display name.
uri	OptSipUriWithScheme	TestUA SIP URI.

### 17.2.306. db.sip.testua\_acl

SIP TestUA server access control list.

Field Name	Field Type	Explanation
client_netgroup	NetgroupReference	Allowed netgroups for clients.
transport	TestuaTransportSel	Allowed SIP transport for incoming INVITE.

### 17.2.307. db.sip.testua\_active

Turns the SIP TestUA on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.308. db.sip.testua\_client

SIP TestUA client configuration.

Field Name	Field Type	Explanation
call_duration	TestuaDurationLimit	Test call duration.
call_interval	PositiveSysInteger	Interval between test calls.
call_preferred_pt	RtpPayloadTypeSel	Preferred payload type.
call_ptime	RtpPacketizationTime	Packetization time.
call_to	OptSipUriWithScheme	Test call destination URI.

### 17.2.309. db.sip.testua\_client\_active

Turns the SIP TestUA call client on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.310. db.sip.testua\_server\_active

Turns the SIP TestUA echo server on and off.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.311. db.sip.thirdpcc\_codecs

Codecs in dummy SDP used when forwarding initial INVITEs without SDP, i.e. in third party call control (3pcc) scenarios.

Field Name	Field Type	Explanation
fmt	OptString	Fmt attribute.
name	Identifier	Name of codec.
number	Integer	Order of preference.
params	OptString	Encoding parameters.
pt	OptRtpPayloadType	Payload type, not needed for static codecs.
rate	OptPositiveSysInteger	Clock rate, not needed for static codecs.

### 17.2.312. db.sip.tls\_cacerts

List of CA certificates for TLS connections.

Field Name	Field Type	Explanation
ca	CaReference	A CA certificate.

### 17.2.313. db.sip.tls\_client\_cfg

Default settings for making TLS connections. Exceptions for certain IP addresses listed in *db.sip.tls\_server\_cfg*.

Field Name	Field Type	Explanation
default_cert	OptCertReference	The X.509 certificate to use for TLS connections initiated by the Ingate.
tls	TlsReference	The TLS settings to use for connections initiated by the Ingate.

### 17.2.314. db.sip.tls\_server\_cfg

List of IP addresses on which to accept TLS connections. For the listed IP addresses, the corresponding certificate is also used when making TLS connections from this IP address.

Field Name	Field Type	Explanation
cert	CertReference	The certificate to use for TLS connections on this IP address.
ip	OwnIpReference	An IP address for TLS connections.

Field Name	Field Type	Explanation
require_client_cert	OnOffToggle	Require that the client present a certificate.
tls	TlsReference	The TLS settings to use for connections to this IP.
use_fqdn	OnOffToggle	Present the FQDN from certificate CN.

### 17.2.315. db.sip.tls\_settings

Check that the remote certificate matches the domain.

Field Name	Field Type	Explanation
check_x509_server_subject	OnOffToggle	Turn the setting on or off.
check_x509_server_wildcard	OnOffToggle	Turn wildcard matching on or off.
enabled	OnOffToggle	Turn TLS on or off.

### 17.2.316. db.sip.transaction\_config

Timeouts for SIP requests.

Field Name	Field Type	Explanation
default_timeout	PositiveSysInteger	Default timeout for INVITE requests (seconds).
inv_rt	InviteRetransmitCount	Maximum number of retransmissions for INVITE requests.
max_timeout	PositiveSysInteger	Maximum timeout for INVITE requests (seconds).
ninv_rt	NonInviteRetransmitCount	Maximum number of retransmissions for non-INVITE requests.
timer_a	TimerA_Float	Base retransmission timeout for SIP requests (seconds).

### 17.2.317. db.sip.trusted\_domain

A list of trusted servers and networks for the P-Asserted-Identity header.

Field Name	Field Type	Explanation
cert	OptCaReference	A trusted certificate.
group	AuthGroupSel	Authorized group.
transport	TrustedDomainTransportSel	The transport used by the trusted server(s).

Field Name	Field Type	Explanation
trusted_netgroup	NetgroupReference	A trusted server or network.

### 17.2.318. db.sip.ua\_register

Values used when the UA registers.

Field Name	Field Type	Explanation
expires	UaRegisterInteger	Expires used when registering ourselves.
reg_retries	OnOffToggle	Enables the algorithms for retrying a failed REGISTER.
retry_time	UaRegisterInteger	Retry a failed registration after this long.

### 17.2.319. db.sip.uri\_encode\_update\_on\_refer\_to

Interop fix for Ingate Bug #5255.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.320. db.sip.uri\_encoding

How to encode URIs.

Field Name	Field Type	Explanation
type	UriEncodingSel	Type of URI encoding to do.

### 17.2.321. db.sip.use\_cancel\_body\_in\_ack

Use packet body of CANCEL in corresponding ACK.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.322. db.sip.use\_endpoint\_session\_id

Interop fix for Ingate Bug #5109.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.323. db.sip.use\_rtcp\_attribute

Use the rtcp attribute in the SDP.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.324. db.sip.username\_is\_consecutive\_numbers

Choose algorithm used for selecting IP alias.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on or off.

### 17.2.325. db.sipswitch.accounts

A list of SIP accounts for this Ingate.

Field Name	Field Type	Explanation
auth_name	OptString	The authentication name for the account, if different from the username.
comment	OptComment	A comment field for the administrator.
display_name	OptString	The display name for the account.
domain	SipUserDomain	The domain for the account.
p_asserted_id	OptSipUri	The P-Asserted-Identity for the account.
password	SipUserPassword	The password for the account.
type	AccountTypeSel	The account type for the account.
user	SipUserName	The username for this SIP account.

### 17.2.326. db.sipswitch.b2bua\_transfer\_enable

A list of criteria of when to handle REFER locally.

Field Name	Field Type	Explanation
always	OnOffButton	Always
clients_lack_refer	OnOffButton	For clients that cannot handle REFER.
clients_lack_replace	OnOffButton	For clients that cannot handle Replaces.
use_from_uri	OnOffButton	For requests with listed From URIs.

Field Name	Field Type	Explanation
use_user_agent	OnOffButton	For requests from listed User-Agents.

### 17.2.327. db.sipswitch.b2bua\_transfer\_for\_client

A list of the User-Agents for which REFER requests should be handled locally.

Field Name	Field Type	Explanation
client	NoDoubleQuoteString	The User-Agent field.

### 17.2.328. db.sipswitch.b2bua\_transfer\_from\_user

A list of the From headers for which REFER requests should be handled locally.

Field Name	Field Type	Explanation
user	SipFromUser	The From header.

### 17.2.329. db.sipswitch.dial\_plan

A list of request types and how to process them.

Field Name	Field Type	Explanation
action	DialPlanActionSel	The action to take for this type of SIP request.
comment	OptComment	A comment field for the administrator.
enum_prefix	OptString	A prefix to add to the Request-URI before looking it up in ENUM.
enum_root	EnumReference	The ENUM root to use when performing ENUM lookups.
forward_prefix	OptString	A prefix to add to the Request-URI before it is forwarded.
forward_to	OptForwardToReference	Where to forward the SIP request.
number	Integer	The priority of this row.
reqfrom	OptRequestFromReference	The sender of the SIP request.
ruri	OptRequestToReference	The Request-URI of the SIP request.
timeclass	OptTimeclassReference	When this row is active.

### 17.2.330. db.sipswitch.dial\_plan\_enable

Use the Dial Plan.

Field Name	Field Type	Explanation
enabled	FallbackSel	Use the Dial Plan.

### 17.2.331. db.sipswitch.dial\_plan\_methods

A list of methods which should be routed using the Dial Plan.

Field Name	Field Type	Explanation
method	NonemptyString	A SIP method. Cannot be any of ACK, CANCEL, PRACK, BYE UPDATE, or INFO.

### 17.2.332. db.sipswitch.enum\_root

A list of ENUM roots to use.

Field Name	Field Type	Explanation
name	GroupName	The name of this ENUM root. This name is used to refer to the root in other tables.
number	Integer	The priority of this row.
root	DomainName	The ENUM root.

### 17.2.333. db.tls.ciphers

A table of TLS ciphers.

Field Name	Field Type	Explanation
ciphers	NonemptyString	A cipher string understood by OpenSSL.
name	Name	A name of the ciphers. It is used to refer to these ciphers.

### 17.2.334. db.sipswitch.forward\_to

A list of SIP destinations for the Dial Plan.

Field Name	Field Type	Explanation
account	OptAccountReference	The SIP account to use when the request is forwarded.
alias_ip	OptAliasIpReference	The IP alias to use as source address when the request is forwarded.
domain	OptUnresolvedReachableOrLocalHost	The replacement domain to use when the request is forwarded.

Field Name	Field Type	Explanation
name	GroupName	The name of this destination. This name is used to refer to the destination in other tables.
number	SmallInteger	The priority of this row.
port	OptPortNumber	The destination port to use when the request is forwarded.
regex	OptString	An expression for the Request-URI to use when the request is forwarded.
transport	OptSipTransportSel	The SIP transport to use when the request is forwarded.
trunk	OptTrunkReference	The SIP trunk to use when the request is forwarded.

### 17.2.335. db.sipswitch.incoming\_unauth

A list of SIP users allowed to call local users for which the *restrict\_incoming* function in *db.sipswitch.user\_routing* is enabled.

Field Name	Field Type	Explanation
url	SipWildcardUrl	A matching From header.

### 17.2.336. db.sipswitch.request\_from

A list of matchings on the From header and sending computer.

Field Name	Field Type	Explanation
client_netgroup	OptNetgroupReference	Computer or network from which the request was sent.
domain	OptSipUserDomain	The SIP domain name in the From header.
name	NonemptyString	The name of this sender match. This name is used to refer to the sender in other tables.
regex	OptRegexWithAt	A regular expression to match the From header.
transport	BypassTransportSel	The SIP transport of the incoming request.
username	OptString	The SIP user name in the From header.

### 17.2.337. db.sipswitch.request\_to

A list of matchings on the Request-URI.

Field Name	Field Type	Explanation
domain	OptSipUserDomain	The Request-URI domain part.
head	HeadString	The start of the Request-URI username part (when the prefix has been stripped).
min_tail_length	OptPositiveSysInteger	The minimum number of characters in the tail.
name	NonemptyString	The name of this Request-URI match. This name is used to refer to the Request-URI in other tables.
prefix	OptString	The start of the Request-URI username part. The prefix is stripped when the request is forwarded.
regexp	OptRegexWithAt	Regular expression to match the Request-URI.
tail	RestFuncSel	The rest of the Request-URI username part (after the prefix and head).

### 17.2.338. db.sipswitch.trunk\_main\_lines

New SIP Trunk main lines configuration.

Field Name	Field Type	Explanation
aliases	OptRegex	Incoming Trunk Match.
auth_name	OptString	Optional authentication user id.
from_dn	UseRegex	Optional SIP display name to use for outgoing calls.
from_user	OptRegex	From Number/User.
fwd	UseRegex	Forward to.
is_reg	OnOffToggle	Set to Yes if this account should be registered at the ITSP.
number	SmallInteger	Row number.
p_asserted_identity	UseRegex	Optional value to use in P-Asserted-Identity.
password	TrunkUserPassword	Optional authentication password.
trunk	PositiveSysInteger	Trunk id.
user	UseRegex	The SIP user name to use in the From SIP URI for outgoing calls.

## 17.2.339. db.sipswitch.trunk\_params

New SIP Trunk parameters configuration.

Field Name	Field Type	Explanation
alias_ip	OptAliasIpReference	Use alias IP address.
domain	OptLongStringList	Service Provider Domain.
domain_id	OptLongString	Trunk ID - Domain name.
enabled	OnOffToggle	Use parameters from other SIP trunk
from_domain	FromDomainSel	From header domain selection.
from_domain_str	OptLongString	From domain string.
fwd_refer	OnOffToggle	Forward outgoing REFER to the ITSP.
gin_reg	OnOffToggle	<i>gin</i> registration (RFC 6140).
hide_rr	OnOffToggle	Hide Record-Route.
hide_to_tags	OnOffToggle	Show only one To tag.
itsp_host_addr	OptNetgroupReference	Restrict to calls from.
ltrunk_group_param	OptLongString	Local Trunk Group Parameters (RFC 4904).
ltrunk_group_usage	OptTrunkGroupUsageSel	Local Trunk Group Parameters (RFC 4904) used as.
max_calls_per_line	OptPositiveSysInteger	Max simultaneous calls per Trunk Line.
max_calls_total	OptPositiveSysInteger	Max simultaneous calls (Call Admission Control).
name	OptLongString	Service name.
outbound_gw	OptExtraGwReference	Outbound Gateway.
outbound_proxy	OptLongString	Outbound Proxy.
port	OptPortNumber	Port number.
preserve_max_forwards	OnOffToggle	Preserve Max-Forwards.
redirect_caller_domain	OnOffToggle	SIP 3xx redirection to caller domain.
redirect_home_domain	OnOffToggle	SIP 3xx redirection to provider domain.
referto_domain	OptSipUriAfterAt	Refer-To header domain.
relay_media	OnOffToggle	Relay media.
remove_via	OnOffToggle	Exactly one Via header.
route_incoming	RouteIncomingSel	Route incoming based on.
send_dtmf_via_sip_info	OnOffToggle	Send DTMF via SIP INFO.

Field Name	Field Type	Explanation
transport	OptSipTransportSel	Signaling Transport.
trunk	PositiveSysInteger	SIP Trunk to use parameters from.
trunk_group_param	OptLongString	Remote Trunk Group Parameters (RFC 4904).
trunk_group_usage	OptTrunkGroupUsageSel	Remote Trunk Group Parameters used as.
trusted_networks_enable	OnOffToggle	Service Provider domain is trusted.
use_preferred_identity	OnOffToggle	Use P-Preferred-Identity.

### 17.2.340. db.sipswitch.trunk\_pbx

New SIP Trunks pbx configuration.

Field Name	Field Type	Explanation
alias_ip	OptAliasIpReference	Alias IP address from our side.
auth_name	OptString	Authentication user ID.
common_user_suffix	OptLongString	Common User Name suffix.
domain	OptLongStringList	PBX Domain Name.
enabled	OnOffToggle	Use PBX from other SIP trunk.
from_matching	FromMatchingSel	Match From Number/User in field.
from_matching_str	OptLongString	Match From Number/User field string.
fwd_refer	OnOffToggle	Forward incoming REFER to the PBX.
incoming_fwd_port	OptPortNumber	PBX port number.
incoming_fwd_transport	OptSipTransportSel	PBX Signaling transport.
ipaddr	OptDnsReachableHost	PBX IP Address.
ltrunk_group_usage	OptTrunkGroupUsageSel	Local Trunk Group Parameters usage.
name	OptLongString	PBX name.
password	SipUserPassword	Authentication password.
pbx_host_addr	OptNetgroupReference	PBX Network.
referto_domain	OptSipUriAfterAt	Refer-To header domain.
send_dtmf_via_sip_info	OnOffToggle	Send DTMF via SIP INFO.
to_str	OptLongString	To header field string.
to_type	PbxToHeaderSel	To header field.

Field Name	Field Type	Explanation
trunk	PositiveSysInteger	Trunk id to use PBX settings from.
trunk_group_usage	OptTrunkGroupUsageSel	Remote Trunk Group Parameters usage.
uri	OptLongString	PBX Registration SIP Address.

### 17.2.341. db.sipswitch.trunk\_pbx\_lines

New SIP Trunk PBX lines configuration.

Field Name	Field Type	Explanation
aliases	OptRegexp	Incoming Trunk Match.
auth_name	OptString	Optional authentication user id.
from_dn	UseRegexp	Optional SIP display name to use for outgoing calls.
from_user	OptRegexp	From Number/User.
fwd	UseRegexp	Forward to.
is_reg	OnOffToggle	Set to Yes if this account should be registered at the ITSP.
number	SmallInteger	Row number.
p_asserted_identity	UseRegexp	Optional value to use in P-Asserted-Identity.
password	TrunkUserPassword	Optional authentication password.
trunk	PositiveSysInteger	Trunk id.
user	UseRegexp	The SIP user name to use in the From SIP URI for outgoing calls.

### 17.2.342. db.sipswitch.trunk\_sip\_lines

New SIP Trunk SIP lines configuration.

Field Name	Field Type	Explanation
aliases	OptRegexp	Incoming Trunk Match.
auth_name	OptString	Optional authentication user id.
from_dn	UseRegexp	Optional SIP display name to use for outgoing calls.
from_user	OptRegexp	From Number/User.
fwd	UseRegexp	Forward to.
is_reg	OnOffToggle	Set to Yes if this account should be registered at the ITSP.

Field Name	Field Type	Explanation
number	SmallInteger	Row number.
p_asserted_identity	UseRegex	Optional value to use in P-Asserted-Identity.
password	TrunkUserPassword	Optional authentication password.
trunk	PositiveSysInteger	Trunk id.
user	UseRegex	The SIP user name to use in the From SIP URI for outgoing calls.

### 17.2.343. db.sipswitch.trunks

New SIP Trunks configuration.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Enable SIP Trunk.
id	PositiveSysInteger	SIP Trunk id.
params	OptSipTrunkParamsReference	SIP Trunk parameters.
pbx	OptSipPbxParamsReference	SIP Trunk PBX parameters.

### 17.2.344. db.sipswitch.user\_routing

Routing settings for calls to local SIP users.

Field Name	Field Type	Explanation
action	AccountFwdActionSel	How to process the call.
aliases	OptAliasList	Other SIP names for this user (connections etc.).
comment	OptComment	A comment field for the administrator.
forward_to	FwdToList	Where to send the call.
restrict_incoming	OnOffToggle	Select to restrict incoming calls to only local users and users defined in the <i>db.sipswitch.incoming_unauth</i> table.
timeclass	OptTimeclassReference	When this row is active.
user	SipLocalUserReference	The user for which routing settings are made.
voice_mail	AccountVoiceMailSel	When to send calls to a voice mail server.

### 17.2.345. db.sipswitch.users

A list of SIP users for this Ingate.

Field Name	Field Type	Explanation
auth_name	OptString	The authentication name for the user, if different from the username.
client_netgroup	NetgroupReference	The network from which the user can register.
comment	OptComment	A comment field for the administrator.
domain	SipUserDomain	The SIP domain for the user.
password	SipUserPassword	The password for the user.
user	SipUserName	The name of this SIP user.

### 17.2.346. db.sipswitch.voicemail

A list of Request-URIs to use for sending calls to voice mail servers.

Field Name	Field Type	Explanation
number	Integer	The priority of this row.
request_uri	NoCommaString	The Request-URI to use when the call is sent to the voice mail server. The Request-URI must in some way point to the voice mail server.

### 17.2.347. db.tls.dhparams

A table of DH parameters.

Field Name	Field Type	Explanation
dhparam	NonemptyString	PEM encoded Diffie-Hellman group.
name	Name	A name of the DH group. It is used to refer to this group.

### 17.2.348. db.tls.protocols

A table of TLS protocols.

Field Name	Field Type	Explanation
name	GroupName	A name of the protocols. It is used to refer to these protocols.
protocol	TlsProtocolSel	A TLS protocol.

### 17.2.349. db.tls.tls

A table of TLS protocols, ciphers and DH groups.

Field Name	Field Type	Explanation
ciphers	TlsCipherReference	A cipher string understood by OpenSSL.
dhparam	OptDhParamsReference	A reference to a predefined Diffie-Hellman Group.
ecdh	EcdhCurveSel	A ECDH curve.
name	Name	A name of the TLS config. It is used to refer to this config.
protocols	TlsProtocolReference	A reference to a name in the TLS Protocols table.

### 17.2.350. db.userdb.radius\_local\_endpoint

IP address and identifier to use when connecting to a RADIUS server.

Field Name	Field Type	Explanation
nas_identifier	NasIdentifier	A NAS-Identifier.
radius_local_ip	OptOwnIpReference	The IP address to use when contacting the RADIUS
use_nas_ip_address	OnOffToggle	Use NAS-IP-Address as identifier.

### 17.2.351. db.userdb.radius\_servers

A list of RADIUS servers to use for authentication and accounting.

Field Name	Field Type	Explanation
port	RadiusServerPort	The port of the RADIUS server.
secret	RadiusSecret	The shared secret of the RADIUS server.
server	DnsReachableHost	The IP address of the RADIUS server.

### 17.2.352. db.voipsm.voipsm

Settings for VoIP Survival.

Field Name	Field Type	Explanation
areacode	OptDigitString	The local phone area code.
cachettl	OptPositiveSysInteger	Time to store subscriber data (days).

Field Name	Field Type	Explanation
enabled	OnOffToggle	Turns the setting on and off.
maxnrlen	OptPositiveSysInteger	The maximum number of digits in local phone numbers (not including area code).
registration_time	OptPositiveSysInteger	Registration time for clients during survival mode (seconds).
timeout	OptPositiveSysInteger	How often the servers are checked (seconds).

### 17.2.353. db.voipsm.voipsm\_domains

A list of the domains monitored for VoIP Survival.

Field Name	Field Type	Explanation
domain	DomainNameOrIpStr	The SIP domain to be monitored.
user_data_method	VoipSurvivalMethodSel	The method to use when requesting user information.

### 17.2.354. db.voipsm.voipsm\_pstn\_gateways

A list of PSTN gateways to use when in Survival mode.

Field Name	Field Type	Explanation
gateway	UnresolvedReachableHost	A PSTN gateway.

### 17.2.355. db.webgui.certparams

Create Certificate or Certificate Request.

Field Name	Field Type	Explanation
alt_dns	OptLongStringList	SubjectAltName DNS.
alt_email	OptLongStringList	SubjectAltName email.
alt_ip	OptLongStringList	SubjectAltName IP.
alt_uri	OptLongStringList	SubjectAltName URI.
c	OptCountryCode	Country code ©.
cn	OptString	Common Name (CN).
email	OptString	Email address.
key_length	KeyLengthSel	Key length.
l	OptString	Locality/town (L).
o	OptString	Organization (O).
ou	OptString	Organizational Unit (OU).

Field Name	Field Type	Explanation
serial	NonNegativeInteger	Serial number.
sig_algorithm	SigAlgorithmSel	Signature algorithm.
st	OptString	State/province (ST).
validity	CertValidity	Expire in (days).

### 17.2.356. db.webgui.editcol\_settings

Edit Column.

Field Name	Field Type	Explanation
limit	NonNegativeInteger	Tables with at least this many rows have an Edit column.
show	EditcolSel	Show the edit column.

### 17.2.357. db.webgui.failover\_dedicated

Failover Settings.

Field Name	Field Type	Explanation
interface	InterfaceSel	The dedicated interface to use.
network	DnsIpNetwork_Filter	Dedicated Failover Network.

### 17.2.358. db.webgui.loadview\_interfaces

Display load interface.

Field Name	Field Type	Explanation
interface	LoadviewInterface	Display load interface.
use	OnOffButton	Show this interface.

### 17.2.359. db.webgui.loadview\_params

Display Load.

Field Name	Field Type	Explanation
diagram_heading	OptLatin1String	Diagram heading.
diagram_height	PositiveSysInteger	Diagram height.
diagram_width	PositiveSysInteger	Diagram width.
dir_rcvd	OnOffButton	Show received.
dir_sent	OnOffButton	Show sent.
dir_sum	OnOffButton	Show sent+received.
from_date	OptDate	Time period from date.

Field Name	Field Type	Explanation
from_time	OptTime	Time period from time.
max_kbps	OptPositiveSysInteger	Max value (empty for auto).
max_pps	OptPositiveSysInteger	Max value (empty for auto).
measure_avg	OnOffButton	Show average values.
measure_max	OnOffButton	Show max values.
measure_min	OnOffButton	Show min values.
measurement_unit	LoadviewUnitSel	Packet unit.
period_sel	LoadviewPeriodSel	Time period.
show_cpuuse	OnOffButton	Show CPU load.
show_memuse	OnOffButton	Show memory load (RAM).
show_swapuse	OnOffButton	Show swap usage.
to_date	OptDate	Time period to date.
to_time	OptTime	Time period to time.

### 17.2.360. db.webgui.logview

Display Log.

Field Name	Field Type	Explanation
addr_a	OptIpRangeList	IP address A.
addr_b	OptIpRangeList	IP address B.
addr_direction	LogviewDirectionSel	IP address direction.
addr_not_a	OnOffButton	Not IP address A.
addr_not_b	OnOffButton	Not IP address B.
addr_not_op	OnOffButton	Not this address combination
autorefresh	OnOffButton	Periodical search.
export_format	LogviewExportFormatSel	Export log format.
from_date	OptDate	Time limits from date.
from_time	OptTime	Time limits from time.
function	LogviewFunctionSel	Packet type selection.
icmp_not_code	OnOffButton	Not ICMP code.
icmp_not_type	OnOffButton	Not ICMP type.
icmpcode	OptIcmpRangeList	ICMP code.
icmptype	OptIcmpRangeList	ICMP type.
ipproto_not_num	OnOffButton	Not protocol number.
ipproto_num	OptProtocolRangeList	Protocol number.
ipproto_sel	LogviewIpProtoSel	Protocol selection.

Field Name	Field Type	Explanation
ipver_sel	LogviewIpVerSel	IP version.
max_export_size	LogviewExportMaxSize	Max export size.
max_lines	PositiveSysInteger	Max display log lines.
ports_a	OptPortRangeList	Ports for A.
ports_b	OptPortRangeList	Ports for B.
ports_direction	LogviewDirectionSel	port direction.
ports_not_a	OnOffButton	Not ports for A.
ports_not_b	OnOffButton	Not ports for B.
ports_not_op	OnOffButton	Not this port combination.
ports_sel	LogviewPortsSel	Selected ports.
refresh_interval	NonNegativeInteger	Periodical search interval in seconds.
reverse	OnOffButton	Show newest at top.
show_blacklistings	OnOffButton	Show IPsec Blacklisting events.
show_cfg_auth	OnOffButton	Show Configuration server logins.
show_cfg_mgmt	OnOffButton	Show Administration and configuration.
show_cwmp_debug	OnOffButton	Show CWMP debug messages.
show_cwmp_error	OnOffButton	Show CWMP error messages.
show_cwmp_info	OnOffButton	Show CWMP info messages.
show_dhcp_client	OnOffButton	Show DHCP/PPPoE client.
show_hardware_errors	OnOffButton	Show Hardware errors.
show_ipsec_tunnels	OnOffButton	Show Negotiated IPsec tunnels.
show_ipsec_userauth	OnOffButton	Show IPsec user authentication.
show_mail_errors	OnOffButton	Show Mail errors.
show_pluto_messages	OnOffButton	Show IPsec key negotiations.
show_pluto_verbose_messages	OnOffButton	Show IPsec key negotiation debug messages.
show_pptp_negotiations	OnOffButton	Show PPTP negotiations.
show_radius_errors	OnOffButton	Show RADIUS errors.
show_reconfig	OnOffButton	Manual reconfigurations and reboots.
show_sip_debug	OnOffButton	Show SIP debug messages.
show_sip_errors	OnOffButton	Show SIP errors.
show_sip_idsips	OnOffButton	Show SIP IDS/IPS messages.
show_sip_license	OnOffButton	Show SIP license messages.

Field Name	Field Type	Explanation
show_sip_media	OnOffButton	Show SIP media messages.
show_sip_packets	OnOffButton	Show SIP packets.
show_sip_signalling	OnOffButton	Show SIP signaling.
show_snmp_agent	OnOffButton	Show SNMP problems.
show_time_settings	OnOffButton	Show Time changes.
show_timed_reconfig	OnOffButton	Show Time-controlled reconfigurations.
show_traffic	OnOffButton	Show IP packets as selected.
sip_query_call_ids	OptStringList	SIP Call-ID.
sip_query_cseq_methods	OptStringList	SIP Methods.
sip_query_from_uris	OptStringList	SIP From header.
sip_query_peer_ips	OptStringList	SIP IP addresses.
sip_query_show_associated	OnOffButton	SIP show associated.
sip_query_show_loopback	OnOffButton	Show internal SIP signaling.
sip_query_to_uris	OptStringList	SIP To header.
support_includes_db	OnOffButton	Include configuration database in support report.
timeout	PositiveSysInteger	Display log timeout.
to_date	OptDate	Time limits to date.
to_time	OptTime	Time limits to time.

### 17.2.361. db.webgui.netsniff\_selection

Packet capture.

Field Name	Field Type	Explanation
addr_a	OptIpRangeList	IP address A.
addr_b	OptIpRangeList	IP address B.
addr_direction	LogviewDirectionSel	Address direction.
addr_not_a	OnOffButton	Not IP address A.
addr_not_b	OnOffButton	Not IP address B.
addr_not_op	OnOffButton	Not this address combination.
icmp_not_code	OnOffButton	Not ICMP code.
icmp_not_type	OnOffButton	Not ICMP type.
icmpcode	OptIcmpRangeList	ICMP code.
icmptype	OptIcmpRangeList	ICMP type.
interface	NetsniffInterfaceSel	Interface.
ipproto_not_num	OnOffButton	Not protocol number.

Field Name	Field Type	Explanation
ipproto_num	OptProtocolRangeList	Protocol number.
ipproto_sel	LogviewIpProtoSel	Protocol selection.
ipver_sel	LogviewIpVerSel	IP version.
ports_a	OptPortRangeList	Ports for A.
ports_b	OptPortRangeList	Ports for B.
ports_direction	LogviewDirectionSel	Ports direction.
ports_not_a	OnOffButton	Not ports for A.
ports_not_b	OnOffButton	Not ports for B.
ports_not_op	OnOffButton	Not this port combination.
ports_sel	LogviewPortsSel	Port selection.

### 17.2.362. db.webgui.pending\_apply

Show Message About Unapplied Changes.

Field Name	Field Type	Explanation
verbosity	PendingApplySel	Pending apply selection.

### 17.2.363. db.webgui.ping\_parameters

Ping host.

Field Name	Field Type	Explanation
target_host	OptDomainOrIp	Target host to ping.

### 17.2.364. db.webgui.testmode

Test Run and Apply Conf.

Field Name	Field Type	Explanation
timelimit	Testmode_TimeLimit	Duration of limited test mode in seconds.

### 17.2.365. db.webgui.testua

Test Agent.

Field Name	Field Type	Explanation
call_duration	TestuaDurationLimit	Duration.
call_preferred_pt	RtpPayloadTypeSel	Preferred payload type (pt).
call_ptime	RtpPacketizationTime	Packetization time (ptime).
call_to	OptSipUriWithScheme	To URI.

### 17.2.366. db.webgui.trunk\_selection

Trunk selection.

Field Name	Field Type	Explanation
id	TrunkSel	Trunk id.

### 17.2.367. db.password.admin\_password

The password for the *admin* user.

Field Name	Field Type	Explanation
password	OptPassword	A password.

### 17.2.368. db.password.admin\_users

A list of the users allowed to access the Ingate web administrator interface.

Field Name	Field Type	Explanation
password	AdminPassword	The password for this administrator user.
type	AdminTypeSel	The administrator type.
user	AdminUser	The name of this administrator user.

### 17.2.369. db.password.config\_transfer\_encryption

Settings for encrypted failover communication.

Field Name	Field Type	Explanation
enabled	OnOffToggle	Enable encryption of failover communication.
passphrase	ConfigEncPassphrase	The passphrase used when encrypting the communication.

## 17.3. Field Types

Here, all field types used in the tables are listed. For **selection** types, you can only use the listed keywords. Note that the CLI is case sensitive!

### 17.3.1. AdminPassword

A password for an admin user.

### 17.3.2. AdminUser

A user name for an admin user.

### 17.3.3. AliasIpReference

A reference to the *name* field of *db.network.alias\_addresses*. In other words, one of the machine's own IP alias addresses.

### 17.3.4. AuthData

Authentication data for IPsec peers.

The first character of the secret column determines the type of the secret: *s*: Shared secret (aka PSK, pre-shared key). *x*: X.509 certificate in PEM format. *a*: The name of an X.509 CA certificate. *c*: X.509 Distinguished Name. *p*: XAUTH + PSK

### 17.3.5. Blacklist

An optional non negative integer.

### 17.3.6. CaReference

A reference to the *name* field of *db.cert.cas*. In other words, a CA certificate.

### 17.3.7. CertReference

A reference to one of the Ingate's private certificates.

### 17.3.8. CertValidity

An integer denoting certificate validity in days.

### 17.3.9. ConfigEncPassphrase

A failover passphrase.

### 17.3.10. CryptoDefReference

A reference to the *name* field of *db.ipsec.crypto\_def*.

In other words, a crypto definition.

### 17.3.11. DepUsableVlanInterface

A reference to a defined VLAN or interface, with an internal key.

A VLAN will look like *eth0.27* where *eth0* is the physical interface for which this VLAN is defined, and *27* is the number assigned to this VLAN.

An interface will look like *eth2*, where *eth2* is the name of the physical interface.

### 17.3.12. DhcpLeaseTime

An integer between 60 and 604800.

### 17.3.13. DhcpOptionCode

An integer between 1 and 254.

### 17.3.14. DnsDynIpAddress

A datatype for DNS/ipaddr values.

The address may be dynamically assigned.

The cooked value can be:

- `FieldError` — an error has occurred.
- `DynipAssignedIP` — for dynamically assigned addresses.
- `ipaddr.ipaddr` — for manually configured IP addresses.
- `AutoAssignedIP` — only in derived classes that specify `AUTOAVAIL = True`.

### 17.3.15. DnsDynIpNetwork\_Interface

A datatype for DNS/ipaddr and netmask values.

DEMAND\_INTERFACE: The netmask must be 1-30 The host part must **not** be all zeroes (the network address) or all ones (the broadcast address).

### 17.3.16. DnsDynIpOtherHost

A DNS name or IP address that does not belong to this unit, but is on a directly connected network.

### 17.3.17. DnsDynIpReachableHost

A DNS name or IP address that does not belong to this unit, with the option of getting it dynamically through DHCP/PPPoE.

### 17.3.18. DnsIp4Network\_Filter

A datatype for DNS/IPv4 ipaddr and netmask values.

DEMAND\_FILTER: The host part must be all zeroes.

### 17.3.19. DnsIpAddress

A datatype for DNS/ipaddr values.

### **17.3.20. DnsIpNetwork\_Filter**

A datatype for DNS/ipaddr and netmask values.

DEMAND\_FILTER: The host part must be all zeroes.

### **17.3.21. DnsReachableHost**

A DNS name or IP address that does not belong to this unit.

### **17.3.22. DomainGroup**

SIP domain group.

### **17.3.23. DomainName**

Datatype used for domain names.

### **17.3.24. DomainNameOrIpStr**

Datatype used for domain names (or IP addresses).

### **17.3.25. DpdDelay**

An integer between 0 and 172800.

### **17.3.26. DpdTimeout**

An integer between 0 and 172800.

### **17.3.27. DyndnsPassword**

A password for a DynDNS user.

### **17.3.28. EnumReference**

A reference to the *name* field of *db.sipswitch.enum\_root*. In other words, an ENUM root.

### **17.3.29. EspCryptoReference**

A reference to the *name* field of *db.ipsec.esp\_proposals*.

In other words, an ESP crypto proposal.

### **17.3.30. FirewallLogclassReference**

A reference to the *name* field of *db.monitor.logclasses*. In other words, a log class.

### **17.3.31. FwdToList**

A list of SIP addresses separated by comma.

### **17.3.32. GroupName**

Datatype used as name of groups.

### **17.3.33. HeadString**

A string to define the Head of the SIP URI.

Without a SIP Trunk or Advanced SIP Routing module, the only allowed characters are *1234567890+-\**.

### **17.3.34. HeaderPattern**

A SIP URI header. Can contain wildcards.

### **17.3.35. Hits**

A positive integer with standard value 30.

### **17.3.36. IPv4MaskLen**

An IPv4 mask length (0-31).

### **17.3.37. Identifier**

An identifier.

### **17.3.38. IkeCryptoReference**

A reference to the *name* field of *db.ipseccrypto.proposals*.

In other words, an IKE crypto proposal.

### **17.3.39. Integer**

An integer, possibly within a specified interval.

This class specifies no limits, so any integer is OK. Subclasses can specify the interval by setting either or both of *\_MIN* and *\_MAX*.

### **17.3.40. InterfaceSel**

Select one of the installed physical interfaces.

This behaves as if it were a reference to the *interface* column on *db.network.interfaces*.

### **17.3.41. InviteRetransmitCount**

An integer between 1 and 16.

### **17.3.42. IpsRuleName**

Datatype used for rate limited IPS rule names.

### **17.3.43. IpsecPeerGroup**

A reference to the *name* field of *db.ipsec.peers*.

In other words, an IPsec peer.

### **17.3.44. IpsecSALife**

An integer between 60 and 172800.

### **17.3.45. IsakmpSALife**

An integer between 60 and 172800.

### **17.3.46. LoadviewInterface**

An interface name (may also include specials for VPN and total).

### **17.3.47. LogclassReference**

A reference to the *name* field of *db.monitor.logclasses*. In other words, a log class.

### **17.3.48. LogviewExportMaxSize**

Megabytes. Must fit in a signed int after conversion to bytes.

### **17.3.49. LongRegexp**

A non-empty regular expression.

### **17.3.50. LongStringListQuote**

A comma separated list of strings (long). Allows comma in quoted strings.

### **17.3.51. MaxBPCSize**

An integer between 0 and 10000.

### **17.3.52. MaxMessageSizeInteger**

An integer between 1024 and 67108864.

### **17.3.53. MaxReg**

An integer between 1 and 100.

### **17.3.54. MaxSenders**

An integer between 0 and 65535. Zero (0) means an unlimited number of senders.

### **17.3.55. MaxStreamsPerSession**

An integer between 1 and 10.

### **17.3.56. MimeType**

A MIME type. The format is *type/name*. The \* wildcard is accepted to use as a type/name.

### **17.3.57. Name**

Datatype used for names. Names must not be empty, and must not be a dash (-).

### **17.3.58. NasIdentifier**

A NAS-Identifier string, as defined in RFC 2138.

### **17.3.59. NetgroupReference**

A reference to the *name* field of *db.firewall.network\_groups*.

In other words, the name of a group defined in the Networks and Computers table.

### **17.3.60. NetsniffInterfaceSel**

Select one of the active interfaces or the special value *any*.

### **17.3.61. NoCommaString**

A string. The comma character (,) is not allowed.

### **17.3.62. NoDoubleQuoteString**

A string. The double quote character is not allowed.

### **17.3.63. NonInviteRetransmitCount**

An integer between 1 and 32.

### **17.3.64. NonNegativeInteger**

A positive or zero integer.

### **17.3.65. NonWhiteSpace**

Datatype used for names without whitespace. Names must not be empty, a dash (-), or contain whitespace.

### **17.3.66. NonemptyString**

A string.

### **17.3.67. OptAccountReference**

A reference to an account defined in *db.sipswitch.accounts*. The reference is written on the form *accountname@domain*.

### **17.3.68. OptAliasIpReference**

An optional reference to the *name* field of *db.network.alias\_addresses*. In other words, one of the machine's own IP alias addresses.

### **17.3.69. OptAliasList**

An optional list of SIP user names.

### **17.3.70. OptBandWidth**

An optional integer with a minimum value of 12.

### **17.3.71. OptCACertificate**

An optional X.509 CA certificate.

### **17.3.72. OptCaReference**

A reference to the *name* field of *db.cert.cas*. In other words, a CA certificate.

### **17.3.73. OptCertCrl**

An optional X.509 CRL.

### **17.3.74. OptCertReference**

An optional reference to one of the Ingate's private certificates.

### **17.3.75. OptComment**

An optional comment field for user consumption only.

### 17.3.76. OptCountryCode

Optional country code.

### 17.3.77. OptDSCPInteger

An optional integer between 0 and 63.

### 17.3.78. OptDate

An optional date (year, month, day). The cooked value is a `datetime.date` object or `None`.

### 17.3.79. OptDateISO8601

An optional ISO 8601 date-time. Example: `2012-03-26T15:56:00+02:00`.

### 17.3.80. OptDepNetgroupReference

Optional reference to the *name* field of `db.firewall.network_groups`.

In other words, the name of a group defined in the Networks and Computers table.

### 17.3.81. OptDepOwnIpReference

An optional reference to the *name* field of `db.network.interfaces` or `db.network.alias_addresses`. In other words, one of the machine's own IP addresses.

### 17.3.82. OptDepString

An optional string.

Unlike most other optional types, the cooked value when no value is given isn't `None`. It is the empty string.

Subclasses may override `CHARSET` to specify a character set the string must be able to be encoded as. (Note that the cooked value is always UTF-8, regardless of `CHARSET`).

### 17.3.83. OptDepUsableVlanInterface

An optional reference to a defined VLAN or interface, with an internal key.

A VLAN will look like `eth0.27` where `eth0` is the physical interface for which this VLAN is defined, and `27` is the number assigned to this VLAN.

An interface will look like `eth2`, where `eth2` is the name of the physical interface.

### 17.3.84. OptDhParamsReference

A reference to a Diffie-Hellman group.

### 17.3.85. OptDigitString

An optional string that may only contain numeric data.

This may be practical e. g. when storing telephone numbers that may start with 0.

### 17.3.86. OptDnsAutoIpAddress

A datatype for optional DNS/ipaddr values.

The address may be automatically assigned.

### 17.3.87. OptDnsAutoRuntimeNoPARPHost

An optional DNS name or IP address that does not belong to this unit, with the option of doing the DNS lookup at runtime, and additional requirement that it is not on a proxy ARPed interface.

### 17.3.88. OptDnsDynIpAddress

A datatype for optional DNS/ipaddr values.

The address may be dynamically assigned.

The cooked value can be:

- None — no value supplied.
- FieldError — an error has occurred.
- DynipAssignedIP — for dynamically assigned addresses.
- ipaddr.ipaddr — for manually configured IP addresses.
- AutoAssignedIP — only in derived classes that specify AUTOAVAIL = True.

### 17.3.89. OptDnsIpAddress

A datatype for optional DNS/ipaddr values.

Note: the DNS lookup is performed by the client of dbserver, such as the web server or CLI process. This ensures that the dbserver process is never blocked for long periods of time.

Derived classes may define the following attributes:

```
_OPTIONAL -- True if the network is optional.
```

```
AUTOAVAIL -- True if the IP address may be AUTO_IP_STR.  
Exactly what it means is not specified here.
```

### **17.3.90. OptDnsIpNetwork\_Filter**

A datatype for optional DNS/ipaddr and netmask values.

DEMAND\_FILTER: The host part must be all zeroes.

### **17.3.91. OptDnsReachableHost**

An optional DNS name or IP address that does not belong to this unit.

### **17.3.92. OptDomainName**

Datatype used for optional domain names.

### **17.3.93. OptDomainNameOrIpStr**

Datatype used for optional domain names (or IP addresses).

### **17.3.94. OptDomainOrIp**

An optional domain name, or IP address.

This datatype is used for domains that are resolved at runtime. The cooked value is an `unresolved_domain` object (or `None` or `FieldError`).

### **17.3.95. OptDynipReference**

An optional reference to a dynamic IP address.

### **17.3.96. OptExtraGwReference**

A reference to the *name* field of *db.network.extra\_gw*. In other words, an additional default gateway.

### **17.3.97. OptForwardToReference**

A reference to the *name* field of *db.sipswitch.forward\_to*. In other words, a destination for the SIP request.

### **17.3.98. OptIDSIPSPacketMatchingReference**

A reference to the *name* field of *db.idsips.packet\_matching*. In other words, a SIP packet matching rule.

### **17.3.99. OptIcmpRangeList**

An optional list of ICMP numbers.

### 17.3.100. OptIpRangeList

Datatype class for a list of IP addresses and address ranges.

The raw value is a comma-separated list, possibly empty, of numeric IP addresses (dotted quads) or address ranges. A range is two numeric IP addresses (dotted quads) with a minus sign inbetween.

Grammar: `optiprangelist ::= "" | iprangelist iprangelist ::= ip-or-iprange | ip-or-iprange ";" iprangelist ip-or-iprange ::= ipaddr | ipaddr "-" ipaddr ipaddr ::= octet "." octet "." octet "." octet`

The cooked value is an `ipaddr.ip_set` object (even if it is empty).

### 17.3.101. OptIpsecModeCfgReference

A reference to the *name* field of *db.ipsec.modecfg*.

### 17.3.102. OptIpsecNetReference

A reference to the *name* field of *db.ipsec.ipsec\_nets*. In other words, an IPsec network.

### 17.3.103. OptIpsecPeerReference

A reference to the *name* field of *db.ipsec.peers*. In other words, an IPsec peer.

### 17.3.104. OptLatin1String

An optional string that must be valid ISO-8859-1.

### 17.3.105. OptLongRegexp

An optional regular expression.

### 17.3.106. OptLongString

An optional string (long).

Unlike most other optional types, the cooked value when no value is given isn't None. It is the empty string.

Subclasses may override CHARSET to specify a character set the string must be able to be encoded as. (Note that the cooked value is always UTF-8, regardless of CHARSET).

### 17.3.107. OptLongStringList

An optional comma separated list of strings (long).

### 17.3.108. OptMediaEncryptionSuiteReference

Refers to the *name* field in *db.sip.media\_encryption\_suite*.

### **17.3.109. OptName**

Datatype used for optional names.

### **17.3.110. OptNetgroupReference**

Optional reference to the *name* field of *db.firewall.network\_groups*.

In other words, the name of a group defined in the Networks and Computers table.

### **17.3.111. OptNonNegativeInteger**

An optional positive or zero integer.

### **17.3.112. OptNonNegativeSysInteger**

An optional positive or zero integer that fits in an "int".

### **17.3.113. OptNonWhiteSpace**

An optional string with no whitespace allowed.

### **17.3.114. OptOwnIpReference**

An optional reference to the *name* field of *db.network.interfaces* or *db.network.alias\_addresses*. In other words, one of the machine's own IP addresses.

### **17.3.115. OptPacketSize**

A optional packet size in the range 1-65535 bytes.

### **17.3.116. OptPassword**

Datatype for optional passwords.

### **17.3.117. OptPercent**

An optional integer from nothing to everything in percent (0-100).

### **17.3.118. OptPercentFloat**

An optional float from nothing to everything in percent (0-100).

Values are normalized to integers if possible.

### **17.3.119. OptPortNumber**

A optional port number in the range 1-65535. Zero not normally allowed.

### 17.3.120. OptPortRangeList

An optional list of TCP or UDP ports.

### 17.3.121. OptPositiveSysInteger

An optional strictly positive integer that fits in an "int".

### 17.3.122. OptPrivCert

A datatype for optional private key/certificate pairs.

The cooked value can be either of:

- an `fuegoutils.x509.privcert` object, possibly with an extra "req" attribute that is an `fuegoutils.x509.request` object.
- an `fuegoutils.x509.privreq` object.
- `FieldError`
- `None` (only if the datatype is optional)

### 17.3.123. OptProtocolRangeList

An optional list of protocol numbers.

### 17.3.124. OptProtocolReference

An optional reference to the *name* field of *db.firewall.protocols*. In other words, a transport protocol.

### 17.3.125. OptRegexp

A regular expression.

### 17.3.126. OptRegexpWithAt

A regular expression, which requires exactly one @.

### 17.3.127. OptRequestFromReference

A reference to the *name* field of *db.sipswitch.request\_from*. In other words, a matching From header.

### 17.3.128. OptRequestToReference

A reference to the *name* field of *db.sipswitch.request\_to*. In other words, a matching Request-URI.

### 17.3.129. OptRtpPacketizationTime

Optional RTP Packet size in milliseconds, represented by an integer between 1 and 1000.

### **17.3.130. OptRtpPayloadType**

Optional RTP payload type. 0 ≤ pt ≤ 127.

### **17.3.131. OptServicesReference**

An optional reference to the *name* field of *db.firewall.services*. In other words, a defined service.

### **17.3.132. OptSipPbxParamsReference**

A reference to the *sipswitch.trunk\_pbx* compiler.

### **17.3.133. OptSipTrunkParamsReference**

A reference to the *sipswitch.trunk\_params* compiler.

### **17.3.134. OptSipUri**

An optional SIP URI that doesn't require a SIP scheme.

### **17.3.135. OptSipUriAfterAt**

An optional part of a SIP URI after the @-sign.

### **17.3.136. OptSipUriWithScheme**

An optional SIP URI that requires a SIP scheme.

### **17.3.137. OptSipUserDomain**

An optional domain name or IP address. The \* wildcard can be used, meaning any SIP domain. \**local* means any SIP domain for which this Ingate acts as registrar.

### **17.3.138. OptString**

An optional string.

Unlike most other optional types, the cooked value when no value is given isn't None. It is the empty string.

Subclasses may override CHARSET to specify a character set the string must be able to be encoded as. (Note that the cooked value is always UTF-8, regardless of CHARSET).

### **17.3.139. OptStringList**

An optional comma separated list of strings.

### 17.3.140. OptTime

An optional time of day (hour, minute, second). The cooked value is a `datetime.time` object or `None`.

### 17.3.141. OptTlsReference

A reference to a TLS setting.

### 17.3.142. OptTimeclassReference

A reference to the *name* field of `db.firewall.timeclasses`. In other words, the name of a time class.

### 17.3.143. OptTrunkReference

A reference to the `sipswitch.trunks` compiler.

### 17.3.144. OptUnresolvedReachableOrLocalHost

An optional DNS name or IP address that may belong to this unit.

### 17.3.145. OptUsableVlanInterface

An optional reference to a defined VLAN or interface, with an internal key.

A VLAN will look like `eth0.27` where `eth0` is the physical interface for which this VLAN is defined, and `27` is the number assigned to this VLAN.

An interface will look like `eth2`, where `eth2` is the name of the physical interface.

### 17.3.146. OptVlanId

An integer between 1 and 4094.

### 17.3.147. OptVlanIfReference

An optional reference to a defined VLAN or interface, with an internal key.

A VLAN will look like `eth0.27` where `eth0` is the physical interface for which this VLAN is defined, and `27` is the number assigned to this VLAN.

An interface will look like `eth2`, where `eth2` is the name of the physical interface.

### 17.3.148. OptVlanTunnelOrIfReference

An optional reference to a tunnel or interface, with an internal key.

TODO explain format of tunnel name.

An interface will look like `eth2`, where `eth2` is the name of the physical interface.

### **17.3.149. OptionTimeout**

An integer between 0 and 600.

### **17.3.150. OwnIp4Reference**

An reference to the *name* field of *db.network.interfaces* or *db.network.alias\_addresses*. In other words, one of the machine's own IPv4 addresses.

### **17.3.151. OwnIpReference**

A reference to the *name* field of *db.network.interfaces* or *db.network.alias\_addresses*. In other words, one of the machine's own IP addresses.

### **17.3.152. PasswordTimeout**

Authenticated session timeout in seconds, represented by an integer between 300 and 28800.

### **17.3.153. Percent**

An integer from nothing to everything in percent (0-100).

### **17.3.154. PortNumber**

A port number in the range 1-65535. Zero not normally allowed.

### **17.3.155. PortRange**

A port range. Zero not normally allowed.

### **17.3.156. PositiveSysInteger**

A strictly positive integer that fits in an "int".

### **17.3.157. PptpPassword**

A password for a PPTP user.

### **17.3.158. ProtocolRangeList**

A list of protocol numbers.

### **17.3.159. QTurnUserName**

A Q-Turn user name.

### **17.3.160. QTurnUserPassword**

A password for a Q-Turn user.

### **17.3.161. QoSClassReference**

A reference to the *name* column of *db.qos.classes*.

In other words, a QoS class.

### **17.3.162. RadiusSecret**

A RADIUS server secret.

### **17.3.163. RadiusServerPort**

A port number. The default value is 1812.

### **17.3.164. RegTimeout**

An integer between 1 and 86400.

### **17.3.165. Rfc2782Priority**

An integer between 0 and 65535.

### **17.3.166. Rfc2782Weight**

An integer between 0 and 65535.

### **17.3.167. RouteDestination**

A network (network address and netmask), or *default*.

### **17.3.168. RoutePriority**

An optional integer between 1 and 9.

### **17.3.169. RtpPacketizationTime**

RTP Packet size in milliseconds, represented by an integer between 1 and 1000.

### **17.3.170. SIPLogclassReference**

A reference to the *name* field of *db.monitor.logclasses*. In other words, a log class.

### **17.3.171. ServerName**

Server/User-Agent value for locally generated messages.

### **17.3.172. ServicesReference**

A reference to the *name* field of *db.firewall.services*. In other words, a defined service.

### **17.3.173. SessionTimeout**

An integer between 90 and 86400.

### **17.3.174. SipAliasAlias**

A SIP URI/username (including domain) that must not have a sip scheme.

### **17.3.175. SipFromUser**

A SIP URI/username (including domain).

### **17.3.176. SipLocalUserReference**

A reference to a locally handled SIP user or an account. This looks at *db.sipswitch.users* and *db.sipswitch.accounts*. The reference is written on the form *user@domain*.

### **17.3.177. SipMethod**

A SIP method (uppercase).

### **17.3.178. SipUriWithUserWildcardDomain**

A SIP URI that doesn't require a SIP scheme but that must contain a user.

### **17.3.179. SipUserDomain**

A domain name or IP address. The \* wildcard can be used, meaning any SIP domain. *\*local* means any SIP domain for which this Ingate acts as registrar.

### **17.3.180. SipUserDomainDefaultAll**

A domain name or IP address. The default value for this field is \*.

### **17.3.181. SipUserName**

A SIP user name.

### **17.3.182. SipUserPassword**

A password for a SIP user.

### **17.3.183. SipWildcardUrl**

SIP URL with wildcards.

? represents any single character while \* represents a string of characters of any length. \* is only allowed first, last and just before or after @.

### 17.3.184. SmallInteger

Input for *small* integers. Allows size < 6 for INPUT boxes. (see programs/webserver/webdatatype.py)

### 17.3.185. SnmpPassword

A password for a SNMP v3 user.

### 17.3.186. SubGroup

A reference to another group in the same table. The default is to reference the column *name*, but a subclass may set the class attribute REFERRED\_COLUMN to specify another column. REFERRED\_TABLE must not be touched.

See class OptReference for additional attributes that may be set.

### 17.3.187. Testmode\_TimeLimit

An integer between 10 and 3600.

### 17.3.188. TestuaDurationLimit

An integer between 1 and 3600.

### 17.3.189. Time\_HH\_MM

A time of day (00:00 ≤ value ≤ 24:00).

The cooked value is a tuple (h, m, s) where h, m and s are ints representing hour, minute and second. s will always be 0.

Since 24:00 is acceptable, we cannot use the standard time class from the datetime module introduced in Python 2.3.

### 17.3.190. TimeclassReference

A reference to the *name* field of *db.firewall.timeclasses*. In other words, the name of a time class.

### 17.3.191. TimerA\_Float

A number between 0.1 and 16.0.

### 17.3.192. TlsCipherReference

A reference to a TLS cipher group.

### 17.3.193. TlsProtocolReference

A reference to a TLS protocol group.

### **17.3.194. TlsReference**

A reference to a TLS setting.

### **17.3.195. TrunkSel**

Select one of the SIP Trunks.

### **17.3.196. TrunkUserPassword**

A password for a SIP user.

### **17.3.197. TunnelIdentifier**

An tunnel identifier.

### **17.3.198. TunnelOrIfReference**

A reference to a tunnel or interface, with an internal key.

TODO explain format of tunnel name.

An interface will look like *eth2*, where *eth2* is the name of the physical interface.

### **17.3.199. UaRegisterInteger**

An integer between 60 and 86400.

### **17.3.200. UnresolvedReachableHost**

A DNS name or IP address that does not belong to this unit.

### **17.3.201. UnresolvedReachableOrLocalHost**

A DNS name or IP address that may belong to this unit.

### **17.3.202. UsableVlanInterface**

A reference to a defined VLAN or interface, with an internal key.

A VLAN will look like *eth0.27* where *eth0* is the physical interface for which this VLAN is defined, and *27* is the number assigned to this VLAN.

An interface will look like *eth2*, where *eth2* is the name of the physical interface.

### **17.3.203. UseRegexp**

Input where regexp matches (substrings) can be used. Allows size > 12 for INPUT boxes. (see [programs/webserver/webdatatype.py](#))

### **17.3.204. VPNLogclassReference**

A reference to the *name* field of *db.monitor.logclasses*. In other words, a log class.

### **17.3.205. VlanId**

An integer between 1 and 4094.

### **17.3.206. VlanIfReference**

A reference to a defined VLAN or interface, with an internal key.

A VLAN will look like *eth0.27* where *eth0* is the physical interface for which this VLAN is defined, and *27* is the number assigned to this VLAN.

An interface will look like *eth2*, where *eth2* is the name of the physical interface.

### **17.3.207. WildcardDomainOrIp**

Datatype used for domain names or IP addresses which may contain wildcard characters (\* and ?).

### **17.3.208. WildcardIdentifier**

Identifier, or wildcard "\*".

### **17.3.209. Window**

A positive integer with standard value 60.

### **17.3.210. XauthPassword**

A password for a XAUTH user.

### **17.3.211. cwmp\_acs\_password**

ACS password.

### **17.3.212. cwmp\_cpe\_password**

CPE password.

### **17.3.213. cwmp\_port**

ACS/CPE CWMP port number. The default value is 7547.

### **17.3.214. dhcp\_server\_data\_type\_reference**

Refers to the *name* field in *db.misc.dhcp\_server\_data\_type*.

### 17.3.215. dhcp\_server\_options\_reference

Refers to the *name* field in *db.misc.dhcp\_server\_options*.

### 17.3.216. radvd\_interface\_ref

Refers to the *name* field in *db.misc.radvd\_interface\_settings*.

### 17.3.217. radvd\_prefix\_ref

Refers to the *name* field in *db.misc.radvd\_prefixes*.

### 17.3.218. AccountFwdActionSel

A selection of actions to take for SIP requests.

Selection	Explanation
-	Not applicable.
reject	Reject the request.
forward	Forward the request to listed users, not to the original user.
parallel	Forward the request to the original user and all listed users.
sequence	Forward the request to the original user, then to listed users in sequence.
random	Forward the request to a randomly selected user among the listed and original users. If there is no response a new user is selected to forward the request to.

### 17.3.219. AccountTypeSel

A selection of SIP account types.

Selection	Explanation
reg	A registration account. The Ingate registers the account with the server managing that domain.
xf	A forwarding account. The Ingate replaces the From header in the incoming request with the username and domain of this account. The request is then forwarded to the address entered in the <i>db.sipswitch.dial_plan</i> table.
xf+reg	A combination of the <i>xf</i> and <i>reg</i> accounts.
domain	An authentication account. When this account is used, the Ingate will respond with authentication details to authentication requests from the domain.

Selection	Explanation
mr	A B2BUA account. The Ingate replaces the From header as for an <i>xf</i> account. The SDPs are rewritten to make SIP media always go via the Ingate.
mr+reg	A combination of the <i>mr</i> and <i>reg</i> accounts.

### 17.3.220. AccountVoiceMailSel

A selection of when to forward calls.

Selection	Explanation
-	Not applicable.
on	Always.
after5	After 5 seconds.
after10	After 10 seconds.
after15	After 15 seconds.
after25	After 25 seconds.
busy	When busy.
busy5	When busy or after 5 seconds.
busy10	When busy or after 10 seconds.
busy15	When busy or after 15 seconds.
busy25	When busy or after 25 seconds.

### 17.3.221. AddExpireHeaderSel

A selection of when to perform certain actions based on the SIP request.

Selection	Explanation
always	Always perform this action.
never	Never perform this action.
if_in_request	Only perform this action when the request matched certain criteria.

### 17.3.222. AddressTypeSel

Selection	Explanation
static	Static IP address.
dhcp	Acquire an IP address via DHCP.
dhcp6	Acquire an IP address via DHCPv6.
pppoe	Acquire an IP address via PPPoE.

### 17.3.223. AdminTypeSel

A list of administrator account types.

Selection	Explanation
off	The user is disabled.
ro	The user can view any configuration and make log searches, but cannot change any configuration.
debug	The user can take packet captures, download support reports, and view internal dump pages.
bk	The user can download the configuration to file, and upload a configuration file to the Ingate. The user is also allowed to apply configurations.
rw	The user can make any changes to the configuration.
vpn	The user can make any changes in the VPN settings and apply configurations, but cannot change any other configuration.
sip	The user can make any changes in the SIP settings and apply configurations, but cannot change any other configuration.
vpnreneg	The user is allowed to press the <i>Renegotiate IPsec tunnels</i> button in the GUI to negotiate new IPsec tunnels, but cannot change any configuration.

### 17.3.224. AuthGroupSel

A selection of authorization groups.

Selection	Explanation
authenticated	Authenticated users (digest or trusted).
friendly	Users which are allowed to make incoming calls.

### 17.3.225. AuthTypeSel

A selection of IPsec authentication methods.

Selection	Explanation
-	Not applicable.
psk	A shared secret.
x509	An X.509 certificate.
x509ca	A trusted CA.

Selection	Explanation
x509ca_dn	A trusted CA, with added Distinguished Name for the peer.
xauth_psk	Extended Authentication + A shared secret.

### 17.3.226. AutoConfOffSel

Selection	Explanation
auto	Assign automatically from other configuration.
configured	Assign from configuration connected to this setting.
off	Do not assign.

### 17.3.227. AutonegSel

Selection	Explanation
auto	Automatic negotiation.
1000half	Use 1000 Mbit/s, half duplex.
1000full	Use 1000 Mbit/s, full duplex.
100half	Use 100 Mbit/s, half duplex.
100full	Use 100 Mbit/s, full duplex.
10half	Use 10 Mbit/s, half duplex.
10full	Use 10 Mbit/s, full duplex.

### 17.3.228. BlindSel

A selection of policies for packets from inactive gateways.

Selection	Explanation
discard	Drop the packets silently.
accept	Accept the packets.

### 17.3.229. BypassTransportSel

A selection of SIP transports.

Selection	Explanation
tcp	TCP.
udp	UDP.
any	Any SIP transport.
ws	WS.
tls	TLS.

Selection	Explanation
wss	WSS.
tcp,tls	TCP or TLS.

### 17.3.230. Class3Sel

Selection	Explanation
all	Send all messages on.
recurse	Use the information in the messages locally.

### 17.3.231. ConfigAuthSel

A selection of authentication types for configuring the unit.

Selection	Explanation
local	A local database.
radius	A RADIUS database.
any	Use the local database as well as the RADIUS database.

### 17.3.232. ConfigProtoSel

A selection of protocols for configuring the unit.

Selection	Explanation
http	HTTP.
https	HTTPS.
ssh	SSH.

### 17.3.233. DialPlanActionSel

A selection of forwarding actions.

Selection	Explanation
fwd	Forward the request to the selected destination.
a+fwd	Authenticate, then forward the request.
enum/a+allow	Look up destination in ENUM, then authenticate and allow the request.
deny	Reject the request.
enum/allow	Look up destination in ENUM, then allow the request.
allow	Allow the request.

Selection	Explanation
enum/a+fwd	Look up destination in ENUM, then authenticate and forward the request.
a+enum/a+fwd	Authenticate and look up destination in ENUM, then authenticate again and forward the request.
enum/fwd	Look up destination in ENUM, then forward the request.
a+enum/a+allow	Authenticate and look up destination in ENUM, then authenticate again and allow the request.
a+allow	Authenticate, then allow the request.

### 17.3.234. DnsPreferenceSel

A selection of DNS lookup preferences.

Selection	Explanation
auto	Automatic
ipv4	Only resolve IPv4.
ipv4_ipv6	Prefer IPv4.
ipv6	Only resolve IPv6.
ipv6_ipv4	Prefer IPv6.

### 17.3.235. DpdActionSel

A selection that selects which action that should be taken when a peer is detected as dead.

Selection	Explanation
hold	Try to re-negotiate the connection if matching traffic arrives.
clear	The connection is closed and no re-negotiation will happen.
restart	The connection will be re-negotiated.

### 17.3.236. DyndnsServiceSel

A selection of DynDNS services.

Selection	Explanation
-	Not applicable.
dyndns	Dynamic DNS.
statdns	Static DNS.
custom	Custom DNS.

Selection	Explanation
he_tun	Hurricane Electric IPv6 Tunnel Broker
he_dns	Hurricane Electric Free DNS

### 17.3.237. EcdhCurveSel

TLS ECDH curve to use.

Selection	Explanation
prime256v1	NIST P-256 (secp256r1)
secp384r1	NIST P-384 (secp384r1)

### 17.3.238. EditcolSel

Edit column.

Selection	Explanation
always	Always have an Edit column.
sometimes	Sometimes have an Edit column.
never	Never have an Edit column.

### 17.3.239. FallbackSel

A selection of dial plan modes.

Selection	Explanation
off	Turned off.
on	Turned on.
fallback	Used if nothing else matches.

### 17.3.240. FentKeepaliveSel

A selection of how to keep bindings for fented clients alive.

Selection	Explanation
options	Use OPTIONS.
registrations	Use short registration times.
both	Use both OPTIONS and short registration times.
off	Use neither OPTIONS or short registration times.

### 17.3.241. FilterTypeSel

A selection of the firewall types in the Ingate.

Selection	Explanation
-	Not applicable.
dynamic	Dynamic session management.
static	Packet filtering.
ftp	Dynamic FTP management.
pptp	Dynamic PPTP management.
rtsp	Dynamic RTSP management.
tftp	Dynamic TFTP management.

### 17.3.242. FromDomainSel

Replace From Domain:

Selection	Explanation
pdomain	Provider domain
edomain	Enterprise domain
ifaddr	External IP address
other	As entered by the user

### 17.3.243. FromMatchingSel

Match From Number/User in field:

Selection	Explanation
from_uri	From URI
from_dname	From Display Name
pai_uri	P-Asserted-Id. URI
pai_dname	P-Asserted-Id. Display Name
pref_uri	P-Preferred-Id. URI
pref_dname	P-Preferred-Id. Display Name
other	As entered by user

### 17.3.244. FunctionSel

A selection of policies for traffic through the Ingate.

Selection	Explanation
discard	Drop the packets silently.
reject	Drop the packets and send an ICMP message back.
accept	Allow the packets.

### 17.3.245. IdTypeSel

A selection that selects which ID type to use.

Selection	Explanation
-	Not applicable.
ipaddress	An IPv4 or an IPv6 address.

### 17.3.246. Ikev2EsnSel

A selection that selects support for IKEv2 Extended Sequence Number (ESN) transforms.

Selection	Explanation
no	Don't support ESN.
yes	Support ESN.
either	Sent as an initiator, the responder will decide. Received as a responder, no will be picked.

### 17.3.247. Ikev2Sel

A selection of IKEv2 modes.

Selection	Explanation
-	Not applicable.
allow	Allow IKEv1 but use IKEv2 if the other end wants to use it.
suggest	Allow IKEv2 and use it as default over IKEv1.
force	Allow IKEv2 but do not allow IKEv1.
disallow	Allow IKEv1 but do not allow IKEv2.

### 17.3.248. InhibitHoldSel

Inhibit hold options.

Selection	Explanation
no	Do not inhibit hold.
yes	Inhibit hold.
only_fented	Only inhibit hold for FENTed clients.

### 17.3.249. IpsecAuthSel

Authentication algorithm to use.

Selection	Explanation
sha1	SHA1 HMAC.
sha2_256	SHA2 256 bit HMAC.
sha2_512	SHA2 512 bit HMAC.
md5	MD5 HMAC.

### 17.3.250. IpsecEncSel

Encryption algorithm to use.

Selection	Explanation
aes128	AES with 128 bits key.
aes192	AES with 192 bits key.
aes256	AES with 256 bits key.
3des	3DES (112 effective bits key).

### 17.3.251. IpsecNetLocalSel

A selection of which local IP addresses can use the IPsec connection.

Selection	Explanation
exact	The exact network selected.
peerip	The IP address used for the negotiation.

### 17.3.252. IpsecNetRemoteSel

A selection of which remote IP addresses can use the IPsec connection.

Selection	Explanation
exact	The exact network selected.
subset	The network selected, or a subset of the network.
peerip	The IP address used for the negotiation.
private	One IP address from the private IP address ranges.
peerip/private	One IP address from the private IP address ranges, or the IP address used for the negotiation.

### 17.3.253. IsakmpGroupSel

Diffie-Hellman (DH) group to use.

<b>Selection</b>	<b>Explanation</b>
modp1024	Group 2.
modp1536	Group 5.
modp2048	Group 14.
modp3072	Group 15.
modp4096	Group 16.
modp6144	Group 17.
modp8192	Group 18.
dh19	Group 19.
dh20	Group 20.
dh21	Group 21.
dh23	Group 23.
dh24	Group 24.

### 17.3.254. KeyLengthSel

Certificate key length.

<b>Selection</b>	<b>Explanation</b>
2048	2048 bits.
4096	4096 bits.
8192	8192 bits.

### 17.3.255. LoadviewPeriodSel

Load view time period.

<b>Selection</b>	<b>Explanation</b>
lasth	Last hour.
last24	Last 24 hours.
today	Today.
yesterday	Yesterday.
thisweek	This week.
lastweek	Previous week.
thismonth	This month.
lastmonth	Previous month.
other	Other period.

### 17.3.256. LoadviewUnitSel

Load view packet units.

Selection	Explanation
bps	Bit/s.
pps	Packets/s.

### 17.3.257. LogviewDirectionSel

Log view IP address direction.

Selection	Explanation
a_src	A src.
a_dst	A dst.
a_any	A any.
a_to_b	A to B.
b_to_a	B to A.
between	Between A&B.

### 17.3.258. LogviewExportFormatSel

Log view export format.

Selection	Explanation
commaseparated	Comma-separated file.
tabseparated	TAB-separated file.
welf	WELF.

### 17.3.259. LogviewFunctionSel

Log view packet type selection.

Selection	Explanation
all	All packets.
all_accepted	Accepted.
accepted_nonat	Accepted (no NAT).
accepted_nat	Accepted (NAT).
all_denied	Not accepted.
dropped	Not accepted (discarded).
rejected	Not accepted (rejected).
blacklisted	Not accepted (blacklisted).

### 17.3.260. LogviewIpProtoSel

Log view IP protocol selection.

Selection	Explanation
all	All IP protocols.
tcp	TCP.
udp	UDP.
tcp_or_udp	TCP/UDP.
icmp	ICMP.
icmpv6	ICMPv6.
esp	ESP.
numeric	Protocol number.

### 17.3.261. LogviewIpVerSel

Log view IP version selection.

Selection	Explanation
all	All versions.
ipv4	Version 4.
ipv6	Version 6.

### 17.3.262. LogviewPortsSel

Log view port selection.

Selection	Explanation
all	All ports.
selected	Selected ports.

### 17.3.263. MediaEncryptionSuiteSel

A selection of the crypto algorithms which the Ingate can handle.

Selection	Explanation
cleartext	The media is unencrypted.
dtls-srtp	DTLS-SRTP (requires a certificate and mediafw).
microsoft-wm5-DES_CBC_56_NONE	Windows Messenger's standard encryption.
sdescriptions-AES_256_CM_HMAC_SHA1_32	SRTP using the AES-CM algorithm with a 256 bit key for encryption and the HMAC-SHA1 algorithm with a 32 bit tag for authentication.
sdescriptions-AES_256_CM_HMAC_SHA1_80	SRTP using the AES-CM algorithm with a 256 bit key for encryption and the HMAC-SHA1 algorithm with a 80 bit tag for authentication.

Selection	Explanation
sdescriptions-AES_CM_128_HMAC_SHA1_32	SRTP using the AES-CM algorithm with a 128 bit key for encryption and the HMAC-SHA1 algorithm with a 32 bit tag for authentication.
sdescriptions-AES_CM_128_HMAC_SHA1_80	SRTP using the AES-CM algorithm with a 128 bit key for encryption and the HMAC-SHA1 algorithm with a 80 bit tag for authentication.
sdescriptions-F8_128_HMAC_SHA1_80	SRTP using the AES-f8 algorithm with a 128 bit key for encryption and the HMAC-SHA1 algorithm with a 80 bit tag for authentication.
snom-srtp-AES_CM_128_NONE	SRTP using the AES-CM algorithm with a 128 bit key for encryption and an unknown authentication algorithm.
unknown-k-param	All other encryption offers using the k parameter.
unknown-sdescriptions	All other encryption offers using sdescriptions.

### 17.3.264. MediaLockSel

Media stream limitation options.

Selection	Explanation
any	Allow multiple sender IP addresses and ports.
lock	Lock IP address and port to first sender.
any_restricted	Only allow receiving IP address, but multiple ports.

### 17.3.265. NatTraversalSel

A selection that selects if NAT Traversal should be automatically detected or if it should be forced.

Selection	Explanation
auto	Automatically detect NAT Traversal.
force	Force NAT traversal (ESP in UDP encapsulation).

### 17.3.266. NetbiosNodeTypeSel

Selection	Explanation
-	Not applicable.
b_node	Broadcast: no WINS.
p_node	Peer: WINS only.
m_node	Mixed: broadcast, then WINS.
h_node	Hybrid: WINS, then broadcast.

### 17.3.267. OnOffButton

Selection	Explanation
on	This setting is enabled.
off	This setting is disabled.

### 17.3.268. OnOffToggle

Selection	Explanation
on	This setting is enabled.
off	This setting is disabled.

### 17.3.269. OnOffToggleOn

Selection	Explanation
on	This setting is enabled.
off	This setting is disabled.

### 17.3.270. OptCodecTypeSel

Selection	Explanation
-	Not applicable.
audio	An audio type codec.
video	A video type codec.
text	A text type codec.
application	An application type codec.

### 17.3.271. OptOnOffToggle

Selection	Explanation
on	This setting is enabled.
off	This setting is disabled.
-	Not applicable.

### 17.3.272. OptOnOffToggleOn

Selection	Explanation
on	This setting is enabled.
off	This setting is disabled.
-	Not applicable.

### 17.3.273. OptSipMessagePartSel

Selection	Explanation
-	Whole SIP message.
startline	SIP message start-Line.
method	SIP request method.
ruri	SIP request-uri.
header	SIP message header.
body	SIP message body.

### 17.3.274. OptSipMessageSel

Selection	Explanation
-	Not applicable.
request	Use the request.
response	Use the response.

### 17.3.275. OptSipTransportSel

Selection	Explanation
-	Not applicable.
tcp	Use TCP as transport.
udp	Use UDP as transport.
ws	Use WS as transport.
tls	Use TLS as transport.
wss	Use WSS as transport.

### 17.3.276. OptTosSel

A selection of TOS values. The field can also be set to -.

Selection	Explanation
-	Not applicable.
empty	The TOS field is not set.
md	The TOS field is set to Minimize Delay.
mt	The TOS field is set to Maximize Throughput.
mr	The TOS field is set to Maximize Reliability.

### 17.3.277. OptTransportSel

Selection	Explanation
-	Not applicable.
tcp	Use TCP as transport.
udp	Use UDP as transport.

### 17.3.278. OptTrunkGroupUsageSel

Trunk Group Parameter Usage

Selection	Explanation
-	Request URI
origin	Originating Trunk Group Parameters
dest	Destination Trunk Group Parameters
origin_dest	Originating and Destination T.G.P.

### 17.3.279. OriginSchemeSel

The allowed WebSocket Origin's scheme.

Selection	Explanation
http	http.
https	https.

### 17.3.280. OverrideSel

Options of logging of firewall traffic.

Selection	Explanation
never	Don't log traffic regardless of other configuration.
marked	Log traffic according to other configuration.
always	Log traffic according to selected master log class.

### 17.3.281. PbxToHeaderSel

PBX To header field:

Selection	Explanation
ruri	Request URI
trunk	Copy from trunk
init_ruri	Initial Request URI
other	As entered by user

### 17.3.282. PendingApplySel

Show Message About Unapplied Changes.

Selection	Explanation
always	On every page.
apply_page	On the Save/Load Configuration page.
never	Never.

### 17.3.283. PfsGroupSel

Perfect Forward Secrecy (PFS) group to use.

Selection	Explanation
-	Do not use Perfect Forward Secrecy.
modp1024	Group 2.
modp1536	Group 5.
modp2048	Group 14.
modp3072	Group 15.
modp4096	Group 16.
modp6144	Group 17.
modp8192	Group 18.
dh19	Group 19.
dh20	Group 20.
dh21	Group 21.
dh23	Group 23.
dh24	Group 24.
phase1	Use the same group as the DH group in phase1.

### 17.3.284. PingPolicySel

A selection of the ping policies that can be used by the Ingate.

Selection	Explanation
local	Only reply to ping from units on the same interface.
never	Never reply to ping.
always	Reply to ping on all IP addresses.

### 17.3.285. PolicySel

A selection of policies for blocked traffic.

Selection	Explanation
discard	Drop the packets silently.
reject	Drop the packets and send an ICMP message back.

### 17.3.286. PriorityQueueSel

A selection of priority queues.

Selection	Explanation
prio1	Priority queue 1 (highest).
prio2	Priority queue 2.
prio3	Priority queue 3.
prio4	Priority queue 4.
prio5	Priority queue 5.
prio6	Priority queue 6.
prio7	Priority queue 7.
prio8	Priority queue 8 (lowest).

### 17.3.287. PtChangesSel

A selection of when to detect pt changes.

Selection	Explanation
first	It will only detect changes to the first pt listed. Endpoints typically uses this first payload type.
all	All payload types (except dynamic) are compared.
none	Will not detect pt changes in mid call answers.

### 17.3.288. QTurnAccountingSel

A selection of accounting for Q-Turn.

Selection	Explanation
off	Off.
on	On.
verbose	Verbose.

### 17.3.289. QTurnDebugLevelSel

A selection of debug level for Q-Turn.

Selection	Explanation
0	normal.
1	verbose.
2	very verbose.

### 17.3.290. QTurnTransportListenSel

A selection of transports for Q-Turn signaling.

Selection	Explanation
udp	UDP.
tcp	TCP.
tls	TLS.
dtls	DTLS.

### 17.3.291. QoSTypeSel

Type of QoS to use.

Selection	Explanation
priority	Use strict priority queues.
dynamic	Use dynamic bandwidth allocation.

### 17.3.292. ReferToReplacementSel

Replace Refer-To Domain:

Selection	Explanation
never	Never
blind	In blind transfers
both	In blind and attended transfers

### 17.3.293. RelayTypeSel

The relays available in the Ingate.

Selection	Explanation
tcp_relay	TCP relay. Will rewrite the entire packet.
tcp_relay_nat	TCP port forwarding. Will rewrite the source and destination addresses of the packet.
tcp_relay_nat_transp	Semi-transparent TCP port forwarding. Will rewrite the destination address of the packet.
udp_relay	UDP relay. Will rewrite the entire packet.

Selection	Explanation
udp_relay_nat	UDP port forwarding. Will rewrite the source and destination addresses of the packet.
udp_relay_nat_transp	Semi-transparent UDP port forwarding. Will rewrite the destination address of the packet.
ftp	FTP relay. Monitors FTP signaling and opens a channel for data transport.
tls_relay_server	TLS decrypting TCP relay.

### 17.3.294. RestFuncSel

A selection of SIP URI tails.

Selection	Explanation
telchar	0-9, +, -, #, *
digit	0-9.
nothing	No tail.
alpha	a-z, A-Z.
-	Not applicable.
alnum	a-z, A-Z, 0-9.
anychar	Any character.
xdigit	0-9, a-f, A-F (hexadecimal numbers).

### 17.3.295. ReuseMediaPortSel

Reuse Port Numbers Within Same Session options.

Selection	Explanation
off	Don't reuse port numbers.
on	Reuse port numbers.
ip	Reuse port numbers also on IP change.

### 17.3.296. RingToneTypeSel

A selection of ring tone type.

Selection	Explanation
us	US ring tone.
uk	UK ring tone.

### 17.3.297. RingbackSel

A selection of when to play ringback RTP to transferee.

Selection	Explanation
never	Never play ringback RTP to transferee.
if_transfer_target_rings	Play ringback RTP if transfer target rings.
if_transferer_hangs_up	Play ringback RTP if transferer hangs up.
if_transfer_target_progress	Play ringback RTP if transfer target rings or makes progress.

### 17.3.298. RouteIncomingSel

Route incoming based on:

Selection	Explanation
ruri	Request URI
to	To header
pcpid	P-Called-Party-ID

### 17.3.299. RoutingPrioritySel

A list of different routing methods in the Ingate.

Selection	Explanation
dns_override	Use the <i>db.sip.external_relay</i> table.
registrar	Use the local registrar, including the <i>db.sip.sip_alias</i> table.
dialplan	Use the <i>db.sipswitch.dial_plan</i> table.

### 17.3.300. RtpPayloadTypeSel

A selection of RTP payload types used by RTP player.

Selection	Explanation
pcmu	PCMU.
pcma	PCMA.

### 17.3.301. RtpProfileSelection

RTP Profile options.

Selection	Explanation
savp	Prefer RTP/SAVP (sdescriptions)
avp	Prefer RTP/AVP (cleartext and legacy encryptions)
avp_with_sdesc	Prefer RTP/AVP (together with sdescriptions)

### 17.3.302. SigAlgorithmSel

Certificate signature algorithm.

Selection	Explanation
sha1	SHA-1.
sha224	SHA-224.
sha256	SHA-256.
sha384	SHA-384.
sha512	SHA-512.

### 17.3.303. SipAuthDirSel

Selection	Explanation
in	Requests for local domains.
out	Requests for other domains.
both	All requests.

### 17.3.304. SipFilterActionSel

Selection	Explanation
process	Allow the request.
reject	Reject the request.

### 17.3.305. SipFunctionSel

A selection of which SIP requests to process, based on the Request-URI domain.

Selection	Explanation
proxy	Process all requests.
process	Only process requests to domains local to this unit.
reject	Process no requests.

### 17.3.306. SipPreloadedRouteActionSel

Selection	Explanation
reject	Reject the request.
auth	Require authentication.
remove	Remove the preloaded routes.
allow	Allow the request.

### 17.3.307. SipRadiusSel

A selection of SIP user databases.

Selection	Explanation
local	A local database.
radius	A RADIUS database.

### 17.3.308. SipSel

A selection of traffic types.

Selection	Explanation
nonsip	Non-SIP traffic.
signaling	SIP signaling.
media	SIP media.

### 17.3.309. SipTransportListenSel

A selection of transports for SIP signaling.

Selection	Explanation
tcp	TCP.
udp	UDP.
udp,tcp	UDP and TCP.
ws	WS.
tls	TLS.
wss	WSS.

### 17.3.310. SipTransportSel

Selection	Explanation
tcp	Use TCP as transport.
udp	Use UDP as transport.
ws	Use WS as transport.
tls	Use TLS as transport.
wss	Use WSS as transport.

### 17.3.311. SipsSel

Selection	Explanation
sip	Use <i>SIP</i> in the Request-URI.

Selection	Explanation
sips	Use <i>SIPS</i> in the Request-URI.

### 17.3.312. SnmpTrapVersionSel

A selection of SNMP versions.

Selection	Explanation
v1	Version 1.
v2c	Version 2c.

### 17.3.313. SnmpV3AuthSel

A selection of authentication algorithms.

Selection	Explanation
sha-1	SHA-1.
md5	MD5.

### 17.3.314. SnmpV3PrivacySel

A selection of encryption algorithms.

Selection	Explanation
aes	AES encryption.
des	DES encryption.
none	No encryption.

### 17.3.315. StTypeSel

A selection of the SIParator types available.

Selection	Explanation
DMZ	DMZ type. Uses only one interface.
DMZ/LAN	DMZ/LAN type. Uses two or more interfaces.
standalone	Standalone type. Uses two or more interfaces.
manual	Manual type. Uses two or more interfaces with manual surroundings setup.
WAN	SIParator in front of firewall. Uses three or more interfaces.

### 17.3.316. StandbyAccessProtoSel

A selection of protocols for accessing the standby unit's gui.

Selection	Explanation
http	HTTP.
https	HTTPS.

### 17.3.317. SyslogFacilitySel

A selection of syslog facilities.

Selection	Explanation
-	Not applicable.
Kern	Kernel.
User	User.
Mail	Mail.
Daemon	Daemon.
Auth	Auth.
Lpr	Lpr.
News	News.
Uucp	Uucp.
Cron	Cron.
Local0	Local0.
Local1	Local1.
Local2	Local2.
Local3	Local3.
Local4	Local4.
Local5	Local5.
Local6	Local6.
Local7	Local7.

### 17.3.318. SyslogLevelSel

A selection of syslog levels.

Selection	Explanation
-	Not applicable.
Emerg	Emergency.
Alert	Alert.
Crit	Critical.
Err	Error.
Warning	Warning.
Notice	Notice.

Selection	Explanation
Info	Informational.
Debug	Debug messages.

### 17.3.319. TestuaTransportSel

A selection of SIP transports.

Selection	Explanation
udp,tcp	TCP or UDP.
any	Any SIP transport.
tls	TLS.

### 17.3.320. TlsProtocolSel

TLS Protocol to use.

Selection	Explanation
DTLSv1	DTLSv1.
DTLSv1_2	DTLSv1.2.
TLSv1	TLSv1.0.
TLSv1_1	TLSv1.1.
TLSv1_2	TLSv1.2.
SSLv3	SSLv3.0.

### 17.3.321. TransportSel

Selection	Explanation
tcp	Use TCP as transport.
udp	Use UDP as transport.

### 17.3.322. TrustedDomainTransportSel

A selection of transports for SIP signaling.

Selection	Explanation
any	TCP or TLS.
tcp	TCP.
tls	TLS.

### 17.3.323. UriEncodingSel

URI encoding options.

Selection	Explanation
encrypt	Always encrypt URIs.
db	Store URI and generate random username, only when needed.
escape	Escape URIs as usernames, only when needed.
preserve_db	Store URI and preserve username, only when needed.
gruu	"self-made GRUU"
preserve_registration	"Use registration"

### 17.3.324. VoipSurvivalMethodSel

A selection of codings to request extra user information with REGISTER messages.

Selection	Explanation
generic	A generic XML coding.
Broadsoft	A Broadsoft specific XML coding.
swisscom	Constructs an alias using the value of display name in To header, appending a swisscom suffix that is found in user part of to URI.
dname	Use aliases in To header display name.

### 17.3.325. WeekdaySel

The days of the week.

Selection	Explanation
monday	Monday
tuesday	Tuesday
wednesday	Wednesday
thursday	Thursday
friday	Friday
saturday	Saturday
sunday	Sunday

### 17.3.326. cwmp\_acs\_sslver

TLS version used when connecting to the ACS through https.

Selection	Explanation
-	Not applicable.
sslv3	SSLv3.

Selection	Explanation
tlsv1	TLSv1.0.
tlsv1_1	TLSv1.1.
tlsv1_2	TLSv1.2.
tlsv1_x	Any of TLSv1.x.

### 17.3.327. cwmp\_urischeme

Protocol used when connecting to the ACS/CPE.

Selection	Explanation
-	Not applicable.
http	The HTTP protocol.
https	The HTTPS protocol.

### 17.3.328. dhcp\_server\_data\_type\_sel

DHCP server data types.

Selection	Explanation
BOOLEAN	An option of type boolean is a flag with a value of either on or off (or true or false).
UINT8	Unsigned integer with width 8.
UINT16	Unsigned integer with width 16.
UINT32	Unsigned integer with width 32.
INT8	Signed integer with width 8.
INT16	Signed integer with width 16.
INT32	Signed integer with width 32.
IPv4	IPv4 address.
IPv6	IPv6 address.
TEXT	An option whose type is text will encode an ASCII text string.
STRING	An option whose type is a data string is essentially just a collection of bytes, and can be specified either as quoted text, like the text type, or as a list of hexadecimal contents separated by colons whose values must be between 0 and FF.

## 17.4. CLI command examples

In this section, you can find some examples of how to use the CLI commands to create and change your configuration.

The CLI commands can be entered directly via the serial console or an ssh connection to the unit configuration interface. You can also enter all commands in a text file and upload it via the unit web GUI.

### 17.4.1. Add and change firewall rules

To add new firewall rules, you first need network definitions for the networks that will send and receive the traffic. These are made in the **firewall.netdefs** table.

If you just want to add rows to an existing configuration, use the **add-row**. If you want to remove old configuration in this table first, use the **clear-table** command before you start adding rows. This example will remove old networks and then add two new network rows:

```
clear-table firewall.netdefs

add-row firewall.netdefs interface=eth3 lower_ip=10.5.1.0 name=LAN subgroup=- \
    upper_ip=10.5.1.255

add-row firewall.netdefs interface=eth0 lower_ip=0.0.0.0 name=internet \
    subgroup=- upper_ip=255.255.255.255
```

After that, the firewall rule can be added to the **firewall.forwarding\_rules** table. Here too, the **clear-table** command can be used to remove all old rules.

The commands below clears the table and adds two firewall rules for traffic from the LAN to the Internet.

```
clear-table firewall.forwarding_rules

add-row firewall.forwarding_rules (id 4) client=LAN comment="" enabled=on \
    fromtunnel=- function=accept logclass=Local number=3 server=internet \
    service=tcp timeclass=24/7 totunnel=-

add-row firewall.forwarding_rules (id 4) client=LAN comment="" enabled=on \
    fromtunnel=- function=accept logclass=Local number=3 server=internet \
    service=udp timeclass=24/7 totunnel=-
```

### 17.4.2. Apply a configuration

You can use CLI commands to apply the changed settings. Note that you need to perform approximately the same steps as when you apply in the web GUI; first start a test run (corresponds to pressing the **Apply configuration** button in the web GUI), and then confirm it (corresponds to pressing the **Save configuration** button on the test run page). If you need to test the new configuration for a longer period than you originally set as the test mode duration, you can enter a command to extend the test run (corresponds to pressing the **Continue test run** button on the test run page).

This command sequence will start a test run with a test mode duration of 200 seconds, then extend

the test run and finally confirm it.

```
start-testrun 200
```

```
continue-testrun
```

```
confirm-testrun
```

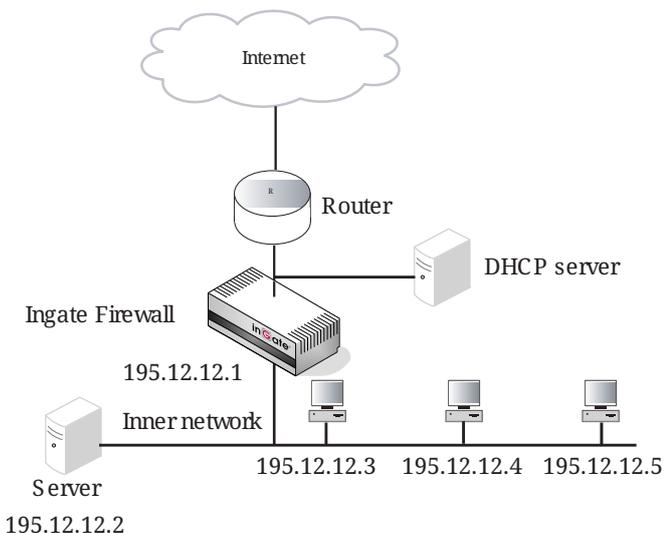
# Part IV. How To Guides

# Chapter 18. Network

## 18.1. Unit with two interfaces, using NAT

A sample company (Example Company) will be used in this example. Company has a small local network with a server and some workstations at one location. This network connects to the Internet through a gateway. To protect the local network, an Ingate unit is installed between this gateway and the local network.

The internal server has the IP address 195.12.12.2 and the workstations have 195.12.12.3, 195.12.12.4, and 195.12.12.5. The IP address given to the unit on the inside is 195.12.12.1. For the outside, the unit will request an IP address from a DHCP server.



The first thing to do is to install the unit. Connect a computer to the unit with a serial cable and turn the unit on. Access the administration interface (see also [Installation](#)). Log on as the user admin. The installation program will start automatically.

The first thing to do is to install the unit. Connect a computer to the unit with a serial cable and turn the unit on. Access the administration interface (see also [Installation](#)). Log on as the user admin. The installation program will start automatically.

## Administration

=====

(Navigation tip: You may use Ctrl-d to skip back to this menu.)

1. Basic configuration
2. Download/Upload
3. Join a failover team and become slave
5. Wipe email logs
6. Set password
7. Command line interface
8. Clear the log database
- a. About
- reboot. Reboot
- reset. Factory reset
- q. Exit admin

==>

Basic unit installation program version 6.1.4

Press return to keep the default value

Network configuration inside:

Physical device name[eth0]:

IP address [0.0.0.0]: 195.12.12.1

Netmask/bits [255.255.255.0]:

Deactivate other interfaces? (y/n) [n]

Computers from which configuration is allowed:

You can select either a single computer or a network.

Configure from a single computer? (y/n) [y]

IP address [0.0.0.0]: 195.12.12.3

Password [ ]: mopscot

Other configuration

Do you want to reset the rest of the configuration? (y/n) [n]

You have now entered the following configuration

Network configuration inside:

Physical device: eth0

IP address: 195.12.12.1

Netmask: 255.255.255.0

Deactivate other interfaces: no

Computer allowed to configure from:

IP address: 195.12.12.3

Password: mopscot

The rest of the configuration is kept.

Is this configuration correct (yes/no/abort)? yes

Now, exit the administration program. The unit will boot with the configuration just entered. As it boots, disconnect the serial cable, go to the client computer 195.12.12.3 to start a web browser and log on the unit.

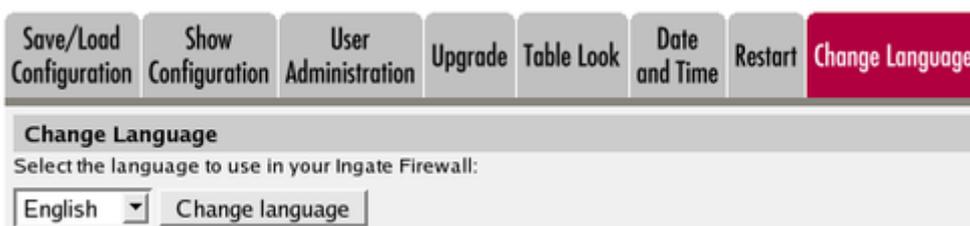
You were not logged on.

### Local password

Username:

Password:

If you want to change language in the web interface, go to the **Change Language** page.



Now go to **Network** and check the **Eth0** configuration. Most of it was made by the installation program. The configuration will be as follows:

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | **Eth0** | Eth1 | Eth2 | Interface Status | PPPoE | Topology

### General

Physical device: **eth0**

This interface is:  Active  Inactive

Interface name:

### Speed and Duplex

- Automatic negotiation
- 100 Mbit/s, full duplex
- 100 Mbit/s, half duplex
- 10 Mbit/s, full duplex
- 10 Mbit/s, half duplex

**Directly Connected Networks** [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Inside	Static	195.12.12.1	195.12.12.1	24	195.12.12.0	195.12.12.255		-	<input type="checkbox"/>

Continue with the configuration for **Eth1**. Activate the DHCP client and create a directly connected network.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | **Eth1** | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE

### General

Physical device: **eth1**

This interface is:  Active  Inactive

Interface name:

### Speed and Duplex

- Automatic negotiation
- 100 Mbit/s, full duplex
- 100 Mbit/s, half duplex
- 10 Mbit/s, full duplex
- 10 Mbit/s, half duplex

**Directly Connected Networks** [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Outside	DHCP		dhcp		-	-		-	<input type="checkbox"/>

On the NAT page, turn NAT on from the eth0 interface to the eth1 interface. Since all IP addresses behind eth0 should be NATed, no networks are required.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
<b>NAT</b>												
Select if packets that originate from a unit behind the <b>From</b> interface should be NAT:ed when they are sent to a unit behind the <b>To</b> interface. Optionally you can also select specific networks to be NAT:ed, as well as the address to use.												
Edit Row	No.	From			To			NAT As (optional)	Delete Row			
		Interface	Network (optional)		Interface	Network (optional)						
			DNS Name or Network Address	Network Address	Netmask / Bits		DNS Name or Network Address	Network Address	Netmask / Bits			
<input type="checkbox"/>	1	Internal (eth0)				External (eth1)				-	<input type="checkbox"/>	

Go to the **Networks and Computers** page and name the internal server. The network on the inside is called Company network and includes all computers on the local network. The outside world is called Internet and is connected to the External interface. Make a separate network for the server, since much of the traffic from the outside should only be allowed to reach the server.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
<b>Networks and Computers</b>												
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row				
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address						
<input type="checkbox"/>	+ Company network	-	195.12.12.1	195.12.12.1	195.12.12.254	195.12.12.254	Internal (eth0 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>				
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ Server	-	195.12.12.2	195.12.12.2			Internal (eth0 untagged)	<input type="checkbox"/>				

Go to the **Default Gateways** page and enter a default gateway for the unit. Note that in this case, you must enter "\*" as the **Default gateway**, for the unit to use the default gateway assigned by the DHCP server.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
<b>Main Default Gateways (Help)</b>												
Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row						
<input type="checkbox"/>		Outside		Outside	External (eth1)	<input type="checkbox"/>						

On the **Basic Configuration** page under **Basic Configuration** the unit is given a name. Select to reject all traffic to which no rules apply. The unit should reply to ping only to the interface receiving the original ping packet, i.e., should not "tunnel" the ping request to another interface or alias.

Basic Configuration | Access Control | RADIUS | SNMP | DHCP Server | DHCP Server Status | Dynamic DNS Update | Certificates | Advanced

**General**

Name of this firewall:

Default domain:

**IP Policy**

Discard IP packets  
 Reject IP packets

**Version of Ingate Firewall**

Check for new versions of Ingate Firewall:  Yes  No

Date of last successful version check: 2009-10-31 23:23:02

Software version in use: 4.8.2

**Policy For Ping to Your Ingate Firewall**

Never reply to ping  
 Only reply to ping to the same interface  
 Reply to ping to all IP addresses

The unit also needs a DNS server. Enter "\*" to use DNS server information from the DHCP server. It could also use the DNS server located on the LAN.

**DNS Servers** (Help)

Edit Row	No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	1	Outside		Outside	<input type="checkbox"/>

Go to the **Access Control** page and select the unit IP address to use for access to the web interface. Specify that configuration traffic can only be sent to the unit via the Eth0 interface and that only the computer with the IP address 192.12.12.3 on the inner network can configure the unit. Select authentication via local password only as there is no RADIUS server being used.

Basic Configuration | Access Control | RADIUS | SNMP | DHCP Server | DHCP Server Status

**Configuration Transport** (Help)

**Configuration via HTTP**

Direct your web browser to this address:  Port:

**Configuration via HTTPS**

Direct your web browser to this address:  Port:

Certificate to use:

**Configuration via SSH**

Connect your SSH client to this address:  Port:

**User Authentication For Web Interface Access** [\(Help\)](#)

Local users  
 RADIUS database  
 Local users or RADIUS database

**Configuration Allowed Via Interface** [\(Help\)](#)

Interface or Tunnel	Allowed	Delete Row
Ethernet0 (eth0) ▼	Yes ▼	<input type="checkbox"/>

Add new rows  rows.

**Configuration Computers** [\(Help\)](#)

Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	195.12.12.3	195.12.12.3	32	195.12.12.3	-	Yes	Yes	No	Local	<input type="checkbox"/>

To help other computers find the unit outside, when its IP address is acquired via DHCP, you must use the DynDNS service. Go to the Dynamic DNS update page to make configuration for this.

This service must be ordered from DynDNS.org.

Turn the DynDNS service on and select which DynDNS service you have ordered. Also select which IP address of the unit should be updated. For this example , it is the outside IP of the unit.

[Basic Configuration](#)
[Access Control](#)
[RADIUS](#)
[SNMP](#)
[DHCP Server](#)
[DHCP Server Status](#)
[Dynamic DNS Update](#)
[Certificates](#)
[Advanced](#)

**DynDNS** [\(Help\)](#)

Enable DynDNS  
 Disable DynDNS

DynDNS service: 
 Use wildcard hostnames:  Yes  No  
 Offline URL redirection:  Yes  No

IP address for updates:

Enter the username and password at DynDNS.org.

<p><b>User</b></p> <p>Username:</p> <input type="text" value="tester"/> <p>Password:</p> <input type="password"/> <p><a href="#">Change Password</a></p>	<p><b>SMTP Server</b></p> <p>SMTP server:</p> <input type="text"/> <p>SMTP server is backup: <input type="radio"/> Yes <input checked="" type="radio"/> No</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

Enter the domain(s) to be associated with the unit.

When any computer on the Internet wants to contact the unit or the server behind it, they will get the IP address from DynDNS.

DNS Names to Update at DynDNS <a href="#">(Help)</a>		
Edit Row	DNS Name	Delete Row
<input type="checkbox"/>	company.dyndns.org	<input type="checkbox"/>

For **Log Classes**, **Logging Configuration** and **Protocols**, use the standard settings of the unit.

Check **Time Classes** under **Rules and Relays** to make sure everything is OK. Here, new time classes for office hours and off-duty hours are defined.

Rules	Relays	DHCP Relay	Services	Protocols	Time Classes	
<b>Time Classes</b>						
Edit Row	Name	From Weekday	To Weekday	From Time	To Time	Delete Row
<input type="checkbox"/>	+ 24/7	Monday	Sunday	00:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>	+ off-duty hours	Monday	Friday	00:00	07:00	<input type="checkbox"/>
<input type="checkbox"/>		Monday	Friday	18:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>		Saturday	Sunday	00:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>	+ office hours	Monday	Friday	07:00	18:00	<input type="checkbox"/>
Add new rows <input type="text" value="1"/> groups with <input type="text" value="1"/> rows per group.						

After networks, computers, and services are defined, it is time to set up rules for the traffic that is allowed.

Since NAT is used, no computers on the Internet will know about the computers on the local network. Rules that allow traffic from the Internet to the Company network are therefore worthless. Also, when NAT is used, the reply traffic will automatically have rules, so there is no need to specify them separately. These are the **Rules** needed:

- Allow SMTP from the server so that email can come out.
- Allow retrieval of files from the Internet via FTP, but only during off-duty hours.
- Allow DNS from the server to enable name queries on the Internet. DNS queries from the company network go through the internal server.
- Allow WWW to the Internet.
- Allow Company network to make terminal connections outwards through SSH.

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Server	-	Internet	-	Internal -> External (NAT:ed)	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Server	-	Internet	-	Internal -> External (NAT:ed)	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Company network	-	Internet	-	Internal -> External (NAT:ed)	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	4	Yes	Company network	-	Internet	-	Internal -> External (NAT:ed)	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	5	Yes	Company network	-	Internet	-	Internal -> External (NAT:ed)	ftp	Allow	off-duty hours	Local		<input type="checkbox"/>

To let traffic in from the Internet, **Relays** must be used instead. Define one relay to forward smtp traffic (on port 25) and two relays for the WWW traffic (ports 80 and 443). All smtp and WWW traffic is forwarded to the server.

Relays (Help)												
Edit Row	Listen To ...		Relay To ...		Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class	Log Class	Delete Row	
	IP Address	Port	DNS Name or IP Address	IP Address		Port	Network					IPsec Peer
<input type="checkbox"/>	Outside (119.15.17.2)	25	195.12.12.2	195.12.12.2	25	TCP relay	Internet	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	Outside (119.15.17.2)	80	195.12.12.2	195.12.12.2	80	Semi-transparent TCP port forwarding	Internet	-	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	Outside (119.15.17.2)	443	195.12.12.2	195.12.12.2	443	Semi-transparent TCP port forwarding	Internet	-	-	24/7	Local	<input type="checkbox"/>

Once configuration is complete, go to **Administration** and select **Apply configuration**, then during the test run, select **Save configuration**. Store the configuration to a file as a backup, by clicking on **Save to local file**. The unit is now up and running.

<b>Save/Load Configuration</b>	<b>Show Configuration</b>	<b>User Administration</b>
<b>Test Run and Apply Conf (Help)</b>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

## 18.2. Unit with two interfaces, no NAT

In this example, the same network configuration is used as in the previous one (example 1a). The only difference is that here, NAT is turned off from the Inside to the Outside. These are the pages on which the configuration differs from the previous example.

Since NAT is not used, rules for the UDP reply traffic will also need to be specified (TCP has a built-

in session management which handles this automatically). Specify the following:

### 18.2.1. Incoming traffic

- Allow WWW traffic from the outside to the server to make the WWW server run on the server available for the outside (rule 9).
- Allow SMTP traffic to the server to enable incoming email (rule 11).
- Allow DNS traffic to the server so that name queries are possible (rules 7 and 10).
- To protect from NFS mounting from the Internet, block out incoming NFS traffic (rule 1). Insert this rule before the DNS reply rule (rule 4) from the Internet to the Server on the Inside.

There are no more services that must be blocked.

### 18.2.2. Outgoing traffic

- Allow DNS from the server (rules 3-4) to enable name queries on the Internet. DNS queries from the company network go through the internal server.
- Allow SMTP from the server so that email can come out (rule 6).
- Allow Company network to make terminal connections outward through SSH (rule 2).
- Allow WWW to the Internet (rule 5).
- Allow retrieval of files from the Internet via FTP, but only during off-duty hours (rule 8).

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Internet	-	Company network	-	External -> Internal	nfs-tcp	Discard	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Company network	-	Internet	-	Internal -> External	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Server	-	Internet	-	Internal -> External	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	4	Yes	Internet	-	Server	-	External -> Internal	dns-reply	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	5	Yes	Company network	-	Internet	-	Internal -> External	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	6	Yes	Server	-	Internet	-	Internal -> External	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	7	Yes	Company network	-	Internet	-	Internal -> External	ftp	Allow	off-duty hours	Local		<input type="checkbox"/>
<input type="checkbox"/>	8	Yes	Internet	-	Server	-	External -> Internal	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	9	Yes	Server	-	Internet	-	Internal -> External	dns-reply	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	10	Yes	Internet	-	Server	-	External -> Internal	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	11	Yes	Internet	-	Server	-	External -> Internal	smtp	Allow	24/7	Local		<input type="checkbox"/>

As the inside computers are visible to the Internet, no relays are needed.

The rest of the configuration is the same as for the previous example. Make sure to apply the configuration on the **Save/Load Configuration** page.

## 18.3. Unit with four interfaces and DMZ

For this example, the sample company "Company" will be used. Company has two servers that it wants to make available from the Internet. Company also has an internal network with workstations and internal servers, and a local network for the service department. The service department's network is accessible via a router from Company's internal network. This router has the IP address 172.22.1.2. Company has an Internet connection through a router with the IP address 119.15.17.1.

This example will illustrate how to set up Company's firewall. A unit with four interfaces is used, though only three of the interfaces are activated.

The servers that are to be accessible both from the Internet and the two internal networks are placed on a separate network. This makes it easy to set up different rules for the computers on the Internet and for the computers on the internal networks to access these servers. This separate network is a DMZ (Demilitarized Zone).

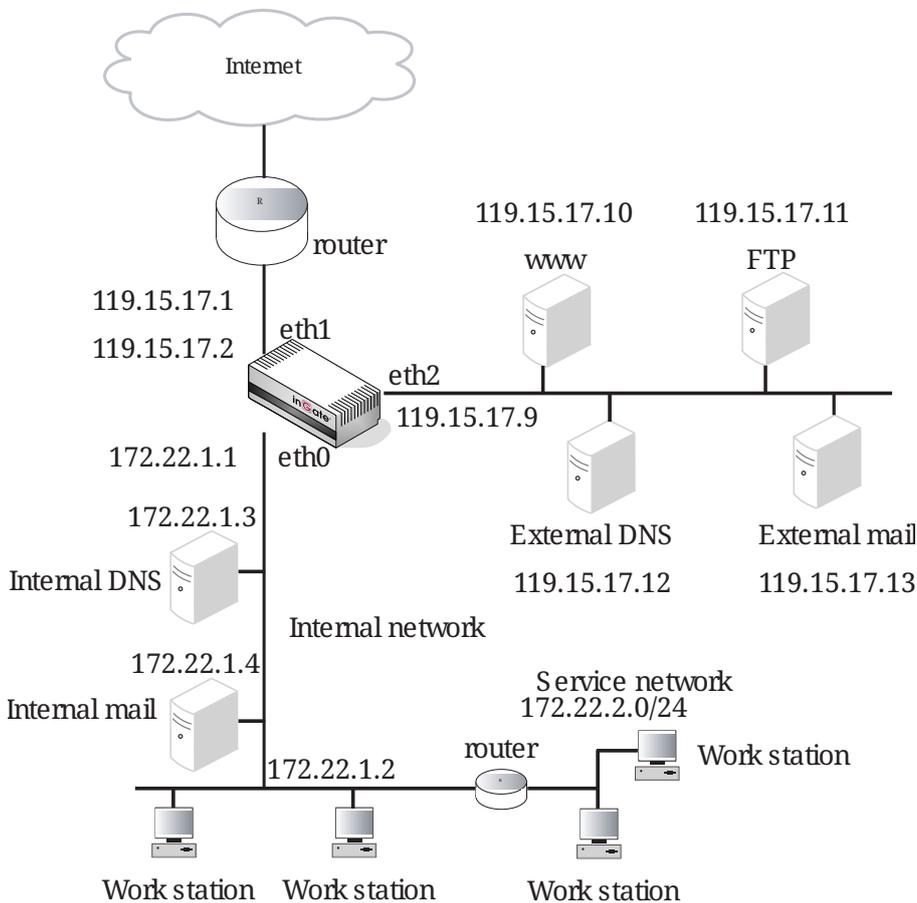
Company currently has a public network with 16 IP addresses. These will be divided evenly; half for the network between the unit and the gateway to the Internet; other half as a DMZ, making the network masks 255.255.255.248. The network supplier gave the gateway the IP address 119.15.17.1 and Company gives the unit the IP address 119.15.17.2 on the network interface connected to this gateway.

Assign the IP address 119.15.17.9 to the unit's network interface that is linked to the DMZ (119.15.17.8 is the network address of the half used as the DMZ).

Make sure that the network supplier knows that the IP addresses 119.15.17.8 - 15 are located behind the unit 119.15.17.2, or the routing won't work for these addresses.

Company's internal network, to which most of the workstations and internal servers are connected, has the network address 172.22.1.0. The unit receives the IP address 172.22.1.1 on the network interface that is connected to this network. There is also a service network with network address 172.22.2.0. Since Company uses IP addresses reserved for private use, the internal networks are NAT:ed.

The diagram shows this network.



Run the installation program.

The unit receives the IP address 172.22.1.1 and network interface eth0 is connected to the internal network. The other network interfaces should not be active yet.

The unit can be configured from all computers on the service department's network, 172.22.2.0. The mask for allowing all computers on this network to configure is 255.255.255.0. This network is accessed via a router with the IP address 172.22.1.2.

```
Basic unit installation program version 6.1.4
```

```
Press return to keep the default value
```

```
Network configuration inside:
```

```
Physical devicename [eth0]:
```

```
IP address [0.0.0.0]: 172.22.1.1
```

```
Netmask/bits [255.255.255.0]:
```

```
Deactivate other interfaces? (y/n) [n] y
```

```
Computers from which configuration is allowed:
```

```
You can select either a single computer or a network.
```

```
Configure from a single computer? (y/n) [y] n
```

```
Network address [0.0.0.0]: 172.22.2.0
```

```
Netmask/bits [255.255.255.255]: 255.255.255.0
```

For the unit to contact the service network, and to enable configuration from the service network, set up a static route. Also set a temporary password and choose not to remove other configuration.

Static routing:

The network allowed to configure from is not on a network local to the firewall. You must configure a static route for it. Give the IP number of the router on the network the firewall is on.

The IP address of the router [0.0.0.0]: 172.22.1.2

Network address [172.22.2.0]:

Netmask [255.255.255.0]:

Password []: advent

Other configuration on the firewall

Do you want to reset the rest of the configuration? (y/n) [n]

The installation program now shows where the configuration was changed. If it looks good, answer **yes**.

Network configuration inside:

Physical device: eth0

IP address: 172.22.1.1

Netmask: 255.255.255.0

Deactivate other interfaces: yes

Network allowed to configure from:

IP address: 172.22.2.0

Netmask: 255.255.255.0

Password: advent

Static routing:

Network address: 172.22.2.0

Netmask: 255.255.255.0

Router: 172.22.1.2

The rest of the configuration is kept.

Is this configuration correct (yes/no/abort)? yes

After the installation program has been run, go to a workstation on the service network to finish configuration. Eth0 is connected to the inside, so start with checking the configuration for **Eth0**. Most configuration has already been made by the installation program. The unit can be configured via this interface.

### General

Physical device: **eth0**

This interface is:  Active  Inactive

Interface name:

### Speed and Duplex

- Automatic negotiation
- 100 Mbit/s, full duplex
- 100 Mbit/s, half duplex
- 10 Mbit/s, full duplex
- 10 Mbit/s, half duplex

#### Directly Connected Networks [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Inside	Static	172.22.1.1	172.22.1.1	24	172.22.1.0	172.22.1.255		-	<input type="checkbox"/>

A static route to the service network should be found under **Static Routing**.

#### Static Routing [\(Help\)](#)

Edit Row	Routed Network			Router			Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
<input type="checkbox"/>	172.22.2.0	172.22.2.0	24	-	172.22.1.2	172.22.1.2	<input type="checkbox"/>

Network interface **Eth1** is connected to the outside. The unit has the IP address 119.15.17.2 on this interface. Divide the network between 119.15.17.0 and 119.15.17.15 into two parts, one of which will be used as the DMZ network. This makes the network mask 255.255.255.248.

### General

Physical device: **eth1**

This interface is:  Active  Inactive

Interface name:

### Speed and Duplex

- Automatic negotiation
- 100 Mbit/s, full duplex
- 100 Mbit/s, half duplex
- 10 Mbit/s, full duplex
- 10 Mbit/s, half duplex

#### Directly Connected Networks [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Outside	Static	119.15.17.2	119.15.17.2	29	119.15.17.0	119.15.17.7		-	<input type="checkbox"/>

Give **Eth2** the name DMZ, IP address 119.15.17.9 and mask 255.255.255.248. The unit should have an additional IP address, an Alias, to NAT traffic from the internal mail server to a specific IP address.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | **Eth2** | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE

**General**

Physical device: eth2

This interface is:  Active  Inactive

Interface name:

**Speed and Duplex**

Automatic negotiation

100 Mbit/s, full duplex

100 Mbit/s, half duplex

10 Mbit/s, full duplex

10 Mbit/s, half duplex

**Directly Connected Networks** [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	DMZ	Static	119.15.17.9	119.15.17.9	29	119.15.17.8	119.15.17.15		-	<input type="checkbox"/>

**Alias** [\(Help\)](#)

Below are the ranges from which you can select aliases.

Edit Row	Name	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	Mail	119.15.17.14	119.15.17.14	<input type="checkbox"/>

NAT should be used for traffic from eth0 to the other active network interfaces. Traffic from the internal to the external SMTP (email) server should use a specified IP address.

Create one row where traffic come from the internal mail server and is destined to the external mail server. Select to NAT this traffic as the alias created on the **Eth2** page.

Below this row, create two rows where all other traffic from eth0 destined to eth1 or eth2 is NATed. This is all NATing the unit should perform.

Networks and Computers | Default Gateways | All Interfaces | **NAT** | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE

**NAT**

Select if packets that originate from a unit behind the **From** interface should be NAT:ed when they are sent to a unit behind the **To** interface. Optionally you can also select specific networks to be NAT:ed, as well as the address to use.

Edit Row	No.	From			To			NAT As (optional)	Delete Row		
		Interface	Network (optional)		Interface	Network (optional)					
			DNS Name or Network Address	Network Address		Netmask / Bits	DNS Name or Network Address			Network Address	Netmask / Bits
<input type="checkbox"/>	1	Internal (eth0)	172.22.1.4	172.22.1.4	32	DMZ (eth2)	119.15.17.13	119.15.17.13	32	Mail (119.15.17.14)	<input type="checkbox"/>
<input type="checkbox"/>	2	Internal (eth0)				DMZ (eth2)				-	<input type="checkbox"/>
<input type="checkbox"/>	3	Internal (eth0)				External (eth1)				-	<input type="checkbox"/>

The default gateway out to the Internet is 119.15.17.1. You enter this on the **Default Gateways** page.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Main Default Gateways <a href="#">(Help)</a>												
Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row						
<input type="checkbox"/>		-	119.15.17.1	119.15.17.1	External (eth1)	<input type="checkbox"/>						

To establish different rules for the computers on the DMZ, these computers should be defined on separate lines on the **Networks and Computers** page. The same applies to the internal DNS server and the internal mail server. Define the three networks; DMZ, Internal network and Internet.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Networks and Computers												
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row				
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address						
<input type="checkbox"/>	+ DMZ	-	119.15.17.9	119.15.17.9	119.15.17.14	119.15.17.14	DMZ (eth2 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ Everything	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>				
<input type="checkbox"/>	+ External DNS	-	119.15.17.12	119.15.17.12			DMZ (eth2 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ External email	-	119.15.17.13	119.15.17.13			DMZ (eth2 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ FTP server	-	119.15.17.11	119.15.17.11			DMZ (eth2 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ Internal DNS	-	172.22.1.3	172.22.1.3			Internal (eth0 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ internal email	-	172.22.1.4	172.22.1.4			Internal (eth0 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ internal network	-	172.22.0.0	172.22.0.0	172.22.255.255	172.22.255.255	Internal (eth0 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ internet + DMZ	DMZ					-	<input type="checkbox"/>				
<input type="checkbox"/>		internet					-	<input type="checkbox"/>				
<input type="checkbox"/>	+ Web server	-	119.15.17.10	119.15.17.10			DMZ (eth2 untagged)	<input type="checkbox"/>				

Go to the **Access Control** page under **Basic Configuration** and make settings for accessing the unit web interface.

The configuration IP address (the IP address you direct your web browser to) was set by the installation program. You have also already entered which computers should be allowed to configure the unit.

The administrator should be able to use a local password or RADIUS as authentication methods.

Access traffic to the unit web interface should only be allowed via Eth0 - no one on the Internet should be allowed to browse or change the settings.

### Configuration Transport [\(Help\)](#)

Protocol	IP Address	Port	Cert	TLS	Delete Row
HTTP ▾	eth0 (172.22.1.1) ▾	80	· ▾	· ▾	<input type="checkbox"/>
HTTPS ▾	· ▾	443	· ▾	· ▾	<input type="checkbox"/>
SSH ▾	· ▾	22	· ▾	· ▾	<input type="checkbox"/>

Add new rows  rows.

### User Authentication For Web Interface Access [\(Help\)](#)

Local users  
 RADIUS database  
 Local users or RADIUS database

### Configuration Allowed Via Interface [\(Help\)](#)

Interface or Tunnel	Allowed	Delete Row
Ethernet0 (eth0) ▾	Yes ▾	<input type="checkbox"/>

Add new rows  rows.

### Configuration Computers [\(Help\)](#)

Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	172.22.2.0	172.22.2.0	24	172.22.2.0 - 172.22.2.255	·	No	Yes	Yes	Local	<input type="checkbox"/>

To enable authentication of the administrator via RADIUS, a **RADIUS** server must be defined on the **RADIUS** page under **Basic Configuration**. Remember to add the unit and the administrator to the RADIUS server database.

[Basic Configuration](#)
[Access Control](#)
[RADIUS](#)
[SNMP](#)
[DHCP Server](#)
[DHCP Server Status](#)
[Dynamic DNS Update](#)
[Certificates](#)
[Advanced](#)

### RADIUS Servers [\(Help\)](#)

Edit row	RADIUS server		Port	Secret	Delete row
	DNS name or IP address	IP address			
<input type="checkbox"/>	172.22.1.13	172.22.1.13	1645		<input type="checkbox"/>

Add new rows  rows.

**Contact IP Address** [\(Help\)](#)      **Identifier** [\(Help\)](#)  
 Contact RADIUS servers from:      Use NAS-IP-Address:  Yes  No  
 ▾      NAS-Identifier:

When all network interfaces and the RADIUS server are set up, there is still some **Basic Configuration** left. Give the unit the name Ingate Firewall and set it to use the IP policy Reject IP packets. The unit should only reply to ping from the same interface.

Basic Configuration | Access Control | RADIUS | SNMP | DHCP Server | DHCP Server Status | Dynamic DNS Update | Certificates | Advanced

**General**

Name of this firewall:

Default domain:

**IP Policy**

Discard IP packets  
 Reject IP packets

**Version of Ingate Firewall**

Check for new versions of Ingate Firewall:  Yes  No

Date of last successful version check: 2009-10-31 23:23:02

Software version in use: 4.8.2

**Policy For Ping to Your Ingate Firewall**

Never reply to ping  
 Only reply to ping to the same interface  
 Reply to ping to all IP addresses

The log classes used by the unit are defined on the **Log Classes page**. Some log classes are predefined; Company defines some new ones.

Display Log | Packet Capture | Check Network | Display Load | Hardware Monitoring | Logging Configuration | **Log Classes** | Log Sending

**Log Classes**

Edit Row	Name	Log Locally?	Syslog		Email Address	Delete Row
			Facility	Level		
<input type="checkbox"/>	Alarm	Yes	Local0	Alert	admin@ingate.com	<input type="checkbox"/>
<input type="checkbox"/>	Local	Yes	-	-		<input type="checkbox"/>
<input type="checkbox"/>	Local+Syslog	Yes	Auth	Notice		<input type="checkbox"/>
<input type="checkbox"/>	Syslog	No	Auth	Notice		<input type="checkbox"/>

Syslog is used; the IP address of a syslog server must be given.

For logging via email, give the DNS name or IP address of the mail server.

Display Log | Packet Capture | Check Network | Display Load | Hardware Monitoring | Logging Configuration | Log Classes | **Log Sending**

**SMTP Server (Help)**

DNS Name or IP Address	IP Address
<input type="text" value="172.22.1.4"/>	172.22.1.4

**Syslog Servers (Help)**

Edit Row	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	-	172.22.2.4	172.22.2.4	<input type="checkbox"/>

Add new rows  rows.

A number of **Services** are needed: dns and dns-reply for name server queries, ftp for FTP transfers, icmp for network analysis, nfs-udp for NFS mounting, smtp to send e-mail, ssh to ensure encrypted connections to other computers over the network, and www to view WWW pages. All of these are predefined in the unit. Services for all UDP, all TCP and all ICMP, UDP and TCP are defined here.

Services								
Edit Row	Name	Subgroup	Protocol	Firewall type	Client ports	Server ports	ICMP type	Delete Row
<input type="checkbox"/>	+ dns	-	UDP	Packet filter	53,1024-65535	53		<input type="checkbox"/>
<input type="checkbox"/>	+ dns-reply	-	UDP	Packet filter	53	53,1024-65535		<input type="checkbox"/>
<input type="checkbox"/>	+ ftp	-	TCP	Dynamic FTP management	1024-65535	21		<input type="checkbox"/>
<input type="checkbox"/>	+ icmp	-	ICMP	Packet filter			0-120	<input type="checkbox"/>
<input type="checkbox"/>	+ icmp/udp/tcp	icmp	-	-				<input type="checkbox"/>
<input type="checkbox"/>		tcp	-	-				<input type="checkbox"/>
<input type="checkbox"/>		udp	-	-				<input type="checkbox"/>
<input type="checkbox"/>	+ nfs-udp	-	UDP	Packet filter	1024-65535	2049		<input type="checkbox"/>
<input type="checkbox"/>	+ smtp	-	TCP	Dynamic session management	1024-65535	25		<input type="checkbox"/>
<input type="checkbox"/>	+ ssh	-	TCP	Dynamic session management	1024-65535	22		<input type="checkbox"/>
<input type="checkbox"/>	+ tcp	-	TCP	Dynamic session management	0-65535	0-65535		<input type="checkbox"/>
<input type="checkbox"/>	+ udp	-	UDP	Packet filter	0-65535	0-65535		<input type="checkbox"/>
<input type="checkbox"/>	+ www	-	TCP	Dynamic session management	1024-65535	80,443		<input type="checkbox"/>

**Time Classes** are also needed. There is a predefined class "24/7" (always). Here, classes for office hours and off-duty hours (evenings, nights and weekends) are defined.

Rules	Relays	DHCP Relay	Services	Protocols	Time Classes	
Time Classes						
Edit Row	Name	From Weekday	To Weekday	From Time	To Time	Delete Row
<input type="checkbox"/>	+ 24/7	Monday	Sunday	00:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>	+ off-duty hours	Monday	Friday	00:00	07:00	<input type="checkbox"/>
<input type="checkbox"/>		Monday	Friday	18:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>		Saturday	Sunday	00:00	24:00	<input type="checkbox"/>
<input type="checkbox"/>	+ office hours	Monday	Friday	07:00	18:00	<input type="checkbox"/>

Add new rows  groups with  rows per group.

Once computers, networks, time classes, and services are defined, Rules can be set up. Computers on the Internet should not have access to anything other than the services on the DMZ network's servers: WWW, FTP, email and DNS.

Set up rules to grant everyone on the Internet access to the DMZ services FTP and WWW (rules 9 and 10).

On the DMZ network, the name server must be able to query other name servers on the Internet (rules 1-2), and receive and reply on queries from other name servers (rules 4-5).

Enable queries from the internal name server to the external name server (rule 3). The reply traffic

for those queries will automatically be let through as the internal networks are NAT:ed. The computers on the internal networks use the internal name server for name queries. The internal name server queries external names and IP addresses via the external name server.

The external mail server is set up to receive email from the Internet (rule 13) and forward it to the internal mail server (via a TCP relay). The internal mail server forwards external emails to the external mail server (rule 11), which in turn forwards the emails to other mail servers on the Internet (rule 12).

Enable the internal viewing of WWW pages on own web server and external (Internet) web servers, but the latter only during off-duty hours (rules 6-7). Retrieve files with FTP from Company's FTP server and FTP servers on the Internet (rule 8).

No one on the Internet should be allowed to connect to Company's servers with ssh. Reject this traffic and alert the administrator via syslog (rule 14).

Since the internal networks are NAT:ed to the Internet and to the DMZ network, set-up of blocking rules for services like NFS and X-Window System is not necessary. Last, set up a rule to warn if any unexpected traffic is sent from the DMZ to the Internet (rule 15). This would probably mean that a cracker attack to a DMZ computer was successful, and the cracker now uses the computer to reach other computers on the Internet. To alert Company, the unit will send an email at any attempt and warn via syslog. Also reject the packets.

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	External DNS	-	Internet	-	DMZ -> External	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Internet	-	External DNS	-	External -> DMZ	dns-reply	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Internal DNS	-	External DNS	-	Internal -> DMZ (NAT:ed)	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	4	Yes	Internet	-	External DNS	-	External -> DMZ	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	5	Yes	Internal network	-	Internet	-	Internal -> External (NAT:ed)	www	Reject	Office hours	Local		<input type="checkbox"/>
<input type="checkbox"/>	6	Yes	External DNS	-	Internet	-	DMZ -> External	dns-reply	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	7	Yes	Internal network	-	Internet + DMZ	-	Internal -> Indeterminate interface (NAT:ed)	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	8	Yes	Internal network	-	Internet + DMZ	-	Internal -> Indeterminate interface (NAT:ed)	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	9	Yes	Internet	-	Web server	-	External -> DMZ	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	10	Yes	Internet	-	FTP server	-	External -> DMZ	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	11	Yes	External email	-	Internet	-	DMZ -> External	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	12	Yes	Internet	-	External email	-	External -> DMZ	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	13	Yes	Internal email	-	External email	-	Internal -> DMZ (NAT:ed)	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	14	Yes	Internet	-	DMZ	-	External -> DMZ	ssh	Reject	24/7	Local+Syslog		<input type="checkbox"/>
<input type="checkbox"/>	15	Yes	DMZ	-	Internet	-	DMZ -> External	icmp/udp/tcp	Reject	24/7	Alarm		<input type="checkbox"/>

The external mail server will not be able to forward mails to the internal mail server via rules, as the internal networks are NAT:ed. Therefore, go to the **Relays** page and define a TCP relay for the e-mail traffic from the external mail server to the internal mail server. The relay listens for traffic on port 25 (SMTP traffic) to the DMZ network interface. Only the external mail server can use this relay.

Relays											
Edit row	Listen to ...		Relay to ...			Relay type	Allow access from ...		Time class	Log class	Delete row
	IP address	Port	DNS name or IP address	IP address	Port		Network	IPsec peer			
<input type="checkbox"/>	DMZ (119.15.17.9)	25	172.22.1.4	172.22.1.4	25	TCP relay	External email	-	24/7	Local	<input type="checkbox"/>

Now all configuration is done. Store all this on a file for safekeeping, then click on **Apply configuration**.

Save/Load Configuration	Show Configuration	User Administration
<b>Test Run and Apply Conf</b> <a href="#">(Help)</a>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

## 18.4. How To Configure VLANs

In the unit you can use VLANs to mark IP packets. Here is a short description of what you need to do to make it work.

### 18.4.1. VLAN

On the **VLAN** page, you define and name the VLANs you want to use.

You must name VLANs that should be used in any network defined on the **Networks and Computers** page, which means all networks that should be used in **Rules** or **Relays**, from which SIP users should register, or any units allowed to send SNMP queries to the unit.

Named VLANs <a href="#">(Help)</a>					
Edit row	Name	Interface	VLAN id	Status	Delete row
<input type="checkbox"/>	admin	Internal (eth0)	14	On	<input type="checkbox"/>
<input type="checkbox"/>	company1	Internal (eth0)	20	On	<input type="checkbox"/>
<input type="checkbox"/>	company2	Internal (eth0)	30	On	<input type="checkbox"/>

### 18.4.2. Interface

On the **Interface** page for the interface where the VLANs are, you enter your networks and assign VLANs to them.

Directly Connected Networks (Help)										
Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Company1 lab	Static	192.168.15.1	192.168.15.1	24	192.168.15.0	192.168.15.255	20	company1	<input type="checkbox"/>
<input type="checkbox"/>	Company1 main	Static	192.168.10.1	192.168.10.1	24	192.168.10.0	192.168.10.255	20	company1	<input type="checkbox"/>
<input type="checkbox"/>	Company2	Static	192.168.18.1	192.168.18.1	24	192.168.18.0	192.168.18.255	30	company2	<input type="checkbox"/>
<input type="checkbox"/>	Inside	Static	10.47.2.243	10.47.2.243	16	10.47.0.0	10.47.255.255	14	admin	<input type="checkbox"/>

### 18.4.3. Networks and Computers

On the **Networks and Computers** page, you enter the networks that will use the VLANs, and select the proper VLAN for each of them.

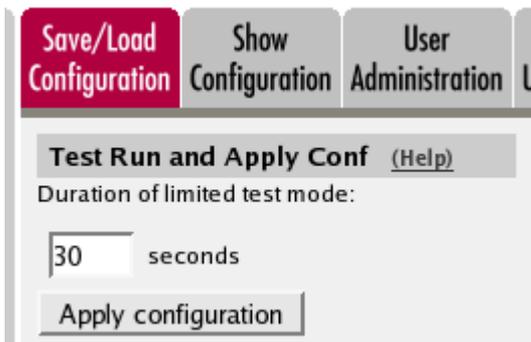
This is needed for all VLAN networks that should be used in **Rules** or **Relays**, from which SIP users should register, or any units allowed to send SNMP queries to the unit.

Networks and Computers										
<span style="background-color: #e91e63; color: white; padding: 2px;">Networks and Computers</span> <span style="background-color: #ccc; padding: 2px;">Default Gateways</span> <span style="background-color: #ccc; padding: 2px;">All Interfaces</span> <span style="background-color: #ccc; padding: 2px;">NAT</span> <span style="background-color: #ccc; padding: 2px;">VLAN</span> <span style="background-color: #ccc; padding: 2px;">Eth0</span> <span style="background-color: #ccc; padding: 2px;">Eth1</span> <span style="background-color: #ccc; padding: 2px;">Eth2</span> <span style="background-color: #ccc; padding: 2px;">Eth3</span> <span style="background-color: #ccc; padding: 2px;">Eth4</span> <span style="background-color: #ccc; padding: 2px;">Eth5</span> <span style="background-color: #ccc; padding: 2px;">Interface Status</span> <span style="background-color: #ccc; padding: 2px;">PPPoE</span>										
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row		
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address				
<input type="checkbox"/>	+ Admin network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	admin (eth0.14)	<input type="checkbox"/>		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>		
<input type="checkbox"/>	+ Company 1	-	192.168.10.0	192.168.10.0	192.168.10.255	192.168.10.255	company1 (eth0.20)	<input type="checkbox"/>		
<input type="checkbox"/>		-	192.168.15.0	192.168.15.0	192.168.15.255	192.168.15.255	company1 (eth0.20)	<input type="checkbox"/>		
<input type="checkbox"/>	+ Company 2	-	192.168.18.0	192.168.18.0	192.168.18.255	192.168.18.255	company2 (eth0.30)	<input type="checkbox"/>		
<input type="checkbox"/>	+ DMZ	-	172.16.0.0	172.16.0.0	172.16.0.255	172.16.0.255	DMZ (eth2 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	+ VPN everything	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>		

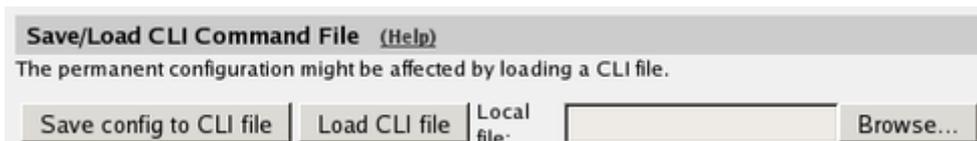
Then, you use the networks as usual in the configuration. Note that when the unit is configured to use a VLAN on a network, untagged packets coming in to the unit on that network will not be accepted.

### 18.4.4. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 18.5. How To Configure a Semi-transparent FTP Relay

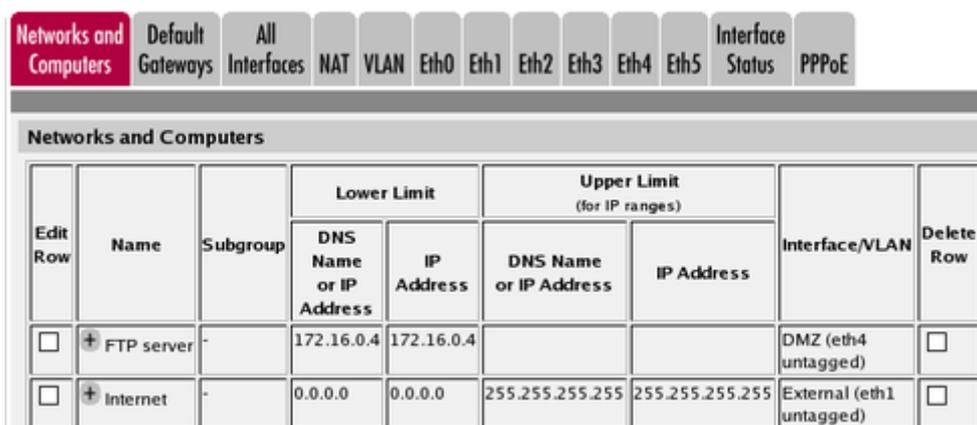
With an FTP server on the inside or a DMZ, incoming traffic is normally conveyed using an FTP relay. The flaw of this relay is that for the FTP server, all connections look like they originate from the unit, which means that the server has no possibility of authenticating or blocking units based on their IP addresses.

The ideal function in this situation would be a semi-transparent FTP relay, analogous with the semi-transparent TCP relay, where the original sender IP address is kept when the packet is forwarded to the FTP server. Unfortunately, there is no such relay today, but with a combination of settings, the function can be achieved. Here are the necessary settings for a semi-transparent FTP relay.

### 18.5.1. Networks and Computers

On the **Networks and Computers** page, you need a network containing all IP addresses allowed to access the FTP server. Usually, this is the entire Internet.

You also need a network with the IP address of the FTP server itself.



## 18.5.2. Relays

Then, go to the **Relays** page under **Rules and Relays** and add a new row to the table. Select the outside IP address and port 21 to listen for FTP requests. It is very important to use port 21, or this won't work properly. Enter the FTP server's private IP address to forward to, and select a Semi-transparent TCP port forwarding.

Relays (Help)												
Edit	Listen To ...		Relay To ...			Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class	Log Class	Delete
	IP Address	Port	DNS Name or IP Address	IP Address	Port		Network	IPsec Peer				
<input type="checkbox"/>	Outside (193.12.253.115)	21	172.16.0.4	172.16.0.4	21	Semi-transparent TCP port forwarding	Internet	-	-	24/7	Local	<input type="checkbox"/>

## 18.5.3. Rules

Go to the **Rules** page and create a rule for traffic from Internet to the FTP server. Use FTP as the service.

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Internet	-	FTP server	-	External -> DMZ	ftp	Allow	24/7	Local		<input type="checkbox"/>

## 18.5.4. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** Show Configuration User Administration

**Test Run and Apply Conf (Help)**

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File (Help)**

The permanent configuration might be affected by loading a CLI file.

Local file:

# Chapter 19. Administration

In this chapter, you find guidance for setting a new password for the unit's administrator user, whether you know the old password or not.

You also find a guide about moving configuration files between units.

## 19.1. Changing Password

To change the password via the web interface see [Password For the \*admin\* Account](#).

If you forgot the old *admin* password, you need physical access to the unit to set a new one. This also requires a reboot of the unit to make it accept a new password.

In short the procedure to change password is to:

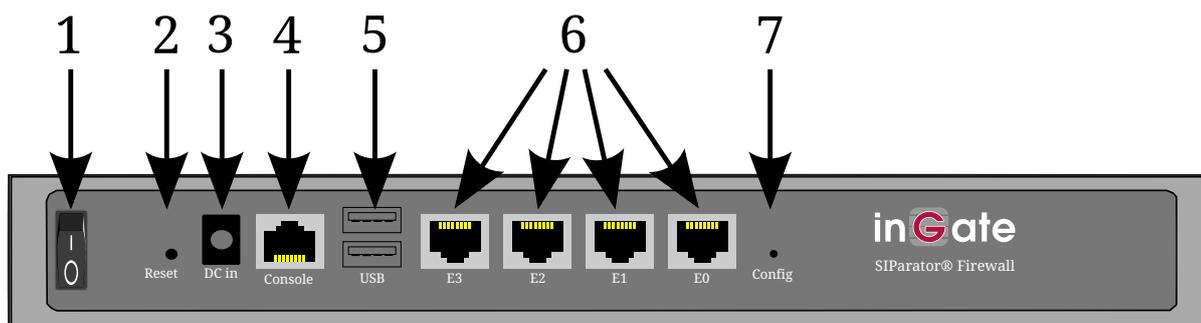
1. Change the unit to Unconfigured mode by special actions during a reboot.
2. Connect to the unit via a serial console.
3. Change the password.

**NOTE** During this reset sequence there will be no traffic through the unit.

### 19.1.1. Reboot the unit and change it to Unconfigured mode

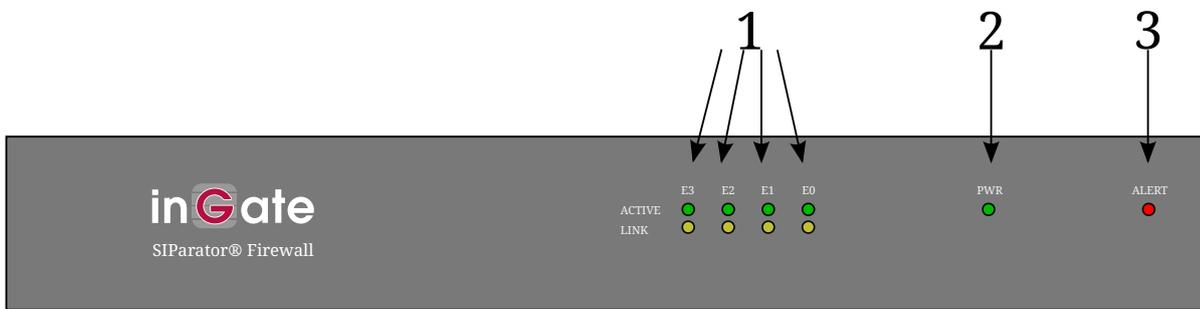
Depending on the model of the unit the reboot is done in different ways. See below:

#### Reboot an Ingate SIParator/Firewall S21 rev A



The unit can be rebooted in several ways. You can switch the Power button (item 1 in the figure) off and on or you can press the RESET button (item 2 in the figure) located at the back (a bent steel paper clip or other thin device is needed).

When the unit is booting up, the CONFIG button (item 7 in the figure) should be pressed at a certain time.

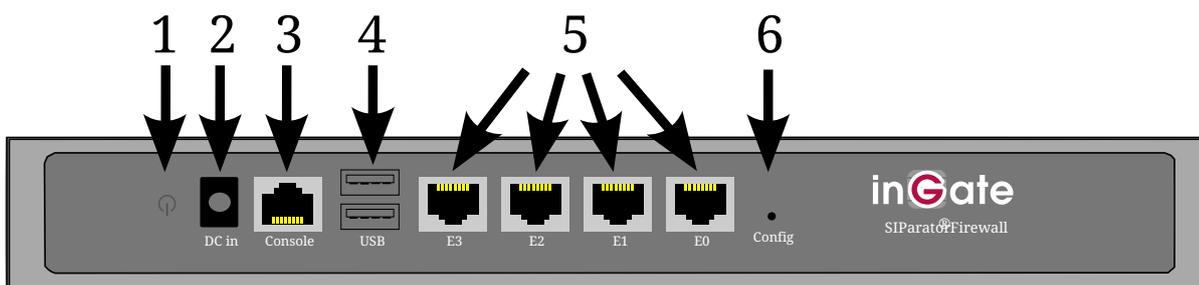


The Alert LED (item 3 in the figure) on the unit front will light up, go out and then light up again. The second time it is lit, the CONFIG button should be pressed. The LED will then go out to indicate that the pressed CONFIG button was detected, and you can stop pressing the button.

If you find it hard to find the right timing, you can start pressing the CONFIG button when the Alert LED is lit the first time. You must then keep on pressing it until the LED has been lit and gone out twice.

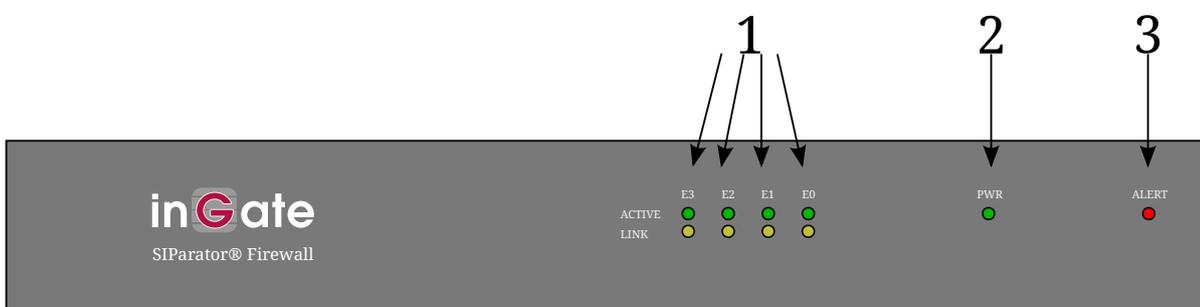
Wait until the unit has finished booting. Now, the Alert LED should double blink (two blinks followed by a short pause) to indicate that it has changed to Unconfigured mode, that implies it can receive a new password, and also a new IP address, if required.

### Reboot an Ingate SIParator/Firewall S21 rev B



The unit can be rebooted by pressing the Power button once (item 1 in the figure), wait about 10 seconds until the Power button turns blue and then press it again.

When the unit is booting up, the CONFIG button (item 6 in the figure) should be pressed at a certain time.



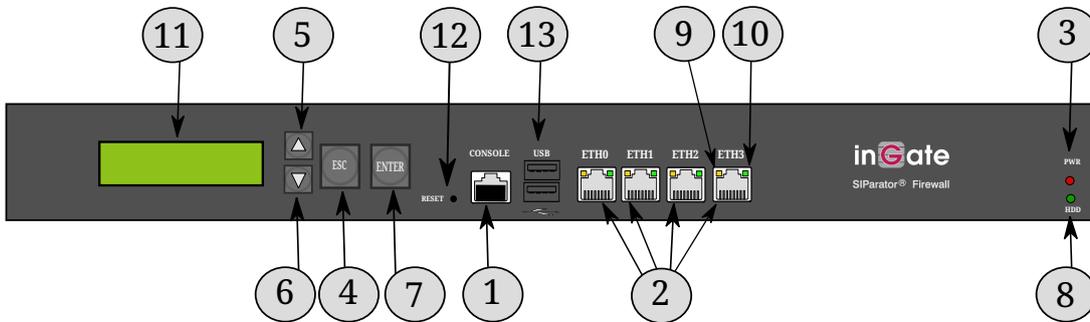
The Alert LED (item 3 in the figure) on the unit front will light up, go out and then light up again. The second time it is lit, the CONFIG button should be pressed. The LED will then go out to indicate that the pressed CONFIG button was detected, and you can stop pressing the button.

If you find it hard to find the right timing, you can start pressing the CONFIG button when the Alert

LED is lit the first time. You must then keep on pressing it until the LED has been lit and gone out twice.

Wait until the unit has finished booting. Now, the Alert LED should double blink (two blinks followed by a short pause) to indicate that it has changed to Unconfigured mode, that implies it can receive a new password, and also a new IP address, if required.

### Reboot an Ingate SIParator/Firewall S51

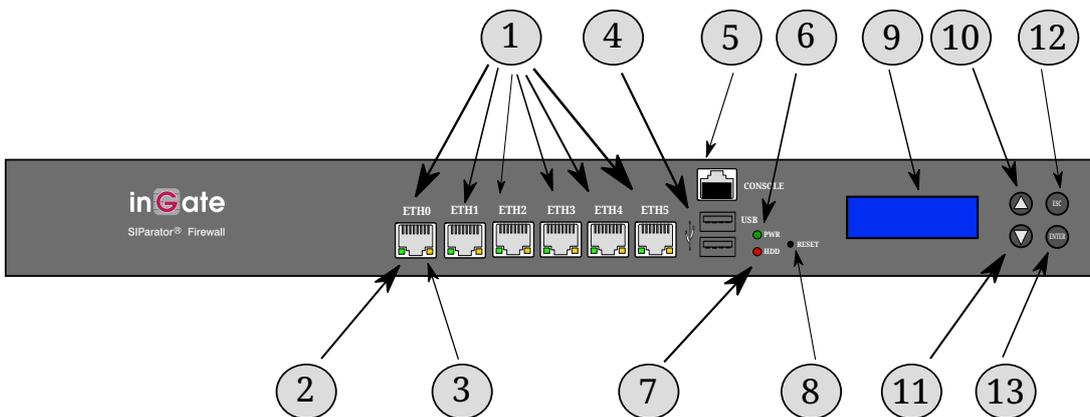


The unit can be rebooted in several ways. You can switch the Power button, located at the back, off and on or you can press the RESET button (item 12 in the figure) on the front (a bent steel paper clip or other thin device is needed).

At a certain time during boot, the text "PRESS ESC for UNCONFIGURED" will be displayed on the LCD display. When ESC is pressed, the text "UNCONFIGURED STATE CONFIRMED" will be shown.

When the unit is ready to receive new configuration, the text "UNCONFIGURED" and the first line of a menu is shown on the LCD display. You cannot set a new password via that menu.

### Reboot an Ingate SIParator/Firewall S52

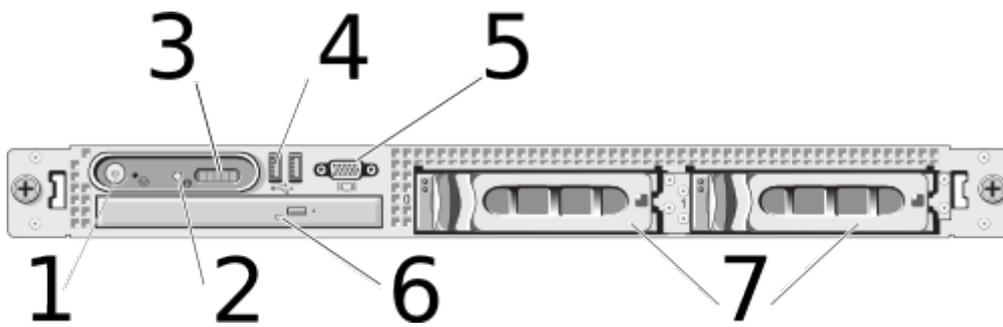


The unit can be rebooted in several ways. You can switch the Power button, located at the back, off and on or you can press the RESET button (item 8 in the figure) on the front (a bent steel paper clip or other thin device is needed).

At a certain time during boot, the text "ESC+ENTER for UNCONFIGURED" will be displayed on the LCD display. When ESC and Enter are pressed at the same time, the text "UNCONFIGURED STATE CONFIRMED" will be shown.

When the unit is ready to receive new configuration, the text "UNCONFIGURED" and the first line of a menu is shown on the LCD display. You cannot set a new password via that menu.

## Reboot an Ingate SIParator/Firewall S95/S96/S97/S98



Reboot the unit with the Ingate CD, that includes a factory reset function, in the drive during the boot sequence. This is the CD, including the user documentation, that was delivered together with your unit in the box. To reboot the unit switch the Power button, located at the back, off and on.

The admin password is erased and the unit is placed into an UNCONFIGURED state.

**NOTE** Eject the CD before next reboot.

### 19.1.2. Connect to the unit with a serial cable and a terminal program

See [Installation with a serial cable](#) for how to connect to the unit with a serial cable.

### 19.1.3. Enter a new password

Log on as admin from the serial console. You will see this menu:

```
Administration
=====

(Navigation tip: You may use Ctrl-d to skip back to this menu.)

1.      Basic configuration
2.      Download/Upload
3.      Join a failover team and become slave
5.      Wipe email logs
6.      Set password
7.      Command line interface
8.      Clear the log database
a.      About
reboot. Reboot
reset.  Factory reset
q.      Exit admin

==>
```

Select **6. Set password** and set a new password, you will be asked to write it again.

Select **q. Exit admin**.

After that, log on to the web interface as *admin*, using the new password.

## 19.2. Changing Password for Software SIParator/Firewalls

If you forgot the old *admin* password, this procedure describes how to set a new password. This requires a reboot of the unit with some special actions taken.

In short the procedure to change password is to:

1. Change the unit to Unconfigured mode by special actions during a reboot.
2. Connect to the unit via a serial console.
3. Change the password.

**NOTE** | During this reset sequence there will be no traffic through the unit.

### 19.2.1. Reboot the Software SIParator/Firewall and change it to Unconfigured mode

Reboot the Ingate Software SIParator/Firewall with the ISO file from the installation as the second alternative in the boot order. Installed SW should still be the first alternative.

The *admin* password is erased and the unit is placed into an UNCONFIGURED state.

Note: Unselect the ISO file afterwards, so next boot will be from the installed software instead of the ISO file (how this is done differs depending on hypervisor you have).

### 19.2.2. Connect to the Ingate Software SIParator/Firewall via the console

You will use the console of your virtual machine as terminal.

Click at the console tab in your virtual machine.

You have to press Return to get the login prompt in the console window.

### 19.2.3. Enter a new password

Log on as admin from the serial console. You will see this menu:

## Administration

=====

(Navigation tip: You may use Ctrl-d to skip back to this menu.)

1. Basic configuration
2. Download/Upload
3. Join a failover team and become slave
5. Wipe email logs
6. Set password
7. Command line interface
8. Clear the log database
- a. About
- reboot. Reboot
- reset. Factory reset
- q. Exit admin

==>

Select **6. Set password** and set a new password, you will be asked to write it again.

Select **q. Exit admin**.

After that, log on to the web interface as *admin*, using the new password.

## 19.3. Moving Configurations Between Ingate Units

There are two types of configuration files that can be downloaded from Ingate products; configuration databases (.cfg files) and CLI files (.cli files).

### 19.3.1. Configuration Databases

Configuration databases can generally be moved between units. These are the criteria for a successful configuration move from unit A to unit B:

- The units must be of the same type (you can't move a firewall configuration to a SIParator or vice versa).
- Unit A must not have a higher version number than unit B.
- Unit A must not have more interfaces than unit B.

### 19.3.2. CLI Files

CLI files can be moved between units, with slightly different criteria for the move. The criteria also change depending on if you edit the CLI file before you upload it again.

If you just download and upload again, these are the criteria for a successful move:

- The units must be of the same type (you can't move a firewall configuration to a SIParator or vice versa).

- Unit A must not have a higher version number than unit B. (However, when moving a configuration from a newer version into an older, the CLI file can be used if any settings for new functions are removed from the CLI file.)
- Unit A must not have more interfaces than unit B.
- Unit B must have all the extra software modules that unit A has.

If you edit the CLI file, you can remove all the SIParator- or firewall-specific settings, all extra interface settings and all extra module settings, and by this overcome restrictions for moving the CLI file. You can also make it not remove the old configuration on the box.

All the descriptions below are for the 4.6 (and higher) version of the CLI.

### 19.3.3. Keep Configuration

This is the command to remove from the CLI file if the old configuration should be kept.

```
load-factory --all
```

### 19.3.4. Firewall-specific Settings

When moving a configuration from a firewall to a SIParator, you must remove all lines concerning these settings.

- firewall.dhcp\_relay
- firewall.forwarding\_rules
- firewall.master\_logclass
- firewall.protocols
- firewall.relays
- firewall.services (if the SIParator does not have the Quality of Service module)
- firewall.timeclasses (if the SIParator does not have the SIP Trunking or Advanced SIP Routing module)
- ipsec.blacklisted\_packets
- ipsec.blacklisting
- misc.dhcp\_server
- misc.dhcp\_server\_dns\_servers
- misc.dhcp\_server\_domain
- misc.dhcp\_server\_give\_ns
- misc.dhcp\_server\_leasetime
- misc.dhcp\_server\_netbios\_nodetype
- misc.dhcp\_server\_status
- misc.dhcp\_server\_wins\_servers

- network.masquerading

### 19.3.5. SIParator-specific Settings

When moving a configuration from a SIParator to a firewall, you must remove all lines concerning these settings.

- sip.public\_ip
- sip.st\_type
- sip.surroundings

### 19.3.6. Fewer Interfaces

When moving a configuration to a box with fewer interfaces, you need to look for the settings below and remove the lines for the extra interfaces.

If you move a configuration to a box with only three interfaces, there will only be eth0, eth1, and eth2 on that box. All configuration lines for eth3 and higher must be removed.

- config.allow\_via\_interface
- failover.iface\_ref\_hosts
- firewall.network\_groups
- network.alias\_addresses
- network.interfaces
- network.local\_nets
- network.masquerading
- network.routes
- network.vlans
- qos.egress\_default\_queueing
- qos.egress\_queueing
- qos.ingress\_default\_queueing
- qos.ingress\_queueing

### 19.3.7. Settings for SIP Trunking

When moving a configuration from a unit with the SIP Trunking module onto one without it, you must remove all lines concerning these settings.

- sipswitch.b2bua\_transfer\_enable
- sipswitch.b2bua\_transfer\_from\_user
- sipswitch.dial\_plan\_methods
- sipswitch.enum\_root

- sipswitch.incoming\_unauth
- sipswitch.request\_from
- sipswitch.user\_routing

From the sipswitch.dial\_plan settings, you must remove the "reqfrom", "enum\_prefix" and "forward\_prefix" fields.

From the sipswitch.forward\_to settings, you must remove the "account" and "regexp" fields.

From the sipswitch.request\_to settings, you must remove the "prefix", "min\_tail\_length" and "regexp" fields.

From the sipswitch.users settings, you must remove all lines where the "type" field is not set to "user".

### 19.3.8. Settings for Remote SIP Connectivity

When moving a configuration from a unit with the Remote SIP Connectivity module onto one without it, you must remove all lines concerning these settings.

- fent.fent
- fent.fent\_keepalive
- fent.media\_release

### 19.3.9. Settings for Advanced SIP Routing

When moving a configuration from a unit with the Advanced SIP Routing module onto one without it, but with the SIP Trunking module, you must remove all lines concerning these settings.

- sipswitch.incoming\_unauth
- sipswitch.voicemail

From the sipswitch.user\_routing settings, you must remove the "aliases", "timeclass", "restrict\_incoming", and "voice\_mail" fields.

When moving a configuration from a unit with the Advanced SIP Routing module onto one without it, and without the SIP Trunking module, you must also remove all lines concerning these settings.

sipswitch.user\_routing

From the sipswitch.users settings, you must remove all lines where the "type" field is not set to "user".

### 19.3.10. Settings for Enhanced Security

When moving a configuration from a unit with the Enhanced Security module onto one without it, you must remove all lines concerning these settings.

- idsips.active

- idsips.predefined\_ips\_rules
- idsips.rate\_limited\_ips
- sip.tls\_cacerts
- sip.tls\_client\_cfg
- sip.tls\_server\_cfg
- sip.tls\_settings
- sip.use\_tls

From the sip.media\_encryption\_rules and sip.media\_encryption\_policy settings, you must remove the "allow\_transcoding" field.

### **19.3.11. Settings for VoIP Survival**

When moving a configuration from a unit with the VoIP Survival module onto one without it, you must remove all lines concerning these settings.

- voipsm.voipsm
- voipsm.voipsm\_domains
- voipsm.voipsm\_pstn\_gateways

# Chapter 20. SIP

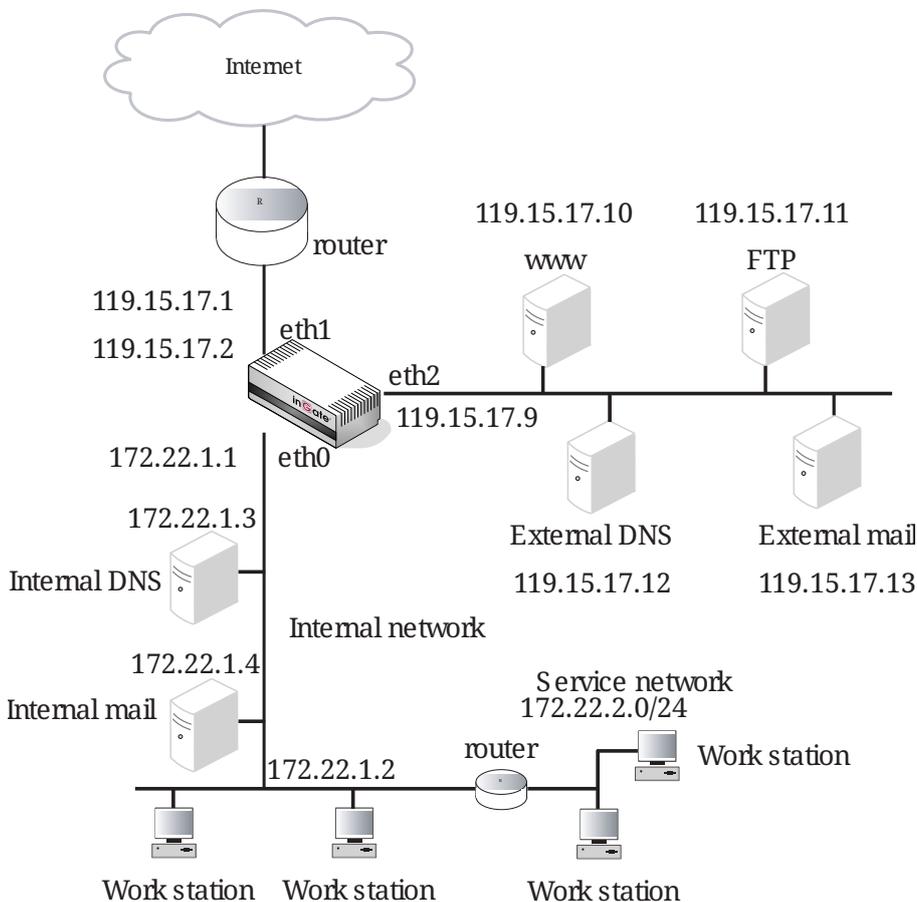
## 20.1. SIP and IPv4/IPv6

To be able to separate IPv4-only/IPv6-only hosts the following settings must be enabled.

- Select a [SIParator Type](#).
- Enable the [Media Proxy](#).

## 20.2. SIP Configuration

Here is a complete SIP configuration for a unit with three active interfaces. The network looks like this:



First, make sure that the IP address for a **Default gateway** is entered on the **Default Gateways** page. This is needed when the SIP requests are routed.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Main Default Gateways <a href="#">(Help)</a>												
Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row						
<input type="checkbox"/>		-	119.15.17.1	119.15.17.1	External (eth1)	<input type="checkbox"/>						

Enter a **DNS server** on the **Basic Configuration** page. This is needed to look up other SIP domains.

DNS Servers <a href="#">(Help)</a>					
Edit Row	No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	1	-	119.15.17.12	119.15.17.12	<input type="checkbox"/>

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

Basic
Signaling Encryption
Media Encryption
Interoperability
Sessions and Media
Remote SIP Connectivity
VoIP Survival
VoIP Survival Status

**SIP Module** [\(Help\)](#)

- Enable SIP module
- Disable SIP module

### 20.2.1. SIP registrar handled by the unit

Go to the **Filtering** page. SIP requests from the internal network should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

SIP Methods
Filtering
Local Registrar
Authentication and Accounting
SIP Accounts
Dial Plan
Routing
SIP Status
IDS/IPS
IDS/IPS Status

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Internal network	Process all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

- Process all
- Local only
- Reject all

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain looks just like the ordinary Internet domain for the company.

Some IP telephones register on IP addresses (their own or that of the registrar) instead of domains. If you use this type of telephones, add the IP address of the registrar as a **Locally handled domain**.

SIP Methods
Filtering
Local Registrar
Authentication and Accounting
SIP Accounts
Dial Plan
Routing
SIP Status
IDS/IPS
IDS/IPS Status

**Local SIP Domains** [\(Help\)](#)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	172.22.1.1	<input type="checkbox"/>
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

To enable SIP clients to receive SIP requests, they must be allowed to register. Add one row for each

domain, where all users in the domains are allowed to register. With this setting, you can allow users to register without authentication, or use authentication, but all users have the same password. Note that with the settings shown in the image, users who use the IP address of the unit as their SIP domain can only register from the Internal network.

Local SIP User Database <a href="#">(Help)</a>						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	*	172.22.1.1			Internal network	<input type="checkbox"/>
<input type="checkbox"/>	*	ingate.com			Everything	<input type="checkbox"/>

The recommended setting is to let all SIP proxies perform authentication. Go to the **Authentication and Accounting** page to turn authentication on.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status
-------------	-----------	-----------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------	----------	-----------------

### Brute Force Authentication Protection [\(Help\)](#)

Maximum amount of attempts:

Time interval:  seconds

Stop responding after interval:  seconds

Max number of clients:

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication (enabled below).

### SIP Authentication

Enable SIP authentication  
 Disable SIP authentication

### SIP Realm

If you want the unit to authenticate users you must also decide what to authenticate for. Select the methods to allow and authenticate on the **SIP Methods** page.

**SIP Methods** [\(Help\)](#)  
 Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

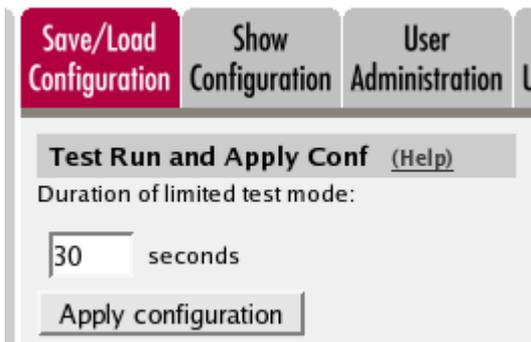
Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Then go to the **Local Registrar** page and list the SIP users. You must enter all users on separate lines to give them individual passwords.

**Local SIP User Database** [\(Help\)](#)

Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	lab1	172.22.1.1			Internal network	<input type="checkbox"/>
<input type="checkbox"/>	lab2	172.22.1.1			Internal network	<input type="checkbox"/>
<input type="checkbox"/>	charlie	ingate.com	c5481		Everything	<input type="checkbox"/>
<input type="checkbox"/>	chris	ingate.com	c2089		Everything	<input type="checkbox"/>
<input type="checkbox"/>	linda	ingate.com	l2731		Everything	<input type="checkbox"/>
<input type="checkbox"/>	maude	ingate.com	m2247		Everything	<input type="checkbox"/>
<input type="checkbox"/>	tom	ingate.com	t8738		Everything	<input type="checkbox"/>

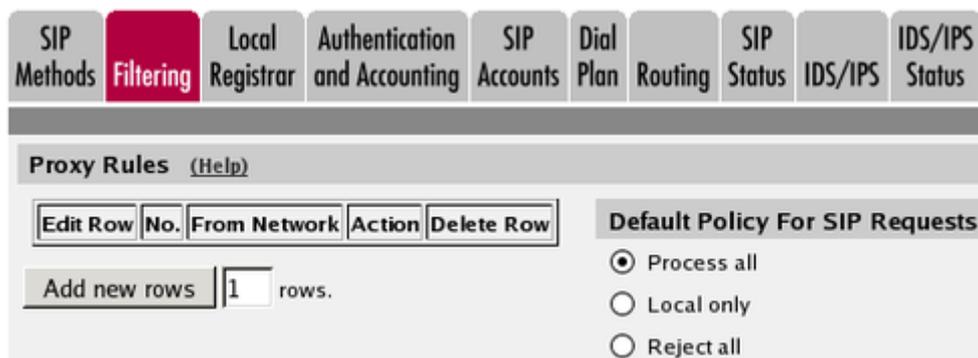
This is all configuration needed for the unit to manage SIP traffic. Apply the configuration on the **Save/Load Configuration** page.



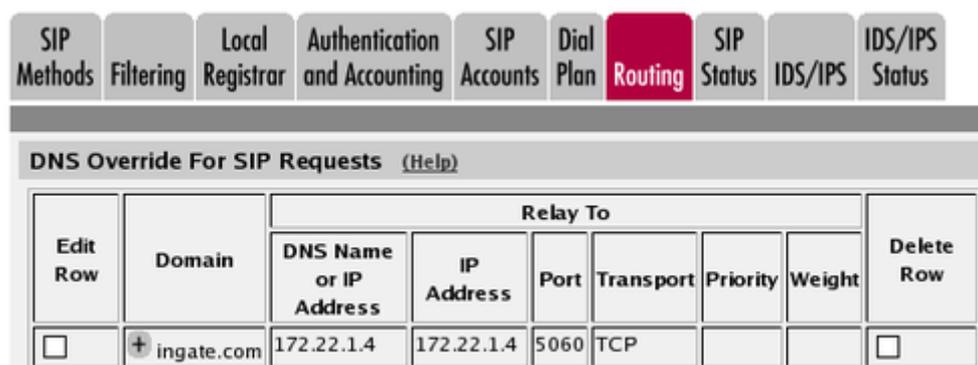
## 20.2.2. SIP server on the LAN

If you don't want to use the built-in SIP registrar in the unit, you will have to do some other settings. Maybe you also want to use an external SIP server, and use the unit just as a SIP proxy.

On the **Filtering** page, all SIP requests must be processed, as the unit does not have any **Locally handled domains**. If any of the other options are selected, no requests will be processed.



On the **Routing** page, enter the SIP domain used, and the SIP server (IP address and port) you want to forward your SIP requests to.



Some SIP server do not accept SIP elements between themselves and the SIP clients. The SIP server deduce that other SIP elements are involved by counting Via headers in the received SIP packet.

On the **Interoperability** page, you can make the unit remove all Via headers for certain servers, to trick them to believe that there are no other elements involved.

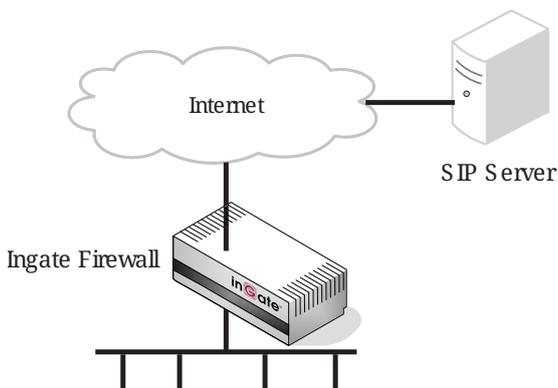
Remove Via Headers <a href="#">(Help)</a>			
Edit	SIP Server		Delete
	DNS Name or IP Address	IP Address	
<input checked="" type="checkbox"/>	172.22.1.4	172.22.1.4	<input type="checkbox"/>

These are the SIP settings needed. **Apply the configuration** on the **Save/Load Configuration** page.

Save/Load Configuration	Show Configuration	User Administration	U
<b>Test Run and Apply Conf</b> <a href="#">(Help)</a>			
Duration of limited test mode:			
<input type="text" value="30"/>	seconds		
<input type="button" value="Apply configuration"/>			

## 20.3. SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the unit SIP function is only used to traverse NAT.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.3.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:

Log class for SIP packets:

Log class for SIP license messages:

Log class for SIP errors:

Log class for SIP media messages:

Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

### 20.3.2. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS SIP Status

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row

Add new rows  rows.

**Default Policy For SIP Requests**

Process all

Local only

Reject all

### 20.3.3. Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

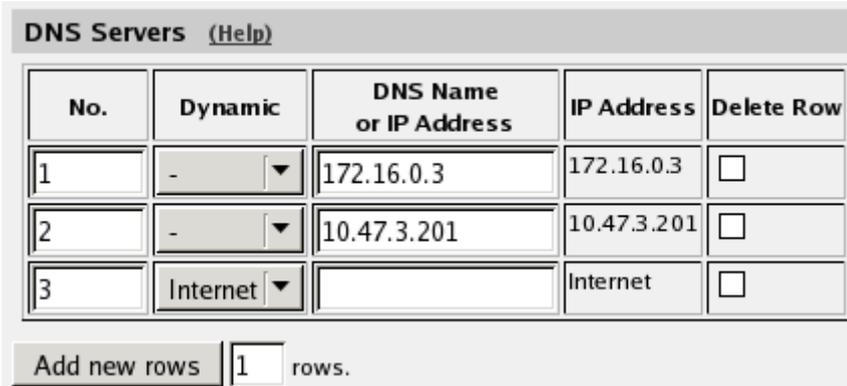
If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

**Outbound Proxy** [\(Help\)](#)

Edit Row	From Domain	Request-URI Domain	Domain or IP Address	Port	Gateway	Delete Row
<input type="checkbox"/>	*	*	3.22.39.7	5060	-	<input type="checkbox"/>

### 20.3.4. Basic Configuration

If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.



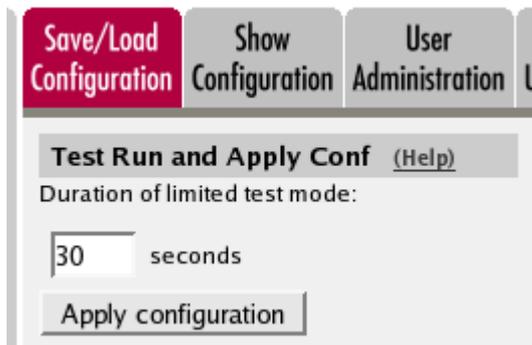
The screenshot shows a table titled "DNS Servers" with a "(Help)" link. The table has five columns: "No.", "Dynamic", "DNS Name or IP Address", "IP Address", and "Delete Row". There are three rows of data. Below the table is a button "Add new rows" followed by a text input field containing "1" and the text "rows.".

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

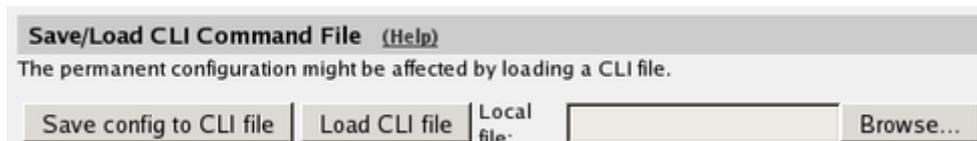
### 20.3.5. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



The screenshot shows a navigation bar with "Save/Load Configuration" (highlighted in red), "Show Configuration", "User Administration", and "U". Below the navigation bar is a section titled "Test Run and Apply Conf" with a "(Help)" link. It contains the text "Duration of limited test mode:" followed by a text input field containing "30" and the text "seconds". Below this is a button labeled "Apply configuration".

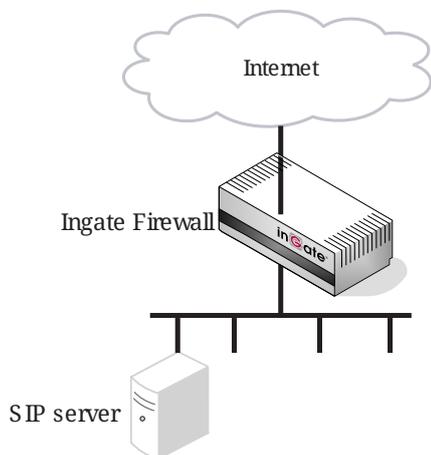
When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



The screenshot shows a section titled "Save/Load CLI Command File" with a "(Help)" link. Below the title is the text "The permanent configuration might be affected by loading a CLI file." At the bottom, there are three buttons: "Save config to CLI file", "Load CLI file", and "Browse...". To the right of the "Load CLI file" button is a text input field labeled "Local file:".

## 20.4. SIP server

You might want to have most SIP functions in one box. The unit can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.4.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:	Log class for SIP packets:
<input style="width: 100%;" type="text" value="Local"/>	<input style="width: 100%;" type="text" value="Local"/>
Log class for SIP license messages:	Log class for SIP errors:
<input style="width: 100%;" type="text" value="Local"/>	<input style="width: 100%;" type="text" value="Local"/>
Log class for SIP media messages:	Log class for SIP debug messages:
<input style="width: 100%;" type="text" value="Local"/>	<input style="width: 100%;" type="text" value="Local"/>
Log class for SIP IDS/IPS:	
<input style="width: 100%;" type="text" value="Local"/>	
Hide sensitive data: <input checked="" type="radio"/> Yes <input type="radio"/> No	

### 20.4.2. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status
-------------	-----------	-----------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------	----------	-----------------

### Brute Force Authentication Protection [\(Help\)](#)

Maximum amount of attempts:

Time interval:  seconds

Stop responding after interval:  seconds

Max number of clients:

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication (enabled below).

### SIP Authentication

Enable SIP authentication  
 Disable SIP authentication

### SIP Realm

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.

<h4 style="background-color: #d3d3d3; padding: 2px;">Select SIP User Database <a href="#">(Help)</a></h4> <p>Use SIP user database: <input type="radio"/> Local <input checked="" type="radio"/> RADIUS</p>	<h4 style="background-color: #d3d3d3; padding: 2px;">RADIUS Database Settings</h4> <p>RADIUS users register from:</p> <p><input type="text" value="Office network"/> <span style="border: 1px solid #ccc; padding: 2px;">▼</span></p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 20.4.3. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	No	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

### 20.4.4. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	10.47.2.243	<input type="checkbox"/>
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database (Help)						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

## 20.4.5. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also [RADIUS](#) for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	DHCP Server	DHCP Server Status	Dynamic DNS Update	Certificates	Advanced
<b>RADIUS Servers (Help)</b>								
	<b>RADIUS Server</b>							
<b>Edit Row</b>	<b>DNS Name or IP Address</b>	<b>IP Address</b>	<b>Port</b>	<b>Secret</b>	<b>Delete Row</b>			
<input type="checkbox"/>	193.180.23.77	193.180.23.77	1645		<input type="checkbox"/>			
Add new rows		<input type="text" value="1"/>	rows.					

## 20.4.6. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to Process all.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

Create rules for traffic from the inside (Process all) and the DMZ (Reject all). Let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status SIP Test SIP Test Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Office network	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.4.7. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.4.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** Show Configuration User Administration U

**Test Run and Apply Conf** (Help)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** (Help)

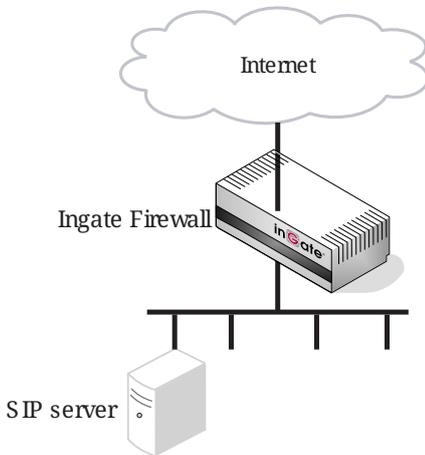
The permanent configuration might be affected by loading a CLI file.

Local file:

## 20.5. SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the unit. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the unit, which in turn will forward the SIP traffic to the server.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.5.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool



### 20.5.2. Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the unit, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The unit will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status
-------------	-----------	-----------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------

DNS Override For SIP Requests <a href="#">(Help)</a>								
Edit Row	Domain	Relay To						Delete Row
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
<input type="checkbox"/>	+ ingate.com	10.47.2.246	10.47.2.246	5060	UDP			<input type="checkbox"/>

### 20.5.3. Interoperability

If Windows Messenger is used for SIP communication, you need to set a parameter on the **Interoperability** page. Set **lr=true** status to **On** under **Loose routing**.



If the SIP server is an LCS (Live Communications Server) or some other server that does not accept more than one **Via** header in SIP packets, you must enter the SIP server IP address in the **Remove Via Headers** table. This will make the unit strip SIP packets of extra **Via** headers when it sends those packets to the server, and add the **Via** headers when the response packets are received.

Remove Via Headers <a href="#">(Help)</a>		
SIP Server		Delete Row
DNS Name or IP Address	IP Address	
<input type="button" value="Add new rows"/> <input type="text" value="1"/> ROWS.		
<input type="checkbox"/> Remove Via Headers for all SIP servers		

### 20.5.4. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS IDS/IPS Status

**Proxy Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
Add new rows   1 rows.				

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

### 20.5.5. Basic Configuration

If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows | 1 rows.

### 20.5.6. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** Show Configuration User Administration U

**Test Run and Apply Conf** (Help)

Duration of limited test mode:

30 seconds

Apply configuration

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

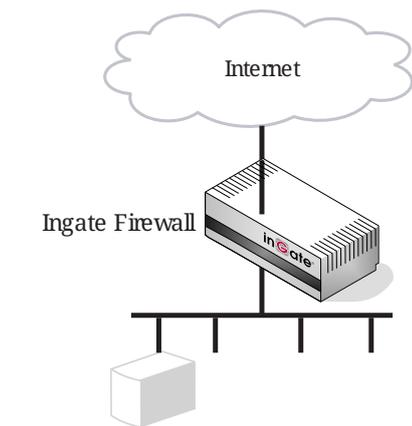
**Save/Load CLI Command File** (Help)

The permanent configuration might be affected by loading a CLI file.

Save config to CLI file | Load CLI file | Local file:  | Browse...

SIP server in the unit, PSTN gateway inside ..... You might want to have most SIP functions in one box. The unit can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.

A function not included in the unit is to connect to the PSTN network. If you want to do this, you must use a PSTN gateway.



PSTN gateway

Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.5.7. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

<b>SIP Logging</b> <a href="#">(Help)</a>	
Log class for SIP signaling:	Log class for SIP packets:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP license messages:	Log class for SIP errors:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP media messages:	Log class for SIP debug messages:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP IDS/IPS:	
<input type="text" value="Local"/>	
Hide sensitive data:	<input checked="" type="radio"/> Yes <input type="radio"/> No

### 20.5.8. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status
-------------	-----------	-----------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------	----------	-----------------

**Brute Force Authentication Protection** [\(Help\)](#)

Maximum amount of attempts:

Time interval:  seconds

Stop responding after interval:  seconds

Max number of clients:

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication (enabled below).

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

### 20.5.9. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	No	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

## 20.5.10. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	10.47.2.243	<input type="checkbox"/>
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database (Help)						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

## 20.5.11. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also [RADIUS](#) for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	DHCP Server	DHCP Server Status	Dynamic DNS Update	Certificates	Advanced
<b>RADIUS Servers (Help)</b>								
	<b>RADIUS Server</b>							
<b>Edit Row</b>	<b>DNS Name or IP Address</b>	<b>IP Address</b>	<b>Port</b>	<b>Secret</b>	<b>Delete Row</b>			
<input type="checkbox"/>	193.180.23.77	193.180.23.77	1645		<input type="checkbox"/>			
Add new rows		<input type="text" value="1"/>	rows.					

## 20.5.12. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to Process all.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

Create rules for traffic from the inside (Process all) and the DMZ (Reject all). Let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status SIP Test SIP Test Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Office network	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

### 20.5.13. Routing

To redirect traffic to the PSTN network, you can use the **Dial Plan**. You can state that all SIP traffic to user names that consist of digits only (that is, the user names are phone numbers) to be redirected to the local PSTN gateway. You can also direct different numbers to different gateways.

If there are SIP clients which can't use authentication for INVITE (the method used to start calls), you can except these from authentication when calling to PSTN. Select the network for these clients in the **Matching From Header** table and create a row in the **Dial Plan** table, where Forward is selected as the **Action** (which means that authentication is not required).

**Matching From Header** (Help)

Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

In the example below, all phone numbers beginning with 01146 or +46 are redirected to a server in Sweden, numbers beginning with 01144 or +44 are redirected to a server in England, and calls to all other phone numbers are directed to the local PSTN gateway. Note that the table is read from the top and down, and the first matching row is used to route the call.

You should also restrict the redirections to only calls for local domains. Enter "\*local" under **Domain** when creating patterns in the **Matching Request-URI** table.

**Matching Request-URI** (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	Any number			0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden1		01146	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden2		+46	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK1		01144	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK2		+44	0..9		*local		<input type="checkbox"/>

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ Local PSTN	1	-	pstn.us.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ London PSTN	1	-	pstn.uk.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ Stockholm PSTN	1	-	pstn.sthlm.ingate.com		UDP		<input type="checkbox"/>

To prevent unauthorized use of your PSTN gateway, you should require authentication for all these redirections. Select Auth&Forward as the **Action** to manage this.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	Office	UK1	Forward	London PSTN			-	-	Redirect calls to UK	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	UK2	Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	3	-	UK1	Auth & Forward	London PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	4	-	UK2	Auth & Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	5	Office	Sweden1	Forward	Stockholm PSTN			-	-	Redirect calls to Sweden	<input type="checkbox"/>
<input type="checkbox"/>	6	Office	Sweden2	Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	7	-	Sweden1	Auth & Forward	Stockholm PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	8	-	Sweden2	Auth & Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	9	Office	Any number	Forward	Local PSTN			-	-	Redirect to local PSTN	<input type="checkbox"/>
<input type="checkbox"/>	10	-	Any number	Auth & Forward	Local PSTN			-	-	Auth if not from Office	<input type="checkbox"/>

## 20.5.14. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

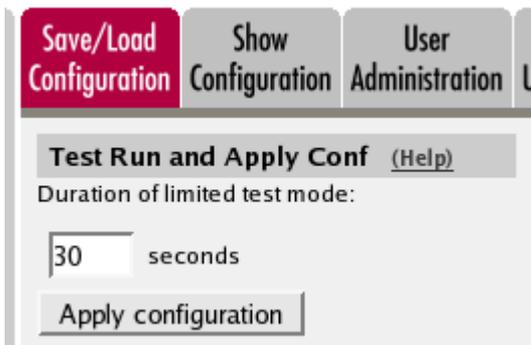
This setting is made by the Startup Tool

DNS Servers (Help)				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

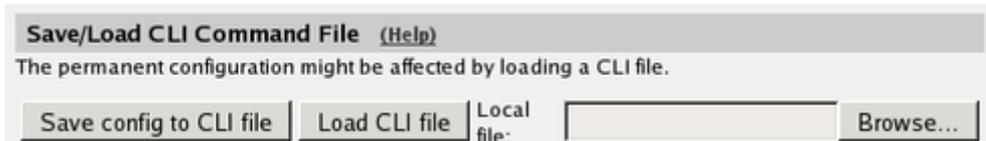
Add new rows  rows.

## 20.5.15. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 20.6. How To Use Your SIP Operator Account Via the Ingate Unit

This is how to configure your unit to register at your SIP operator, and to use that SIP account for your local users.

Enter your SIP operator account on the **Local Registrar** page. You enter the username and password from the operator, and select the *XF/Register* account type. This account type will make the unit register at the SIP operator with the credentials you enter.

Some operators don't require registration. In this case, select the *XF* account type instead.

You can select any network in the Register from field, as it is not used for these account types.

SIP Accounts (Help)							
Edit Row	Username	Domain	Authentication Name	Display Name	Password	Account Type	Delete Row
<input type="checkbox"/>	24285722	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>
<input type="checkbox"/>	24285723	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>
<input type="checkbox"/>	24285724	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>
<input type="checkbox"/>	24285725	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>

If the unit should act as the registrar, define a local SIP domain. This can be any domain name you like, as long as it isn't an existing domain somewhere else. A good choice is to use your company *www* domain, but replace the "www" with "sip", like *sip.ingate.com*. The same domain can also be used in pure SIP-to-SIP calls.

This domain should be entered on the **Local Registrar** page under **SIP Traffic**.

SIP Methods	Filtering	<b>Local Registrar</b>	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status
-------------	-----------	------------------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------

---

**Local SIP Domains** [\(Help\)](#)

Edit Row	Domain	Delete Row
<input checked="" type="checkbox"/>	ingate.com	<input type="checkbox"/>

Then, you define your local users in the **Local SIP User Database** table. These users will register on the unit with the usernames you enter here. Enter also their passwords and select a network from which they are allowed to register.

Note that no local user can have the same username as any of your operator account names.

**Local SIP User Database** [\(Help\)](#)

Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	harry	ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	helen	ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	mark	ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	ingate.com			Office network	<input type="checkbox"/>

Go to the **Authentication and Accounting** page and turn authentication on. Also enter your SIP domain as the Realm.

SIP Methods	Filtering	Local Registrar	<b>Authentication and Accounting</b>	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status
-------------	-----------	-----------------	--------------------------------------	--------------	-----------	---------	------------	---------	----------------

---

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

ingate.com

### 20.6.1. Outgoing Calls

For outgoing calls, you have to define when your SIP operator account should be used. Usually, you use this type of account to call to the PSTN network ("ordinary telephones").

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.

<b>Use Dial Plan</b> <a href="#">(Help)</a>	<b>Emergency Number</b> <a href="#">(Help)</a>
<input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	911

## 20.6.2. Show One Number When Calling

You can select to show one single calling number regardless of which user makes the call. This is useful when you want others to use your Answering service/Auto Attendant when calling back to you.

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

Matching From Header <a href="#">(Help)</a>							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	ingate	*	ingate.com		Any	-	<input type="checkbox"/>
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

Add new rows  rows.

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like helen@sip.ingate.com should not be routed via the SIP operator, but be handled by the unit itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	External numbers			0..9	4	*local		<input type="checkbox"/>
<input type="checkbox"/>	International numbers	+		0..9	4	*local		<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

The calls can also be forwarded to your SIP operator using the operator's IP address in the **Replacement URI** field.

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...		... Or This		... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ SIP Operator	1	24285722@sipoperator.com			-		<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table. Make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	Office	International numbers	Forward	SIP Operator	00		-	24/7	Change prefix for international calls	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	External numbers	Forward	SIP Operator			-	24/7	External calls sent to operator	<input type="checkbox"/>

Now, when a local user calls an external phone number, the unit will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

### 20.6.3. Show Different Numbers When Calling

You can select to show different calling numbers based on which user makes the call. This is useful when you want to let the called person use number presentation to see who is calling.

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

Create one row per user. These will be used to present the correct calling number for the called user.

Matching From Header (Help)							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	From Arthur	arthur	*local		Any	Office network	<input type="checkbox"/>
<input type="checkbox"/>	From Harry	harry	*local		Any	Office network	<input type="checkbox"/>
<input type="checkbox"/>	From Helen	helen	*local		Any	Office network	<input type="checkbox"/>
<input type="checkbox"/>	From Mark	mark	*local		Any	Office network	<input type="checkbox"/>

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like helen@sip.ingate.com should not be routed via the SIP operator, but be handled by the unit itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.

Matching Request-URI (Help)								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	External numbers			0..9	4	*local		<input type="checkbox"/>
<input type="checkbox"/>	International numbers	+		0..9	4	*local		<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, calls from one user should be forwarded to the corresponding SIP operator account. Create one row per user and select the account under **Account**.

Forward To (Help)							
Edit Row	Name	Subno.	Use This ...	... Or This			Delete Row
			Account	Replacement Domain	Port	Transport	
<input type="checkbox"/>	Arthur PSTN	1	24285723@sipoperator.com			-	<input type="checkbox"/>
<input type="checkbox"/>	Harry PSTN	1	24285724@sipoperator.com			-	<input type="checkbox"/>
<input type="checkbox"/>	Helen PSTN	1	24285725@sipoperator.com			-	<input type="checkbox"/>
<input type="checkbox"/>	Mark PSTN	1	24285722@sipoperator.com			-	<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table. For each user, make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	From Helen	International numbers	Forward	Helen PSTN	00		-	24/7	Change prefix for international calls.	<input type="checkbox"/>
<input type="checkbox"/>	2	From Helen	External numbers	Forward	Helen PSTN			-	24/7	External calls sent to operator.	<input type="checkbox"/>
<input type="checkbox"/>	3	From Arthur	International numbers	Forward	Arthur PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	4	From Arthur	External numbers	Forward	Arthur PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	5	From Harry	International numbers	Forward	Harry PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	6	From Harry	External numbers	Forward	Harry PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	7	From Mark	International numbers	Forward	Mark PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	8	From Mark	External numbers	Forward	Mark PSTN			-	24/7		<input type="checkbox"/>

Now, when a local user calls an external phone number, the unit will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

## 20.6.4. Incoming Calls

If your SIP account provides several phone numbers, you can assign separate numbers for your local users. You do that on the **Routing** page.

There are two different ways of mapping phone numbers to users; either the PSTN numbers are mapped to users or the users are given numbers as aliases. The latter only works when the

Advanced SIP Routing module has been installed and the SIP operator does not require registration.

In the **User Routing** table, you can select a local user and assign a SIP operator phone number as an Alias for that user. This will only work when the Advanced SIP Routing module has been installed and the SIP operator does not require registration.

User Routing <a href="#">(Help)</a>									
Edit Row	User	Alias	Restrict Incoming Callers	Forward		Send To Voice Mail	Time Class	Comment	Delete Row
				Action	To				
<input type="checkbox"/>	arthur@sip.ingate.com	24285723	No	-	-	-	-		<input type="checkbox"/>
<input type="checkbox"/>	harry@sip.ingate.com	24285724	No	-	-	-	-		<input type="checkbox"/>
<input type="checkbox"/>	helen@sip.ingate.com	24285725	No	-	-	-	-		<input type="checkbox"/>
<input type="checkbox"/>	mark@sip.ingate.com	24285722	No	-	-	-	-		<input type="checkbox"/>

You can also select each phone number, and enter which user calls should be forwarded to.

User Routing <a href="#">(Help)</a>									
Edit Row	User	Alias	Restrict Incoming Callers	Forward		Send To Voice Mail	Time Class	Comment	Delete Row
				Action	To				
<input type="checkbox"/>	24285722@sipoperator.com		No	Forward	mark@sip.ingate.com	-	-		<input type="checkbox"/>
<input type="checkbox"/>	24285723@sipoperator.com		No	Forward	arthur@sip.ingate.com	-	-		<input type="checkbox"/>
<input type="checkbox"/>	24285724@sipoperator.com		No	Forward	harry@sip.ingate.com	-	-		<input type="checkbox"/>
<input type="checkbox"/>	24285725@sipoperator.com		No	Forward	helen@sip.ingate.com	-	-		<input type="checkbox"/>

Now, when someone calls 34382753, the call will be routed from the SIP operator to the unit and finally to harry@sip.ingate.com.

Note that you can only use the **User Routing** table for incoming call forwarding. The **Static Registrations** should not be used when XF or XF/Register accounts are involved.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration
Show Configuration
User Administration

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

Apply configuration

## 20.7. How To Use Your SIP Operator Account and Your IP-PBX Via the Ingate Unit

This is how to configure your unit to forward requests between your SIP operator and your local IP-PBX.

The configuration varies slightly depending on if the operator uses accounts or IP addresses for the authentication.

Instead of configuring this manually, you can use the Ingate Startup Tool, which can be found at [https://www.ingate.com/Startup\\_Tool\\_TG.php](https://www.ingate.com/Startup_Tool_TG.php).

## 20.7.1. Outgoing Calls

### Authentication by Accounts a.k.a SIP Trunk via SIP accounts

Enter your SIP operator account on the **Local Registrar** page. You enter the username and password from the operator, and select the XF/Register account type. This account type will make the unit register at the SIP operator with the credentials you enter.

Some operators don't require registration. In this case, select the XF account type instead.

You can select any network in the Register from field, as it is not used for these account types.

SIP Accounts <small>(Help)</small>							
Edit Row	Username	Domain	Authentication Name	Display Name	Password	Account Type	Delete Row
<input type="checkbox"/>	24285722	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>
<input type="checkbox"/>	24285723	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>
<input type="checkbox"/>	24285724	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>
<input type="checkbox"/>	24285725	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>

For outgoing calls, you have to define when your SIP operator account should be used. Usually, you use this type of account to call to the PSTN network ("ordinary telephones").

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.

Use Dial Plan <small>(Help)</small>	Emergency Number <small>(Help)</small>
<input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<input type="text" value="911"/>

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this case, we want to match on calls coming from the IP-PBX. This will ensure that only users who have been authorized by the PBX to use the SIP trunk will be able to make outgoing calls.

Matching From Header (Help)							
Edit Row	Name	Use This ...			... Or This		Delete Row
		Username	Domain	Reg Expr	Transport	Network	
<input type="checkbox"/>	IP-PBX	*	*		Any	IP-PBX	<input type="checkbox"/>

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like helen@sip.ingate.com should not be routed via the SIP operator, but be handled by the unit itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.

Matching Request-URI (Help)								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	External numbers			0..9	4	*local		<input type="checkbox"/>
<input type="checkbox"/>	International numbers	+		0..9	4	*local		<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

The calls can also be forwarded to your SIP operator using the operator's IP address in the **Replacement URI** field.

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...		... Or This			Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ SIP Operator	1	24285722@sipoperator.com			-		<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table. Make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.

Dial Plan <a href="#">(Help)</a>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	From Helen	International numbers	Forward	Helen PSTN	00		-	24/7	Change prefix for international calls.	<input type="checkbox"/>
<input type="checkbox"/>	2	From Helen	External numbers	Forward	Helen PSTN			-	24/7	External calls sent to operator.	<input type="checkbox"/>
<input type="checkbox"/>	3	From Arthur	International numbers	Forward	Arthur PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	4	From Arthur	External numbers	Forward	Arthur PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	5	From Harry	International numbers	Forward	Harry PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	6	From Harry	External numbers	Forward	Harry PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	7	From Mark	International numbers	Forward	Mark PSTN			-	24/7		<input type="checkbox"/>
<input type="checkbox"/>	8	From Mark	External numbers	Forward	Mark PSTN			-	24/7		<input type="checkbox"/>

Now, when a local user calls an external phone number, the unit will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

### Authentication by IP Addresses a.k.a SIP Trunk via IP address

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.

Use Dial Plan <a href="#">(Help)</a>	Emergency Number <a href="#">(Help)</a>
<input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<input type="text" value="911"/>

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

Matching From Header <a href="#">(Help)</a>							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	Ingate	*	ingate.com		Any	-	<input type="checkbox"/>
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

Add new rows  rows.

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your SIP operator, which is call destinations where the usernames consist of numbers only, as these most likely are intended to go to the PSTN network. Call destinations that look like helen@sip.ingate.com should not be routed via the SIP operator, but be handled by the unit itself.

You can let users call international numbers with a + sign instead of the international prefix. For this, define the + sign as a **Prefix**, which means that it will be stripped before the call is forwarded.

The **Min. Tail** is set to 4 here, to open for the possibility of three-digit local extensions, which should not be handled by the **Dial Plan**.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	External numbers			0..9	4	*local		<input type="checkbox"/>
<input type="checkbox"/>	International numbers	+		0..9	4	*local		<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

The calls can also be forwarded to your SIP operator using the operator's IP address in the **Replacement URI** field.

Forward To <a href="#">(Help)</a>								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ SIP Operator	1	-	202.202.202.202		-		<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table. Make one line for international calls and one for other calls, because we need to add the international prefix for international calls only.

Dial Plan <a href="#">(Help)</a>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	IP-PBX	International numbers	Forward	SIP Operator	00		-	24/7	Change prefix for international calls.	<input type="checkbox"/>
<input type="checkbox"/>	2	IP-PBX	External numbers	Forward	SIP Operator			-	24/7	External calls sent to operator.	<input type="checkbox"/>

Now, when a local user calls an external phone number, the unit will route this call to your SIP operator and rewrite the signaling to use your SIP operator account.

## 20.7.2. Incoming Calls

All incoming calls from the operator should be forwarded to the PBX. This is done on the Dial Plan page.

On the **Dial Plan** page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.

<b>Use Dial Plan <a href="#">(Help)</a></b> <input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<b>Emergency Number <a href="#">(Help)</a></b> <input type="text" value="911"/>
---------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

In the **Matching From Header** table, you define from which network the calls can come. You can

also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this case, we only need to define the operator by its sending network.

Matching From Header <a href="#">(Help)</a>							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	SIP Operator	*	*		Any	SIP Operator	<input type="checkbox"/>

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define the calls that should be routed to your PBX, which is call destinations where the usernames consist of numbers only. For extra matching, enter the outside IP address of the unit, which the operator will be using.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	Incoming calls			0..9	4	193.12.253.115		<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to your SIP operator account that was defined before. You select the account under **Account**.

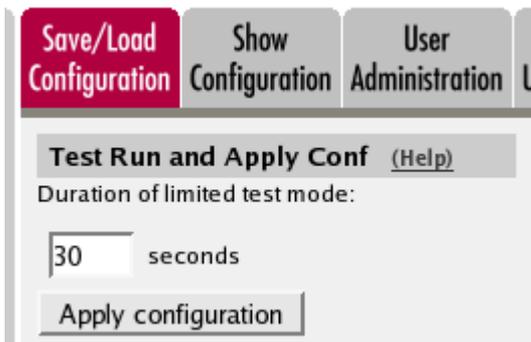
Enter the IP address of the IP-PBX in the **Replacement URI** field. This will make the unit replace the domain part in the incoming call with this IP address. The username part of the URI will be kept.

Forward To <a href="#">(Help)</a>								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ PBX	1	-	10.47.2.77		-		<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table. Select the operator and the Request-URI, and forward to the PBX.

Dial Plan <a href="#">(Help)</a>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	SIP Operator	Incoming calls	Forward	PBX			-	24/7		<input type="checkbox"/>

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



## 20.8. How To Use Multiple SIP Operators or IP-PBXs Via the Ingate Unit

This is how to configure your unit to forward requests between your SIP operator and your local IP-PBX.

The configuration varies slightly depending on if the operator uses accounts or IP addresses for the authentication.

This description is targeted for multiple operators or PBXs where the unit selects destination based on the called number and the caller.

### 20.8.1. Multiple Operators (Least Cost Routing)

If any of the SIP operators use accounts, enter that on the **Local Registrar** page. You enter the username and password from the operator, and select the XF/Register account type. This account type will make the unit register at the SIP operator with the credentials you enter.

Some operators don't require registration. In this case, select the XF account type instead.

You can select any network in the Register from field, as it is not used for these account types.

SIP Accounts <a href="#">(Help)</a>							
Edit Row	Username	Domain	Authentication Name	Display Name	Password	Account Type	Delete Row
<input type="checkbox"/>	24285722	sipoperator.com	123456789			XF/Register	<input type="checkbox"/>

On the Dial Plan page, you define what type of calls should be redirected to your SIP operator. First, turn the Dial Plan on.

Use Dial Plan <a href="#">(Help)</a>	Emergency Number <a href="#">(Help)</a>
<input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<input type="text" value="911"/>

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this office, there is a group of phones that always put a "+" first in the phone number when dialing a non-US number. We need to match on these to handle them specially.

Matching From Header (Help)							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	+ phones	*	*		Any	+ phones	<input type="checkbox"/>
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to sort out calls that should be routed to the different operators. You might have a UK operator and a US operator, and thus you want to be able to recognize these calls.

The basic way of recognizing calls is to check the country code, which is the first part of the phone number. In the table, there are three rows for matching UK calls. The two "UK numbers 00" rows give the same result, as does the two "US numbers" rows. The 10.47.2.243 IP address is that of the unit itself.

The ".\*" expression in the **Reg Expr** fields match 0 or more characters of any kind. The parantheses show how much of the incoming Request-URI we want to keep when forwarding the request.

For more information about regular expressions see [Regular Expressions](#).

Matching Request-URI (Help)								
Edit Row	Name	Use This ...				... Or This	Delete Row	
		Prefix	Head	Tail	Min. Tail	Domain		Reg Expr
<input type="checkbox"/>	UK numbers +	+	44	0..9	8	10.47.2.243	<input type="checkbox"/>	
<input type="checkbox"/>	UK numbers 00		0044	0..9, +, -, #, *		10.47.2.243	<input type="checkbox"/>	
<input type="checkbox"/>	UK numbers 00 regexp			-			sip:(0044.*)@10.47.2.243	<input type="checkbox"/>
<input type="checkbox"/>	US numbers		1	0..9	10	10.47.2.243	<input type="checkbox"/>	
<input type="checkbox"/>	US numbers regexp			-			sip:(1.*)@10.47.2.243	<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, define your two SIP operators. One may use accounts and the other IP addresses for authentication.

The two "UK Operator" rows are nearly the same.

With the "UK Operator" row, the Request-URI in the incoming call will have the domain part replaced with what is entered in the **Replacement URI** field. The username part of the URI will be kept.

With the "UK Operator regexp" row, the unit will get whatever was in the first set of parantheses in the **Matching Request-URI** table, and use that as the username part. The domain part is "sipoperator.co.uk;b2bua". The ";b2bua" parameter makes the unit handle all REFER requests itself; instead of forwarding them. This can be useful as many operators do not support the REFER method, which is used for call transfers.

For more information about regular expressions see [Regular Expressions](#).

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ UK Operator	1	-	sipoperator.co.uk	-	-	-	<input type="checkbox"/>
<input type="checkbox"/>	+ UK Operator regexp	1	-	-	-	-	sip:11@sipoperator.co.uk;b2bua	<input type="checkbox"/>
<input type="checkbox"/>	+ US Operator	1	24285722@sipoperator.com	-	-	-	-	<input type="checkbox"/>

At last, you combine these definitions in the **Dial Plan** table.

For UK calls, the operator requires that the phone number begins with "00", which means that some calls can be forwarded directly (row 2), but for calls where the number starts with "+", this has to be replaced with "00" (row 3). This means the calls that originate from the "+ phones".

For US calls, use any of the defined US Request-URIs, and forward to the US operator.

Note that if you want to use a Reg Expr definition for **Forward To**, you also need to use a Reg Expr definition for the **Request-URI**.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	+ phones	UK numbers +	Forward	UK Operator	00		-	-	Change prefix for UK calls	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	UK numbers 00 regexp	Forward	UK Operator regexp			-	-	UK calls	<input type="checkbox"/>
<input type="checkbox"/>	3	Office	US numbers	Forward	US Operator			-	-	US calls	<input type="checkbox"/>

## 20.8.2. Multiple PBXs

If you have multiple PBXs on the inside, you might want to send calls to different servers based on the sender or the called number.

On the Dial Plan page, you define which calls should be redirected to which PBX. First, turn the **Dial Plan** on.

Use Dial Plan (Help)	Emergency Number (Help)
<input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<input type="text" value="911"/>

In the **Matching From Header** table, you define from which network the calls can come. You can also select what the From header (that tells who is calling) should look like. This is used when matching requests in the **Dial Plan** table below. Name each definition properly, to make it easier to use further on.

In this case, we define one entry for each operator.

Matching From Header <a href="#">(Help)</a>								
Edit Row	Name	Use This ...			... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr				
<input type="checkbox"/>	UK operator	*	*			Any	UK server IPs	<input type="checkbox"/>
<input type="checkbox"/>	US operator	*	*			Any	US server IPs	<input type="checkbox"/>

In the **Matching Request-URI** table, you define callees. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to sort out which calls go to which PBX.

Assuming that each PBX manage a phone number range where the leading digits are different, it is easy to make matching definitions.

As the UK operator will send phone numbers that start with a "1", we allow for that, but by putting the "1" in the **Prefix** column, it will be stripped from the phone number when the unit forwards the call.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain		
<input type="checkbox"/>	Phone range 1358	1	358	0..9		193.12.253.115		<input type="checkbox"/>
<input type="checkbox"/>	Phone range 177	1	77	0..9		193.12.253.115		<input type="checkbox"/>
<input type="checkbox"/>	Phone range 358		358	0..9		193.12.253.115		<input type="checkbox"/>
<input type="checkbox"/>	Phone range 77		77	0..9		193.12.253.115		<input type="checkbox"/>

The same matching definitions can be made with regular expressions. Here, each number range only needs one definition, as the "?" sign marks that the previous character can appear 0 or 1 times. The part of the number that we want to forward should be within parantheses.

For more information about regular expressions see [Regular Expressions](#).

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain		
<input type="checkbox"/>	Phone range 358			-			sip:1?(358.*)@193.12.253.115	<input type="checkbox"/>
<input type="checkbox"/>	Phone range 77			-			sip:1?(77.*)@193.12.253.115	<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, define your two PBXs, simply by entering their respective IP addresses in the **Replacement URI** field.

Forward To <a href="#">(Help)</a>								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ PBX 358	1	-	10.47.2.58		-		<input type="checkbox"/>
<input type="checkbox"/>	+ PBX 77	1	-	10.47.2.77		-		<input type="checkbox"/>

The same forwarding definitions can be made with regular expressions. The "\$1" expression collects the number that matched the expression inside the parantheses in the **Matching Request-URI** table.

For more information about regular expressions see [Regular Expressions](#).

Forward To <a href="#">(Help)</a>								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ PBX 358	1	-			-	sip:\$1@10.47.2.58	<input type="checkbox"/>
<input type="checkbox"/>	+ PBX 77	1	-			-	sip:\$1@10.47.2.77	<input type="checkbox"/>

At last, you combine these definitions in the Dial Plan table.

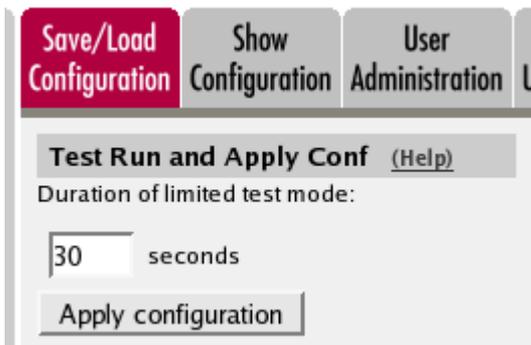
Select the operator, range, and then select to which PBX to send this call.

Dial Plan <a href="#">(Help)</a>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	UK operator	Phone range 1358	Forward	PBX 358			-	-		<input type="checkbox"/>
<input type="checkbox"/>	2	US operator	Phone range 358	Forward	PBX 358			-	-		<input type="checkbox"/>
<input type="checkbox"/>	3	UK operator	Phone range 177	Forward	PBX 77			-	-		<input type="checkbox"/>
<input type="checkbox"/>	4	US operator	Phone range 77	Forward	PBX 77			-	-		<input type="checkbox"/>

If regular expressions were used, you only need one line per PBX. As the expressions were designed to match calls from both operators, you don't need to select an operator here.

Dial Plan <a href="#">(Help)</a>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	US operator	Phone range 358	Forward	PBX 358			-	-		<input type="checkbox"/>
<input type="checkbox"/>	2	US operator	Phone range 77	Forward	PBX 77			-	-		<input type="checkbox"/>

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



### 20.8.3. Successive Failover with multiple Operators or PBXs

If you wish to try multiple destinations in a sequential failover manner as part of a single call attempt, click on the "+" symbol in the Forward-To rule, and add the destinations in order of precedence under the same rule.

Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	
+ Multi-destination	1	-	abc.com		-		<input type="checkbox"/>
	2	-	def.com		-		<input type="checkbox"/>
	3	-	ghi.com		-		<input type="checkbox"/>
	4	abc@xyz.com			-		<input type="checkbox"/>

When this Forward-To rule is invoked, each destination is tried successively until all rules are exhausted. Cases where processing will stop are when previous destinations return 5xx or 6xx SIP error responses and successive destinations will not be tried, since they might also produce similar errors.

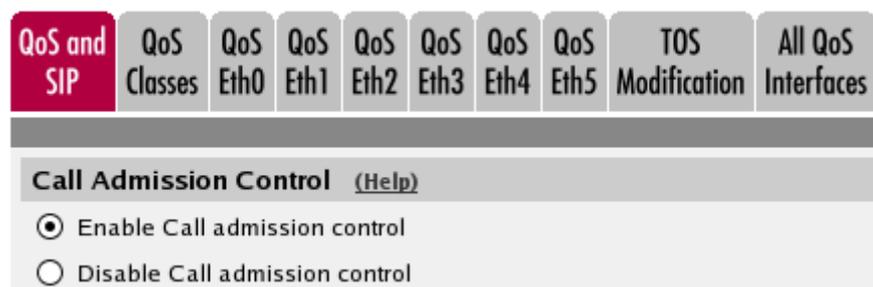
Cases where you may wish to try this include

- routing single call attempts to different providers
- routing inbound calls to multiple PBXs during busy periods

## 20.9. How To Use Ingate Call Admission Control

This is how to configure your unit to keep track of SIP calls through it and to reject new calls when there is not enough bandwidth for the new media.

On the **QoS and SIP** page, you turn the Call admission control on.



For each interface where Call admission control should be used, enter bandwidth limits for media

streams.

Bandwidths For SIP Media <a href="#">(Help)</a>				
Interface	Outgoing (kbit/s)		Incoming (kbit/s)	
	Allowed for Media (kbit/s)	Allowed for Emergency (kbit/s)	Allowed for Media (kbit/s)	Allowed for Emergency (kbit/s)
Internal (eth0)	1000		1000	
External (eth1)	600	200	700	
External2 (eth2)				
DHCP clients (eth3)	1500		1500	
SIP-1 (eth4)				
SIP-2 (eth5)				

For the unit to know when to reject calls, it needs to know how much bandwidth an audio or video stream will consume. The bandwidth largely depends on which codecs are used.

Enter bandwidths used for the various codecs. There is also a generic bandwidth for each codec type, which is used by the unit when a specific codec can't be found in the table.

Codec Bandwidths <a href="#">(Help)</a>					
Edit Row	Type	Codec Name	Bandwidth (kbit/s)	Allowed	Delete Row
<input type="checkbox"/>	audio	*	32	Yes	<input type="checkbox"/>
<input type="checkbox"/>	video	*	150	No	<input type="checkbox"/>

Add new rows  rows.

When a new call request is received by the unit, it calculates the bandwidth still free and which media streams the new call asks for. If there is enough bandwidth left for all media streams, the call is allowed. If there is not bandwidth enough, the call will be denied. The response 486 (Busy Here) will be sent to the call requestor.

The settings hitherto explained will ensure that SIP media is allowed a certain bandwidth, and also limit it to that bandwidth. If you want to control SIP signaling too, more settings are needed.

First, select to control traffic through prioritization (different types of traffic are assigned different priorities), or bandwidth limitation (different types of traffic are assigned bandwidth limits).

In this example, traffic prioritization is used.

QoS and SIP **QoS Classes** QoS Eth0 QoS Eth1 QoS Eth2 QoS Eth3 TOS Modification All QoS Interfaces

---

**Type of QoS** [\(Help\)](#)

- Priority queues
- Bandwidth allocation

Then, create **QoS Classes** for the types of traffic you want to prioritize. There is no need to create a class for SIP media; as soon as priorities are made for other traffic, the unit will automatically give

SIP media traffic the highest priority.

QoS Classes <a href="#">(Help)</a>											
Edit Row	No.	Class Name	Client	Server	Service	SIP	Packet Size (bytes)		TOS Octet		Delete Row
							Min	Max	TOS	DSCP	
<input type="checkbox"/>	1	TCP out	Office network	-	tcp	Non-SIP			-		<input type="checkbox"/>
<input type="checkbox"/>	2	UDP SIP signaling	-	-	udp	Signaling			-		<input type="checkbox"/>
<input type="checkbox"/>	3	TCP SIP signaling	-	-	tcp	Signaling			-		<input type="checkbox"/>

For every interface where QoS should be used, you need to define how much bandwidth can be used for different types of traffic. You do that on the **QoS Interfaces** pages.

As prioritization is used here, there is a setting called **Loose Priority**. With this setting, you control if a higher priority traffic can use the entire bandwidth, or if some lower priority traffic should be allowed even if there is high priority traffic enough to fill the bandwidth.

Here, we select to allow 5 % of lower priority traffic.

QoS and SIP
QoS Classes
QoS Eth0
QoS Eth1
QoS Eth2
QoS Eth3
TOS Modification
All QoS Interfaces

**Loose Priority (global setting)** [\(Help\)](#)

Save  % for lower priority traffic

Turn **Egress QoS** on and enter a **Total bandwidth** for the interface. Due to the configuration previously made on the **QoS and SIP** page, some bandwidth is already reserved for SIP media.

**General** [\(Help\)](#)

Outgoing QoS:  Active  Inactive

**Bandwidths** [\(Help\)](#)

Total bandwidth limit:  kbit/s  
 Reserved for SIP media: 900 kbit/s  
 Available bandwidth: 1100 kbit/s

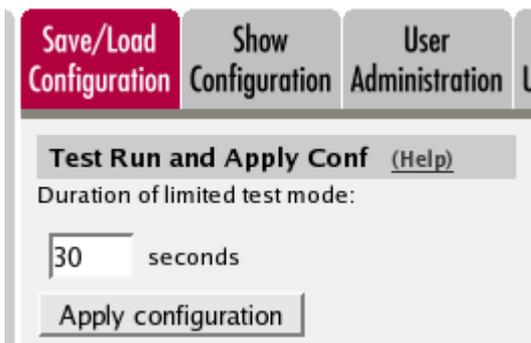
Assign priorities for the traffic classes you created. We want SIP signaling to have a high priority.

Classification <a href="#">(Help)</a>			
Edit	Class	Priority	Delete
<input type="checkbox"/>	TCP out	1 (highest)	<input type="checkbox"/>
<input type="checkbox"/>	UDP SIP signaling	1 (highest)	<input type="checkbox"/>
<input type="checkbox"/>	TCP SIP signaling	2	<input type="checkbox"/>

You also need to assign a priority for traffic that is not defined in the **Classification** table.



Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



## 20.10. How To Translate SIP Signaling Between UDP and TCP

This is how to configure your unit to translate SIP signaling between UDP and TCP.

This is useful when some SIP units can only send and receive SIP signaling over UDP, and others can only send and receive over TCP.

The simplest case is when the unit should only translate SIP traffic between two specific servers.

The settings are slightly different depending on how the sending server addresses the SIP messages when sending to the unit, especially what the Request-URI looks like. The two main cases are that the Request-URI domain is either the final receiving IP address, or the unit IP address. This is how to configure for these two cases.

### 20.10.1. The Request-URI Contains the Final Receiving IP Address

#### Networks and Computers

Start on the **Networks and Computers** page and define one network for each of the involved SIP servers.

Networks and Computers								
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ TCP server	-	192.168.0.28	192.168.0.28			Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ UDP server	-	192.168.0.25	192.168.0.25			Internal (eth0 untagged)	<input type="checkbox"/>

## Dial Plan

Then go to the **Dial Plan** page.

First, switch the Dial Plan on.

<b>Use Dial Plan</b> <a href="#">(Help)</a> <input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<b>Emergency Number</b> <a href="#">(Help)</a> <input type="text" value="911"/>
---------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

Add two rows to the **Matching From Header** table. One of the rows should match traffic coming from the UDP server, and the other row matches traffic coming from the TCP server.

Matching From Header <a href="#">(Help)</a>							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	TCP server	*	*		TCP or TLS	TCP server	<input type="checkbox"/>
<input type="checkbox"/>	UDP server	*	*		UDP	UDP server	<input type="checkbox"/>

Add one row in the **Matching Request-URI** table. This row should match all incoming requests to this unit. We want the Request-URI to be untouched when forwarding it, as the ultimate receiver IP address is already there. This is best achieved by using a regular expression.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	All			-			sip:(.*)@(.*)	<input type="checkbox"/>

After that, add two rows to the **Forward To** table. One row makes the traffic using that row to be sent out over UDP, and the other sends traffic over TCP. The Request-URI is unchanged (the \$1 and \$2 expressions refer back to the first and second pairs of parantheses in the **Matching Request-URI** table), including the IP address of the other server.

Forward To (Help)										
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This			Delete Row
				Account	Replacement Domain	Port	Transport	Reg Expr		
<input type="checkbox"/>	+ TCP server	1	-				-	sip:\$1@\$2;transport=tcp		<input type="checkbox"/>
<input type="checkbox"/>	+ UDP server	1	-				-	sip:\$1@\$2;transport=udp		<input type="checkbox"/>

These lines are combined in the **Dial Plan** table. Traffic from the UDP server is forwarded to the TCP server, and vice versa.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	TCP server	All	Forward	UDP server			-	-		<input type="checkbox"/>
<input type="checkbox"/>	2	UDP server	All	Forward	TCP server			-	-		<input type="checkbox"/>

### Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

## 20.10.2. The Request-URI Contains the Unit's IP Address

### Networks and Computers

Start on the **Networks and Computers** page and define one network for each of the involved SIP servers.

Networks and Computers								
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ TCP server	-	192.168.0.28	192.168.0.28			Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ UDP server	-	192.168.0.25	192.168.0.25			Internal (eth0 untagged)	<input type="checkbox"/>

## Dial Plan

Then go to the **Dial Plan** page.

First, switch the Dial Plan on.

<b>Use Dial Plan</b> <a href="#">(Help)</a> <input checked="" type="radio"/> On <input type="radio"/> Off <input type="radio"/> Fallback	<b>Emergency Number</b> <a href="#">(Help)</a> <input type="text" value="911"/>
---------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

Add two rows to the **Matching From Header** table. One of the rows should match traffic coming from the UDP server, and the other row matches traffic coming from the TCP server.

Matching From Header <a href="#">(Help)</a>							
Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	TCP server	*	*		TCP or TLS	TCP server	<input type="checkbox"/>
<input type="checkbox"/>	UDP server	*	*		UDP	UDP server	<input type="checkbox"/>

Add one row in the **Matching Request-URI** table. This row should match all incoming requests. We want to replace the domain part of the Request-URI when forwarding it, as it now contains unit's IP address. The most convenient way of doing this is to select "any character" and enter the unit's IP address as the Domain.

Matching Request-URI <a href="#">(Help)</a>								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	All			any character		192.168.0.22		<input type="checkbox"/>

After that, add two rows to the **Forward To** table. One row makes the traffic using that row to be sent out over UDP, and the other sends traffic over TCP. The domain part is replaced by entering the target IP address as the Replacement URI.

Forward To <a href="#">(Help)</a>								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ TCP server	1	-	192.168.0.28		TCP		<input type="checkbox"/>
<input type="checkbox"/>	+ UDP server	1	-	192.168.0.25		UDP		<input type="checkbox"/>

These lines are combined in the **Dial Plan** table. Traffic from the UDP server is forwarded to the TCP server, and vice versa.

Dial Plan <a href="#">(Help)</a>											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	TCP server	All	Forward	UDP server			-	-		<input type="checkbox"/>
<input type="checkbox"/>	2	UDP server	All	Forward	TCP server			-	-		<input type="checkbox"/>

### Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration
Show Configuration
User Administration

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** [\(Help\)](#)

The permanent configuration might be affected by loading a CLI file.

Local file:

## 20.11. How To Use RADIUS Accounting

This is how to configure your unit to use RADIUS Accounting for calls to or from local users.

If you are only interested in accounting for calls to other domains, you only have to turn the RADIUS Accounting on.

If you want to bill for local calls too, you will have to force the users to go via the unit even when they are both on the same side. For this, the unit will have to act as a back-to-back user agent (B2BUA) for all calls.

First, define the RADIUS server to receive accounting ticks. This is done on the **RADIUS** page. If the RADIUS server should only be used for accounting, you can enter any port number in the table. The unit will use port 1813 for accounting.

If you use the unit as the SIP registrar, and the RADIUS server should be used for SIP authentication as well, you need to enter the port number on which the RADIUS server listens for authentication requests (usually ports 1812 or 1645).

**RADIUS Servers** (Help)

Edit Row	RADIUS server		Port	Secret	Delete Row
	DNS name or IP address	IP address			
<input checked="" type="checkbox"/>	193.180.23.77	193.180.23.77	1812	Change Secret	<input type="checkbox"/>

Add new rows  rows.

**Contact IP Address** (Help)  
Contact RADIUS servers from:

**Identifier** (Help)  
Use NAS-IP-Address:  Yes  No  
NAS-Identifier:

If the unit should act as the registrar, define a local SIP domain. This can be any domain name you like, as long as it isn't an existing domain somewhere else. A good choice is to use your company www domain, but replace the "www" with "sip", like sip.ingate.com. The same domain can also be used in pure SIP-to-SIP calls.

This domain should be entered on the **Local Registrar** page under **SIP Traffic**.

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input checked="" type="checkbox"/>	ingate.com	<input type="checkbox"/>

Go to the **Authentication and Accounting** page and turn authentication on. Also enter your SIP domain as the Realm.

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

If the unit should be used as registrar, you select to use the RADIUS user database for SIP users and also select which network the SIP users can register from.

On the Dial Plan page, you define how calls should be routed through the unit. First, turn the Dial Plan on.

In the **Matching Request-URI** table, you define call destinations. This is used when matching requests in the **Dial Plan** table below.

In this case, you want to define a **Reg Exp** (regular expression) which matches all Request-URIs. Enter "(.+)@(.+)" in the Reg Exp field.

Matching Request-URI (Help)								
Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	Any			-			(.+)@(.+)	<input type="checkbox"/>

In the **Forward To** table, you define where calls should be forwarded. This is used in the **Dial Plan** table below.

In this case, the calls should be forwarded to their original destination, but the unit should forward them as a B2BUA. Enter "\$0;b2bua" in the Reg Exp field. This will reuse the incoming Request-URI, but make the unit act as a B2BUA instead of a proxy.

Forward To (Help)									
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row	
			Account	Replacement Domain	Port	Transport	Reg Expr		
<input type="checkbox"/>	+ Same but b2bua	1	-			-	\$0;b2bua	<input type="checkbox"/>	

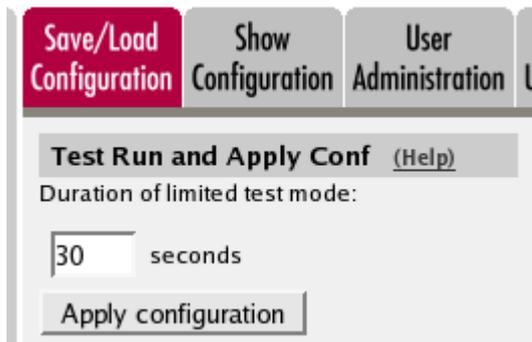
At last, you combine these definitions in the **Dial Plan** table. Make a new row in the table and select the definitions from the tables above.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	-	Any	Forward	Same but b2bua			-	-	Use the built-in B2BUA	<input type="checkbox"/>

Now, when a SIP user calls another SIP user, the unit will step in and always stay in the path for the call. Both SIP clients will signal to the unit only, and the unit will forward signaling between them.

Media will still go directly between the clients.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



## 20.12. How To Configure TLS

Prerequisites:

- You have access to a CA that will sign your certificate requests
- You have each signing-CAs public certificate
- You understand the GNU X.509 trust model

This is how to configure your unit to encrypt SIP media or force the SIP clients to use signaling encryption with TLS.

The settings for SIP signaling encryption are made on the **Signaling Encryption** page under SIP Services. You also need a certificate, which is created on the **Certificates** page under **Basic Configuration**.

### 20.12.1. Certificates

Create certificates on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new** and enter the certificate information.

If you want to make TLS connections on the LAN and the Internet, you will need one certificate for each interface. Note: set the certificates CN= field to the IP/DNS name of the interface.

Private Certificates (Help)						
Edit Row	Name	Certificate	Information			Delete Row
<input type="checkbox"/>	inside				Subject: /CN=10.47.3.243 Issuer: /CN=10.47.3.243 MD5 Fingerprint: 96:3F:8A:4A:90:A4:7C:C4:4D:E2:E9:03:51:AD:FA:37 Valid to: 2010-07-21 14:24:58	<input type="checkbox"/>
<input type="checkbox"/>	main cert				Subject: /CN=sip.ingate.com Issuer: /CN=sip.ingate.com MD5 Fingerprint: 5E:5A:C8:DC:A0:DC:42:FE:C0:BB:FA:B5:5C:60:5E:D0 Valid to: 2010-07-01 14:25:20	<input type="checkbox"/>

If the unit should use TLS to connect to another SIP server, you must upload the CA certificate for that server here. You don't need CA certificates for SIP clients.

Create a new row in the **CA Certificates** table and upload the CA certificate.

CA Certificates (Help)						
Edit Row	Name	CA Certificate	CA CRL	Information		Delete Row
<input type="checkbox"/>	SIP server CA			Subject: /CN=ca.example.com Issuer: /CN=ca.example.com MD5 Fingerprint: 37:8D:16:82:CD:8C:D4:D9:4F:64:7C:75:9B:78:D0:DF Valid to: 2010-07-01 14:17:46	<input type="checkbox"/>	

## 20.12.2. Signaling Encryption

Go to the **Signaling Encryption** page to make TLS settings.

First, select the allowed SIP transports. If you want to allow signaling via TCP or UDP e.g. on the "inside", select "Any".

To initiate TLS signaling, set transport to TLS in the Dial-Plan or DNS override table if the DNS record for a domain has no TLS entry.

If "TLS" is selected, no connections via UDP or TCP will be initiated or accepted, on **any** interface. In this case, you must make sure that all clients and servers that the unit should communicate with can be reached via TLS.

Basic
Signaling Encryption
Media Encryption
Interoperability
Sessions and Media
Remote SIP Connectivity
VoIP Survival
VoIP Survival Status

**SIP Transport (Help)**

Enable signaling encryption

Disable signaling encryption

If the unit should communicate with other SIP servers, you have already imported their CA certificates. In the **TLS CA Certificates** table, you select these certificates to allow them to be used in TLS connections.

TLS CA Certificates <a href="#">(Help)</a>		
Edit Row	CA	Delete Row
<input type="checkbox"/>	SIP server CA	<input type="checkbox"/>

In the **TLS Connections On Different IP Addresses** table, create one row for the inside and one for the outside IP address. For each IP address, select which certificate should be used for authentication when a TLS connection is made to that IP address, and if the unit should require the client to send its own certificate for authentication, too.

You also select which TLS methods should be accepted for each IP address.

Note that the unit will not accept TLS connections to an IP address which is not listed in this table!

TLS Connections On Different IP Addresses <a href="#">(Help)</a>					
IP Address	Own Certificate	Use CN FQDN	Require Client Cert	TLS	Delete Row
eth0 (10.48.28.61) ▼	MyCert ▼	Yes ▼	Yes ▼	TLsv1.x ▼	<input type="checkbox"/>

Add new rows  rows.

### 20.12.3. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration
Show Configuration
User Administration

---

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** [\(Help\)](#)

The permanent configuration might be affected by loading a CLI file.

Local file:

### 20.12.4. Settings in the Other Server

You need to upload the unit certificate to the other SIP server if the unit should be able to make connections to the server.

## 20.13. How To Use SIP Media Encryption

This is how to configure your unit to encrypt SIP media or force the SIP clients to use media encryption.

The settings for SIP media encryption are made on the **Media Encryption** page under **SIP Services**.

First, switch the media encryption on.

**Media Encryption** (Help)

Enable media encryption

Disable media encryption

Group the encryption algorithms that you want to use. There are predefined crypto suite groups, but you might need to define your own if you have special requirements.

**Crypto Suite Groups** (Help)

Edit Row	Name	Suite	Delete Row
<input type="checkbox"/>	+ All transcodable	Cleartext (no encryption)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>
<input type="checkbox"/>	+ Cleartext	Cleartext (no encryption)	<input type="checkbox"/>
<input type="checkbox"/>	+ SRTP encryption	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
<input type="checkbox"/>		SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>

Select for each interface or VLAN if media going in or out from that interface/VLAN should be encrypted, and which encryption algorithms to allow.

If the unit should terminate encrypted media streams coming in to one interface (and send it out unencrypted or encrypted with a different algorithm), you must allow transcoding for that interface.

**SIP Media Encryption Policy** (Help)

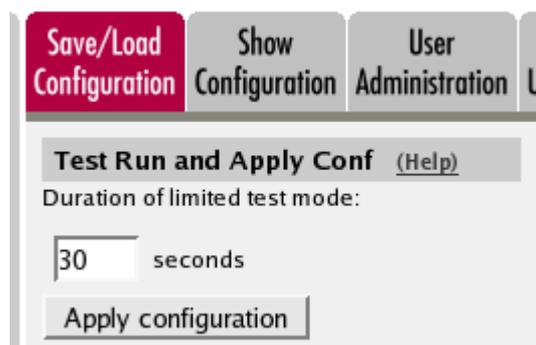
Edit Row	Media Via Interface/VLAN	Suite Requirements	Allow Transcoding	Delete Row
<input type="checkbox"/>	Internal (eth0 untagged)	-	No	<input type="checkbox"/>
<input type="checkbox"/>	External (eth1 untagged)	SRTP encryption	Yes	<input type="checkbox"/>

For interfaces (VLANs) not explicitly configured above, you need to select a default media encryption.



When SIP media encryption is used, the SIP signaling should also be encrypted (using TLS). If it isn't, the encryption keys will be sent unencrypted over the network.

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

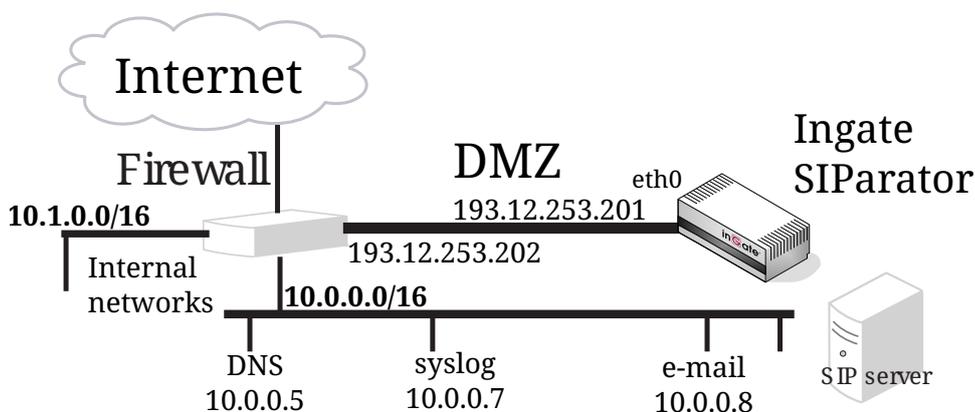


## 20.14. The DMZ SIParator Type

The DMZ SIParator Type requires that the unit is connected to the *firewall* on an interface separate from the Internet and internal network interfaces.

Note that the unit must have a public (non-NAT:ed) IP address.

In this example, the company has two internal networks, each one connected to a separate interface on the company *firewall*. One internal network (10.0.0.0/16) is used for office workstations and servers, and the other (10.1.0.0/16) is used for lab purposes. They also have a DMZ (193.12.253.200/29) where some public servers are located. The unit is connected to the DMZ interface.



If you have made any configuration on the unit, revert to the factory configuration and apply the configuration. After that, start the new unit configuration.

The first thing to do is to set the **SIParator Type** under **Basic Configuration**.

Basic Configuration | Access Control | RADIUS | SNMP | Dynamic DNS Update | Certificates | Advanced | **SIParator Type**

### Type of SIParator [\(Help\)](#)

The SIParator can be connected to your network in four different ways, depending on your needs.

SIParator type:

DMZ ▼

On the **Eth0** page under **Network**, the interface name and IP address are set.

Networks and Computers | Default Gateways | All Interfaces | VLAN | **Eth0** | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Topology

### General

Physical device: **eth0**

This interface is:  Active  Inactive

Interface name:

### Speed and Duplex

Automatic negotiation

100 Mbit/s, full duplex

100 Mbit/s, half duplex

10 Mbit/s, full duplex

10 Mbit/s, half duplex

### Directly Connected Networks [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	DMZ	Static	193.12.253.201	193.12.253.201	29	193.12.253.200	193.12.253.207		-	<input type="checkbox"/>

Define groups of computers on the **Networks and Computers** page.

All computers which are on the same network (meaning that they can reach each other without going through the *firewall* to which the unit is connected) should have a separate network group.

**Networks and Computers**

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	<input type="checkbox"/>
<input type="checkbox"/>		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Lab+Office	Laboratory					-	<input type="checkbox"/>
<input type="checkbox"/>		Office					-	<input type="checkbox"/>
<input type="checkbox"/>	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	<input type="checkbox"/>
<input type="checkbox"/>	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	<input type="checkbox"/>
<input type="checkbox"/>		-	10.1.0.17	10.1.0.17			-	<input type="checkbox"/>

Add new rows  groups with  rows per group.

Select the networks connected to the *firewall* on the **Topology** page. Select only the networks which are not reached via the *firewall's* default gateway.

Networks and Computers | Default Gateways | All Interfaces | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | **Topology**

**Surroundings** [\(Help\)](#)

If your SIParator type is not set to **DMZ**, the settings in this section will have no effect.

Edit Row	Network	Additional Negotiators	Delete Row
<input type="checkbox"/>	Office	-	<input type="checkbox"/>
<input type="checkbox"/>	DMZ	-	<input type="checkbox"/>
<input type="checkbox"/>	Laboratory	-	<input type="checkbox"/>

After that, set **Default gateway** on the **Default Gateways** page. The default gateway for the unit is the *firewall*.

Networks and Computers **Default Gateways** All Interfaces VLAN Eth0 Eth1 Eth2 Eth3 Eth4 Eth5 Interface Status PPPoE Topology

**Main Default Gateways** (Help)

Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
<input type="checkbox"/>	1	-	193.12.253.202	193.12.253.202	DMZ (eth0)	<input type="checkbox"/>

Add new rows  rows.

Enter a **DNS server** on the **Basic Configuration** page. This is needed to look up other SIP domains.

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="text" value="1"/>	-	<input type="text" value="172.16.0.3"/>	<input type="text" value="172.16.0.3"/>	<input type="checkbox"/>
<input type="text" value="2"/>	-	<input type="text" value="10.47.3.201"/>	<input type="text" value="10.47.3.201"/>	<input type="checkbox"/>
<input type="text" value="3"/>	Internet	<input type="text"/>	Internet	<input type="checkbox"/>

Add new rows  rows.

Go to the **Access Control** page and select the IP address the unit's web interface should have. Also enter the IP addresses of the computers allowed to configure the unit.

We select to configure via HTTP. Only a small group of workstations are allowed to configure the unit.

Basic Configuration **Access Control** RADIUS SNMP Dynamic DNS Update C

**Configuration Transport** (Help)

**Configuration via HTTP**  
 Direct your web browser to this address: Port:

**Configuration via HTTPS**  
 Direct your web browser to this address: Port:

Certificate to use:

**Configuration via SSH**  
 Connect your SSH client to this address: Port:

Configuration Computers <a href="#">(Help)</a>											
Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	10.0.1.32	10.0.1.32	28	10.0.1.32 - 10.0.1.47	-	No	Yes	Yes	Local	<input type="checkbox"/>
<input type="checkbox"/>	2	10.0.2.0	10.0.2.0	27	10.0.2.0 - 10.0.2.31	-	No	Yes	Yes	Local	<input type="checkbox"/>

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

**Basic** | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VoIP Survival | VoIP Survival Status

**SIP Module** [\(Help\)](#)

- Enable SIP module
- Disable SIP module

Here, you also set the port interval which should be used for media streams. This interval should be let through in the *firewall*.

**SIP Media Port Range** [\(Help\)](#)

Ports:  -

Go to the **Filtering** page. SIP requests from the internal networks should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

SIP Methods | **Filtering** | Local Registrar | Authentication and Accounting | SIP Accounts | Dial Plan | Routing | Time Classes | SIP Status | IDS/IPS | IDS/IPS Status

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

**Default Policy For SIP Requests**

- Process all
- Local only
- Reject all

Add new rows  rows.

Allow the content types which are allowed in SIP media streams. Note that the content types application/sdp, application/xpidf+xml and text/x-msmsgsinvite are always allowed, regardless of what is entered here.

Content Type Filter Rules <a href="#">(Help)</a>			
Edit Row	Content Type	Allowed	Delete Row
<input type="checkbox"/>	image/jpg	Yes	<input type="checkbox"/>
<input type="checkbox"/>	message/sipfrag	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/lpdf	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Yes	<input type="checkbox"/>

Add new rows  rows.

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain looks just like the ordinary Internet domain for the company.

Some IP telephones register on IP addresses (their own or that of the registrar) instead of domains. If you use this type of telephones, add the IP address of the registrar as a **Locally handled domain**.

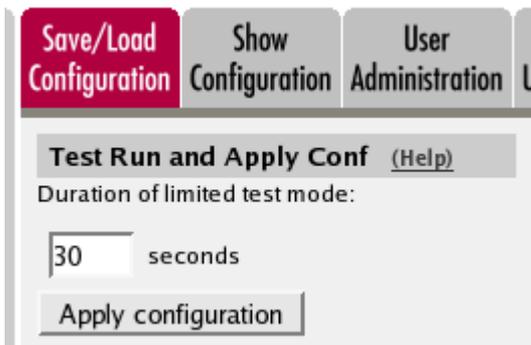
SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	Time Classes	SIP Status	IDS/IPS	IDS/IPS Status
<b>Local SIP Domains <a href="#">(Help)</a></b>										
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Domain	Delete Row								
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>								

Add new rows  rows.

To enable SIP clients to receive SIP requests, they must be allowed to register. Add one row for each domain, where all users in the domains are allowed to register. With this setting, you can allow users to register without authentication, or use authentication, but all users have the same password. Note that with the settings shown in the image, users who use the IP address of the unit as their SIP domain can only register from the Internal network.

Local SIP User Database <a href="#">(Help)</a>						
Edit row	Username	Domain	Authentication name	Password	Register from	Delete row
<input type="checkbox"/>	*	ingate.com			Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	*	193.12.253.201			Lab+Office	<input type="checkbox"/>

This is the configuration needed in the unit. Apply the configuration on the **Save/Load Configuration** page.



The *firewall* to which the unit is connected also requires additional configuration. Let through TCP and UDP traffic on port 5060 between Internet and the unit as well as between the unit and the internal networks. UDP traffic between Internet (all high ports) and the unit (the port interval for media streams) must also be let through. Make the corresponding changes for traffic between the internal networks and the unit. NAT between the unit and the internal networks must not be used.

The DNS server used must have a record for the SIP domain, which states that the unit handles the domain, or the SIP clients won't be able to use it.

### 20.14.1. The Firewall

The *firewall* to which the unit is connected should have the following configuration:

#### *SIP over UDP*

- Let through UDP traffic between the Internet (all high ports) and the unit (port 5060). You must allow traffic in both directions.
- Let through UDP traffic between the internal networks (all high ports) and the unit (port 5060). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the unit (the port interval for media streams which was set on the **Basic** page). You must allow traffic in both directions.
- Let through UDP traffic between the internal networks (all high ports) and the unit (the port interval for media streams which was set on the **Basic** page). You must allow traffic in both directions.
- Let through UDP traffic between the unit (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the unit to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the unit, you don't have to do this step.
- NAT between the unit and the Internet must not be used.
- NAT between the unit and the internal networks must not be used.

#### *SIP over TCP/TLS*

- Let through TCP traffic between the Internet (all high ports) and the unit (ports 1024-32767). You must allow traffic in both directions.
- Let through TCP traffic between the internal networks (all high ports) and the unit (ports 1024-32767). You must allow traffic in both directions.

- Let through UDP traffic between the Internet (all high ports) and the unit (the port interval for media streams which was set on the **Basic** page). You must allow traffic in both directions.
- Let through UDP traffic between the internal networks (all high ports) and the unit (the port interval for media streams which was set on the **Basic** page). You must allow traffic in both directions.
- Let through UDP traffic between the unit (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the unit to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the unit, you don't have to do this step.
- NAT between the unit and the Internet must not be used.
- NAT between the unit and the internal networks must not be used.

## 20.14.2. The SIP clients

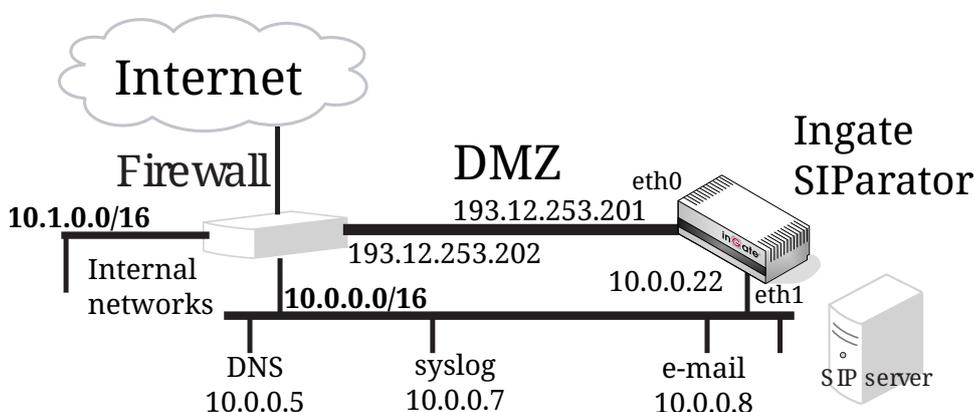
SIP clients will use the unit as their outgoing SIP proxy and as their registrar (if they can't be configured with the domain only). If you don't want to use the unit as the registrar, you should point the clients to the SIP registrar you want to use.

## 20.15. The DMZ/LAN SIParator Type

The DMZ/LAN SIParator Type is connected to the *firewall* with one interface and to an internal network with the other interface. The unit can only handle requests from this internal network and the Internet.

Note that the unit must have a public (non-NAT:ed) IP address.

In this example, the company has two internal networks, each one connected to a separate interface on the company *firewall*. One internal network (10.0.0.0/16) is used for office workstations and servers, and the other (10.1.0.0/16) is used for lab purposes. They also have a DMZ (193.12.253.200/29) where some public servers are located. The unit is connected to the DMZ interface and the office network interface. This means that no one on the lab network will be able to use the unit, since it can only manage one internal network.



The first thing to do is to set the **SIParator Type** under **Basic Configuration**.

Basic Configuration Access Control RADIUS SNMP Dynamic DNS Update Certificates Advanced **SIParator Type**

**Type of SIParator** [\(Help\)](#)

The SIParator can be connected to your network in four different ways, depending on your needs.

SIParator type:

DMZ/LAN ▾

On the **Eth0** page under **Network**, the interface name and IP address are set. Eth0 is connected to the DMZ interface of the *firewall*.

Networks and Computers Default Gateways All Interfaces VLAN **Eth0** Eth1 Eth2 Eth3 Eth4 Eth5 Interface Status PPPoE Topology

**General**

Physical device: **eth0**

This interface is:  Active  Inactive

Interface name:

**Speed and Duplex**

Automatic negotiation

100 Mbit/s, full duplex

100 Mbit/s, half duplex

10 Mbit/s, full duplex

10 Mbit/s, half duplex

**Directly Connected Networks** [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	DMZ	Static	193.12.253.201	193.12.253.201	29	193.12.253.200	193.12.253.207		-	<input type="checkbox"/>

On the **Eth1** page, the interface name and IP address are set. Eth1 is connected to the internal office network.

Networks and Computers Default Gateways All Interfaces VLAN Eth0 **Eth1** Eth2 Eth3 Eth4 Eth5 Interface Status PPPoE Topology

**General**

Physical device: **eth1**

This interface is:  Active  Inactive

Interface name:

**Speed and Duplex**

Automatic negotiation

100 Mbit/s, full duplex

100 Mbit/s, half duplex

10 Mbit/s, full duplex

10 Mbit/s, half duplex

Directly Connected Networks <a href="#">(Help)</a>										
Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Inside	Static	10.0.0.22	10.0.0.22	16	10.0.0.0	10.0.255.255		-	<input type="checkbox"/>

Define groups of computers on the **Networks and Computers** page.

Networks and Computers <a href="#">(Help)</a>										
Networks and Computers										
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row		
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address				
<input type="checkbox"/>	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	DMZ (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>		
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	DMZ (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	DMZ (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	DMZ (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	Internal (eth1 untagged)	<input type="checkbox"/>		

After that, set **Default gateway** on the **Default Gateways** page. The default gateway for the unit is the *firewall*.

Networks and Computers <a href="#">(Help)</a>										
Main Default Gateways <a href="#">(Help)</a>										
Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row				
<input type="checkbox"/>	1	-	193.12.253.202	193.12.253.202	DMZ (eth0)	<input type="checkbox"/>				
<input type="checkbox"/>	2	Outside		Outside	External (eth1)	<input type="checkbox"/>				

Add new rows  rows.

Enter a **DNS server** on the **Basic Configuration** page. This is needed to look up other SIP domains.

**DNS Servers** [\(Help\)](#)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

Go to the **Access Control** page and select the IP address the unit's web interface should have. Also enter the IP addresses of the computers allowed to configure the unit.

We select to configure via HTTP and select an IP address. Configuration traffic is only allowed via Eth1 (the inside interface).

Only a small group of workstations are allowed to configure the unit.

[Basic Configuration](#)
[Access Control](#)
[RADIUS](#)
[SNMP](#)
[Certificates](#)
[SIP Parator Type](#)

**Configuration Transport** [\(Help\)](#)

**Configuration via HTTP**  
 Direct the web browser to this address:

Port:

**Configuration via HTTPS**  
 Direct the web browser to this address:

Port:  Certificate to use:

**Configuration Allowed Via Interface** [\(Help\)](#)

Eth0	Eth1	Eth2	Eth3
<input type="radio"/> On	<input checked="" type="radio"/> On	<input type="radio"/> On	<input type="radio"/> On
<input checked="" type="radio"/> Off	<input type="radio"/> Off	<input checked="" type="radio"/> Off	<input checked="" type="radio"/> Off
Eth4	Eth5		
<input type="radio"/> On	<input type="radio"/> On		
<input checked="" type="radio"/> Off	<input checked="" type="radio"/> Off		

**Configuration Computers** [\(Help\)](#)

Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	10.0.1.32	10.0.1.32	28	10.0.1.32 - 10.0.1.47	-	No	Yes	Yes	Local	<input type="checkbox"/>
<input type="checkbox"/>	2	10.0.2.0	10.0.2.0	27	10.0.2.0 - 10.0.2.31	-	No	Yes	Yes	Local	<input type="checkbox"/>

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

Basic Signaling Encryption Media Encryption Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival VoIP Survival Status

**SIP Module** (Help)

Enable SIP module  
 Disable SIP module

Here, you also set the port interval which should be used for media streams. This interval should be let through in the *firewall*.

**SIP Media Port Range** (Help)

Ports:  -

Go to the **Filtering** page. SIP requests from the internal network should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**Proxy Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

Allow the content types which are allowed in SIP media streams. Note that the content types *application/sdp*, *application/xpidf+xml* and *text/x-msmsgsinvite* are always allowed, regardless of what is entered here.

**Content Type Filter Rules** (Help)

Edit Row	Content Type	Allowed	Delete Row
<input type="checkbox"/>	image/jpg	Yes	<input type="checkbox"/>
<input type="checkbox"/>	message/sipfrag	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/lpidf	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Yes	<input type="checkbox"/>

Add new rows  rows.

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain looks just like the ordinary Internet domain for the company.

Some IP telephones register on IP addresses (their own or that of the registrar) instead of domains. If you use this type of telephones, add the IP address of the registrar as a **Locally handled domain**.

SIP Methods Filtering **Local Registrar** Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Now you can enter users in the **Local SIP User Database** table. You can use the "\*" wildcard for any number of characters. However, you must enter all users on separate lines to give them individual passwords.

**Local SIP User Database** (Help)

Edit row	Username	Domain	Authentication name	Password	Register from	Delete row
<input type="checkbox"/>	charlie	ingate.com			Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	charlie	193.12.253.201			Office	<input type="checkbox"/>
<input type="checkbox"/>	molly	ingate.com			Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	molly	193.12.253.201			Office	<input type="checkbox"/>
<input type="checkbox"/>	brutus	ingate.com			Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	brutus	192.12.253.201			Office	<input type="checkbox"/>

Go to the **Authentication and Accounting** page. Here, authentication is activated. Select to make the authentication active and enter a **Realm**, which is a name which the unit uses to tell the clients which device is requiring authentication.

SIP Methods Filtering Local Registrar **Authentication and Accounting** SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

If you want the unit to authenticate users you must also decide what to authenticate for. Select the methods to allow and authenticate on the **SIP Methods** page.

Here, we require authentication for REGISTER to local domains, which means when a user tries to register on a domain handled by the unit. Authentication is also required for INVITE to other domain, which means that a user who wants to call someone on a domain not handled by the unit needs to provide a password.

**SIP Methods** Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Methods** [\(Help\)](#)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Local domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Other domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

This is the configuration needed in the unit. Apply the configuration on the **Save/Load Configuration** page.

**Save/Load Configuration** Show Configuration User Administration U

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

The *firewall* to which the unit is connected also requires additional configuration. Let through TCP and UDP traffic on port 5060 between Internet and the unit. UDP traffic between Internet (all high ports) and the unit (the port interval for media streams) must also be let through. The SIP clients on the internal office network should have 10.0.0.22 (the units's IP address on the network) as outgoing SIP proxy.

## 20.15.1. The Firewall

The *firewall* to which the unit is connected should have the following configuration:

### *SIP over UDP*

- Let through UDP traffic between the Internet (all high ports) and the unit (port 5060). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the unit (the port interval for media streams which was set on the **Basic** page). You must allow traffic in both directions.
- Let through UDP traffic between the unit (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the unit to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the unit, you don't have to do this step.
- NAT between the unit and the Internet must not be used.

### *SIP over TCP/TLS*

- Let through TCP traffic between the Internet (all high ports) and the unit (ports 1024-32767). You must allow traffic in both directions.
- Let through UDP traffic between the Internet (all high ports) and the unit (the port interval for media streams which was set on the **Basic** page). You must allow traffic in both directions.
- Let through UDP traffic between the unit (all high ports) and the Internet (port 53). You must allow traffic in both directions. This enables the unit to make DNS queries to DNS servers on the Internet. If the DNS server is located on the same network as the unit, you don't have to do this step.
- NAT between the unit and the Internet must not be used.

## 20.15.2. SIP clients

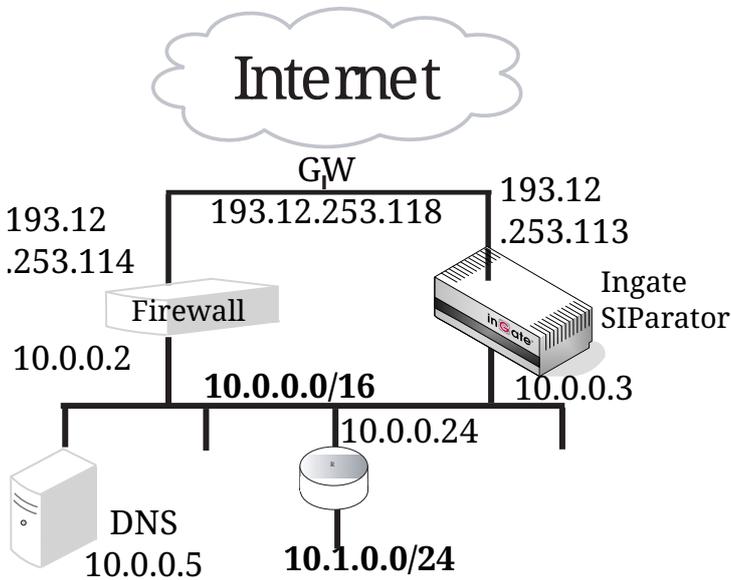
The SIP clients on the internal network should have the unit's IP address on that network as their outgoing SIP proxy and registrar.

## 20.15.3. Other

The DNS server used must have a record for the SIP domain, which states that the unit handles the domain, or many SIP clients won't be able to use it (if you don't use plain IP addresses as domains).

## 20.16. The Standalone SIParator Type

The Standalone SIParator Type is connected to the Internet with one interface and an internal network with the other interface. The unit can only handle SIP requests on and between these two networks. The traffic through the unit will not pass through the *firewall*.



The first thing to do is to set the **SIParator Type** under **Basic Configuration**.

Basic Configuration | Access Control | RADIUS | SNMP | Dynamic DNS Update | Certificates | Advanced | **SIParator Type**

**Type of SIParator** ([Help](#))

The SIParator can be connected to your network in four different ways, depending on your needs.

SIParator type:

Standalone ▾

On the **Eth0** page under **Network**, the interface name and IP address are set. Eth0 is connected to the internal network. There is a system administration network, 10.1.0.0/24, behind the router 10.0.0.24. Configuration is allowed via this interface.

Networks and Computers | Default Gateways | All Interfaces | VLAN | **Eth0** | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Topology

**General**

Physical device: **eth0**

This interface is:  Active  Inactive

Interface name:

**Speed and Duplex**

Automatic negotiation

100 Mbit/s, full duplex

100 Mbit/s, half duplex

10 Mbit/s, full duplex

10 Mbit/s, half duplex

**Directly Connected Networks** ([Help](#))

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Inside	Static	10.0.0.3	10.0.0.3	16	10.0.0.0	10.0.255.255		-	<input type="checkbox"/>

Static Routing <a href="#">(Help)</a>							
Edit Row	Routed Network			Router			Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
<input type="checkbox"/>	10.1.0.0	10.1.0.0	24	-	10.0.0.24	10.0.0.24	<input type="checkbox"/>

On the **Eth1** page, the interface name and IP address are set. Eth1 is connected to the Internet.

Networks and Computers	Default Gateways	All Interfaces	VLAN	Eth0	<b>Eth1</b>	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE	Topology
------------------------	------------------	----------------	------	------	-------------	------	------	------	------	------------------	-------	----------

<p><b>General</b></p> <p>Physical device: <b>eth1</b></p> <p>This interface is: <input checked="" type="radio"/> Active <input type="radio"/> Inactive</p> <p>Interface name: <input type="text" value="External"/></p>	<p><b>Speed and Duplex</b></p> <p><input checked="" type="radio"/> Automatic negotiation</p> <p><input type="radio"/> 100 Mbit/s, full duplex</p> <p><input type="radio"/> 100 Mbit/s, half duplex</p> <p><input type="radio"/> 10 Mbit/s, full duplex</p> <p><input type="radio"/> 10 Mbit/s, half duplex</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Directly Connected Networks <a href="#">(Help)</a>										
Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Outside	Static	193.12.253.113	193.12.253.113	29	193.12.253.112	193.12.253.119		-	<input type="checkbox"/>

Define groups of computers on the **Networks and Computers** page.

Networks and Computers	Default Gateways	All Interfaces	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE	Topology
------------------------	------------------	----------------	------	------	------	------	------	------	------	------------------	-------	----------

**Networks and Computers**

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internal network	-	10.0.0.0	10.0.0.0	10.1.255.255	10.1.255.255	Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>

After that, set **Default gateway** on the **Default Gateways** page. The default gateway for the unit is the same as for the *firewall*; 193.12.253.118.

Networks and Computers **Default Gateways** All Interfaces VLAN Eth0 Eth1 Eth2 Eth3 Eth4 Eth5 Interface Status PPPoE Topology

**Main Default Gateways** (Help)

Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
<input type="checkbox"/>		-	193.12.253.118	193.12.253.118	External (eth1)	<input type="checkbox"/>

Enter a **DNS server** on the **Basic Configuration** page. This is needed to look up other SIP domains.

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

Go to the **Access Control** page and select the IP address the unit's web interface should have. Also enter the IP addresses of the computers allowed to configure the unit.

We select to configure via HTTP and select the inside IP address. Configuration traffic is only allowed via Eth0 (the inside interface).

Only workstations on the system administration network are allowed to configure the unit.

Basic Configuration **Access Control** RADIUS SNMP Certificates SIParator Type

**Configuration Transport** (Help)

**Configuration via HTTP**      **Configuration via HTTPS**  
 Direct the web browser to this address:      Direct the web browser to this address:

Port:      Port:      Certificate to use:  
           

**Configuration Allowed Via Interface** (Help)

Eth0 <input checked="" type="radio"/> On <input type="radio"/> Off	Eth1 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth2 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth3 <input type="radio"/> On <input checked="" type="radio"/> Off
Eth4 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth5 <input type="radio"/> On <input checked="" type="radio"/> Off		

Configuration Computers <a href="#">(Help)</a>											
Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	10.1.0.0	10.1.0.0	255.255.255.0	10.1.0.0 - 10.1.0.255	-	No	Yes	Yes	Local	<input type="checkbox"/>

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

Basic
Signaling Encryption
Media Encryption
Interoperability
Sessions and Media
Remote SIP Connectivity
VoIP Survival
VoIP Survival Status

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

Go to the **Filtering** page. SIP requests from the internal network should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

SIP Methods
Filtering
Local Registrar
Authentication and Accounting
SIP Accounts
Dial Plan
Routing
Time Classes
SIP Status
IDS/IPS
IDS/IPS Status

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Internal network	Process all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

Allow the content types which are allowed in SIP media streams. Note that the content types *application/sdp*, *application/xpidf+xml* and *text/x-msmsgsinvite* are always allowed, regardless of what is entered here.

**Content Type Filter Rules** [\(Help\)](#)

Edit Row	Content Type	Allowed	Delete Row
<input type="checkbox"/>	image/jpeg	Yes	<input type="checkbox"/>
<input type="checkbox"/>	message/sipfrag	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/lpidf	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Yes	<input type="checkbox"/>

Add new rows  rows.

The SIP traffic can be made more secure by encrypting the SIP signaling between the unit and its SIP peers. For this, the TLS protocol is used. Select to **Allow TLS** on the **Signaling Encryption** page.

To use TLS, the unit needs an SSL certificate, which is created on the Certificates page. Select the certificate on this page.

When TLS is used, the unit must also be able to verify the SSL certificates of its SIP peers. To do this, it must have the certificate of the signing CA for the peer certificate. You load the CA certificate on the **Certificates** page. Then, list the trusted TLS CAs on the **Authentication and Accounting** page.

The screenshot shows a web interface for configuring SIP services. At the top, there is a navigation bar with several tabs: SIP Methods, Filtering, Local Registrar, Authentication and Accounting (which is highlighted in red), SIP Accounts, Dial Plan, Routing, Time Classes, SIP Status, IDS/IPS, and IDS/IPS Status. Below the navigation bar, the main content area is titled 'SIP Authentication'. It contains two radio buttons: 'Enable SIP authentication' (which is selected) and 'Disable SIP authentication'. Below this, there is a section titled 'SIP Realm' with a text input field containing the value 'ingate.com'.

If you want the unit to authenticate users you must also decide what to authenticate for. Select the methods to allow and authenticate on the **SIP Methods** page.

Here, we require authentication for REGISTER to local domains, which means when a user tries to register on a domain handled by the unit. Authentication is also required for INVITE to other domain, which means that a user who wants to call someone on a domain not handled by the unit needs to provide a password.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Local domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Other domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain looks just like the ordinary Internet domain for the company.

Some IP telephones register on IP addresses (their own or that of the registrar) instead of domains. If you use this type of telephones, add the IP address of the registrar as a **Locally handled domain**.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	193.12.253.113	<input type="checkbox"/>
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Now you can enter users in the **Local SIP User Database** table. You can use the "\*" wildcard for any number of characters. However, you must enter all users on separate lines to give them individual passwords.

Local SIP User Database <a href="#">(Help)</a>						
Edit row	Username	Domain	Authentication name	Password	Register from	Delete row
<input type="checkbox"/>	lisa	ingate.com	l7631		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	lab1	193.12.253.113			Internal network	<input type="checkbox"/>
<input type="checkbox"/>	harry	ingate.com	h1837		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	annie	ingate.com	a4419		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	john	ingate.com	j2700		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	martin	ingate.com	m5882		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	lab2	193.12.253.113			Internal network	<input type="checkbox"/>

The SIP domain admin.ingate.com is handled by a separate SIP registrar on the IP address 10.0.0.27, and must be defined thus under **DNS Override For SIP Requests** on the **Routing** page (or DNS must point to 10.0.0.27 for the SIP domain admin.ingate.com).

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	Time Classes	SIP Status	IDS/IPS	IDS/IPS Status
DNS Override For SIP Requests <a href="#">(Help)</a>										
Edit Row	Domain	Relay To						Delete Row		
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight			
<input type="checkbox"/>	+ admin.ingate.com	10.0.0.27	10.0.0.27		UDP			<input type="checkbox"/>		

This is the configuration needed in the unit. Apply the configuration on the **Save/Load Configuration** page.

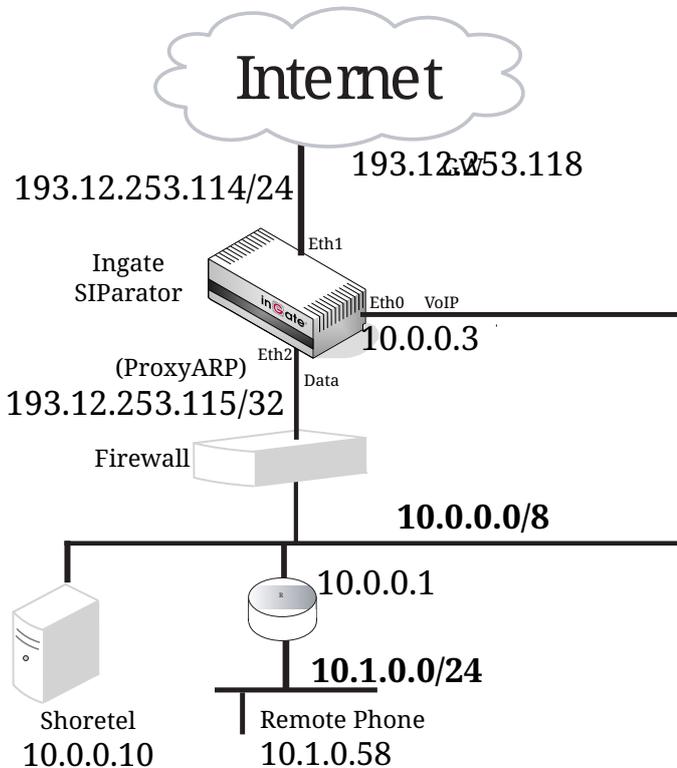
Save/Load Configuration	Show Configuration	User Administration
Test Run and Apply Conf <a href="#">(Help)</a>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

SIP clients will use the unit's internal IP address 10.0.0.3 as their outgoing SIP proxy and as their registrar (if they can't be configured with the domain only). If you don't want to use the unit as the registrar, you should point the clients to the SIP registrar you want to use.

The DNS server used must have a record for the SIP domain, which states that the unit handles the domain, or many SIP clients won't be able to use it (if you don't use plain IP addresses as domains).

## 20.17. The WAN SIParator Type

The WAN SIParator Type is connected to the outside on one interface and your *firewall* on another interface. Between these two interfaces (marked as a Data Interfaces on the Topology page), only data will be sent. Other interfaces can be connected directly to your LAN, DMZ or other networks, and here SIP traffic will be sent.



The first thing to do is to set the **SIParator Type** under **Basic Configuration**.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	<b>SIParator Type</b>
---------------------	----------------	--------	------	--------------------	--------------	----------	-----------------------

**Type of SIParator** ([Help](#))

The SIParator can be connected to your network in four different ways, depending on your needs.

SIParator type:

On the **Eth0** page under **Network**, the interface name and IP address are set. Eth0 is connected to the internal network. There is a system administration network, 10.1.0.0/24, behind the router 10.0.0.1. Configuration is allowed via this interface.

**General**

Physical device: eth0

This interface is:  Active  Inactive

Interface name:

---

**Directly Connected Networks** [\(Help\)](#)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
inside	Static	10.0.0.3	10.0.0.3	8	10.0.0.0	10.255.255.255		-	<input type="checkbox"/>

Add new rows  rows.

---

**Alias** [\(Help\)](#)

**Static Routing** [\(Help\)](#)

Routed Network			Router			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
10.1.0.0	10.1.0.0	24	- ▾	10.0.0.1	10.0.0.1	<input type="checkbox"/>

Add new rows  rows.

On the **Eth1** page, the interface name and IP address are set. Eth1 is connected to the Internet.

**General**

Physical device: eth1

This interface is:  Active  Inactive

Interface name:

---

**Directly Connected Networks** [\(Help\)](#)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
external	Static	193.12.253.114	193.12.253.114	255.255.255.0	193.12.253.0	193.12.253.255		-	<input type="checkbox"/>

Add new rows  rows.

---

**Alias** [\(Help\)](#)

**Static Routing** [\(Help\)](#)

Routed Network			Router			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
default	default		- ▾	193.12.253.118	193.12.253.118	<input type="checkbox"/>

Add new rows  rows.

On the **Eth2** page, the interface name and Proxy ARP are set. Eth2 is connected to the Firewall.

**General**

Physical device: **eth2**

This interface is:  Active  Inactive

Interface name:

**Directly Connected Networks** [\(Help\)](#)

**Proxy ARP** [\(Help\)](#)

Get Network From	Proxy ARPed Network			VLAN Id	VLAN Name	Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits			
external (193.12.253.114) ▾	193.12.253.115	193.12.253.115	32		-	<input type="checkbox"/>

Add new rows  rows.

On the **Topology** page, set the **Data Interfaces**. Between the Data Interfaces listed here, the unit will act as a plain router, and only forward traffic.

**Data Interfaces** [\(Help\)](#)

If your SIParator type is not set to **WAN**, the settings in this section will have no effect.

Interface	Delete Row
outside (eth1 untagged) ▾	<input type="checkbox"/>
Ethernet2 (eth2 untagged) ▾	<input type="checkbox"/>

Add new rows  rows.

Define groups of computers on the **Networks and Computers** page.

Networks and Computers		Default Gateways	All Interfaces	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE	Topology
Networks and Computers													
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row					
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address							
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>					
<input type="checkbox"/>	+ Internal network	-	10.0.0.0	10.0.0.0	10.1.255.255	10.1.255.255	Internal (eth0 untagged)	<input type="checkbox"/>					
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>					

After that, set **Default gateway** on the **Default Gateways** page. The default gateway for the unit is the same as for the *firewall*; 193.12.253.118.

Networks and Computers		Default Gateways	All Interfaces	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE	Topology
Main Default Gateways <a href="#">(Help)</a>													
Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row							
<input type="checkbox"/>		-	193.12.253.118	193.12.253.118	External (eth1)	<input type="checkbox"/>							

Enter a **DNS server** on the **Basic Configuration** page. This is needed to look up other SIP domains.

DNS Servers <a href="#">(Help)</a>				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

Go to the **Access Control** page and select the IP address the unit's web interface should have. Also enter the IP addresses of the computers allowed to configure the unit.

We select to configure via HTTP and select the inside IP address. Configuration traffic is only allowed via Eth0 (the inside interface).

Only workstations on the system administration network are allowed to configure the unit.

Basic Configuration **Access Control** RADIUS SNMP Certificates SIPArator Type

**Configuration Transport** (Help)

**Configuration via HTTP**  
Direct the web browser to this address:

Inside (10.0.0.3)

Port:

**Configuration via HTTPS**  
Direct the web browser to this address:

-

Port:  Certificate to use:

**Configuration Allowed Via Interface** (Help)

Eth0 <input checked="" type="radio"/> On <input type="radio"/> Off	Eth1 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth2 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth3 <input type="radio"/> On <input checked="" type="radio"/> Off
Eth4 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth5 <input type="radio"/> On <input checked="" type="radio"/> Off		

**Configuration Computers** (Help)

Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	10.1.0.0	10.1.0.0	255.255.255.0	10.1.0.0 - 10.1.0.255	-	No	Yes	Yes	Local	<input type="checkbox"/>

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

**Basic** Signaling Encryption Media Encryption Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival VoIP Survival Status

**SIP Module** (Help)

Enable SIP module  
 Disable SIP module

Go to the **Filtering** page. SIP requests from the internal network should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Proxy Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Internal network	Process all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

Allow the content types which are allowed in SIP media streams. Note that the content types application/sdp, application/xpidf+xml and text/x-msmsgsinvoke are always allowed, regardless of what is entered here.

**Content Type Filter Rules** (Help)

Edit Row	Content Type	Allowed	Delete Row
<input type="checkbox"/>	image/jpg	Yes	<input type="checkbox"/>
<input type="checkbox"/>	message/sipfrag	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/lpidf	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Yes	<input type="checkbox"/>

Add new rows  rows.

The SIP traffic can be made more secure by encrypting the SIP signaling between the unit and its SIP peers. For this, the TLS protocol is used. Select to **Allow TLS** on the **Signaling Encryption** page. To use TLS, the unit needs an SSL certificate, which is created on the Certificates page. Select the certificate on this page.

When TLS is used, the unit must also be able to verify the SSL certificates of its SIP peers. To do this, it must have the certificate of the signing CA for the peer certificate. You load the CA certificate on the **Certificates** page. Then, list the trusted TLS CAs on the **Authentication and Accounting** page.

SIP Methods Filtering Local Registrar **Authentication and Accounting** SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

If you want the unit to authenticate users you must also decide what to authenticate for. Select the methods to allow and authenticate on the **SIP Methods** page.

Here, we require authentication for REGISTER to local domains, which means when a user tries to register on a domain handled by the unit. Authentication is also required for INVITE to other domain, which means that a user who wants to call someone on a domain not handled by the unit needs to provide a password.

**SIP Methods** Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Local domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Other domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain looks just like the ordinary Internet domain for the company.

Some IP telephones register on IP addresses (their own or that of the registrar) instead of domains. If you use this type of telephones, add the IP address of the registrar as a **Locally handled domain**.

SIP Methods Filtering **Local Registrar** Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	193.12.253.113	<input type="checkbox"/>
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Now you can enter users in the **Local SIP User Database** table. You can use the "\*" wildcard for any number of characters. However, you must enter all users on separate lines to give them individual

passwords.

Local SIP User Database <a href="#">(Help)</a>						
Edit row	Username	Domain	Authentication name	Password	Register from	Delete row
<input type="checkbox"/>	lisa	ingate.com	l7631		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	lab1	193.12.253.113			Internal network	<input type="checkbox"/>
<input type="checkbox"/>	harry	ingate.com	h1837		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	annie	ingate.com	a4419		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	john	ingate.com	j2700		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	martin	ingate.com	m5882		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	lab2	193.12.253.113			Internal network	<input type="checkbox"/>

The SIP domain admin.ingate.com is handled by a separate SIP registrar on the IP address 10.0.0.27, and must be defined thus under **DNS Override For SIP Requests** on the **Routing** page (or DNS must point to 10.0.0.27 for the SIP domain admin.ingate.com).

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	Time Classes	SIP Status	IDS/IPS	IDS/IPS Status
DNS Override For SIP Requests <a href="#">(Help)</a>										
Edit Row	Domain	Relay To						Delete Row		
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight			
<input type="checkbox"/>	+ admin.ingate.com	10.0.0.27	10.0.0.27		UDP					<input type="checkbox"/>

This is the configuration needed in the unit. Apply the configuration on the **Save/Load Configuration** page.

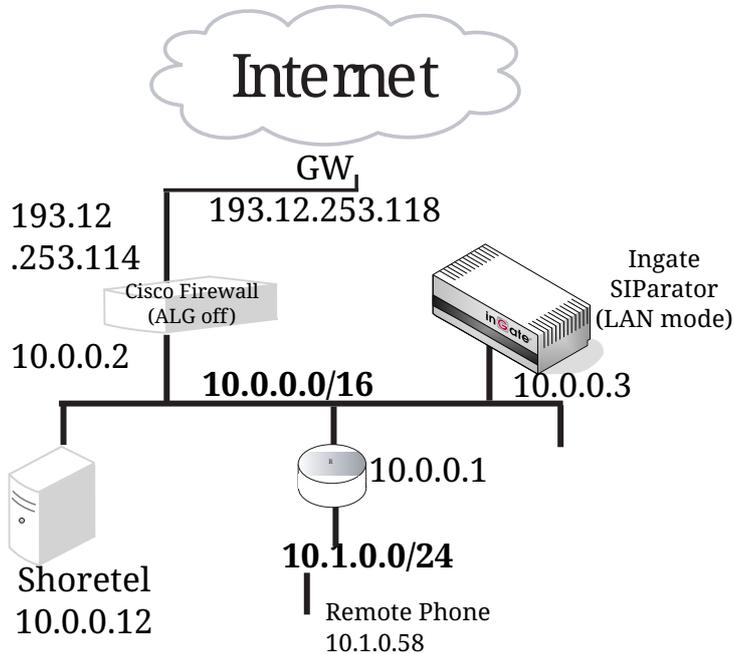
Save/Load Configuration	Show Configuration	User Administration
<b>Test Run and Apply Conf</b> <a href="#">(Help)</a>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

SIP clients will use the unit's internal IP address 10.0.0.3 as their outgoing SIP proxy and as their registrar (if they can't be configured with the domain only). If you don't want to use the unit as the registrar, you should point the clients to the SIP registrar you want to use.

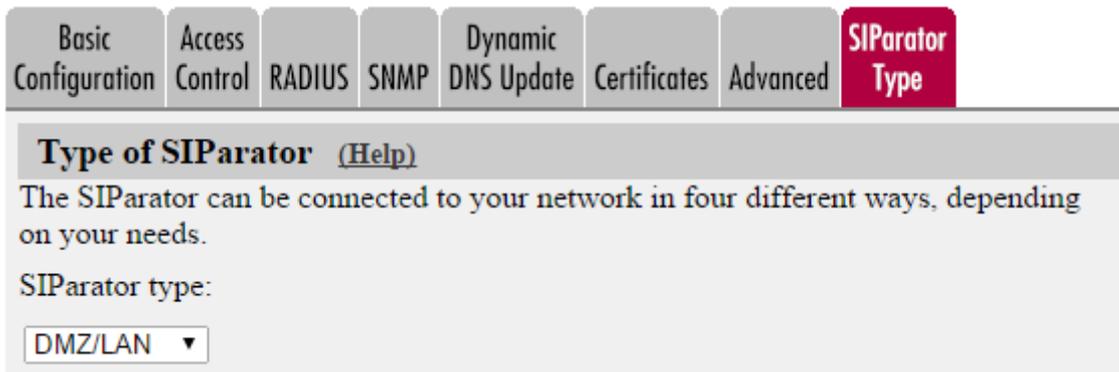
The DNS server used must have a record for the SIP domain, which states that the unit handles the domain, or many SIP clients won't be able to use it (if you don't use plain IP addresses as domains).

## 20.18. The LAN SIParator Type

The LAN SIParator Type is connected to the internal network. The unit handles all SIP requests on the LAN. All traffic goes through the *firewall*. LAN based SIP servers should set the SIP gateway to the LAN SIParator Type. The (Shoretel) SIP PBX at 10.0.0.12 can have clients on both 10.0.0/16 and 10.1.0.0/24 subnets and the Ingate will negotiate media for all.



The first thing to do is to set the **SIParator Type** under **Basic Configuration**.



On the **Eth0** page under **Network**, the interface name and IP address are set. Eth0 is connected to the internal network. There is a system administration network, 10.1.0.0/24, behind the router 10.0.0.24. Configuration is allowed via this interface.

Networks and Computers | Default Gateways | All Interfaces | VLAN | **Eth0** | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Topology

---

**General**

Physical device: **eth0**

This interface is:  Active  Inactive

Interface name:

**Speed and Duplex**

Automatic negotiation

100 Mbit/s, full duplex

100 Mbit/s, half duplex

10 Mbit/s, full duplex

10 Mbit/s, half duplex

**Directly Connected Networks** [\(Help\)](#)

Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	Inside	Static	10.0.0.3	10.0.0.3	16	10.0.0.0	10.0.255.255		-	<input type="checkbox"/>

**Static Routing** [\(Help\)](#)

Edit Row	Routed Network			Router			Delete Row
	DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
<input type="checkbox"/>	10.1.0.0	10.1.0.0	24	-	10.0.0.24	10.0.0.24	<input type="checkbox"/>

Define groups of computers on the **Networks and Computers** page.

**Networks and Computers** | Default Gateways | All Interfaces | VLAN | **Eth0** | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Topology

---

**Networks and Computers**

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internal network	-	10.0.0.0	10.0.0.0	10.1.255.255	10.1.255.255	Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>

After that, set **Default gateway** on the **Default Gateways** page. The default gateway for the unit is the same as for the *firewall*; 193.12.253.118.

Networks and Computers **Default Gateways** All Interfaces VLAN Eth0 Eth1 Eth2 Eth3 Eth4 Eth5 Interface Status PPPoE Topology

**Main Default Gateways** (Help)

Edit Row	Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
<input type="checkbox"/>		-	193.12.253.118	193.12.253.118	External (eth1)	<input type="checkbox"/>

Enter a **DNS server** on the **Basic Configuration** page. This is needed to look up other SIP domains.

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

Go to the **Access Control** page and select the IP address the unit's web interface should have. Also enter the IP addresses of the computers allowed to configure the unit.

We select to configure via HTTP and select the inside IP address. Configuration traffic is only allowed via Eth0 (the inside interface).

Only workstations on the system administration network are allowed to configure the unit.

Basic Configuration **Access Control** RADIUS SNMP Certificates SIParator Type

**Configuration Transport** (Help)

**Configuration via HTTP**      **Configuration via HTTPS**  
 Direct the web browser to this address:      Direct the web browser to this address:

Inside (10.0.0.3)      -

Port:      Port:      Certificate to use:  
 80      443      -

**Configuration Allowed Via Interface** (Help)

Eth0 <input checked="" type="radio"/> On <input type="radio"/> Off	Eth1 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth2 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth3 <input type="radio"/> On <input checked="" type="radio"/> Off
Eth4 <input type="radio"/> On <input checked="" type="radio"/> Off	Eth5 <input type="radio"/> On <input checked="" type="radio"/> Off		

Configuration Computers <a href="#">(Help)</a>											
Edit Row	No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete Row
<input type="checkbox"/>	1	10.1.0.0	10.1.0.0	255.255.255.0	10.1.0.0 - 10.1.0.255	-	No	Yes	Yes	Local	<input type="checkbox"/>

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

Basic
Signaling Encryption
Media Encryption
Interoperability
Sessions and Media
Remote SIP Connectivity
VoIP Survival
VoIP Survival Status

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

Go to the **Filtering** page. SIP requests from the internal network should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

SIP Methods
Filtering
Local Registrar
Authentication and Accounting
SIP Accounts
Dial Plan
Routing
Time Classes
SIP Status
IDS/IPS
IDS/IPS Status

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Internal network	Process all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

Allow the content types which are allowed in SIP media streams. Note that the content types *application/sdp*, *application/xpidf+xml* and *text/x-msmsgsinvite* are always allowed, regardless of what is entered here.

**Content Type Filter Rules** [\(Help\)](#)

Edit Row	Content Type	Allowed	Delete Row
<input type="checkbox"/>	image/jpg	Yes	<input type="checkbox"/>
<input type="checkbox"/>	message/sipfrag	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/html	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/lpidf	Yes	<input type="checkbox"/>
<input type="checkbox"/>	text/plain	Yes	<input type="checkbox"/>

Add new rows  rows.

The SIP traffic can be made more secure by encrypting the SIP signaling between the unit and its SIP peers. For this, the TLS protocol is used. Select to **Allow TLS** on the **Signaling Encryption** page.

To use TLS, the unit needs an SSL certificate, which is created on the Certificates page. Select the certificate on this page.

When TLS is used, the unit must also be able to verify the SSL certificates of its SIP peers. To do this, it must have the certificate of the signing CA for the peer certificate. You load the CA certificate on the **Certificates** page. Then, list the trusted TLS CAs on the **Authentication and Accounting** page.

The screenshot shows a web interface for configuring SIP services. At the top, there is a navigation bar with several tabs: SIP Methods, Filtering, Local Registrar, Authentication and Accounting (highlighted in red), SIP Accounts, Dial Plan, Routing, Time Classes, SIP Status, IDS/IPS, and IDS/IPS Status. Below the navigation bar, the main content area is titled 'SIP Authentication'. It contains two radio buttons: 'Enable SIP authentication' (selected) and 'Disable SIP authentication'. Below this, there is a section titled 'SIP Realm' with a text input field containing the value 'ingate.com'.

If you want the unit to authenticate users you must also decide what to authenticate for. Select the methods to allow and authenticate on the **SIP Methods** page.

Here, we require authentication for REGISTER to local domains, which means when a user tries to register on a domain handled by the unit. Authentication is also required for INVITE to other domain, which means that a user who wants to call someone on a domain not handled by the unit needs to provide a password.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Local domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Other domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain looks just like the ordinary Internet domain for the company.

Some IP telephones register on IP addresses (their own or that of the registrar) instead of domains. If you use this type of telephones, add the IP address of the registrar as a **Locally handled domain**.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	193.12.253.113	<input type="checkbox"/>
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Now you can enter users in the **Local SIP User Database** table. You can use the "\*" wildcard for any number of characters. However, you must enter all users on separate lines to give them individual passwords.

Local SIP User Database <a href="#">(Help)</a>						
Edit row	Username	Domain	Authentication name	Password	Register from	Delete row
<input type="checkbox"/>	lisa	ingate.com	l7631		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	lab1	193.12.253.113			Internal network	<input type="checkbox"/>
<input type="checkbox"/>	harry	ingate.com	h1837		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	annie	ingate.com	a4419		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	john	ingate.com	j2700		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	martin	ingate.com	m5882		Everywhere	<input type="checkbox"/>
<input type="checkbox"/>	lab2	193.12.253.113			Internal network	<input type="checkbox"/>

The SIP domain admin.ingate.com is handled by a separate SIP registrar on the IP address 10.0.0.27, and must be defined thus under **DNS Override For SIP Requests** on the **Routing page** (or DNS must point to 10.0.0.27 for the SIP domain admin.ingate.com).

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	Time Classes	SIP Status	IDS/IPS	IDS/IPS Status
<b>DNS Override For SIP Requests <a href="#">(Help)</a></b>										
Edit Row	Domain	Relay To						Delete Row		
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight			
<input type="checkbox"/>	+ admin.ingate.com	10.0.0.27	10.0.0.27		UDP			<input type="checkbox"/>		

This is the configuration needed in the unit. Apply the configuration on the **Save/Load Configuration** page.

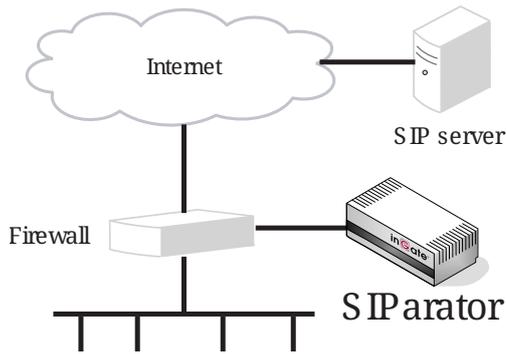
Save/Load Configuration	Show Configuration	User Administration
<b>Test Run and Apply Conf <a href="#">(Help)</a></b>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

The SIP clients should have the unit's internal IP address 10.0.0.3 as their outgoing SIP proxy.

## 20.19. DMZ SIParator, SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the unit's SIP function is only used to traverse NAT.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.19.1. Networks and Computers

The unit must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the unit should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

Networks and Computers
Default Gateways
All Interfaces
VLAN
Eth0
Eth1
Eth2
Eth3
Eth4
Eth5
Interface Status
PPPoE
Topology

**Networks and Computers**

Edit Row	Name	Subgroup	Lower Limit		Upper Limit <small>(for IP ranges)</small>		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	<input type="checkbox"/>
<input type="checkbox"/>		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Lab+Office	Laboratory					-	<input type="checkbox"/>
<input type="checkbox"/>		Office					-	<input type="checkbox"/>
<input type="checkbox"/>	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	<input type="checkbox"/>
<input type="checkbox"/>	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	<input type="checkbox"/>
<input type="checkbox"/>		-	10.1.0.17	10.1.0.17			-	<input type="checkbox"/>

Add new rows  groups with  rows per group.

## 20.19.2. Topology

To make the unit aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** SIParator type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network. When you are finished, there should be one line for each of your *firewall*'s network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the *firewall*.

For DMZ, Manual and LAN SIParators, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Tunnels | **Topology**

### Surroundings [\(Help\)](#)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
DMZ ▼	- ▼	<input type="checkbox"/>
Lab+Office ▼	- ▼	<input type="checkbox"/>

Add new rows  ROWS.

## 20.19.3. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

[Basic](#)
[Signaling Encryption](#)
[Media Encryption](#)
[Interoperability](#)
[Sessions and Media](#)
[Remote SIP Connectivity](#)
[VoIP Survival](#)
[VoIP Survival Status](#)

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling: 
 Log class for SIP packets:

Log class for SIP license messages: 
 Log class for SIP errors:

Log class for SIP media messages: 
 Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

## 20.19.4. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool

[SIP Methods](#)
[Filtering](#)
[Local Registrar](#)
[Authentication and Accounting](#)
[SIP Accounts](#)
[Dial Plan](#)
[Routing](#)
[SIP Status](#)
[IDS/IPS](#)
[IDS/IPS Status](#)

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
Add new rows <input type="text" value="1"/> rows.				

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.19.5. Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

Outbound Proxy <a href="#">(Help)</a>						
Edit Row	From Domain	Request-URI Domain	Domain or IP Address	Port	Gateway	Delete Row
<input type="checkbox"/>	*	*	3.22.39.7	5060	-	<input type="checkbox"/>

## 20.19.6. Basic Configuration

If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

DNS Servers <a href="#">(Help)</a>				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.19.7. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration
Show Configuration
User Administration

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** [\(Help\)](#)

The permanent configuration might be affected by loading a CLI file.

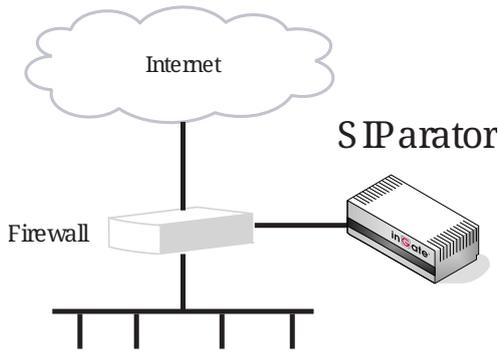
Local file:

## 20.20. DMZ SIParator, SIP server in the SIParator

You might want to have most SIP functions in one box. The Ingate SIParator/Firewall can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed

packets.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.20.1. Networks and Computers

The unit must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the unit should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

Networks and Computers
Default Gateways
All Interfaces
VLAN
Eth0
Eth1
Eth2
Eth3
Eth4
Eth5
Interface Status
PPPoE
Topology

#### Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit <small>(for IP ranges)</small>		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	<input type="checkbox"/>
<input type="checkbox"/>		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Lab+Office	Laboratory					-	<input type="checkbox"/>
<input type="checkbox"/>		Office					-	<input type="checkbox"/>
<input type="checkbox"/>	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	<input type="checkbox"/>
<input type="checkbox"/>	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	<input type="checkbox"/>
<input type="checkbox"/>		-	10.1.0.17	10.1.0.17			-	<input type="checkbox"/>

Add new rows  groups with  rows per group.

## 20.20.2. Topology

To make the unit aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** SIParator type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network. When you are finished, there should be one line for each of your *firewall*'s network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the *firewall*.

For DMZ, Manual and LAN SIParators, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

Network	Additional Negotiators	Delete Row
DMZ ▼	- ▼	<input type="checkbox"/>
Lab+Office ▼	- ▼	<input type="checkbox"/>

Add new rows  ROWS.

## 20.20.3. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

[Basic](#)
[Signaling Encryption](#)
[Media Encryption](#)
[Interoperability](#)
[Sessions and Media](#)
[Remote SIP Connectivity](#)
[VoIP Survival](#)
[VoIP Survival Status](#)

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling: 
 Log class for SIP packets:

Log class for SIP license messages: 
 Log class for SIP errors:

Log class for SIP media messages: 
 Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

## 20.20.4. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.

[SIP Methods](#)
[Filtering](#)
[Local Registrar](#)
[Authentication and Accounting](#)
[SIP Accounts](#)
[Dial Plan](#)
[Routing](#)
[Time Classes](#)
[SIP Status](#)
[IDS/IPS](#)
[IDS/IPS Status](#)

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.

**Select SIP User Database** [\(Help\)](#)

Use SIP user database:  Local  RADIUS

**RADIUS Database Settings**

RADIUS users register from:

## 20.20.5. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

**SIP Methods** Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

## 20.20.6. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

SIP Methods Filtering **Local Registrar** Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

**Local SIP User Database** (Help)

Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

### 20.20.7. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also the [RADIUS](#) section for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration Access Control **RADIUS** SNMP Dynamic DNS Update Certificates Advanced SIPArator Type

**RADIUS Servers** (Help)

Edit Row	RADIUS Server		Port	Secret	Delete Row
	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	193.180.23.239	193.180.23.239	1812		<input type="checkbox"/>

Add new rows  rows.

### 20.20.8. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to **Process all**.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

Create rules for traffic from the inside (Process all) and the DMZ (Reject all). Let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

**Sender IP Filter Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

### 20.20.9. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool

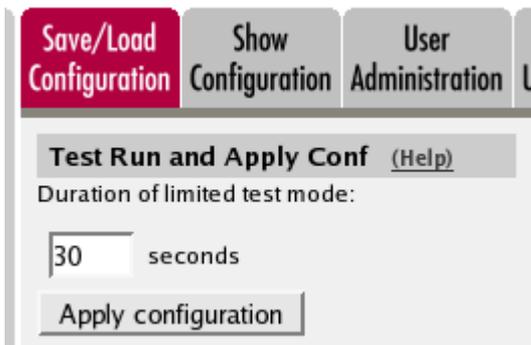
**DNS Servers** [\(Help\)](#)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

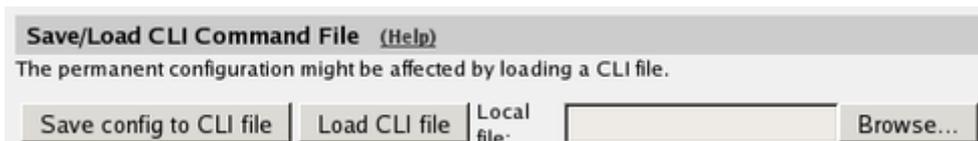
Add new rows  rows.

### 20.20.10. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

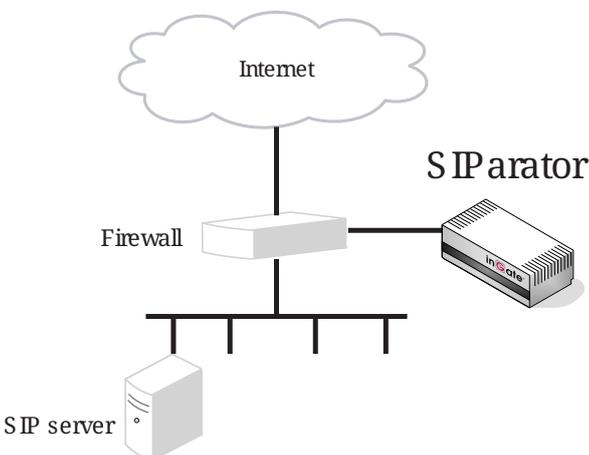


## 20.21. DMZ SIParator, SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the unit. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the unit, which in turn will forward the SIP traffic to the server.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.21.1. Networks and Computers

The unit must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the unit should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having

to go through the *firewall* connected to the unit should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

Networks and Computers    Default Gateways    All Interfaces    VLAN    Eth0    Eth1    Eth2    Eth3    Eth4    Eth5    Interface Status    PPPoE    Topology

**Networks and Computers**

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	<input type="checkbox"/>
<input type="checkbox"/>		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Lab+Office	Laboratory					-	<input type="checkbox"/>
<input type="checkbox"/>		Office					-	<input type="checkbox"/>
<input type="checkbox"/>	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	<input type="checkbox"/>
<input type="checkbox"/>	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	<input type="checkbox"/>
<input type="checkbox"/>		-	10.1.0.17	10.1.0.17			-	<input type="checkbox"/>

Add new rows  groups with  rows per group.

## 20.21.2. Topology

To make the unit aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network. When you are finished, there should be one line for each of your *firewall's* network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the *firewall*.

For DMZ, Manual and LAN SIParators, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Tunnels | **Topology**

**Surroundings** (Help)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
DMZ ▼	- ▼	<input type="checkbox"/>
Lab+Office ▼	- ▼	<input type="checkbox"/>

Add new rows  rows.

### 20.21.3. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

**Basic** | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VoIP Survival | VoIP Survival Status

**SIP Module** (Help)

- Enable SIP module
- Disable SIP module

**SIP Logging** (Help)

Log class for SIP signaling:  ▼

Log class for SIP license messages:  ▼

Log class for SIP media messages:  ▼

Log class for SIP IDS/IPS:  ▼

Log class for SIP packets:  ▼

Log class for SIP errors:  ▼

Log class for SIP debug messages:  ▼

Hide sensitive data:  Yes  No

## 20.21.4. Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the unit, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The unit will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.

SIP Methods	Filtering	Local Registrar	Authentication and Accounting	SIP Accounts	Dial Plan	<b>Routing</b>	SIP Status	IDS/IPS	IDS/IPS Status
<b>DNS Override For SIP Requests</b> <a href="#">(Help)</a>									
Edit Row	Domain	Relay To						Delete Row	
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight		
<input type="checkbox"/>	+ ingate.com	10.47.2.246	10.47.2.246	5060	UDP			<input type="checkbox"/>	

## 20.21.5. Interoperability

If Windows Messenger is used for SIP communication, you need to set a parameter on the **Interoperability** page. Set `lr=true` status to **On** under **Loose routing**.

Basic	SIP Encryption	<b>Interoperability</b>	Sessions and Media	Remote SIP Connectivity	V Sur
<b>Loose Routing</b> <a href="#">(Help)</a>					
<input type="radio"/> Use lr					
<input checked="" type="radio"/> Use lr=true					

If the SIP server is an LCS (Live Communications Server) or some other server that does not accept more than one Via header in SIP packets, you must enter the SIP server IP address in the **Remove Via Headers** table. This will make the unit strip SIP packets of extra Via headers when it sends those packets to the server, and add the Via headers when the response packets are received.

<b>Remove Via Headers</b> <a href="#">(Help)</a>		
<b>SIP Server</b>		<b>Delete Row</b>
<b>DNS Name or IP Address</b>	<b>IP Address</b>	
<input type="button" value="Add new rows"/> <input type="text" value="1"/> ROWS.		
<input type="checkbox"/> Remove Via Headers for all SIP servers		

## 20.21.6. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the

Filtering page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool

The screenshot shows the 'SIP Filtering' configuration page. At the top, there are several tabs: SIP Methods, **Filtering**, Local Registrar, Authentication and Accounting, SIP Accounts, Dial Plan, Routing, SIP Status, IDS/IPS, and IDS/IPS Status. Below the tabs is a section titled 'Proxy Rules (Help)'. It contains a table with columns: Edit Row, No., From Network, Action, and Delete Row. Below the table is a button 'Add new rows' and a text input '1 rows.'. To the right of the table is a section titled 'Default Policy For SIP Requests' with three radio buttons:  Process all,  Local only, and  Reject all.

### 20.21.7. Basic Configuration

If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

The screenshot shows the 'DNS Servers (Help)' configuration page. It features a table with the following columns: No., Dynamic, DNS Name or IP Address, IP Address, and Delete Row. The table contains three rows of data:

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

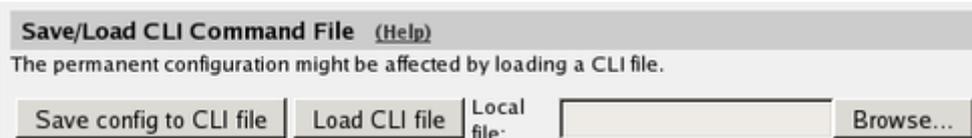
Below the table is a button 'Add new rows' and a text input '1 rows.'.

### 20.21.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

The screenshot shows the 'Save/Load Configuration' page. At the top, there are several tabs: **Save/Load Configuration**, Show Configuration, User Administration, and U. Below the tabs is a section titled 'Test Run and Apply Conf (Help)'. It contains a text input '30 seconds' and a button 'Apply configuration'.

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

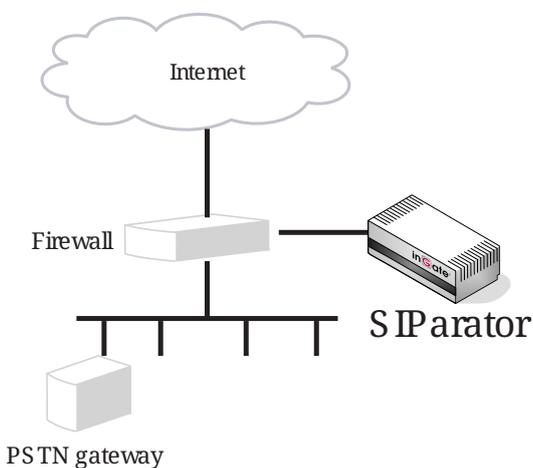


## 20.22. DMZ SIParator, SIP server in the SIParator, PSTN gateway inside

You might want to have most SIP functions in one box. The Ingate SIParator/Firewall can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.

A function not included in the unit is to connect to the PSTN network. If you want to do this, you must use a PSTN gateway.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.22.1. Networks and Computers

The unit must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the unit should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

Networks and Computers								
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ DMZ	-	193.12.253.201	193.12.253.201	193.12.253.207	193.12.253.207	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	9.255.255.255	9.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>		-	11.0.0.0	11.0.0.0	193.12.253.183	193.12.253.183	-	<input type="checkbox"/>
<input type="checkbox"/>		-	193.12.254.0	193.12.254.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Lab+Office	Laboratory					-	<input type="checkbox"/>
<input type="checkbox"/>		Office					-	<input type="checkbox"/>
<input type="checkbox"/>	+ Laboratory	-	10.1.0.0	10.1.0.0	10.1.255.255	10.1.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Office	-	10.0.0.0	10.0.0.0	10.0.255.255	10.0.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ PPTP clients	-	10.2.0.100	10.2.0.100	10.2.0.150	10.2.0.150	-	<input type="checkbox"/>
<input type="checkbox"/>	+ SNMP servers	-	10.0.0.7	10.0.0.7			-	<input type="checkbox"/>
<input type="checkbox"/>		-	10.1.0.17	10.1.0.17			-	<input type="checkbox"/>

Add new rows  groups with  rows per group.

## 20.22.2. Topology

To make the unit aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network. When you are finished, there should be one line for each of your *firewall*'s network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the *firewall*.

For DMZ, Manual and LAN SIParators, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Tunnels | **Topology**

**Surroundings** (Help)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
DMZ ▼	- ▼	<input type="checkbox"/>
Lab+Office ▼	- ▼	<input type="checkbox"/>

Add new rows  rows.

### 20.22.3. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

**Basic** | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VoIP Survival | VoIP Survival Status

**SIP Module** (Help)

Enable SIP module  
 Disable SIP module

**SIP Logging** (Help)

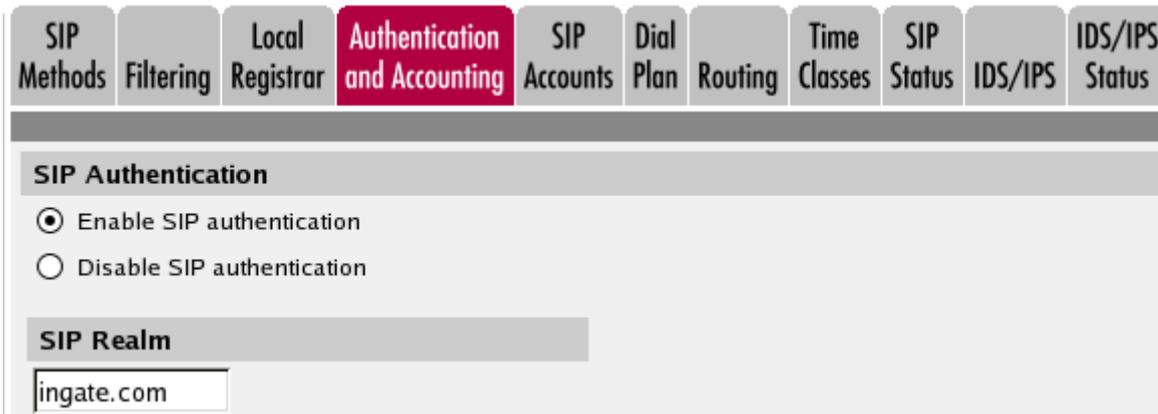
Log class for SIP signaling: <input type="text" value="Local"/> ▼	Log class for SIP packets: <input type="text" value="Local"/> ▼
Log class for SIP license messages: <input type="text" value="Local"/> ▼	Log class for SIP errors: <input type="text" value="Local"/> ▼
Log class for SIP media messages: <input type="text" value="Local"/> ▼	Log class for SIP debug messages: <input type="text" value="Local"/> ▼
Log class for SIP IDS/IPS: <input type="text" value="Local"/> ▼	

Hide sensitive data:  Yes  No

### 20.22.4. Authentication and Accounting

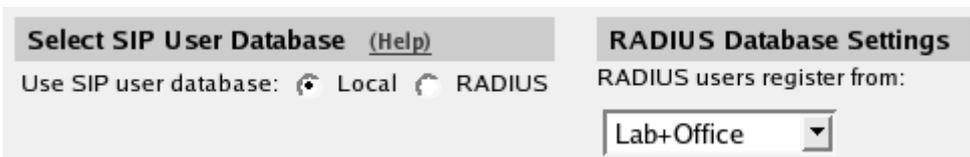
If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain

as the **Realm**.



The screenshot shows a web interface for configuring SIP settings. At the top, there is a navigation bar with tabs: SIP Methods, Filtering, Local Registrar, Authentication and Accounting (highlighted in red), SIP Accounts, Dial Plan, Routing, Time Classes, SIP Status, IDS/IPS, and IDS/IPS Status. Below the tabs, the 'SIP Authentication' section is active, showing two radio buttons: 'Enable SIP authentication' (selected) and 'Disable SIP authentication'. Below that, the 'SIP Realm' section has a text input field containing 'ingate.com'.

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.



The screenshot shows two sections: 'Select SIP User Database' and 'RADIUS Database Settings'. The 'Select SIP User Database' section has a header with '(Help)' and two radio buttons: 'Local' (selected) and 'RADIUS'. The 'RADIUS Database Settings' section has a header and a label 'RADIUS users register from:' followed by a dropdown menu showing 'Lab+Office'.

## 20.22.5. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

**SIP Methods** Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

## 20.22.6. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

SIP Methods Filtering **Local Registrar** Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database (Help)						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

## 20.22.7. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also the [RADIUS](#) section for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIPerator Type
<b>RADIUS Servers (Help)</b>							
Edit Row	RADIUS Server		Port	Secret	Delete Row		
	DNS Name or IP Address	IP Address					
<input type="checkbox"/>	193.180.23.239	193.180.23.239	1812		<input type="checkbox"/>		
Add new rows		<input type="text" value="1"/>	rows.				

## 20.22.8. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to **Process all**.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

Create rules for traffic from the inside (Process all) and the DMZ (Reject all). Let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.22.9. Routing

To redirect traffic to the PSTN network, you can use the **Dial Plan**. You can state that all SIP traffic to user names that consist of digits only (that is, the user names are phone numbers) to be redirected to the local PSTN gateway. You can also direct different numbers to different gateways.

If there are SIP clients which can't use authentication for INVITE (the method used to start calls), you can except these from authentication when calling to PSTN. Select the network for these clients in the **Matching From Header** table and create a row in the **Dial Plan** table, where Forward is selected as the **Action** (which means that authentication is not required).

**Matching From Header** (Help)

Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

In the example below, all phone numbers beginning with 01146 or +46 are redirected to a server in Sweden, numbers beginning with 01144 or +44 are redirected to a server in England, and calls to all other phone numbers are directed to the local PSTN gateway. Note that the table is read from the top and down, and the first matching row is used to route the call.

You should also restrict the redirections to only calls for local domains. Enter "\*local" under **Domain** when creating patterns in the **Matching Request-URI** table.

**Matching Request-URI** (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	Any number			0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden1		01146	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden2		+46	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK1		01144	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK2		+44	0..9		*local		<input type="checkbox"/>

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ Local PSTN	1	-	pstn.us.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ London PSTN	1	-	pstn.uk.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ Stockholm PSTN	1	-	pstn.sthlm.ingate.com		UDP		<input type="checkbox"/>

To prevent unauthorized use of your PSTN gateway, you should require authentication for all these redirections. Select **Auth&Forward** as the **Action** to manage this.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	Office	UK1	Forward	London PSTN			-	-	Redirect calls to UK	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	UK2	Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	3	-	UK1	Auth & Forward	London PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	4	-	UK2	Auth & Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	5	Office	Sweden1	Forward	Stockholm PSTN			-	-	Redirect calls to Sweden	<input type="checkbox"/>
<input type="checkbox"/>	6	Office	Sweden2	Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	7	-	Sweden1	Auth & Forward	Stockholm PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	8	-	Sweden2	Auth & Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	9	Office	Any number	Forward	Local PSTN			-	-	Redirect to local PSTN	<input type="checkbox"/>
<input type="checkbox"/>	10	-	Any number	Auth & Forward	Local PSTN			-	-	Auth if not from Office	<input type="checkbox"/>

## 20.22.10. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

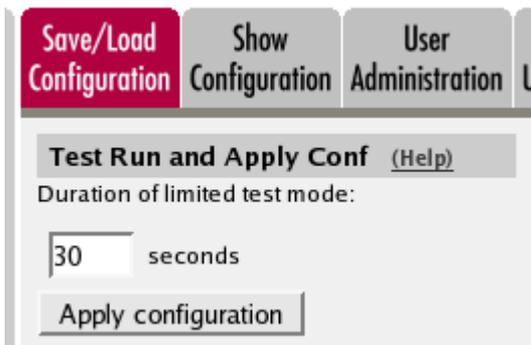
This setting is made by the Startup Tool.

DNS Servers (Help)				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

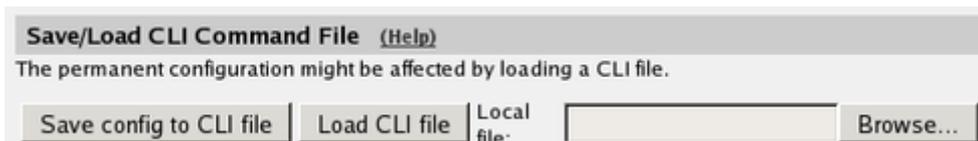
Add new rows  rows.

## 20.22.11. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



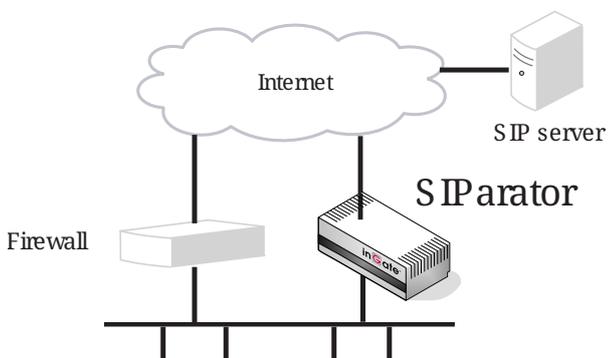
When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 20.23. Standalone SIParator, SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the unit SIP function is only used to traverse NAT.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.23.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

[Basic](#)
[Signaling Encryption](#)
[Media Encryption](#)
[Interoperability](#)
[Sessions and Media](#)
[Remote SIP Connectivity](#)
[VoIP Survival](#)
[VoIP Survival Status](#)

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling: 
 Log class for SIP packets:

Log class for SIP license messages: 
 Log class for SIP errors:

Log class for SIP media messages: 
 Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

### 20.23.2. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool.

[SIP Methods](#)
[Filtering](#)
[Local Registrar](#)
[Authentication and Accounting](#)
[SIP Accounts](#)
[Dial Plan](#)
[Routing](#)
[SIP Status](#)
[IDS/IPS](#)
[IDS/IPS Status](#)

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
Add new rows <input type="text" value="1"/> rows.				

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

### 20.23.3. Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

Outbound Proxy <a href="#">(Help)</a>						
Edit Row	From Domain	Request-URI Domain	Domain or IP Address	Port	Gateway	Delete Row
<input type="checkbox"/>	*	*	3.22.39.7	5060	-	<input type="checkbox"/>

## 20.23.4. Basic Configuration

If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

DNS Servers <a href="#">(Help)</a>				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.23.5. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration
Show Configuration
User Administration

---

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** [\(Help\)](#)

The permanent configuration might be affected by loading a CLI file.

Local file:

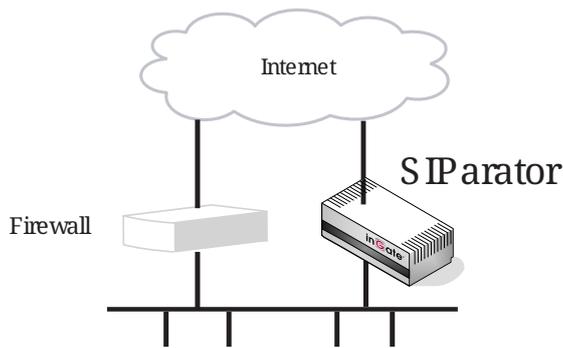
## 20.23.6. Client Settings

SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.24. Standalone SIParator, SIP server in the SIParator

You might want to have most SIP functions in one box. The Ingate SIParator/Firewall can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.24.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

<b>Basic</b>	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
<b>SIP Module</b> <a href="#">(Help)</a>							
<input checked="" type="radio"/> Enable SIP module							
<input type="radio"/> Disable SIP module							

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:  ▼

Log class for SIP packets:  ▼

Log class for SIP license messages:  ▼

Log class for SIP errors:  ▼

Log class for SIP media messages:  ▼

Log class for SIP debug messages:  ▼

Log class for SIP IDS/IPS:  ▼

Hide sensitive data:  Yes  No

## 20.24.2. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.

SIP Methods Filtering Local Registrar **Authentication and Accounting** SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**SIP Authentication**

Enable SIP authentication

Disable SIP authentication

**SIP Realm**

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.

**Select SIP User Database** [\(Help\)](#)

Use SIP user database:  Local  RADIUS

**RADIUS Database Settings**

RADIUS users register from:  ▼

## 20.24.3. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

## 20.24.4. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database <a href="#">(Help)</a>						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

## 20.24.5. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also the [RADIUS](#) section for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIParator Type
<b>RADIUS Servers</b> <a href="#">(Help)</a>							
Edit Row	RADIUS Server		Port	Secret	Delete Row		
	DNS Name or IP Address	IP Address					
<input type="checkbox"/>	193.180.23.239	193.180.23.239	1812		<input type="checkbox"/>		
Add new rows		<input type="text" value="1"/>	rows.				

## 20.24.6. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to **Process all**.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

Create rules for traffic from the inside (Process all) and let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.24.7. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool.

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="text" value="1"/>	-	<input type="text" value="172.16.0.3"/>	172.16.0.3	<input type="checkbox"/>
<input type="text" value="2"/>	-	<input type="text" value="10.47.3.201"/>	10.47.3.201	<input type="checkbox"/>
<input type="text" value="3"/>	Internet	<input type="text"/>	Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.24.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** Show Configuration User Administration U

**Test Run and Apply Conf** (Help)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** (Help)

The permanent configuration might be affected by loading a CLI file.

Local file:

## 20.24.9. Client Settings

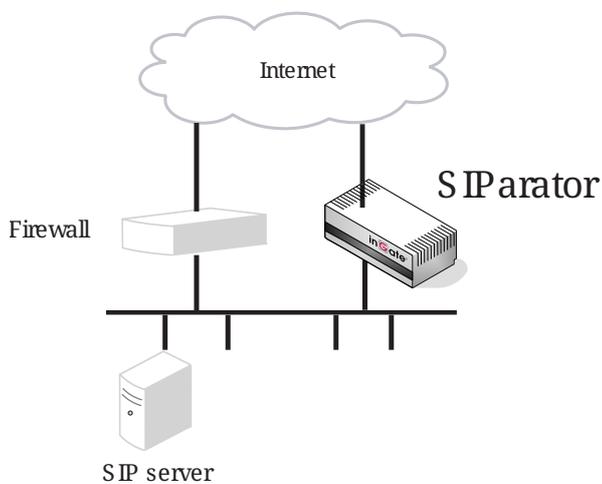
SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.25. Standalone SIParator, SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the unit. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the unit, which in turn will forward the SIP traffic to the server.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.25.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool.

<b>Basic</b>	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
<b>SIP Module</b> <a href="#">(Help)</a>							
<input checked="" type="radio"/> Enable SIP module							
<input type="radio"/> Disable SIP module							

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:

Log class for SIP packets:

Log class for SIP license messages:

Log class for SIP errors:

Log class for SIP media messages:

Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

## 20.25.2. Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the unit, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The unit will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.

SIP Methods   Filtering   Local Registrar   Authentication and Accounting   SIP Accounts   Dial Plan   **Routing**   SIP Status   IDS/IPS   IDS/IPS Status

**DNS Override For SIP Requests** [\(Help\)](#)

Edit Row	Domain	Relay To						Delete Row
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
<input type="checkbox"/>	+ ingate.com	10.47.2.246	10.47.2.246	5060	UDP			<input type="checkbox"/>

## 20.25.3. Interoperability

If Windows Messenger is used for SIP communication, you need to set a parameter on the **Interoperability** page. Set lr=true status to On under **Loose routing**.

Basic   SIP Encryption   **Interoperability**   Sessions and Media   Remote SIP Connectivity   V Sur

**Loose Routing** [\(Help\)](#)

Use lr

Use lr=true

If the SIP server is an LCS (Live Communications Server) or some other server that does not accept more than one Via header in SIP packets, you must enter the SIP server IP address in the **Remove Via Headers** table. This will make the unit strip SIP packets of extra Via headers when it sends those packets to the server, and add the Via headers when the response packets are received.

**Remove Via Headers** [\(Help\)](#)

SIP Server		Delete Row
DNS Name or IP Address	IP Address	
<input type="button" value="Add new rows"/> <input type="text" value="1"/> ROWS.		
<input type="checkbox"/> Remove Via Headers for all SIP servers		

### 20.25.4. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing SIP Status IDS/IPS Status

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="button" value="Add new rows"/> <input type="text" value="1"/> rows.				

**Default Policy For SIP Requests**

- Process all
- Local only
- Reject all

### 20.25.5. Basic Configuration

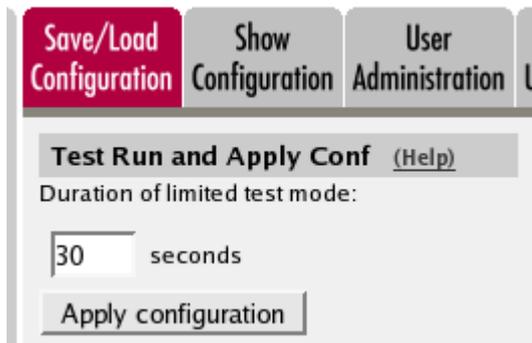
If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

**DNS Servers** [\(Help\)](#)

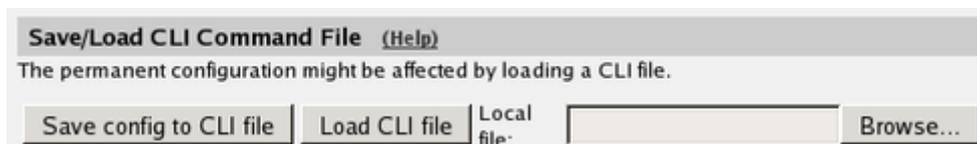
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>
<input type="button" value="Add new rows"/> <input type="text" value="1"/> rows.				

## 20.25.6. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 20.25.7. Client Settings

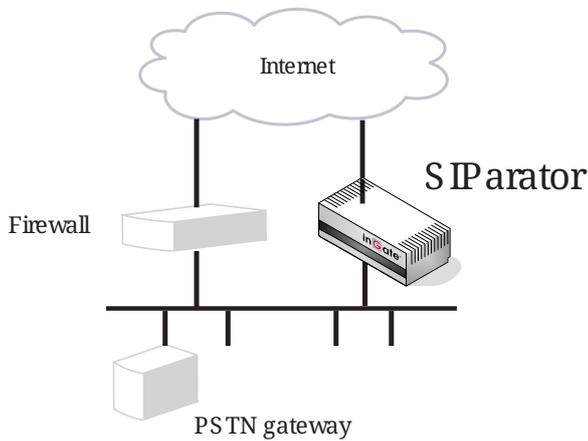
SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.26. Standalone SIParator, SIP server in the SIParator, PSTN gateway inside

You might want to have most SIP functions in one box. The Ingate SIParator/Firewall can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.

A function not included in the unit is to connect to the PSTN network. If you want to do this, you must use a PSTN gateway.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.26.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool.

Basic
Signaling Encryption
Media Encryption
Interoperability
Sessions and Media
Remote SIP Connectivity
VoIP Survival
VoIP Survival Status

**SIP Module** [\(Help\)](#)

Enable SIP module

Disable SIP module

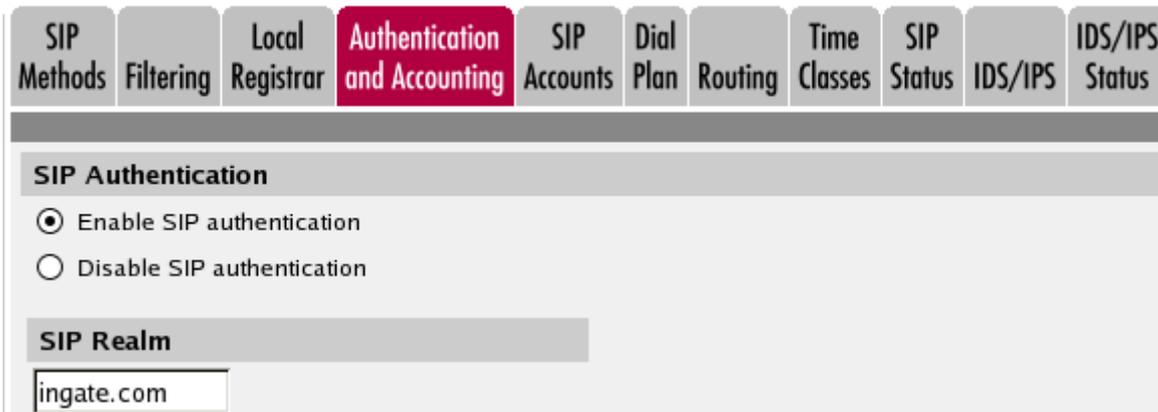
**SIP Logging** [\(Help\)](#)

<p>Log class for SIP signaling:</p> <p><input type="text" value="Local"/> ▼</p> <p>Log class for SIP license messages:</p> <p><input type="text" value="Local"/> ▼</p> <p>Log class for SIP media messages:</p> <p><input type="text" value="Local"/> ▼</p> <p>Log class for SIP IDS/IPS:</p> <p><input type="text" value="Local"/> ▼</p>	<p>Log class for SIP packets:</p> <p><input type="text" value="Local"/> ▼</p> <p>Log class for SIP errors:</p> <p><input type="text" value="Local"/> ▼</p> <p>Log class for SIP debug messages:</p> <p><input type="text" value="Local"/> ▼</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Hide sensitive data:  Yes  No

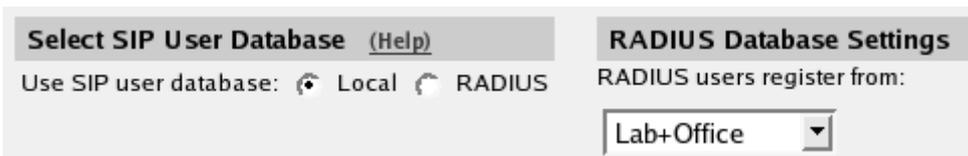
## 20.26.2. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.



The screenshot shows a configuration interface with several tabs: SIP Methods, Filtering, Local Registrar, Authentication and Accounting (selected), SIP Accounts, Dial Plan, Routing, Time Classes, SIP Status, IDS/IPS, and IDS/IPS Status. Below the tabs, the 'SIP Authentication' section has two radio buttons: 'Enable SIP authentication' (selected) and 'Disable SIP authentication'. The 'SIP Realm' section has a text input field containing 'ingate.com'.

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.



The screenshot shows two sections: 'Select SIP User Database (Help)' and 'RADIUS Database Settings'. In the first section, 'Use SIP user database:' has two radio buttons: 'Local' (selected) and 'RADIUS'. In the second section, 'RADIUS users register from:' has a dropdown menu with 'Lab+Office' selected.

## 20.26.3. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

## 20.26.4. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

**Local Registrar** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database <a href="#">(Help)</a>						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

## 20.26.5. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also the [RADIUS](#) section for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIPerator Type
<b>RADIUS Servers</b> <a href="#">(Help)</a>							
Edit Row	RADIUS Server		Port	Secret	Delete Row		
	DNS Name or IP Address	IP Address					
<input type="checkbox"/>	193.180.23.239	193.180.23.239	1812		<input type="checkbox"/>		
Add new rows		<input type="text" value="1"/>	rows.				

## 20.26.6. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to Process all.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

Create rules for traffic from the inside (Process all) and the DMZ (Reject all). Let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.26.7. Routing

To redirect traffic to the PSTN network, you can use the **Dial Plan**. You can state that all SIP traffic to user names that consist of digits only (that is, the user names are phone numbers) to be redirected to the local PSTN gateway. You can also direct different numbers to different gateways.

If there are SIP clients which can't use authentication for INVITE (the method used to start calls), you can except these from authentication when calling to PSTN. Select the network for these clients in the **Matching From Header** table and create a row in the **Dial Plan** table, where Forward is selected as the **Action** (which means that authentication is not required).

**Matching From Header** (Help)

Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

In the example below, all phone numbers beginning with 01146 or +46 are redirected to a server in Sweden, numbers beginning with 01144 or +44 are redirected to a server in England, and calls to all other phone numbers are directed to the local PSTN gateway. Note that the table is read from the top and down, and the first matching row is used to route the call.

You should also restrict the redirections to only calls for local domains. Enter "\*local" under **Domain** when creating patterns in the **Matching Request-URI** table.

**Matching Request-URI** (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	Any number			0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden1		01146	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden2		+46	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK1		01144	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK2		+44	0..9		*local		<input type="checkbox"/>

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ Local PSTN	1	-	pstn.us.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ London PSTN	1	-	pstn.uk.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ Stockholm PSTN	1	-	pstn.sthlm.ingate.com		UDP		<input type="checkbox"/>

To prevent unauthorized use of your PSTN gateway, you should require authentication for all these redirections. Select **Auth&Forward** as the **Action** to manage this.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	Office	UK1	Forward	London PSTN			-	-	Redirect calls to UK	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	UK2	Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	3	-	UK1	Auth & Forward	London PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	4	-	UK2	Auth & Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	5	Office	Sweden1	Forward	Stockholm PSTN			-	-	Redirect calls to Sweden	<input type="checkbox"/>
<input type="checkbox"/>	6	Office	Sweden2	Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	7	-	Sweden1	Auth & Forward	Stockholm PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	8	-	Sweden2	Auth & Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	9	Office	Any number	Forward	Local PSTN			-	-	Redirect to local PSTN	<input type="checkbox"/>
<input type="checkbox"/>	10	-	Any number	Auth & Forward	Local PSTN			-	-	Auth if not from Office	<input type="checkbox"/>

## 20.26.8. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

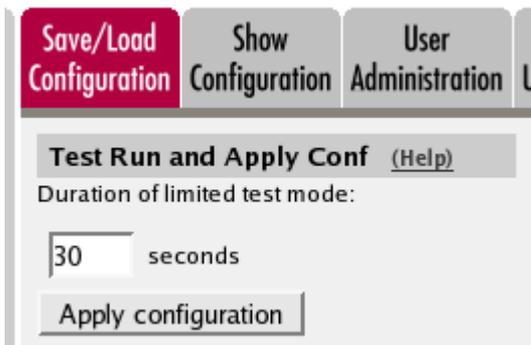
This setting is made by the Startup Tool.

DNS Servers (Help)				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

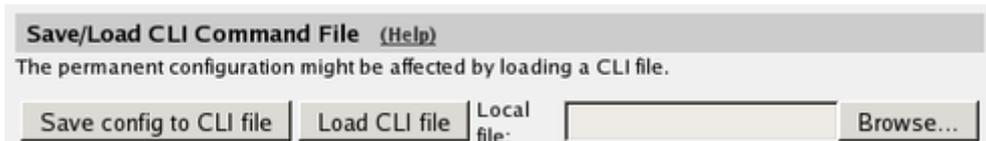
Add new rows  rows.

## 20.26.9. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



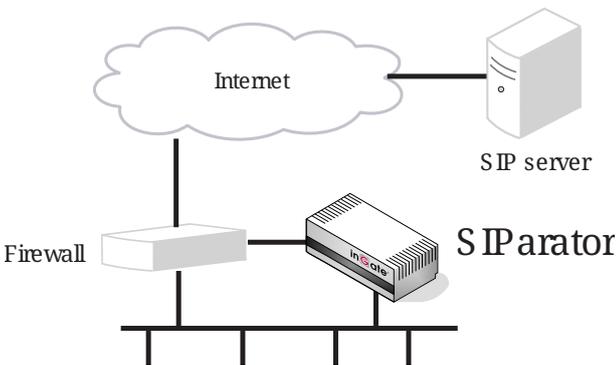
### 20.26.10. Client Settings

SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.27. DMZ/LAN SIParator, SIP server on the WAN

The simplest SIP scenario is when the SIP server is managed by someone else, and the unit SIP function is only used to traverse NAT.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.27.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool.

[Basic](#)
[Signaling Encryption](#)
[Media Encryption](#)
[Interoperability](#)
[Sessions and Media](#)
[Remote SIP Connectivity](#)
[VoIP Survival](#)
[VoIP Survival Status](#)

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling: 
 Log class for SIP packets:

Log class for SIP license messages: 
 Log class for SIP errors:

Log class for SIP media messages: 
 Log class for SIP debug messages:

Log class for SIP IDS/IPS:

Hide sensitive data:  Yes  No

## 20.27.2. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool.

[SIP Methods](#)
[Filtering](#)
[Local Registrar](#)
[Authentication and Accounting](#)
[SIP Accounts](#)
[Dial Plan](#)
[Routing](#)
[SIP Status](#)
[IDS/IPS](#)
[IDS/IPS Status](#)

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
Add new rows <input type="text" value="1"/> rows.				

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.27.3. Routing

On the **Routing** page, you can enter the SIP server managing your SIP domain. Enter the name or IP address of the SIP server under **Outbound proxy**.

If you enter the server name here, all SIP traffic from the inside will be directed to this server, regardless of where it is bound to.

Outbound Proxy <a href="#">(Help)</a>						
Edit Row	From Domain	Request-URI Domain	Domain or IP Address	Port	Gateway	Delete Row
<input type="checkbox"/>	*	*	3.22.39.7	5060	-	<input type="checkbox"/>

## 20.27.4. Basic Configuration

If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

DNS Servers <a href="#">(Help)</a>				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.27.5. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

<b>Save/Load Configuration</b>	Show Configuration	User Administration	U
<b>Test Run and Apply Conf</b> <a href="#">(Help)</a>			
Duration of limited test mode:			
<input type="text" value="30"/>	seconds		
<input type="button" value="Apply configuration"/>			

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

<b>Save/Load CLI Command File</b> <a href="#">(Help)</a>			
The permanent configuration might be affected by loading a CLI file.			
<input type="button" value="Save config to CLI file"/>	<input type="button" value="Load CLI file"/>	Local file: <input type="text"/>	<input type="button" value="Browse..."/>

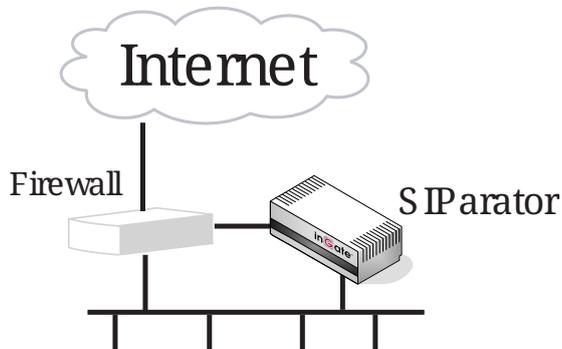
## 20.27.6. Client Settings

SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.28. DMZ/LAN SIParator, SIP server in the SIParator

You might want to have most SIP functions in one box. The Ingate SIParator/Firewall can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.28.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool.

<b>Basic</b>	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
<b>SIP Module</b> <a href="#">(Help)</a>							
<input checked="" type="radio"/> Enable SIP module							
<input type="radio"/> Disable SIP module							

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:  ▼

Log class for SIP packets:  ▼

Log class for SIP license messages:  ▼

Log class for SIP errors:  ▼

Log class for SIP media messages:  ▼

Log class for SIP debug messages:  ▼

Log class for SIP IDS/IPS:  ▼

Hide sensitive data:  Yes  No

## 20.28.2. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.

SIP Methods Filtering Local Registrar **Authentication and Accounting** SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**SIP Authentication**

Enable SIP authentication

Disable SIP authentication

**SIP Realm**

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.

**Select SIP User Database** [\(Help\)](#)

Use SIP user database:  Local  RADIUS

**RADIUS Database Settings**

RADIUS users register from:  ▼

## 20.28.3. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

## 20.28.4. Local Registrar

On the Local Registrar page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

**Local Registrar** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database (Help)						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

## 20.28.5. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also the [RADIUS](#) section for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIPerator Type
<b>RADIUS Servers (Help)</b>							
Edit Row	RADIUS Server		Port	Secret	Delete Row		
	DNS Name or IP Address	IP Address					
<input type="checkbox"/>	193.180.23.239	193.180.23.239	1812		<input type="checkbox"/>		
Add new rows		<input type="text" value="1"/>	rows.				

## 20.28.6. Filtering

On the **Filtering** page, you set Proxy rules. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to **Process all**.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

Create rules for traffic from the inside (Process all) and let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

## 20.28.7. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool.

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="text" value="1"/>	-	<input type="text" value="172.16.0.3"/>	172.16.0.3	<input type="checkbox"/>
<input type="text" value="2"/>	-	<input type="text" value="10.47.3.201"/>	10.47.3.201	<input type="checkbox"/>
<input type="text" value="3"/>	Internet	<input type="text"/>	Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.28.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** Show Configuration User Administration U

**Test Run and Apply Conf** (Help)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** (Help)

The permanent configuration might be affected by loading a CLI file.

Local file:

## 20.28.9. Client Settings

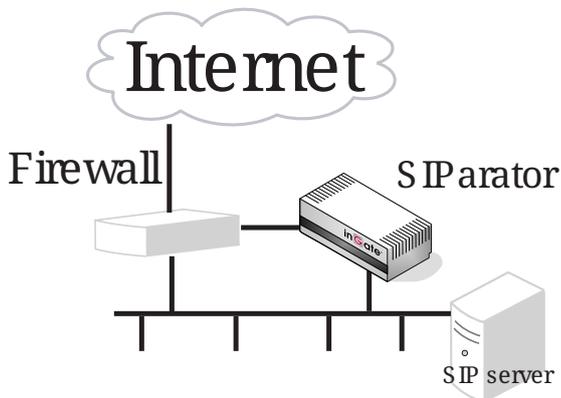
SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.29. DMZ/LAN SIParator, SIP server on the LAN

For various reasons, you might want to use a separate SIP server instead of the built-in server in the unit. That SIP server would be located on the inside or maybe on a DMZ.

If the SIP server is located on a NATed network, DNS queries for the SIP domain should point to the unit, which in turn will forward the SIP traffic to the server.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.29.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool.

<b>Basic</b>	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
<b>SIP Module</b> <a href="#">(Help)</a>							
<input checked="" type="radio"/> Enable SIP module							
<input type="radio"/> Disable SIP module							

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:  ▼

Log class for SIP license messages:  ▼

Log class for SIP media messages:  ▼

Log class for SIP IDS/IPS:  ▼

Log class for SIP packets:  ▼

Log class for SIP errors:  ▼

Log class for SIP debug messages:  ▼

Hide sensitive data:  Yes  No

## 20.29.2. Routing

If the SIP server is located on a NATed network, all SIP traffic from the outside will be directed to the unit, which must know where to forward it.

One way to do this is to enter the SIP domain in the **DNS Override For SIP Requests** table on the **Routing** page, to link the SIP server IP address to the name. The unit will look up the domain here instead of in the DNS server, and send the SIP traffic to the correct IP address.

SIP Methods   Filtering   Local Registrar   Authentication and Accounting   SIP Accounts   Dial Plan   **Routing**   SIP Status   IDS/IPS   IDS/IPS Status

**DNS Override For SIP Requests** [\(Help\)](#)

Edit Row	Domain	Relay To						Delete Row
		DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
<input type="checkbox"/>	+ ingate.com	10.47.2.246	10.47.2.246	5060	UDP			<input type="checkbox"/>

## 20.29.3. Interoperability

If Windows Messenger is used for SIP communication, you need to set a parameter on the **Interoperability** page. Set lr=true status to On under **Loose routing**.

Basic   SIP Encryption   **Interoperability**   Sessions and Media   Remote SIP Connectivity   V Sur

**Loose Routing** [\(Help\)](#)

Use lr

Use lr=true

If the SIP server is an LCS (Live Communications Server) or some other server that does not accept more than one Via header in SIP packets, you must enter the SIP server IP address in the **Remove Via Headers** table. This will make the unit strip SIP packets of extra Via headers when it sends those packets to the server, and add the Via headers when the response packets are received.

**Remove Via Headers** [\(Help\)](#)

SIP Server		Delete Row
DNS Name or IP Address	IP Address	
<input type="button" value="Add new rows"/> <input type="text" value="1"/> ROWS.		
<input type="checkbox"/> Remove Via Headers for all SIP servers		

### 20.29.4. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the **Filtering** page.

As the unit does not manage any SIP domains, there are no Local SIP Domains. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool.

**Proxy Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="button" value="Add new rows"/> <input type="text" value="1"/> rows.				

**Default Policy For SIP Requests**

- Process all
- Local only
- Reject all

### 20.29.5. Basic Configuration

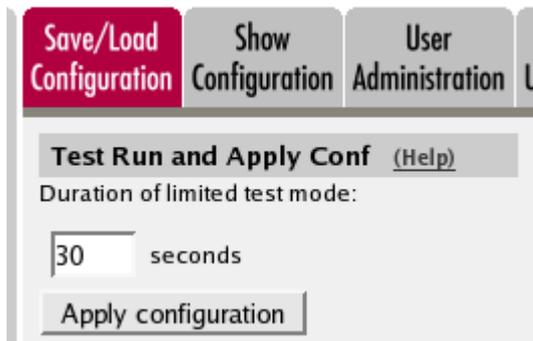
If no Outbound proxy is entered, the unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

**DNS Servers** [\(Help\)](#)

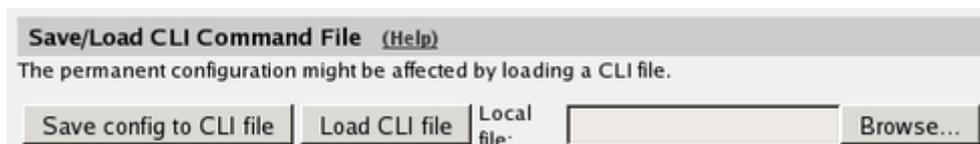
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>
<input type="button" value="Add new rows"/> <input type="text" value="1"/> rows.				

## 20.29.6. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 20.29.7. Client Settings

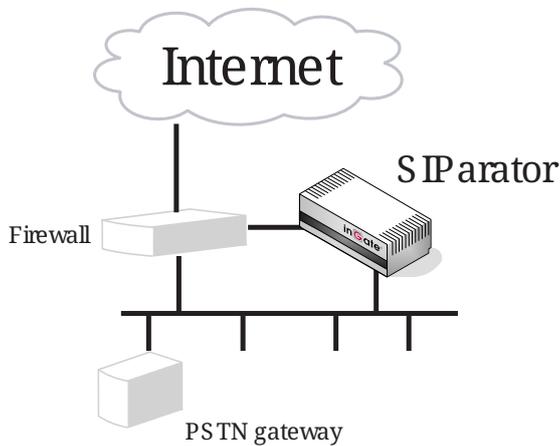
SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.30. DMZ/LAN SIParator, SIP server in the SIParator, PSTN gateway inside

You might want to have most SIP functions in one box. The Ingate SIParator/Firewall can manage most common SIP functions, like user registration, SIP traffic routing and rewriting of NATed packets.

A function not included in the unit is to connect to the PSTN network. If you want to do this, you must use a PSTN gateway.

Note that the unit must have a public (non-NATed) IP address for the SIP signaling to work correctly.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

### 20.30.1. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool.

<b>Basic</b>	Signaling Encryption	Media Encryption	Interoperability	Sessions and Media	Remote SIP Connectivity	VoIP Survival	VoIP Survival Status
--------------	----------------------	------------------	------------------	--------------------	-------------------------	---------------	----------------------

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:	Log class for SIP packets:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP license messages:	Log class for SIP errors:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP media messages:	Log class for SIP debug messages:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP IDS/IPS:	
<input type="text" value="Local"/>	

Hide sensitive data:  Yes  No

## 20.30.2. Authentication and Accounting

If the unit should handle user registration, it should require that users authenticate themselves. Go to the **Authentication and Accounting** page and turn SIP authentication on. Enter your SIP domain as the **Realm**.

The screenshot shows a configuration interface with several tabs: SIP Methods, Filtering, Local Registrar, Authentication and Accounting (selected), SIP Accounts, Dial Plan, Routing, Time Classes, SIP Status, IDS/IPS, and IDS/IPS Status. Below the tabs, the 'SIP Authentication' section has two radio buttons: 'Enable SIP authentication' (selected) and 'Disable SIP authentication'. The 'SIP Realm' section has a text input field containing 'ingate.com'.

Then, select where the SIP user database is. If you run a RADIUS server, you can let the unit use that for user authentication. Usually a local database is used.

The screenshot shows two sections: 'Select SIP User Database (Help)' and 'RADIUS Database Settings'. In the first section, 'Use SIP user database:' has two radio buttons: 'Local' (selected) and 'RADIUS'. In the second section, 'RADIUS users register from:' has a dropdown menu with 'Lab+Office' selected.

## 20.30.3. SIP Methods

Go to the **SIP Methods** page under **SIP Traffic**. You should require authentication of the REGISTER method for local domains. This means that if a user tries to register on your SIP domain, the unit will ask for authentication. Calls and instant messages can then be sent without further authentication.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**SIP Methods** (Help)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PUBLISH	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	UPDATE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

### 20.30.4. Local Registrar

On the **Local Registrar** page, you define which SIP domains are managed by the unit. If you selected to use a local database for SIP users, you enter the users here.

Create a new row in the **Local SIP Domains** table and enter your SIP domain.

SIP Methods Filtering Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Local SIP Domains** (Help)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

Add new rows  rows.

Then, create the local SIP user database. Enter all user names, passwords, and from which network they are allowed to register.

If you selected to use a RADIUS server, you don't need to fill in the local database.

Local SIP User Database (Help)						
Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	sip.ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	sip.ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	sip.ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	sip.ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	sip.ingate.com			Office network	<input type="checkbox"/>

### 20.30.5. RADIUS

If you selected to use an external RADIUS server for the SIP user authentication, you must instead enter the name or IP address of that server. This is done on the **RADIUS** page under **Basic Configuration**. See also the [RADIUS](#) section for more information on how the RADIUS server should be configured for SIP authentication.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIPerator Type
<b>RADIUS Servers (Help)</b>							
Edit Row	RADIUS Server		Port	Secret	Delete Row		
	DNS Name or IP Address	IP Address					
<input type="checkbox"/>	193.180.23.239	193.180.23.239	1812		<input type="checkbox"/>		
Add new rows		<input type="text" value="1"/>	rows.				

### 20.30.6. Filtering

On the **Filtering** page, you set **Proxy rules**. If the unit should process all SIP traffic regardless of sender or receiver, you only need to set the Default policy for requests under **Proxy rules** to **Process all**.

Usually, you want to assign different privileges to different groups of users. One fairly standard configuration is to allow users on the local network to communicate with users on any SIP domain, but SIP traffic from the outside should only be processed if it bound to a local SIP domain.

There should be no SIP requests originating from the DMZ network (if there are, it is fairly safe to suppose that a server on the network was used by a cracker). Set the policy for the DMZ network to **Reject all**.

Create rules for traffic from the inside (Process all) and the DMZ (Reject all). Let the Default policy for requests be Local only, which means that SIP traffic from other networks will only be processed if it is bound to a local domain.

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

### 20.30.7. Routing

To redirect traffic to the PSTN network, you can use the **Dial Plan**. You can state that all SIP traffic to user names that consist of digits only (that is, the user names are phone numbers) to be redirected to the local PSTN gateway. You can also direct different numbers to different gateways.

If there are SIP clients which can't use authentication for INVITE (the method used to start calls), you can except these from authentication when calling to PSTN. Select the network for these clients in the **Matching From Header** table and create a row in the **Dial Plan** table, where Forward is selected as the Action (which means that authentication is not required).

**Matching From Header** (Help)

Edit Row	Name	Use This ...		... Or This	Transport	Network	Delete Row
		Username	Domain	Reg Expr			
<input type="checkbox"/>	Office	*	*		TCP or TLS	Office network	<input type="checkbox"/>

In the example below, all phone numbers beginning with 01146 or +46 are redirected to a server in Sweden, numbers beginning with 01144 or +44 are redirected to a server in England, and calls to all other phone numbers are directed to the local PSTN gateway. Note that the table is read from the top and down, and the first matching row is used to route the call.

You should also restrict the redirections to only calls for local domains. Enter "\*local" under **Domain** when creating patterns in the **Matching Request-URI** table.

**Matching Request-URI** (Help)

Edit Row	Name	Use This ...					... Or This	Delete Row
		Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
<input type="checkbox"/>	Any number			0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden1		01146	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	Sweden2		+46	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK1		01144	0..9		*local		<input type="checkbox"/>
<input type="checkbox"/>	UK2		+44	0..9		*local		<input type="checkbox"/>

Forward To (Help)								
Edit Row	Name	Subno.	Use This ...	... Or This			... Or This	Delete Row
			Account	Replacement Domain	Port	Transport	Reg Expr	
<input type="checkbox"/>	+ Local PSTN	1	-	pstn.us.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ London PSTN	1	-	pstn.uk.ingate.com		-		<input type="checkbox"/>
<input type="checkbox"/>	+ Stockholm PSTN	1	-	pstn.sthlm.ingate.com		UDP		<input type="checkbox"/>

To prevent unauthorized use of your PSTN gateway, you should require authentication for all these redirections. Select **Auth&Forward** as the **Action** to manage this.

Dial Plan (Help)											
Edit Row	No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
						Forward	ENUM				
<input type="checkbox"/>	1	Office	UK1	Forward	London PSTN			-	-	Redirect calls to UK	<input type="checkbox"/>
<input type="checkbox"/>	2	Office	UK2	Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	3	-	UK1	Auth & Forward	London PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	4	-	UK2	Auth & Forward	London PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	5	Office	Sweden1	Forward	Stockholm PSTN			-	-	Redirect calls to Sweden	<input type="checkbox"/>
<input type="checkbox"/>	6	Office	Sweden2	Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	7	-	Sweden1	Auth & Forward	Stockholm PSTN			-	-	Auth if not from Office	<input type="checkbox"/>
<input type="checkbox"/>	8	-	Sweden2	Auth & Forward	Stockholm PSTN			-	-		<input type="checkbox"/>
<input type="checkbox"/>	9	Office	Any number	Forward	Local PSTN			-	-	Redirect to local PSTN	<input type="checkbox"/>
<input type="checkbox"/>	10	-	Any number	Auth & Forward	Local PSTN			-	-	Auth if not from Office	<input type="checkbox"/>

## 20.30.8. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

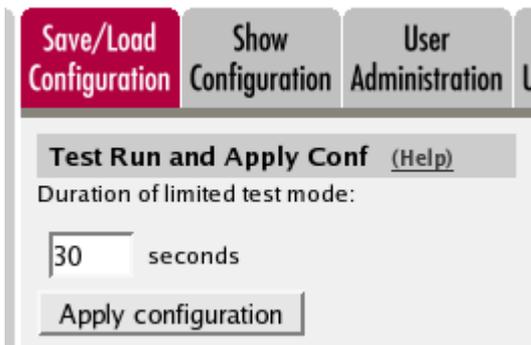
This setting is made by the Startup Tool.

DNS Servers (Help)				
No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

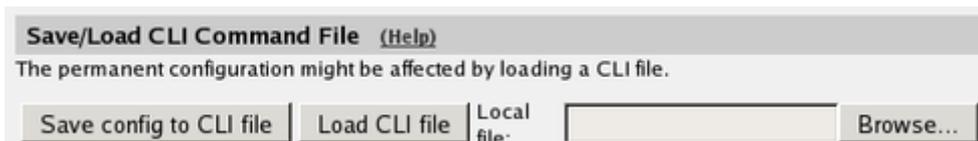
Add new rows  rows.

## 20.30.9. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



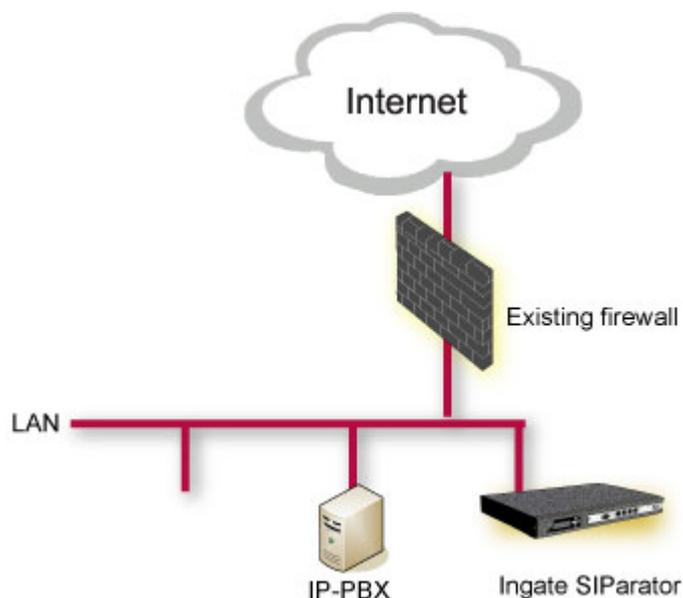
### 20.30.10. Client Settings

SIP clients will use the unit as their outgoing SIP proxy and the SIP domain as the registrar.

## 20.31. LAN SIParator

For various reasons, you might want to use a separate SIP server instead of the built-in server in the unit. That SIP server would be located on the inside or maybe on a DMZ.

With the LAN SIParator, you connect the unit to a NATed network.



Here are the settings needed for this. It is assumed that the unit already has a network configuration. Only the additional SIP settings are listed.

*In the instructions below, some settings are marked like this*

This setting is made by the Startup Tool

This means that if you started by configuring your unit using the Ingate Startup Tool, this setting will already be correct.

### 20.31.1. Networks and Computers

The unit must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the unit should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

This setting is made by the Startup Tool

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ LAN	-	192.168.50.0	192.168.50.0	192.168.50.255	192.168.50.255	-	<input type="checkbox"/>

### 20.31.2. Topology

To make the unit aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network. When you are finished, there should be one line for each of your *firewall's* network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the *firewall*.

For DMZ, Manual and LAN SIParators, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

This setting is made by the Startup Tool

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Tunnels | **Topology**

### Surroundings [\(Help\)](#)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
LAN	-	<input type="checkbox"/>

Add new rows  rows.

### 20.31.3. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

**Basic** | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VoIP Survival | VoIP Survival Status

### SIP Module [\(Help\)](#)

- Enable SIP module
- Disable SIP module

### SIP Logging [\(Help\)](#)

Log class for SIP signaling:	Log class for SIP packets:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP license messages:	Log class for SIP errors:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP media messages:	Log class for SIP debug messages:
<input type="text" value="Local"/>	<input type="text" value="Local"/>
Log class for SIP IDS/IPS:	
<input type="text" value="Local"/>	

Hide sensitive data:  Yes  No

### 20.31.4. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the

Filtering page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select Process all for this setting.

This setting is made by the Startup Tool

**SIP Methods** **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS Status

**Sender IP Filter Rules** (Help)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all  
 Local only  
 Reject all

### 20.31.5. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool

**DNS Servers** (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

### 20.31.6. Remote SIP Connectivity

If you have remote SIP clients behind other NAT boxes, you need to activate **Remote NAT Traversal**.

**Remote NAT Traversal** [\(Help\)](#)

Enable Remote NAT Traversal  
 Disable Remote NAT Traversal

IP address for remote clients: 
                                         
 Forward signaling from IP address:

IP port for remote clients:

NAT keepalive method:
                                         
 Media Route:

Use OPTIONS
                                         
 Route media directly between clients behind the same NAT  
 Use short registration times
                                         
 Always route media through the SIParator  
 Use both OPTIONS and short registration times

NAT timeout for UDP:

seconds

NAT timeout for TCP:

seconds

### 20.31.7. Interoperability

You need to enter the public IP that corresponds to the unit under **Public IP address for NATed SIParator**. This will make the unit able to rewrite outgoing SIP packets properly.

This setting is made by the Startup Tool

**Keep User-Agent Header When Acting as B2BUA** [\(Help\)](#)

Use Ingate SIParator as User-Agent header  
 Keep existing User-Agent header

### 20.31.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

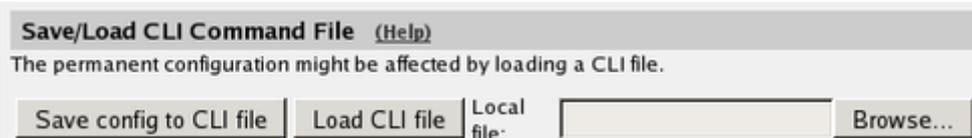
[Save/Load Configuration](#)
[Show Configuration](#)
[User Administration](#)

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 20.31.9. The Firewall

The firewall in front of the LAN SIParator must be configured in this way:

- There must be a static IP address that can be mapped to the unit's private IP address. All traffic to this IP address must be forwarded to the unit.
- When the *firewall* forwards traffic to the unit, it must not NAT this traffic, i.e. the unit needs to see the original sender IP address.
- All outgoing traffic from the unit should be allowed through the *firewall*.
- For outgoing traffic from the unit, the *firewall* needs to use the same IP address as above when performing NAT. If another IP address is used, some SIP signaling will go awry, and Remote SIP Connectivity will not always work properly.
- For outgoing traffic from the unit the *firewall* must not change sender port when performing NAT. If it does change port, Remote SIP Connectivity will not always work properly.

## 20.32. WAN SIParator

With the WAN SIParator, you connect the unit to a public network and to your *firewall's* outside. The other interfaces can be connected to LANs, DMZs or other networks, which can be NATed.

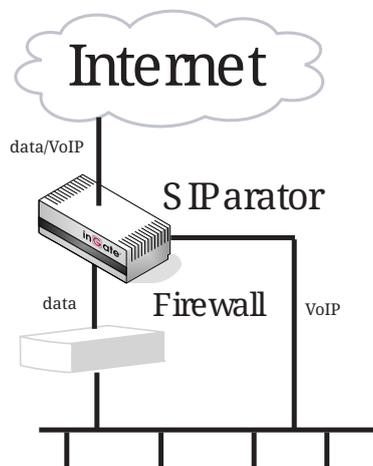


Figure 5. WAN SIParator connected to a LAN.

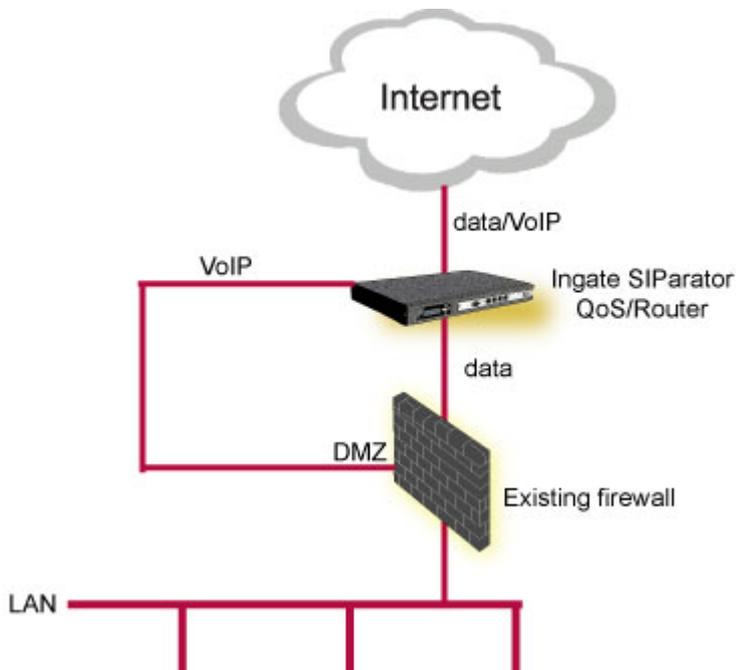


Figure 6. WAN SIParator connected to a DMZ.

### 20.32.1. Networks and Computers

The unit must know the network structure to be able to function properly. On the **Networks and Computers** page, you define all networks which the unit should serve and which are not reached through the default gateway of the *firewall*. All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network.

You can also define networks and parts of networks for other configuration purposes.

This setting is made by the Startup Tool

Networks and Computers		Default Gateways	All Interfaces	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE	Topology
<b>Networks and Computers</b>													
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row					
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address							
<input type="checkbox"/>	+ LAN	-	192.168.50.0	192.168.50.0	192.168.50.255	192.168.50.255	-	<input type="checkbox"/>					

### 20.32.2. Topology

To make the unit aware of the network structure, the networks defined above should be listed on the **Topology** page.

Settings in the **Surroundings** table are only required when the unit has been made the **DMZ** or the **Manual** type.

The unit must know what the networks around it look like. On this page, you list all networks which the unit should serve and which are not reached through the default gateway of the *firewall*.

All computers that can reach each other without having to go through the *firewall* connected to the unit should be grouped in one network. When you are finished, there should be one line for each of your *firewall*'s network connections (not counting the default gateway).

One effect of this is that traffic between two users on different networks, or between one of the listed networks and a network not listed here, is NAT:ed.

Another effect is that for connections between two users on the same network, or on networks where neither is listed in Topology, no ports for RTP sessions will be opened, since the unit assumes that they are both on the same side of the *firewall*.

For DMZ, Manual and LAN SIParators, at least one network should be listed here. If no networks are listed, the unit will not perform NAT for any traffic.

This setting is made by the Startup Tool

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Eth4 | Eth5 | Interface Status | PPPoE | Tunnels | **Topology**

**Surroundings** (Help)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
LAN	-	<input type="checkbox"/>

Add new rows  ROWS.

### 20.32.3. Basic

Go to the **Basic** page under **SIP Services** and turn the SIP module on. Here you also select log classes for SIP event logging.

This setting is made by the Startup Tool

**Basic** | Signaling Encryption | Media Encryption | Interoperability | Sessions and Media | Remote SIP Connectivity | VoIP Survival | VoIP Survival Status

**SIP Module** (Help)

- Enable SIP module
- Disable SIP module

**SIP Logging** [\(Help\)](#)

Log class for SIP signaling:  ▼

Log class for SIP packets:  ▼

Log class for SIP license messages:  ▼

Log class for SIP errors:  ▼

Log class for SIP media messages:  ▼

Log class for SIP debug messages:  ▼

Log class for SIP IDS/IPS:  ▼

Hide sensitive data:  Yes  No

### 20.32.4. Filtering

To allow SIP traffic through the unit, you must change the **Default Policy For SIP Requests** on the Filtering page.

As the unit does not manage any SIP domains, there are no **Local SIP Domains**. This means that you must select **Process all** for this setting.

This setting is made by the Startup Tool

SIP Methods **Filtering** Local Registrar Authentication and Accounting SIP Accounts Dial Plan Routing Time Classes SIP Status IDS/IPS IDS/IPS Status

**Sender IP Filter Rules** [\(Help\)](#)

Edit Row	No.	From Network	Action	Delete Row
<input type="checkbox"/>	1	Lab+Office	Process all	<input type="checkbox"/>
<input type="checkbox"/>	2	DMZ	Reject all	<input type="checkbox"/>

Add new rows  rows.

**Default Policy For SIP Requests**

Process all

Local only

Reject all

### 20.32.5. Basic Configuration

The unit must be able to look up SIP domains in DNS. DNS servers are entered on the **Basic Configuration** page under **Basic Configuration**.

This setting is made by the Startup Tool

**DNS Servers** [\(Help\)](#)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.16.0.3	172.16.0.3	<input type="checkbox"/>
2	-	10.47.3.201	10.47.3.201	<input type="checkbox"/>
3	Internet		Internet	<input type="checkbox"/>

Add new rows  rows.

## 20.32.6. Remote SIP Connectivity

If you have remote SIP clients behind other NAT boxes, you need to activate **Remote NAT Traversal**.

**Remote NAT Traversal** [\(Help\)](#)

Enable Remote NAT Traversal  
 Disable Remote NAT Traversal

IP address for remote clients: 
                                         
 Forward signaling from IP address:

IP port for remote clients:

NAT keepalive method:
                                         
 Media Route:

Use OPTIONS
                                         
 Route media directly between clients behind the same NAT  
 Use short registration times
                                         
 Always route media through the SIParator  
 Use both OPTIONS and short registration times

NAT timeout for UDP:

seconds

NAT timeout for TCP:

seconds

## 20.32.7. Interoperability

You need to enter the public IP that corresponds to the unit under **Public IP address for NATed SIParator**. This will make the unit able to rewrite outgoing SIP packets properly.

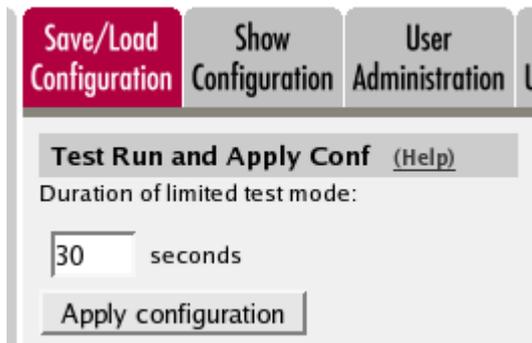
This setting is made by the Startup Tool

**Keep User-Agent Header When Acting as B2BUA** [\(Help\)](#)

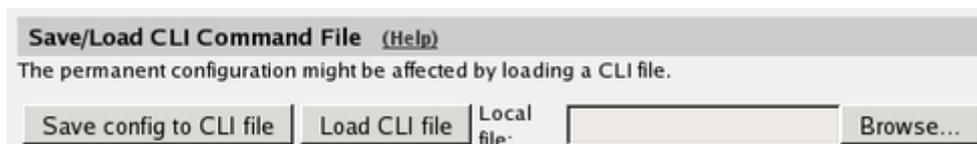
Use Ingate SIParator as User-Agent header  
 Keep existing User-Agent header

## 20.32.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 20.33. Manual SIParator

The Manual SIParator type is designed to be flexible and fit various scenarios and network environments.

Using this configuration, the unit is connected to one or more networks. All the networks that you want to handle must be added to the Surroundings table (found on the [Topology](#) page). If you have default gateways defined, the outside world will be automatically configured.

An example of how the Manual SIParator can be used is found in the howto [SIP communication and road warriors](#).

## 20.34. WebRTC

The Ingate unit supports making calls from a WebRTC enabled web browser. The unit handles the interoperability in both the signaling and media plane.

The unit has support for the WebSocket protocol as a transport for SIP. It can terminate ICE and DTLS-SRTP. Techniques used by WebRTC clients but not supported by all SIP endpoints. This makes it possible for a JavaScript SIP client, running in a web browser, to make calls to SIP endpoints that do not support WebRTC.

It is thus possible to WebRTC-enable current SIP equipment and add features like Click-To-Call to a web page.

Configure the unit for WebRTC:

- Enable the [SIP Module](#).

- Configure Signaling Encryption, see [How To Configure TLS](#).
- Add [SIP Signaling Ports](#) for WebSockets over TLS (WSS).
- Set up [Allowed Origins for SIP over WebSocket](#).
- Configure Media Encryption.
- Enable the [Media Proxy](#) on the [Sessions and Media](#) page.
- Enable [ICE termination](#) and [RTCP-MUX termination](#).
- Allow multiple sender IP addresses and ports, see [Media Configuration](#) on the [Sessions and Media](#) page.
- Set [Always Relay Media](#) on the [Sessions and Media](#) page.
- Set [Use RTCP Attribute in SDP](#) on the [Interoperability](#) page.
- Set [Strip ICE Attributes](#) on the [Interoperability](#) page.

SIP Signaling Ports <a href="#">(Help)</a>					
Active	Port	Transport	Intercept	Comment	Delete Row
Yes ▾	443	WSS ▾	No ▾		<input type="checkbox"/>
Yes ▾	5060	UDP and TCP ▾	Yes ▾	Standard SIP port	<input type="checkbox"/>
No ▾	5061	TLS ▾	Yes ▾	Standard TLS port	<input type="checkbox"/>

Add new rows  rows.

Figure 7. SIP signaling port for WSS.

### 20.34.1. Media Encryption

WebRTC uses DTLS-SRTP for media encryption. If the other endpoint doesn't support DTLS-SRTP the unit can be configured to do media encryption transcoding. See the [Media Encryption](#) page.

In this example we use the [Require TLS](#) setting to separate WebRTC clients from cleartext clients.

- Allow transcoding.
- Require TLS for all cryptos but cleartext.
- Prefer RTP/SAVP.
- Add a certificate for DTLS-SRTP. Can be self-signed. See [Create certificate or certificate request](#).

**Media Encryption** [\(Help\)](#)

Enable media encryption  
 Disable media encryption

---

**SIP Media Encryption Policy** [\(Help\)](#)

No.	Media Network	Suite Requirements	Allow Transcoding	Delete Row
Add new rows <input type="text" value="1"/> rows.				

---

**Default Encryption Policy** [\(Help\)](#)

Suite requirements: 
 Allow transcoding:  Yes  No

---

**Require TLS** [\(Help\)](#)

Require TLS for all cryptos but cleartext  
 Do not require TLS

---

**RTP Profile** [\(Help\)](#)

Prefer RTP/SAVP (sdescriptions)  
 Prefer RTP/AVP (cleartext and legacy encryptions)  
 Prefer RTP/AVP (together with sdescriptions)

---

**Multi Profile** [\(Help\)](#)

Enable Multi Profile  
 Disable Multi Profile

---

**DTLS-SRTP** [\(Help\)](#)

Certificate: 
 DTLS to use:

Ignore invalid dates in the client's certificate:  Yes  No

Figure 8. Media encryption example.

## 20.34.2. Examples

Example JavaScript application.

Check out the demo page here: <https://www.ingate.com/webrtc-examples.html>

You can download the example from here: <https://www.ingate.com/webrtc-examples.zip>

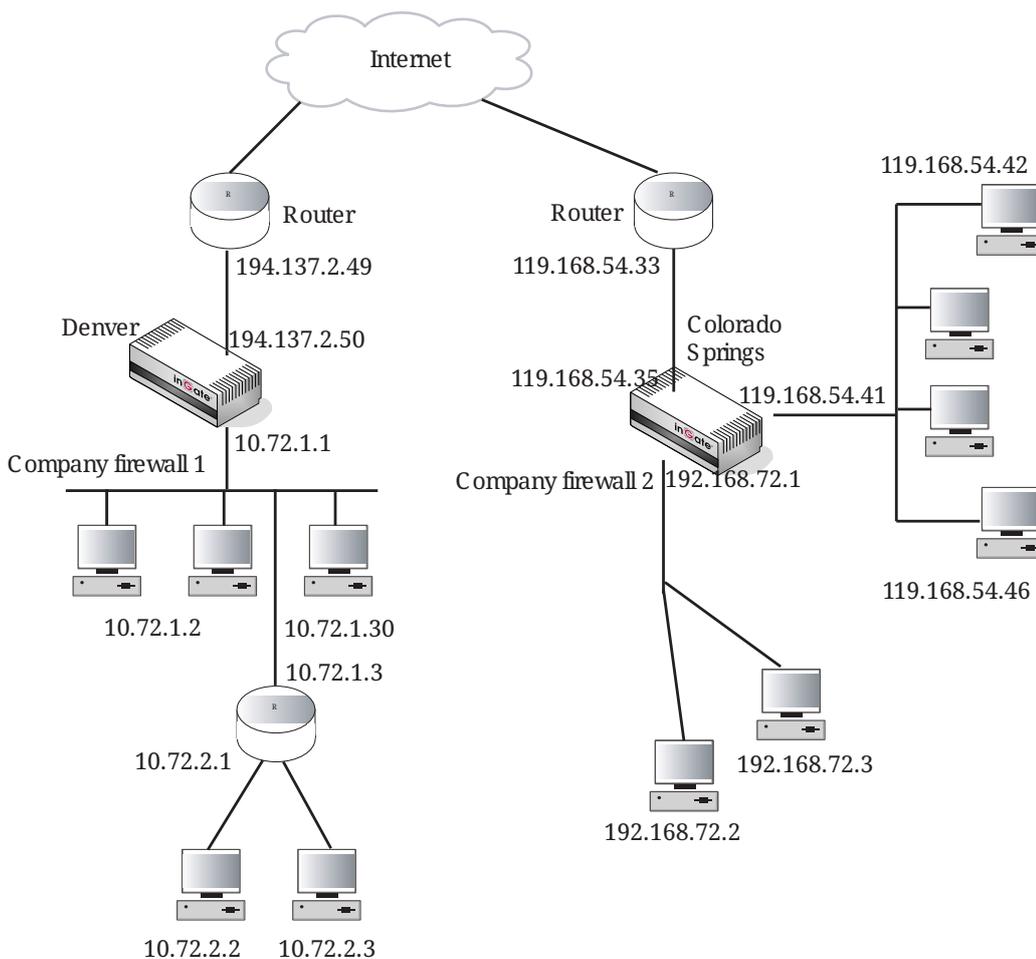
# Chapter 21. VPN

## 21.1. VPN between two Ingate Units

Example Company, Inc. has offices in Denver and Colorado Springs. Company wants to connect the two local networks into a secure private network, using two Ingate units with VPN. All computers on both networks need to communicate with each other through the VPN connection. Here, the extra VPN configuration is presented.

The unit at the Denver office is called Company Firewall 1. It has the IP address 10.72.1.1 on the inside and 194.137.2.50 on the outside. The computers on the office network have the IP addresses 10.72.1.2 to 10.72.1.30. A web server runs on the IP address 10.72.1.4. The router to Internet has the IP address 194.137.2.49 on the office side. There is also a service network behind a router with the IP address 10.72.1.3. The computers on this network have the IP addresses 10.72.2.2 and 10.72.2.3.

The Colorado Springs unit, Company Firewall 2, has three active interfaces. It has the IP address 119.168.54.41 on inside1, 192.168.72.1 on inside2 and 119.168.54.35 on the outside. The computers on the office networks have the IP addresses 119.168.54.42 to 119.168.54.46 and 192.168.72.2 to 192.168.72.15, respectively. The router to the Internet has the IP address 119.168.54.33 on the office side.



### 21.1.1. Denver office

At the Denver office, Company Firewall 1 is configured. Company Firewall 2 (Colorado Springs) is

defined as an IPsec peer on the **IPsec Peers** page. Select **Preshared** secret and type the secret under **Info**.

IPsec Peers (Help)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Springs-VPN		Yes	Outside (194.137.2.50)	119.168.54.35	No	119.168.54.35	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>

Go on to the **IPsec Tunnels** page. In the **IPsec Networks** table, you define the networks which should use the IPsec tunnel.

IPsec Networks (Help)

Edit row	Name	DNS name or network address	Network address	Netmask / bits	Delete row
<input type="checkbox"/>	Local admin net	10.72.2.0	10.72.2.0	29	<input type="checkbox"/>
<input type="checkbox"/>	Local office net	10.72.1.0	10.72.1.0	27	<input type="checkbox"/>
<input type="checkbox"/>	Springs-119	119.168.54.40	119.168.54.40	29	<input type="checkbox"/>
<input type="checkbox"/>	Springs-192	192.168.72.0	192.168.72.0	28	<input type="checkbox"/>

Define the IPsec tunnels for this peers. Since there are two networks at each office, there are a total of four tunnels to define, one for each combination of networks.

IPsec Tunnels (Help)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Springs-VPN	Network	Local admin net	-	Network	Springs-119		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local admin net	-	Network	Springs-192		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local office net	-	Network	Springs-119		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local office net	-	Network	Springs-192		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

On the **Networks and Computers** page, the networks that are using VPN are defined. Please note that the remote networks that will use VPN must have "-" as the interface.

Networks and Computers									
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row	
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Local network	-	10.72.1.0	10.72.1.0	10.72.1.30	10.72.1.30	Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>		-	10.72.2.0	10.72.2.0	10.72.2.7	10.72.2.7	Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Server	-	10.72.1.4	10.72.1.4			Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Springs	-	119.168.54.41	119.168.54.41	119.168.54.46	119.168.54.46	-	<input type="checkbox"/>	
<input type="checkbox"/>		-	192.168.72.1	192.168.72.1	192.168.72.15	192.168.72.15	-	<input type="checkbox"/>	

Finally, **Rules** for the traffic are defined. The Colorado Springs unit is consistently used as peer when running VPN.

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Server	-	Internet	-	Internal -> External (NAT:ed)	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Server	-	Internet	-	Internal -> External (NAT:ed)	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Local network	-	Internet	-	Internal -> External (NAT:ed)	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	4	Yes	Local network	-	Internet	-	Internal -> External (NAT:ed)	www	Allow	Office hours	Local		<input type="checkbox"/>
<input type="checkbox"/>	5	Yes	Local network	-	Internet	-	Internal -> External (NAT:ed)	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	6	Yes	Springs	Springs-VPN	Local network	-	(VPN) -> Internal	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	7	Yes	Local network	-	Springs	Springs-VPN	Internal -> (VPN)	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	8	Yes	Springs	Springs-VPN	Local network	-	(VPN) -> Internal	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	9	Yes	Local network	-	Springs	Springs-VPN	Internal -> (VPN)	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	10	Yes	Springs	Springs-VPN	Local network	-	(VPN) -> Internal	x11-display0	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	11	Yes	Local network	-	Springs	Springs-VPN	Internal -> (VPN)	x11-display0	Allow	24/7	Local		<input type="checkbox"/>

### 21.1.2. Colorado Springs office

The corresponding configuration is done for Company Firewall 2. First the connection is defined on the **IPsec Peers** page. Use the same secret under **Info**.

**IPsec Peers** [\(Help\)](#)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Denver VPN	-	Yes	Outside (119.168.54.35)	194.137.2.50	No	194.137.2.50	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>

The VPN connected networks are defined on the **IPsec Tunnels** page. Since there are two networks at each office, there is a total of four tunnels to define, one for each combination of networks.

**IPsec Networks** [\(Help\)](#)

Edit row	Name	DNS name or network address	Network address	Netmask / bits	Delete row
<input type="checkbox"/>	Denver admin	10.72.2.0	10.72.2.0	29	<input type="checkbox"/>
<input type="checkbox"/>	Denver office	10.72.1.0	10.72.1.0	27	<input type="checkbox"/>
<input type="checkbox"/>	Local DMZ	119.168.54.40	119.168.54.40	29	<input type="checkbox"/>
<input type="checkbox"/>	Local inside	192.168.72.0	192.168.72.0	28	<input type="checkbox"/>

**IPsec Tunnels** [\(Help\)](#)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Denver VPN	Network	Local DMZ	-	Network	Denver admin		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local DMZ	-	Network	Denver office		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local inside	-	Network	Denver admin		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local inside	-	Network	Denver office		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

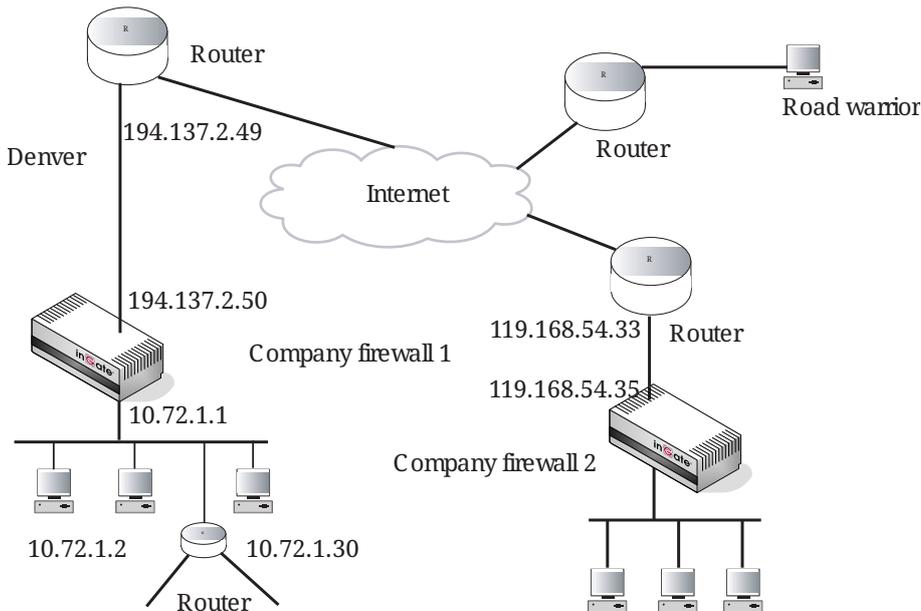
After that, configure the traffic under **Rules** as for Company Firewall 1.

The VPN connection between Company Firewall 1 and Company Firewall 2 will be established as

soon as both configurations have been applied.

## 21.2. VPN connection with road warrior

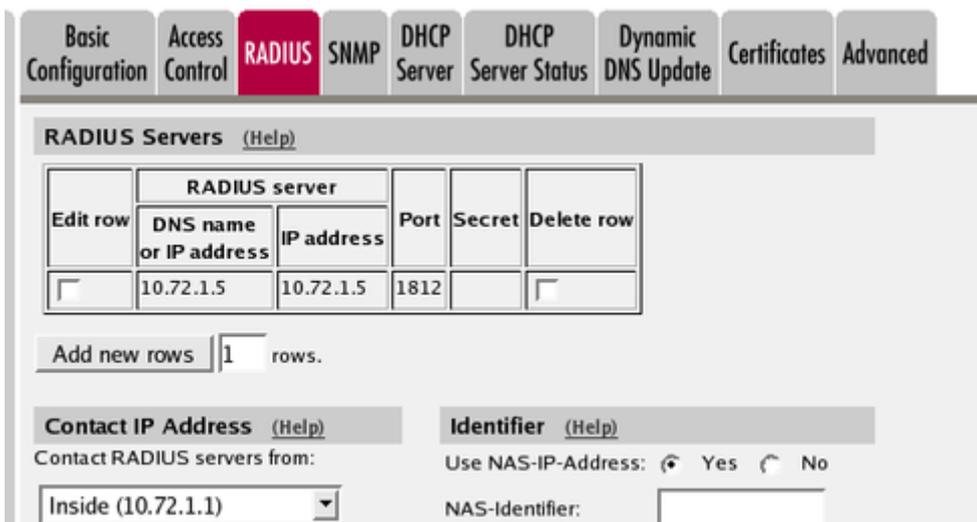
Juliet works as a seller at Example Company, Inc. She does a lot of travelling, so she has a laptop with a VPN client. This enables her to connect to the Denver office network in a secure way. To increase security even more, she is required to identify herself to a RADIUS server with the IP address 10.72.1.5, to be allowed to connect to Company Firewall 1. She also wants to be able to telnet to a computer at the Colorado Springs office, which is enabled by setting up a relay in Company Firewall 2.



Both units need additional configuration for this.

### 21.2.1. Denver office

Begin with Company Firewall 1 and start configuration on the **RADIUS** page under **Basic Configuration**. The RADIUS server has the IP address 10.72.1.5 .



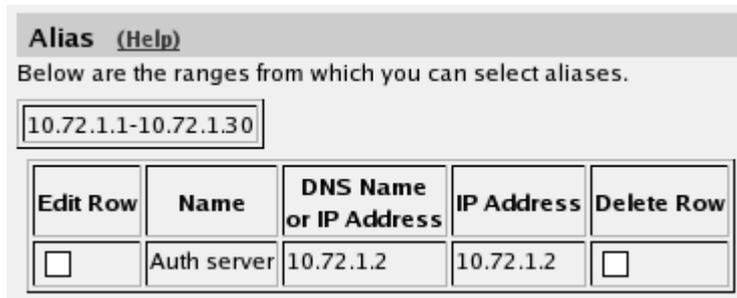
The unit will need at least one X.509 certificate to manage the RADIUS authentication. All local

certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

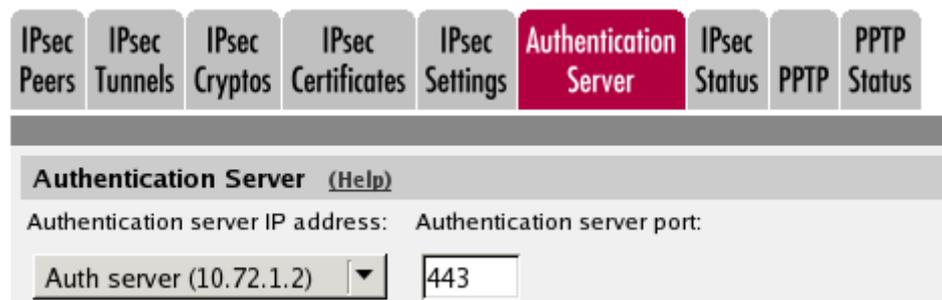


Then, go to the **Eth0** page under **Network** and create an **Alias** for the inside of the unit. The IP address used here must not be used for any other computer on the network.

This alias is used for the authentication server of the unit, which is the part that connects to the RADIUS server to authenticate users.



Then go to the **Authentication Server** page under **Virtual Private Networks**. An IP address for the unit is selected, which is used for Juliet's authentication. Select 10.72.1.2, an alias for the inside interface. A certificate for the authentication server is also required. Select a certificate from the ones created on the **Certificates** page.



Road warriors must use the authentication type X.509 certificates, which means that an X.509 certificate for the unit itself must be created (and, of course, certificates for each laptop wanting to connect to it). Go to the **IPsec Certificates** page and select from the certificates created on the **Certificates** page.

Basic Configuration	Access Control	RADIUS	SNMP	DHCP Server	DHCP Server Status	Dynamic DNS Update	<b>Certificates</b>	Advanced
---------------------	----------------	--------	------	-------------	--------------------	--------------------	---------------------	----------

Private Certificates (Help)						
Edit Row	Name	Certificate			Information	Delete Row
<input checked="" type="checkbox"/>	Inside	Create New	Import	View/Download	Subject: /CN=10.47.3.243 Issuer: /CN=10.47.3.243 MDS Fingerprint: F0:28:F2:F6:96:00:A2:EE:AD:A6:0F:D1:8B:97:9A:99 Valid to: 2008-03-05 13:58:07	<input type="checkbox"/>
<input type="checkbox"/>	RADIUS				Subject: /ST=sweden/O=ingate/CN=isp.ingate.com Issuer: /ST=sweden/O=ingate/CN=isp.ingate.com MDS Fingerprint: 0C:23:74:2F:BA:73:96:9B:2B:E0:46:CC:3A:79:C4:18 Valid to: 2009-04-29 13:02:50	<input type="checkbox"/>
<input type="checkbox"/>	VPN cert				Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MDS Fingerprint: B6:F3:5D:8B:DC:90:86:96:E2:F8:AA:E9:BC:7A:15 Valid to: 2010-02-07 13:03:58	<input type="checkbox"/>
<input type="checkbox"/>	main cert				Subject: /O=ingate/CN=isp.ingate.com Issuer: /O=ingate/CN=isp.ingate.com MDS Fingerprint: 57:45:30:EC:A3:B7:5C:65:87:21:B6:58:82:4F:84:80 Valid to: 2008-02-26 12:51:17	<input type="checkbox"/>

Add new rows | 1 rows.

Juliet's laptop must be defined on the **IPsec Peers** page. Remember to turn **RADIUS** on.

<b>IPsec Peers</b>	IPsec Tunnels	IPsec Cryptos	IPsec Certificates	IPsec Settings	Authentication Server	IPsec Status	PPTP	PPTP Status
--------------------	---------------	---------------	--------------------	----------------	-----------------------	--------------	------	-------------

IPsec Peers (Help)									
These settings are called "Phase 1 settings" in some other IPsec products.									
Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Juliet	-	Yes	Outside (194.137.2.50)	*	No	*	Yes	*
<input type="checkbox"/>	+ Springs-VPN	-	Yes	Outside (194.137.2.50)	119.168.54.35	No	119.168.54.35	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES,3DES	X.509 certificate	Subject: /CN=juliet.home.ingate.com Issuer: /CN=juliet.home.ingate.com MDS Fingerprint: 70:C0:F0:2F:2B:8F:25:1F:21:FD:E6:87:C9:34:33:C0 Valid to: 2011-04-09 12:40:18	<input type="checkbox"/>
3600	Yes	AES,3DES	Preshared secret	MDS Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>

Press the **Change/View** button to load the X.509 certificate for Juliet's laptop.

### Upload X.509 Certificate

Specify the local file, in PEM (.pem) or DER (.cer) format, containing the certificate for "**Juliet**" below, then press the import button.

Local file containing certificate:

On the **IPsec Tunnels** page, define the new IPsec tunnel. It consists of the Denver office network and Juliet's laptop. The laptop's IP will probably be NAT:ed, but we don't know that for sure, so we select Remote/private address, which will allow public as well as private IP addresses for Juliet's

laptop.

IPsec Tunnels (Help)										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	Juliet	Network	Local office net	-	Remote/private address	-		AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>	Springs-VPN	Network	Local admin net	-	Network	Springs-119		AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local admin net	-	Network	Springs-192		AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local office net	-	Network	Springs-119		AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local office net	-	Network	Springs-192		AES,3DES	Same as Phase 1 DH	<input type="checkbox"/>

A new network must be defined on the **Networks and Computers** page to make rules for Juliet's laptop. The network, Internet-VPN, must have the interface "-" to work with VPN.

Networks and Computers										
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row		
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address				
<input type="checkbox"/>	Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	Internet-VPN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>		
<input type="checkbox"/>	Local network	-	10.72.1.0	10.72.1.0	10.72.1.30	10.72.1.30	Internal (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>		-	10.72.2.0	10.72.2.0	10.72.2.7	10.72.2.7	Internal (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	Server	-	10.72.1.4	10.72.1.4			Internal (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	Springs	-	119.168.54.41	119.168.54.41	119.168.54.46	119.168.54.46	-	<input type="checkbox"/>		
<input type="checkbox"/>		-	192.168.72.1	192.168.72.1	192.168.72.15	192.168.72.15	-	<input type="checkbox"/>		

Add **Rules** (No. 12-17) to allow Juliet to work on the office network.

Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Server	-	Internet	-	Internal -> External (NAT:ed)	smtp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Server	-	Internet	-	Internal -> External (NAT:ed)	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Local network	-	Internet	-	Internal -> External (NAT:ed)	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	4	Yes	Local network	-	Internet	-	Internal -> External (NAT:ed)	www	Allow	Office hours	Local		<input type="checkbox"/>
<input type="checkbox"/>	5	Yes	Local network	-	Internet	-	Internal -> External (NAT:ed)	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	6	Yes	Springs	Springs-VPN	Local network	-	(VPN) -> Internal	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	7	Yes	Local network	-	Springs	Springs-VPN	Internal -> (VPN)	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	8	Yes	Springs	Springs-VPN	Local network	-	(VPN) -> Internal	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	9	Yes	Local network	-	Springs	Springs-VPN	Internal -> (VPN)	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	10	Yes	Springs	Springs-VPN	Local network	-	(VPN) -> Internal	x11-display0	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	11	Yes	Local network	-	Springs	Springs-VPN	Internal -> (VPN)	x11-display0	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	12	Yes	Internet-VPN	Juliet	Local network	-	(VPN) -> Internal	dns	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	13	Yes	Local network	-	Internet-VPN	Juliet	Internal -> (VPN)	dns-reply	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	14	Yes	Internet-VPN	Juliet	Local network	-	(VPN) -> Internal	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	15	Yes	Internet-VPN	Juliet	Local network	-	(VPN) -> Internal	ssh	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	16	Yes	Internet-VPN	Juliet	Local network	-	(VPN) -> Internal	ftp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	17	Yes	Internet-VPN	Juliet	Local network	-	(VPN) -> Internal	imap	Allow	24/7	Local		<input type="checkbox"/>

With road warriors connecting to the unit, blacklisting is possible. Configure blacklisting parameters on the **IPsec Settings** page.

IPsec Peers IPsec Tunnels IPsec Cryptos IPsec Certificates **IPsec Settings** Authentication Server IPsec Status PPTP PPTP Status

---

**Blacklisting** [\(Help\)](#)

Blacklist interval:  minutes      Policy for packets from blacklisted IP addresses:

Discard IP packets  
 Reject IP packets

### 21.2.2. Colorado office

Juliet wants to telnet to a workstation with the IP address 174.25.30.3 on the Colorado Springs office network. Enable this by setting up a relay listening to the outside of Company Firewall 2. Since this traffic should be encrypted, too, a VPN tunnel between the laptop and the unit should be defined. First, select a certificate for Company Firewall 2 on the **IPsec Certificates** page.

IPsec Peers IPsec Tunnels IPsec Cryptos **IPsec Certificates** IPsec Settings Authentication Server IPsec Status PPTP PPTP Status

**Local X.509 Certificate** (Help) **IPsec CA Certificates** (Help)

Use this certificate for IPsec:

IPsec ▼

Edit Row CA Delete Row

Add new rows 1 rows.

After that, define Juliet's laptop on the **IPsec Peers** page for Company Firewall 2. The X.509 certificate to Juliet's laptop is imported as before.

**IPsec Peers** (Help) IPsec Tunnels IPsec Cryptos IPsec Certificates IPsec Settings Authentication Server IPsec Status PPTP PPTP Status

**IPsec Peers** (Help)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Denver VPN	-	Yes	Outside (119.168.54.35)	194.137.2.50	No	194.137.2.50	No	
<input type="checkbox"/>	+ Juliet	-	Yes	Outside (119.168.54.35)	*	No	*	No	*

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>
3600	Yes	AES/3DES	X.509 certificate	Subject: /CN=juliet.home.ingate.com Issuer: /CN=juliet.home.ingate.com MD5 Fingerprint: 70:C0:F0:2F:2B:8F:25:1F:21:FD:E6:B7:C9:34:33:C0 Valid to: 2011-04-09 12:40:18	<input type="checkbox"/>

A new IPsec tunnel is required, in this case from the laptop to the unit itself. This is done on the **IPsec Tunnels** page. As we don't know for sure if Juliet's laptop will have a NATed IP address, we select Remote/private address as the **Remote side**.

**IPsec Tunnels** [\(Help\)](#)

These settings are called "Phase 2 settings" in some other IPsec products.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Denver VPN	Network	Local DMZ	-	Network	Denver admin		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local DMZ	-	Network	Denver office		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local inside	-	Network	Denver admin		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Local inside	-	Network	Denver office		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>	+ Juliet	Local side address	-	-	Remote/private address	-		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

Finally, define a TCP relay on the **Relays** page, listening to a high port which is reserved for this telnet connection. The traffic is relayed to port 23 on the workstation.

[Rules](#) [Relays](#) [DHCP Relay](#) [Services](#) [Protocols](#) [Time Classes](#)

**Relays**

Edit row	Listen to ...		Relay to ...			Relay type	Allow access from ...		Time class	Log class	Delete row
	IP address	Port	DNS name or IP address	IP address	Port		Network	IPsec peer			
<input type="checkbox"/>	Outside (119.168.54.35)	1027	192.168.72.10	192.168.72.10	23	TCP relay	Internet-VPN	Juliet	24/7	Local	<input type="checkbox"/>

## 21.3. How to configure PPTP connections

When a VPN connection using PPTP is established, the unit will assign a local IP address to the PPTP client, which then can look like it is located on the local network.

Follow these steps to configure the unit for PPTP connections.

### 21.3.1. Networks and Computers

Go to the **Networks and Computers** page under **Network** and create a new network. The new network should contain IP addresses from the local network which the PPTP clients can use. Select "-" as the Interface for this network.

Also, make sure that there are networks for the computers which the PPTP clients should be allowed to access. These networks are used when rules are set up for the PPTP traffic.

Networks and Computers								
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Office	-	10.7.0.0	10.7.0.0	10.7.0.255	10.7.0.255	Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ PPTP clients	-	10.7.0.220	10.7.0.220	10.7.0.240	10.7.0.240	-	<input type="checkbox"/>

### 21.3.2. PPTP

Go to the **PPTP** page under **Virtual Private Networks** to do settings for the PPTP server in the unit.

First, select that the PPTP server should be On and select an IP address for it. This IP address is one of the unit's own IP addresses and is the one which PPTP clients should access, which means that it must be available from the Internet. It is recommended that you select one of the addresses on the unit outside.

IPsec Peers	IPsec Tunnels	IPsec Cryptos	IPsec Certificates	IPsec Settings	Authentication Server	IPsec Status	<b>PPTP</b>	PPTP Status
<b>PPTP server</b> <a href="#">(Help)</a>								
<input checked="" type="radio"/> Enable PPTP server <input type="radio"/> Disable PPTP server								

Then, select a unit IP address which will act as a local peer for the PPTP clients. You must select an IP address on the same unit interface and logical network as the IP addresses in the PPTP client network.

Select the network created above as the Client IP addresses. When a PPTP client connects, it will be assigned one of these IP addresses on the local network.

<b>Client Network</b> <a href="#">(Help)</a>
PPTP local IP address:
<input type="text" value="Dynamic clients (10.5.1.1)"/>
Client IP addresses:
<input type="text" value="PPTP clients"/>

You can enter local DNS and WINS servers for the PPTP clients to use. This will enable the clients to use local network services.

DNS Servers <a href="#">(Help)</a>		WINS Servers <a href="#">(Help)</a>	
Primary DNS:		Primary WINS:	
DNS name or IP address	IP address	DNS name or IP address	IP address
<input type="text" value="10.7.0.7"/>	10.7.0.7	<input type="text" value="10.7.0.9"/>	10.7.0.9
Secondary DNS:		Secondary WINS:	
DNS name or IP address	IP address	DNS name or IP address	IP address
<input type="text"/>		<input type="text" value="10.7.0.12"/>	10.7.0.12

Enter the users allowed to connect using PPTP, and their passwords. The user must enter this username and password in her PPTP client.

PPTP Users <a href="#">(Help)</a>				
Edit Row	User	Password	Enabled	Delete Row
<input type="checkbox"/>	bob		Yes	<input type="checkbox"/>
<input type="checkbox"/>	cindy		Yes	<input type="checkbox"/>
<input type="checkbox"/>	fred		Yes	<input type="checkbox"/>
<input type="checkbox"/>	lucy		Yes	<input type="checkbox"/>
<input type="checkbox"/>	minnie		Yes	<input type="checkbox"/>
<input type="checkbox"/>	steve		Yes	<input type="checkbox"/>

Add new rows  rows.

### 21.3.3. Rules

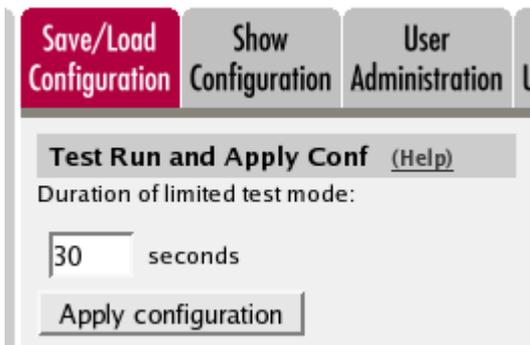
Go to the **Rules** page under **Rules and Relays** and create rules for the traffic between the PPTP clients and the local network. The PPTP clients are represented by the network of local PPTP IP addresses.

If the PPTP clients should initiate all traffic (i.e., they are not supposed to act as servers), you don't need a reply rule for TCP.

Rules	Relays	DHCP Relay	Services	Protocols	Time Classes								
<b>Rules</b>													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	PPTP clients	-	Office	-	Indeterminate interface -> Internal	tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	PPTP clients	-	Office	-	Indeterminate interface -> Internal	udp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Office	-	PPTP clients	-	Internal -> Indeterminate interface	udp	Allow	24/7	Local		<input type="checkbox"/>

### 21.3.4. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



### 21.3.5. Configuring the Client

When the unit has been configured, you also need to configure the PPTP client. This is, of course, done differently with different clients. A Windows XP computer has a built-in PPTP client which is configured under Control Panel → Network connections.

## 21.4. How to configure IPsec connections

With a VPN connection between two firewalls or other VPN gateways, several offices can share servers and other resources without exposing the traffic openly on the Internet.

This is how to set up an IPsec VPN connection to the unit.

### 21.4.1. Certificates

If the units should authenticate using X.509 certificates, the unit needs a certificate of its own. All local certificates for the unit are created on the **Certificates** page under **Basic Configuration**.

Make a new row in the **Private Certificates** table, press **Create new**, and fill in the form. The password fields are only relevant if you want to be able to revoke the certificate.

You can select to let the unit sign its own certificate (this is the simple way) or create a certificate request and make a CA sign it for you. If you use an outside CA, the signed certificate must be uploaded to the unit.

Edit Row	Name	Certificate	Information	Delete Row
<input checked="" type="checkbox"/>	Inside	Create New Import View/Download	Subject: /CN=10.47.3.243 Issuer: /CN=10.47.3.243 MD5 Fingerprint: F0:28:F2:F6:96:D0:A2:EE:AD:A6:0F:D1:8B:97:9A:99 Valid to: 2008-03-05 13:58:07	<input type="checkbox"/>
<input type="checkbox"/>	RADIUS		Subject: /ST=sweden/O=ingate/CN=isp.ingate.com Issuer: /ST=sweden/O=ingate/CN=isp.ingate.com MD5 Fingerprint: 0C:23:74:2F:BA:73:96:9B:2B:E0:46:CC:3A:79:C4:18 Valid to: 2009-04-29 13:02:50	<input type="checkbox"/>
<input type="checkbox"/>	VPN cert		Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MD5 Fingerprint: B6:F3:5D:88:DC:90:86:96:E2:F8:AA:E9:BC:7A:15 Valid to: 2010-02-07 13:03:58	<input type="checkbox"/>
<input type="checkbox"/>	main cert		Subject: /O=ingate/CN=isp.ingate.com Issuer: /O=ingate/CN=isp.ingate.com MD5 Fingerprint: 57:45:30:EC:A3:B7:5C:65:87:21:B6:58:82:4F:84:80 Valid to: 2008-02-26 12:51:17	<input type="checkbox"/>

Add new rows  rows.

## 21.4.2. IPsec Peers

Start on the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the VPN connection should be established. You also define how the VPN peers should authenticate themselves to each other.

Under **Authentication:Type**, select authentication with a Preshared secret or X.509 certificates. To use X.509 certificates, either both units must be able to sign their own certificates, or you must have access to a CA server which will sign certificate requests. If you have your own CA server, you can upload its certificate to the unit and then trust all certificates signed by that CA (select Trusted CA).

Under **Info**, enter the secret or upload the certificate that should be used for authentication. If you use certificates, you should upload the other unit's certificate here, not the unit's own one.

Under **Local side**, select a public IP address of the unit, and enter a public IP address of the other VPN gateway under **Remote side**.

Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.

IPsec Peers (Help)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	Atlantic City		Yes	Outside (193.12.253.115)	198.122.30.2	No	198.122.30.2	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: 4D:B9:D6:CF:9E:BE:CC:37:4E:25:ED:7B:0F:80:C2:12	<input type="checkbox"/>

## 21.4.3. IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. You must define the local office network as well as the network behind the other VPN gateway.

IPsec Networks (Help)

Edit Row	Name	DNS name or network address	Network address	Netmask / bits	Delete Row
<input type="checkbox"/>	Atlantic network	10.20.30.0	10.20.30.0	24	<input type="checkbox"/>
<input type="checkbox"/>	DMZ network	172.16.0.0	172.16.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>

Then, create a new row in the **IPsec Tunnels** table. Under Peer, select the newly created VPN

tunnel.

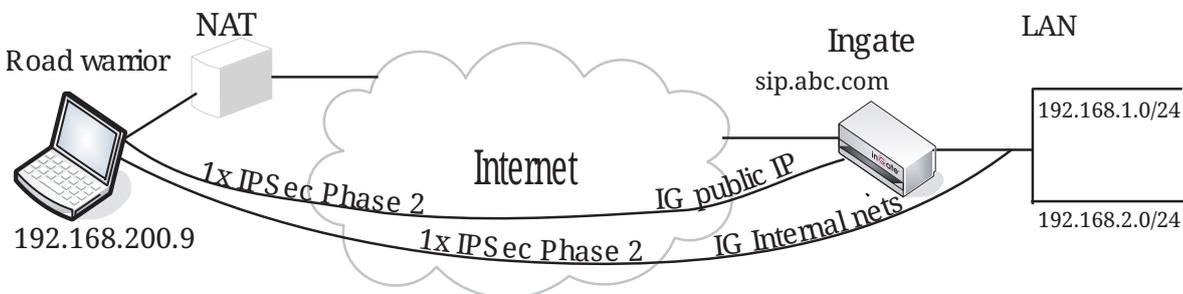
Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under Network.

Under **Remote network**, select Network and the network defined below, which is connected to the remote VPN gateway.

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

IPsec Tunnels (Help)										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Atlantic City	Network	DMZ network	-	Network	Atlantic network	1800	AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>
<input type="checkbox"/>		Network	Home network	-	Network	Atlantic network	1800	AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or

subnet that includes the external IP of the unit, i.e. to a DMZ range.

- The external IP (or DMZ range) of the unit is a network in the IPsec Networks table. In the IPsec Tunnels table, select Network under Address type and select the network you just created under IPsec Networks.

### 21.4.4. IPsec Certificates

Go to the **IPsec Certificates** page under **Virtual Private Networks** and select which certificate the unit should use for VPN connections. Also add all CA servers which have signed certificates for the VPN clients.

### 21.4.5. Networks and Computers

Go to **Networks and Computers** under **Network** to create network groups for the networks that will use the VPN tunnel. These are used for building rules for the VPN traffic.

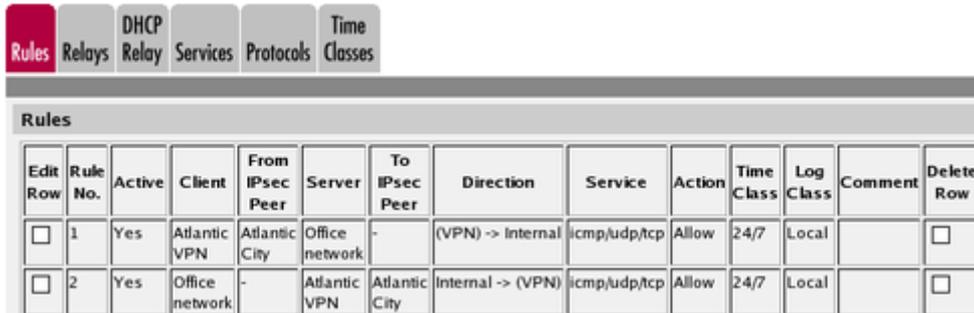
The network on the other side of the VPN tunnel (see Atlantic network in the example) must have "-" selected under Interface.

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Atlantic VPN	-	10.20.30.0	10.20.30.0	10.20.30.255	10.20.30.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ DHCP clients	-	10.5.1.0	10.5.1.0	10.5.1.255	10.5.1.255	DHCP clients (eth3 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ DNS server	-	172.16.0.3	172.16.0.3			Ext2 (eth2 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Office network	-	10.10.0.0	10.10.0.0	10.10.0.255	10.10.0.255	Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>		-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>

## 21.4.6. Rules

Go to the **Rules** page and create rules to let traffic through the VPN tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the VPN tunnel under **From IPsec peer** if the **Client** network is located behind the VPN peer. Select the VPN tunnel under **To IPsec peer** if the **Server** network is located behind the VPN peer.

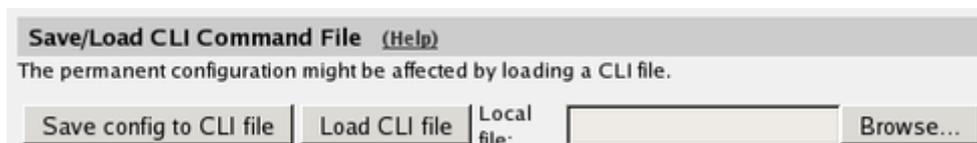


Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Atlantic VPN	Atlantic City	Office network	-	(VPN) -> Internal	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Office network	-	Atlantic VPN	Atlantic City	Internal -> (VPN)	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>

## 21.4.7. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI** file to save the configuration.



**Save/Load CLI Command File** [\(Help\)](#)

The permanent configuration might be affected by loading a CLI file.

Local file:

## 21.5. How to configure IPsec connections from a road warrior

With an IPsec connection between the unit and a road warrior, the user can use servers and other resources from home or a hotel without exposing the traffic openly on the Internet.

Connections with a road warrior require X.509 certificates.

This is how to set up an IPsec VPN connection to the unit.

### 21.5.1. Certificates

If you have many road warriors connecting to the unit and you don't want to upload every client X.509 certificate separately, you can choose to trust certificates signed by a certain CA. For this, the unit requires the CA certificate instead. You upload the CA certificate on the **Certificates** page.

Enter a name for the CA certificate. The name is only used internally in the unit.

CA Certificates (Help)					
Edit Row	Name	CA Certificate	CA CRL	Information	Delete Row
<input checked="" type="checkbox"/>	Main CA	Change/View	Change/View	Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MD5 Fingerprint: 16-7B-3D-D6-D7-56-F4-AE-EB-BD-0D-0B-03-4E-4C-4C Valid to: 2008-04-24 08:12:23	<input type="checkbox"/>

Add new rows  rows.

To authenticate itself, the unit needs an X.509 certificate. This is created on the same page.

Make a new row in the **Private Certificates** table, press **Create new**, and fill in the form. The password fields are only relevant if you want to be able to revoke the certificate.

You can select to let the unit sign its own certificate (this is the simple way) or create a certificate request and make a CA sign it for you. If you use an outside CA, the signed certificate must be uploaded to the unit.

**Create Certificate or Certificate Request**

Fill in the certificate data for "RADIUS" below, then create either a certificate or a certificate request.

After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days): * <input type="text" value="365"/>	Country code (C): <input type="text"/>	Organization (O): <input type="text"/>
Common Name (CN): * <input type="text" value="client.ingate.com"/>	State/province (ST): <input type="text"/>	Organizational Unit (OU): <input type="text"/>
Email address: <input type="text"/>	Locality/town (L): <input type="text"/>	

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number:  
\*

Fields marked with "\*" are mandatory.

Below you can enter an optional challenge password for certificate requests.

Challenge password:

Challenge password again:

## 21.5.2. IPsec Certificates

Go to the **IPsec Certificates** page under **Virtual Private Networks** and select which certificate the unit should use for VPN connections. Also add all CA servers which have signed certificates for the VPN clients.

IPsec Peers
IPsec Tunnels
IPsec Cryptos
IPsec Certificates
IPsec Settings
Authentication Server
IPsec Status
PPTP
PPTP Status

**Local X.509 Certificate (Help)**

Use this certificate for IPsec:

▼

**IPsec CA Certificates (Help)**

Edit Row	CA	Delete Row
<input type="checkbox"/>	Main CA	<input type="checkbox"/>

Add new rows  rows.

### 21.5.3. IPsec Peers

Go to the **IPsec Peers** page under **Virtual Private Networks** to define the IP addresses between which the VPN connection should be established. You also define how the VPN peers should authenticate themselves to each other.

Select **On** under **Status**. Under **Authentication:Type**, select the authentication method. Road warriors must use X.509 certificates, and you can select to upload the client's certificate or trust the CA which signed the client certificate. To use X.509 certificates, you must have access to a CA server (or purchase signings) which will sign certificate requests. If you have your own CA server, you can upload its certificate to the unit and then trust all certificates signed by that CA (select **Trusted CA**).

Under **Info**, upload the client certificate or enter the CA/DN, depending on the authentication type selected above. N.B.: The X.509 certificate you upload here is the client certificate, not the unit's own one.

Under **Local side**, select a public IP address of the unit, and enter a "\*" under **Remote side**. This means that the peer is a road warrior.

Enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.

IPsec Peers	IPsec Tunnels	IPsec Cryptos	IPsec Certificates	IPsec Settings	Authentication Server	IPsec Status	PPTP	PPTP Status	
<b>IPsec Peers</b> <a href="#">(Help)</a>									
These settings are called "Phase 1 settings" in some other IPsec products.									
Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Martin	-	Yes	Internet (193.12.253.113)	*	No	*	Yes	*

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Trusted CA, with DN	/CN=ingate /O=ingate	<input type="checkbox"/>

### 21.5.4. IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the VPN tunnel.

In the **IPsec Networks** table, define the local office network that will be used through the VPN tunnel.

You must also enter the IP address of the authentication server here, either as a part of the office network or as a separate network.

IPsec Networks <a href="#">(Help)</a>					
Edit Row	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
<input type="checkbox"/>	Atlantic network	10.20.30.0	10.20.30.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Boston side	13.7.3.22	13.7.3.22	32	<input type="checkbox"/>
<input type="checkbox"/>	Chicago network	192.168.10.0	192.168.10.0	24	<input type="checkbox"/>
<input type="checkbox"/>	DMZ network	172.16.0.0	172.16.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>

Add new rows  rows.

Under **Peer**, select the newly created VPN tunnel.

Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under **IPsec Networks**.

Under **Remote network**, you have the following options:

- The road warrior has a public IP address on the Internet. Select Remote side address under **Address type**. This means "the same IP address as on the IPsec Peers page".
- The road warrior is located behind a NAT:ing device, and you know which IP network it belongs to. Enter that network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network, allow subset under **Address type** and select the network you just created under **Network**.
- Usually, you won't know the private IP address of the road warrior in advance, or it will change a lot. You might not even know if the client is NAT:ed or not.

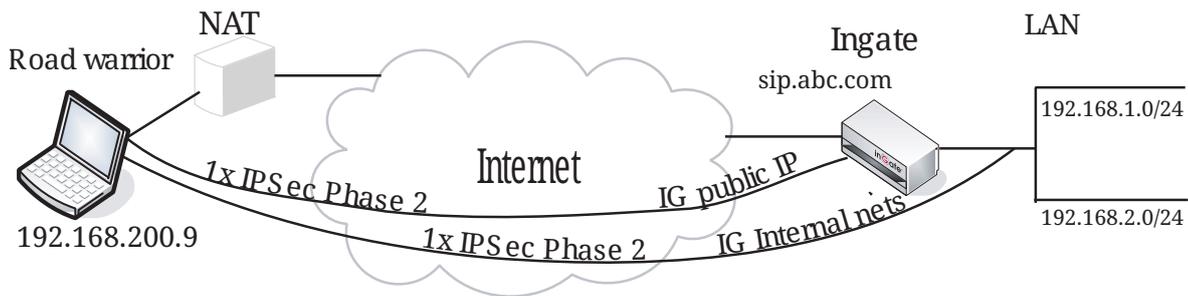
Select Remote/private address as the **Address type**. This will allow all private IP addresses as well as the public address presented by the client at the negotiation.

When **Network** or **Network, allow subset** was selected, there must be a line for every pair of networks that should be able to communicate with each other through the VPN connection.

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both VPN peers.

IPsec Tunnels <a href="#">(Help)</a>										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Martin	Network	Office network	-	Remote/private address	-	1800	AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

### 21.5.5. SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the unit, i.e. to a DMZ range.
- The external IP (or DMZ range) of the unit is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

### 21.5.6. Networks and Computers

Go to the **Networks and Computers** page under **Network** and make sure that there are groups for all networks that will use the VPN tunnel. These are used for building rules for the VPN traffic. You don't need a network for the authentication server.

The network on the other side of the VPN tunnel (see VPN network in the example) must have "-" selected under **Interface**.

Networks and Computers		Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Networks and Computers													
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row					
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address							
<input type="checkbox"/>	+ DHCP clients	-	10.22.0.0	10.22.0.0	10.22.0.255	10.22.0.255	DHCP (eth3 untagged)	<input type="checkbox"/>					
<input type="checkbox"/>	+ DMZ	-	172.16.0.0	172.16.0.0	172.16.0.255	172.16.0.255	DMZ (eth2 untagged)	<input type="checkbox"/>					
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>					
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>					
<input type="checkbox"/>	+ Mail server	-	10.47.2.13	10.47.2.13			Internal (eth0 untagged)	<input type="checkbox"/>					
<input type="checkbox"/>	+ Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>					
<input type="checkbox"/>	+ PPTP	-	10.7.0.100	10.7.0.100	10.7.0.150	10.7.0.150	-	<input type="checkbox"/>					
<input type="checkbox"/>	+ VPN network	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>					

### 21.5.7. Rules

Go to the **Rules** page and create rules to let traffic through the VPN tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the VPN tunnel under **From VPN** if the **Client** network is the road warrior network. Select the VPN tunnel under **To VPN** if the **Server** network is the road warrior network.

Rules		Relays	DHCP Relay	Services	Protocols	Time Classes							
Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	VPN network	Martin	Office network	-	(VPN) -> Internal	tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	VPN network	Martin	Office network	-	(VPN) -> Internal	udp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Office network	-	VPN network	Martin	Internal -> (VPN)	udp	Allow	24/7	Local		<input type="checkbox"/>

### 21.5.8. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration	Show Configuration	User Administration
<b>Test Run and Apply Conf</b> <a href="#">(Help)</a>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

## 21.5.9. Configuring the Client

The road warrior itself must also be configured. The exact moves for this is of course dependant of what client software you use. See <http://www.ingate.com/Interaction.php> for configuration instructions for several VPN clients.

## 21.6. IPSec connections with RADIUS authentication

Connections with a road warrior require X.509 certificates.

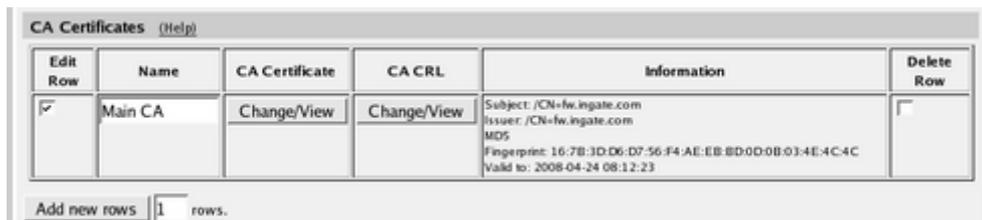
If you want to make the connection even more secure, you can require that the VPN users also authenticate to a local RADIUS server before they can use the IPsec connection.

This is how to set up an IPSec VPN connection with RADIUS authentication to the unit.

### 21.6.1. Certificates

If you have many road warriors connecting to the unit and you don't want to upload every client X.509 certificate separately, you can choose to trust certificates signed by a certain CA. For this, the unit requires the CA certificate instead. You upload the CA certificate on the **Certificates** page.

Enter a name for the CA certificate. The name is only used internally in the unit.



The screenshot shows a table titled "CA Certificates" with a "(Help)" link. The table has six columns: "Edit Row", "Name", "CA Certificate", "CA CRL", "Information", and "Delete Row". There is one row with the name "Main CA". The "CA Certificate" and "CA CRL" columns contain "Change/View" links. The "Information" column contains the following text: "Subject: /CN=fw.ingate.com", "Issuer: /CN=fw.ingate.com", "MD5", "Fingerprint: 16:7B:3D:D6:D7:56:F4:AE:EB:8D:0D:0B:03:4E:4C:4C", and "Valid to: 2008-04-24 08:12:23". Below the table, there is a "Add new rows" button and a text input field containing "1" followed by "rows".

Edit Row	Name	CA Certificate	CA CRL	Information	Delete Row
<input checked="" type="checkbox"/>	Main CA	Change/View	Change/View	Subject: /CN=fw.ingate.com Issuer: /CN=fw.ingate.com MD5 Fingerprint: 16:7B:3D:D6:D7:56:F4:AE:EB:8D:0D:0B:03:4E:4C:4C Valid to: 2008-04-24 08:12:23	<input type="checkbox"/>

Add new rows  rows.

To authenticate itself, the unit needs an X.509 certificate. This is created on the same page.

Make a new row in the **Private Certificates** table, press **Create new**, and fill in the form. The password fields are only relevant if you want to be able to revoke the certificate.

You can select to let the unit sign its own certificate (this is the simple way) or create a certificate request and make a CA sign it for you. If you use an outside CA, the signed certificate must be uploaded to the unit.

**Create Certificate or Certificate Request**

Fill in the certificate data for "RADIUS" below, then create either a certificate or a certificate request.

After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days):  Country code (C):  Organization (O):

Common Name (CN):  State/province (ST):  Organizational Unit (OU):

Email address:  Locality/town (L):

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number:

Fields marked with "\*" are mandatory.

Below you can enter an optional challenge password for certificate requests.

Challenge password:

Challenge password again:

You have now created the certificate that should be used when the unit authenticates itself to the connecting IPsec client.

The unit also needs a certificate to authenticate itself for the connecting web browser when performing the RADIUS authentication. You can use the same certificate for both purposes, or create separate certificates.

## 21.6.2. RADIUS

When RADIUS authentication is used, the unit must know which RADIUS server to contact. Go to the **RADIUS** page under **Basic Configuration** and enter the RADIUS server to use.

Basic Configuration | Access Control | **RADIUS** | SNMP | DHCP Server | DHCP Server Status | Dynamic DNS Update | Certificates | Advanced

**RADIUS Servers** [\(Help\)](#)

	RADIUS server		Port	Secret	Delete
Edit	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	10.47.2.32	10.47.2.32	1645		<input type="checkbox"/>

You must also select which IP address the unit should use when contacting the RADIUS server.

**Contact IP Address** [\(Help\)](#)

Contact RADIUS servers from:

## 21.6.3. Interface

When the IPsec user wants to use the IPsec connection, she will need to connect to an IP address on the unit itself, to make the RADIUS authentication. This connection is made in a web browser over https.

You must select an IP address of the unit to which the user can connect. This IP address must be one

that can be accessed by the user via the IPsec connection. Usually, this means that you need an IP address on the LAN.

You can either use the unit's main IP address (as defined in the **Directly Connected Networks** table), or create an **Alias** to use for this purpose. This is done on the **Interface** pages.

**Alias** [\(Help\)](#)

Below are the ranges from which you can select aliases.

10.47.0.1-10.47.255.254

Edit Row	Name	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	RADIUS	10.47.2.247	10.47.2.247	<input type="checkbox"/>

### 21.6.4. Authentication Server

If RADIUS is used to authenticate the user, the unit must have an SSL certificate for its authentication server.

Go to the **Authentication Server** page and select a public IP address and port of the unit. This is the IP address and port which the user should connect to when opening the IPsec connection.

IPsec Peers | IPsec Tunnels | IPsec Cryptos | IPsec Certificates | IPsec Settings | **Authentication Server** | IPsec Status | PPTP | PPTP Status

**Authentication Server** [\(Help\)](#)

Authentication server IP address:      Authentication server port:

RADIUS (10.47.2.247) ▼      4033

You must also select which certificate the authentication server of the unit should use to identify itself to the connecting client.

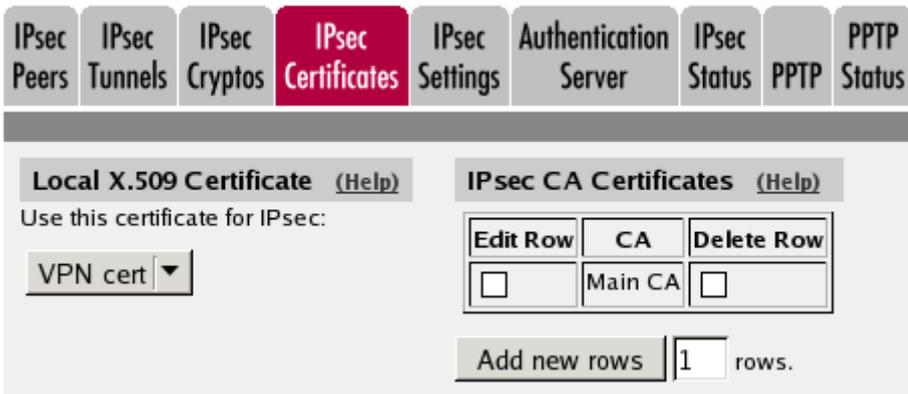
**Authentication Server Certificate** [\(Help\)](#)

Use this certificate for the authentication server:

VPN cert ▼

### 21.6.5. IPsec Certificates

Go to the **IPsec Certificates** page under **Virtual Private Networks** and select which certificate the unit should use for VPN connections. Also add all CA servers which have signed certificates for the VPN clients.



### 21.6.6. IPsec Peers

Go to the **IPsec Peers** page under **Virtual Private Networks** to define the IP addresses between which the VPN connection should be established. You also define how the VPN peers should authenticate themselves to each other.

Select **On** under **Status**. Under **Authentication:Type**, select the authentication method. Road warriors must use X.509 certificates, and you can select to upload the client's certificate or trust the CA which signed the client certificate. To use X.509 certificates, you must have access to a CA server (or purchase signings) which will sign certificate requests. If you have your own CA server, you can upload its certificate to the unit and then trust all certificates signed by that CA (select **Trusted CA**).

Under **Info**, upload the client certificate or enter the CA/DN, depending on the authentication type selected above. N.B.: The X.509 certificate you upload here is the client certificate, not the unit's own one.

Under **Local side**, select a public IP address of the unit, and enter a "\*" under **Remote side**. This means that the peer is a road warrior.

Enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.

Select "On" under **RADIUS** to activate RADIUS authentication for this peer.

Note that when RADIUS authentication is used, the peer name must be the same as the user's RADIUS username. This means that you have to create one row per IPsec user.



ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Trusted CA, with DN	/CN=ingate /O=ingate	<input type="checkbox"/>

## 21.6.7. IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the VPN tunnel.

In the **IPsec Networks** table, define the local office network that will be used through the VPN tunnel.

You must also enter the IP address of the authentication server here, either as a part of the office network or as a separate network.

IPsec Networks <a href="#">(Help)</a>					
Edit Row	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
<input type="checkbox"/>	Atlantic network	10.20.30.0	10.20.30.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Boston side	13.7.3.22	13.7.3.22	32	<input type="checkbox"/>
<input type="checkbox"/>	Chicago network	192.168.10.0	192.168.10.0	24	<input type="checkbox"/>
<input type="checkbox"/>	DMZ network	172.16.0.0	172.16.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>

Add new rows  rows.

Under **Peer**, select the newly created VPN tunnel.

Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under **IPsec Networks**.

Under **Remote network**, you have the following options:

- The road warrior has a public IP address on the Internet. Select Remote side address under **Address type**. This means "the same IP address as on the IPsec Peers page".
- The road warrior is located behind a NAT:ing device, and you know which IP network it belongs to. Enter that network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network, allow subset under **Address type** and select the network you just created under **Network**.
- Usually, you won't know the private IP address of the road warrior in advance, or it will change a lot. You might not even know if the client is NAT:ed or not.

Select Remote/private address as the **Address type**. This will allow all private IP addresses as well as the public address presented by the client at the negotiation.

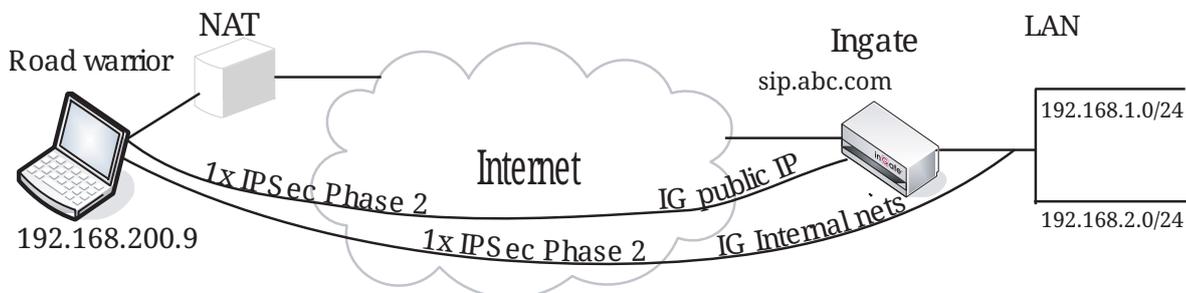
When **Network** or **Network, allow subset** was selected, there must be a line for every pair of

networks that should be able to communicate with each other through the VPN connection.

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both VPN peers.

IPsec Peers		IPsec Tunnels			IPsec Cryptos		IPsec Certificates		IPsec Settings		Authentication Server		IPsec Status		PPTP		PPTP Status	
<b>IPsec Tunnels</b> <a href="#">(Help)</a> These settings are called "Phase 2 settings" in some other IPsec products.																		
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row								
		Address Type	Network	NAT As	Address Type	Network												
<input type="checkbox"/>	+ Martin	Network	Office network	-	Remote/private address	-	1800	AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>								

### 21.6.8. SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the unit, i.e. to a DMZ range.
- The external IP (or DMZ range) of the unit is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

### 21.6.9. Networks and Computers

Go to the **Networks and Computers** page under **Network** and make sure that there are groups for all networks that will use the VPN tunnel. These are used for building rules for the VPN traffic. You

don't need a network for the authentication server.

The network on the other side of the VPN tunnel (see VPN network in the example) must have "-" selected under **Interface**.

Networks and Computers									
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row	
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	+ DHCP clients	-	10.22.0.0	10.22.0.0	10.22.0.255	10.22.0.255	DHCP (eth3 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ DMZ	-	172.16.0.0	172.16.0.0	172.16.0.255	172.16.0.255	DMZ (eth2 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Everywhere	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>	
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Mail server	-	10.47.2.13	10.47.2.13			Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ PPTP	-	10.7.0.100	10.7.0.100	10.7.0.150	10.7.0.150	-	<input type="checkbox"/>	
<input type="checkbox"/>	+ VPN network	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>	

### 21.6.10. Rules

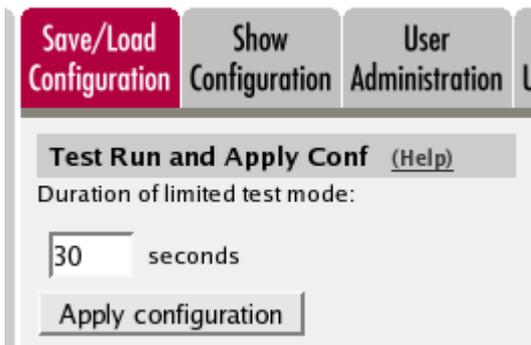
Go to the **Rules** page and create rules to let traffic through the VPN tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the VPN tunnel under **From VPN** if the **Client** network is the road warrior network. Select the VPN tunnel under **To VPN** if the **Server** network is the road warrior network.

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	VPN network	Martin	Office network	-	(VPN) -> Internal	tcp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	VPN network	Martin	Office network	-	(VPN) -> Internal	udp	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	3	Yes	Office network	-	VPN network	Martin	Internal -> (VPN)	udp	Allow	24/7	Local		<input type="checkbox"/>

### 21.6.11. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



### 21.6.12. Configuring the RADIUS Server

Add the unit as a client in the RADIUS server. Make sure that the shared secret here is the same as in the unit.

The unit checks the permissions for a user by looking at its RADIUS attribute *Service-Type*.

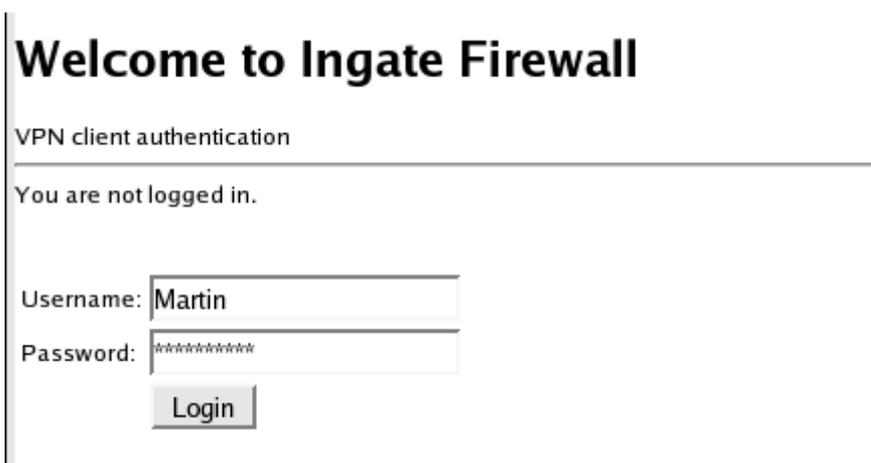
If the value is *Framed (2)*, the user is allowed to connect via VPN.

### 21.6.13. Configuring the Client

The road warrior itself must also be configured. The exact moves for this is of course dependant of what client software you use. See <http://www.ingate.com/Interaction.php> for configuration instructions for several VPN clients.

When the user wants to use the IPsec connection, she starts with directing her web browser to the IP address selected under Authentication Server. Note that https must be used!

This will present a RADIUS login page where the user enters her RADIUS username and password/PIN code.



When the username and password/PIN code has been verified by the RADIUS server, the connection is set up for the user.

## 21.7. How to configure IPsec connections with NAT

You might want to NAT the traffic through an IPsec tunnel. A reason for wanting this could be that the networks on each side of the tunnel clash, thus making routing decisions tricky.

In this example we assume that computers on one side (client side) wants to contact servers on the other side of the tunnel (server side). The configuration needed for this is presented here.

NB! If the IPsec peer is not an Ingate unit, some settings might differ from what is shown here. The primary setting which will not look the same is which networks are involved in the IPsec negotiation. The local networks (sharing the same IP interval) will never be used in the negotiation; only the IP addresses used to NAT the traffic.

### 21.7.1. Client Side

On the client side, the IPsec connection must be defined, and rules to allow traffic going through the tunnel to the server side.

#### IPsec Peers

Start on the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the VPN connection should be established. You also define how the VPN peers should authenticate themselves to each other.

Under **Authentication:Type**, select authentication with a Preshared secret or X.509 certificates. To use X.509 certificates, either both units must be able to sign their own certificates, or you must have access to a CA server which will sign certificate requests. If you have your own CA server, you can upload its certificate to the unit and then trust all certificates signed by that CA (select Trusted CA).

Under **Info**, enter the secret or upload the certificate that should be used for authentication. If you use certificates, you should upload the other unit's certificate here, not the unit's own one.

Under **Local side**, select a public IP address of the unit, and enter a public IP address of the other VPN gateway under **Remote side**.

Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.

The screenshot shows the 'IPsec Peers' configuration page. At the top, there are navigation tabs: IPsec Peers (selected), IPsec Tunnels, IPsec Cryptos, IPsec Certificates, IPsec Settings, Authentication Server, IPsec Status, PPTP, and PPTP Status. Below the tabs, the page title is 'IPsec Peers (Help)' with a note: 'These settings are called "Phase 1 settings" in some other IPsec products.'

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Boston	-	Yes	Outside (193.12.253.115)	13.7.3.22	No	13.7.3.22	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES,3DES	Preshared secret	MD5 Fingerprint: C9:97:87:1F:9E:BF:7C:38:BE:25:85:D6:04:84:2F:F6	<input type="checkbox"/>

## IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. You must define the local office network as well as the IP address or addresses used by the IPsec peer for NATing traffic for its local network.

As the two networks clash, you can't define the remote network directly here. Instead, the local computers need to contact an IP address on the peer outside. The peer then forwards the traffic to the server.

Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Boston	Network	Home network	Outside (193.12.253.115)	Network	Boston side	1800	AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

Then, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under **Network**.

Under **Remote network**, select Network and the network defined below, which consists of the IP address(es) connected to the remote VPN gateway.

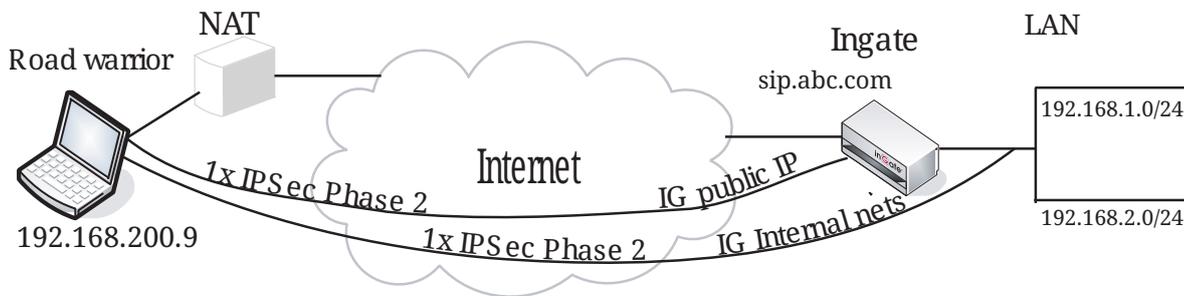
Select to NAT as the outside IP address (the one selected on the **IPsec Peers** page).

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

Edit Row	Name	DNS name or network address	Network address	Netmask / bits	Delete Row
<input type="checkbox"/>	Boston side	13.7.3.22	13.7.3.22	32	<input type="checkbox"/>
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>

## SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the unit, i.e. to a DMZ range.
- The external IP (or DMZ range) of the unit is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

## Networks and Computers

Go to **Networks and Computers** under **Network** to create network groups for the networks that will use the IPsec tunnel. These are used for building rules for the IPsec traffic.

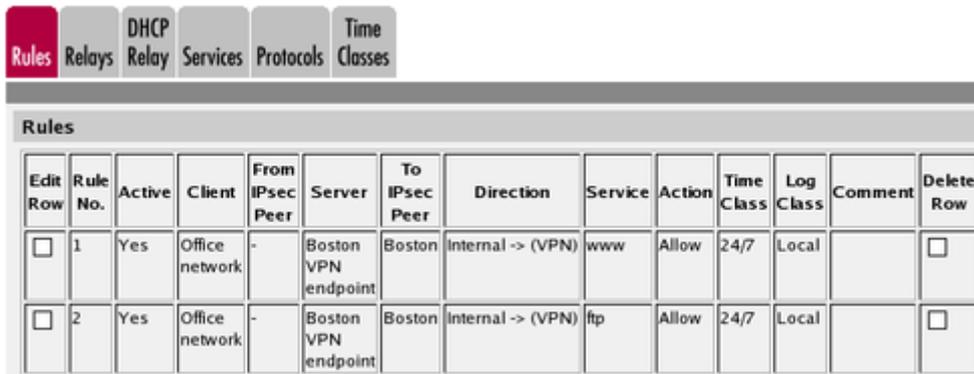
The network on the server side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

Networks and Computers								
<span style="background-color: #800040; color: white; padding: 2px;">Networks and Computers</span> <span style="background-color: #cccccc; padding: 2px;">Default Gateways</span> <span style="background-color: #cccccc; padding: 2px;">All Interfaces</span> <span style="background-color: #cccccc; padding: 2px;">NAT</span> <span style="background-color: #cccccc; padding: 2px;">VLAN</span> <span style="background-color: #cccccc; padding: 2px;">Eth0</span> <span style="background-color: #cccccc; padding: 2px;">Eth1</span> <span style="background-color: #cccccc; padding: 2px;">Eth2</span> <span style="background-color: #cccccc; padding: 2px;">Eth3</span> <span style="background-color: #cccccc; padding: 2px;">Eth4</span> <span style="background-color: #cccccc; padding: 2px;">Eth5</span> <span style="background-color: #cccccc; padding: 2px;">Interface Status</span> <span style="background-color: #cccccc; padding: 2px;">PPPoE</span>								
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ Boston VPN endpoint	-	13.73.22	13.73.22			-	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>

## Rules

Go to the **Rules** page and create rules to let traffic through the IPsec tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the local network under **Client**. Select the IPsec peer under **To IPsec peer** and the peer's network under **Server**. Create rules like this for the services that should be allowed to the server side.

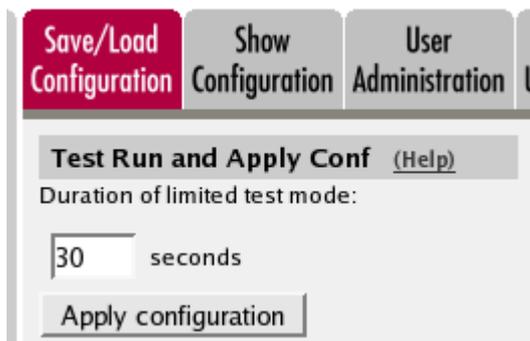


The screenshot shows a web interface with a navigation bar containing 'Rules', 'Relays', 'DHCP Relay', 'Services', 'Protocols', and 'Time Classes'. The 'Rules' tab is active. Below the navigation bar is a table with the following columns: Edit Row, Rule No., Active, Client, From IPsec Peer, Server, To IPsec Peer, Direction, Service, Action, Time Class, Log Class, Comment, and Delete Row. Two rules are listed:

Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Office network	-	Boston VPN endpoint	Boston	Internal -> (VPN)	www	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	Office network	-	Boston VPN endpoint	Boston	Internal -> (VPN)	ftp	Allow	24/7	Local		<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



The screenshot shows a web interface with a navigation bar containing 'Save/Load Configuration', 'Show Configuration', 'User Administration', and 'U'. The 'Save/Load Configuration' tab is active. Below the navigation bar is a section titled 'Test Run and Apply Conf (Help)'. It contains a label 'Duration of limited test mode:' followed by a text input field containing '30' and the word 'seconds'. Below this is a button labeled 'Apply configuration'.

## 21.7.2. Server Side

On the server side, the IPsec connection must be defined, and relays to forward the received traffic to the servers on the inside.

### IPsec Peers

Start on the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the VPN connection should be established. You also define how the VPN peers should authenticate themselves to each other.

Under **Authentication:Type**, select authentication with a Preshared secret or X.509 certificates. To use X.509 certificates, either both units must be able to sign their own certificates, or you must have access to a CA server which will sign certificate requests. If you have your own CA server, you can upload its certificate to the unit and then trust all certificates signed by that CA (select Trusted CA).

Under **Info**, enter the secret or upload the certificate that should be used for authentication. If you

use certificates, you should upload the other unit's certificate here, not the unit's own one.

Under **Local side**, select a public IP address of the unit, and enter a public IP address of the other VPN gateway under **Remote side**.

Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both VPN peers.

IPsec Peers (Help)									
These settings are called "Phase 1 settings" in some other IPsec products.									
Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Seattle	-	Yes	Outside (13.73.22)	193.12.253.115	No	193.12.253.115	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	Preshared secret	MD5 Fingerprint: C9:97:87:1F:9E:BF:7C:38:BE:25:85:D6:04:84:2F:F6	<input type="checkbox"/>

## IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. You must define the local office network as well as the IP address or addresses used by the IPsec peer for NATing traffic from its local network.

As the two networks clash, you can't define the remote network directly here. Instead, use the IP address from which the traffic seems to be sent.

IPsec Networks (Help)					
Edit Row	Name	DNS name or network address	Network address	Netmask / bits	Delete Row
<input type="checkbox"/>	Home network	10.47.0.0	10.47.0.0	16	<input type="checkbox"/>
<input type="checkbox"/>	Seattle side	193.12.253.115	193.12.253.115	32	<input type="checkbox"/>

Then, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under Network.

Under **Remote network**, select Network and the network defined below, which consists of the IP address(es) connected to the remote VPN gateway.

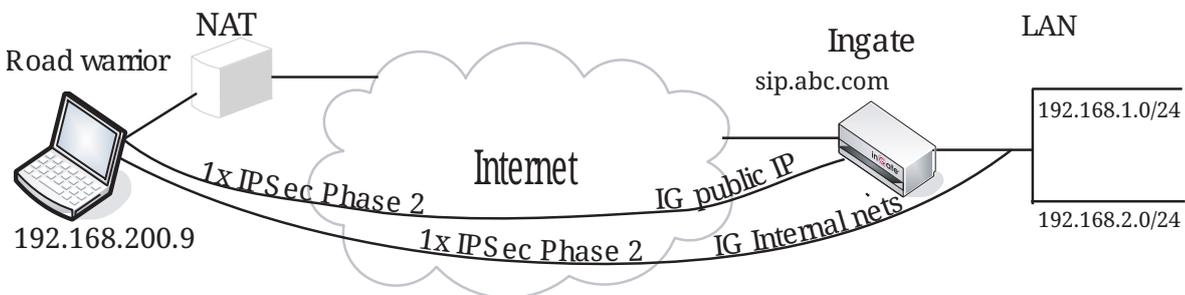
Select to NAT as the outside IP address (the one selected on the **IPsec Peers** page).

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

IPsec Tunnels (Help)										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Seattle	Network	Home network	Outside (13.7.3.22)	Network	Seattle side		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

### SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the unit, i.e. to a DMZ range.
- The external IP (or DMZ range) of the unit is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

### Networks and Computers

Go to **Networks and Computers** under **Network** to create a network group for the remote network

that will use the IPsec tunnel. This will be used to define which computers can use the relay that will forward traffic to the inside servers.

The network on the client side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

Networks and Computers										
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row		
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address				
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	+ Office network	-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>		
<input type="checkbox"/>	+ Seattle VPN endpoint	-	193.12.253.115	193.12.253.115			-	<input type="checkbox"/>		

## Relays

Go to the **Relays** page and create relays to forward traffic from the IPsec tunnel to the inside servers.

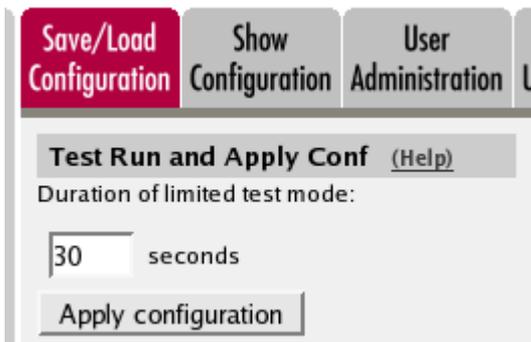
Select to Listen to an IP address on the outside. This IP address must be listed among the IP addresses for which the client side makes the IPsec negotiation.

Enter the IP address and port for the server under **Relay to** and select the appropriate relay type. Select the **IPsec peer** under IPsec peer and the client network under **Network**.

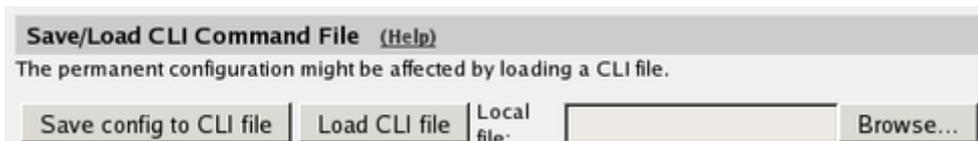
Relays											
Edit Row	Listen to ...		Relay to ...			Relay type	Allow access from ...		Time class	Log class	Delete Row
	IP address	Port	DNS name or IP address	IP address	Port		Network	IPsec peer			
<input type="checkbox"/>	Outside (13.7.3.22)	80	10.47.4.38	10.47.4.38	80	TCP relay	Seattle VPN endpoint	Seattle	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	Outside (13.7.3.22)	21	10.47.4.75	10.47.4.75	21	FTP relay	Seattle VPN endpoint	Seattle	24/7	Local	<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



## 21.8. IPsec Connection With NAT, Client Side has a Dynamic IP Address

You might want to NAT the traffic through an IPsec tunnel. A reason for wanting this could be that the networks on each side of the tunnel clash, thus making routing decisions tricky.

In this example we assume that computers on one side (client side) wants to contact servers on the other side of the tunnel (server side), and that the IPsec peer of the client side has a dynamic IP address. The configuration needed for this is presented here.

NB! If the IPsec peer is not an Ingate unit, some settings might differ from what is shown here. The primary setting which will not look the same is which networks are involved in the IPsec negotiation. The local networks (sharing the same IP interval) will never be used in the negotiation; only the IP addresses used to NAT the traffic.

### 21.8.1. Client Side

On the client side, the IPsec connection must be defined, and rules to allow traffic going through the tunnel to the server side.

#### Certificates

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

Private Certificates (Help)					
Name	Certificate			Information	Delete
VPN cert	Create New	Import	View/Download	Subject: /CN=home.ingate.com Issuer: /CN=home.ingate.com MDS Fingerprint: CD:6F:19:99:1C:4E:3C:94:C0:9B:F8:37:AD:5B:41:E0 Valid to: 2009-07-24 11:53:57	<input type="checkbox"/>

Enter information about the unit in the form, and press **Create a self-signed X.509 certificate**.

**Create Certificate or Certificate Request**  
Fill in the certificate data for "VPN cert" below, then create either a certificate or a certificate request.  
After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days): \* 365  
Country code (C):  
Organization (O):  
Common Name (CN): \* ome.ingate.com  
State/province (ST):  
Organizational Unit (OU):  
Email address:  
Locality/town (L):

If you generate several certificates with identical data you should make sure they have different serial numbers.  
Serial number: \* 0  
Fields marked with "\*" are mandatory.

Below you can enter an optional challenge password for certificate requests.  
Challenge password:  
Challenge password again:

Create a self-signed X.509 certificate | Create an X.509 certificate request | Abort

When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

## IPsec Certificates

Go to **IPsec Certificates** under Virtual Private Networks and select that the unit should use the newly created certificate for IPsec negotiations.

IPsec Peers | IPsec Tunnels | IPsec Cryptos | **IPsec Certificates** | IPsec Settings | Authentication Server | IPsec Status | PPTP | PPTP Status

**Local X.509 Certificate** (Help)  
Use this certificate for IPsec:  
VPN cert ▼

**IPsec CA Certificates** (Help)  
Edit Row | CA | Delete Row  
Add new rows | 1 | rows.

## IPsec Peers

Go to the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the IPsec connection should be established. You also define how the IPsec peers should authenticate themselves to each other.

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the other unit's certificate.

Under **Local side**, select the interface with the dynamic IP address, and enter a public IP address of the other IPsec gateway under **Remote side**.

Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both IPsec peers.

IPsec Peers <a href="#">(Help)</a>									
These settings are called "Phase 1 settings" in some other IPsec products.									
Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Main office		Yes	Internet (eth1)	88.131.69.205	No	88.131.69.205	No	

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/DES	X.509 certificate	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MD5 Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	<input type="checkbox"/>

### IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. You must define the local office network as well as the IP address or addresses used by the IPsec peer for NATing traffic for its local network.

As the two networks clash, you can't define the remote network directly here. Instead, the local computers need to contact an IP address on the peer outside. The peer then forwards the traffic to the server.

IPsec Networks <a href="#">(Help)</a>					
Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
<input type="checkbox"/>	LAN	192.168.0.0	192.168.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Remote side	88.131.69.205	88.131.69.205	32	<input type="checkbox"/>

Then, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under **Network**.

Under **Remote network**, select Network and the network defined below, which consists of the IP address(es) connected to the remote VPN gateway.

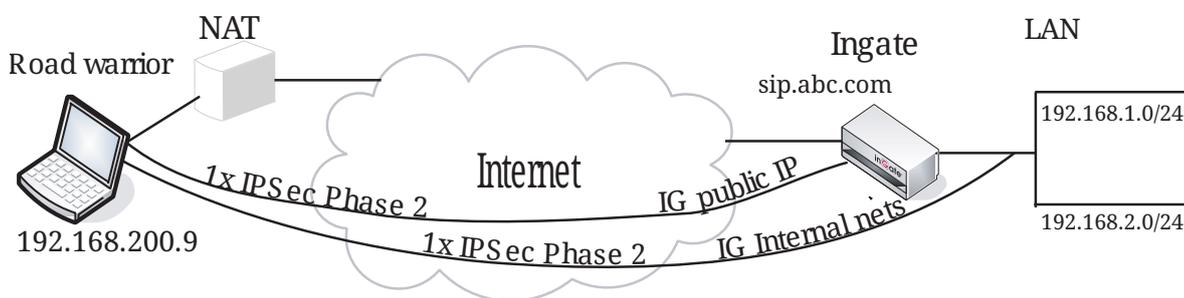
Select to NAT as the outside IP address (the one selected on the **IPsec Peers** page).

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

IPsec Tunnels (Help)										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Main office	Network	LAN	Internet (eth1)	Network	Remote side		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

### SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the unit, i.e. to a DMZ range.
- The external IP (or DMZ range) of the unit is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

### Networks and Computers

Go to **Networks and Computers** under **Network** to create network groups for the networks that will use the IPsec tunnel. These are used for building rules for the IPsec traffic.

The network on the server side of the IPsec tunnel must consist of the IP address(es) that are used

to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

<b>Networks and Computers</b>	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Networks and Computers												
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row				
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address						
<input type="checkbox"/>	+ LAN	-	192.168.0.0	192.168.0.0	192.168.0.255	192.168.0.255	Ethernet2 (eth2 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ Remote VPN	-	88.131.69.205	88.131.69.205			-	<input type="checkbox"/>				

## Rules

Go to the **Rules** page and create rules to let traffic through the IPsec tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the local network under **Client**. Select the IPsec peer under **To IPsec peer** and the peer's network under **Server**. Create rules like this for the services that should be allowed to the server side.

<b>Rules</b>	Relays	DHCP Relay	Services	Protocols	Time Classes								
Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	LAN	-	Remote VPN	Main office	Ethernet2 -> (VPN)	pop3	Allow	24/7	Local		<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

<b>Save/Load Configuration</b>	Show Configuration	User Administration
<b>Test Run and Apply Conf</b> <a href="#">(Help)</a>		
Duration of limited test mode:		
<input type="text" value="30"/>	seconds	
<input type="button" value="Apply configuration"/>		

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

<b>Save/Load CLI Command File</b> <a href="#">(Help)</a>			
The permanent configuration might be affected by loading a CLI file.			
<input type="button" value="Save config to CLI file"/>	<input type="button" value="Load CLI file"/>	Local file:	<input type="text"/> <input type="button" value="Browse..."/>

## 21.8.2. Server Side

On the server side, the IPsec connection must be defined, and relays to forward the received traffic to the servers on the inside.

### Certificates

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

Private Certificates <a href="#">(Help)</a>						
Edit	Name	Certificate			Information	Delete
<input checked="" type="checkbox"/>	VPN cert	Create New	Import	View/Download	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MDS Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	<input type="checkbox"/>

Enter information about the unit in the form, and press **Create a self-signed X.509 certificate**.

#### Create Certificate or Certificate Request

Fill in the certificate data for "VPN cert" below, then create either a certificate or a certificate request.  
After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days):	Country code (C):	Organization (O):
* 365	<input type="text"/>	<input type="text"/>
Common Name (CN):	State/province (ST):	Organizational Unit (OU):
* vpn.ingate.com	<input type="text"/>	<input type="text"/>
Email address	Locality/town (L):	
<input type="text"/>	<input type="text"/>	

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number:

\*

Fields marked with "\*" are mandatory.

Below you can enter an optional challenge password for certificate requests.

Challenge password:

Challenge password again:

### IPsec Certificates

Go to **IPsec Certificates** under Virtual Private Networks and select that the unit should use the newly created certificate for IPsec negotiations.

IPsec Peers	IPsec Tunnels	IPsec Cryptos	<b>IPsec Certificates</b>	IPsec Settings	Authentication Server	IPsec Status	PPTP	PPTP Status
-------------	---------------	---------------	---------------------------	----------------	-----------------------	--------------	------	-------------

#### Local X.509 Certificate [\(Help\)](#)

Use this certificate for IPsec:

▼

#### IPsec CA Certificates [\(Help\)](#)

rows.

### IPsec Peers

Go to the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses

between which the IPsec connection should be established. You also define how the IPsec peers should authenticate themselves to each other.

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the *other* unit's certificate.

Under **Local side**, select the interface with the public IP address. Under **Remote side**, enter "\*", which means that the peer has a dynamic IP address.

Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both IPsec peers.

IPsec Peers (Help)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Branch office	-	Yes	Internet (88.131.69.205)	*	No	*	No	*

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	X.509 certificate	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MD5 Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	<input type="checkbox"/>

## IPsec Tunnels

On the **IPsec Tunnels** page, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Local side address as the **Address type**.

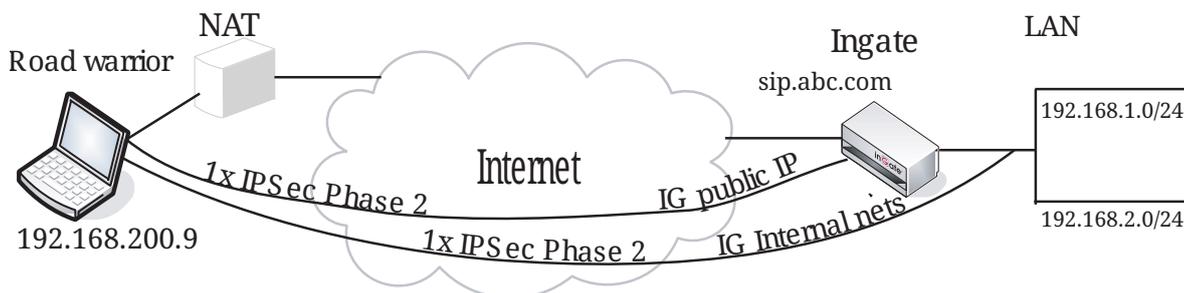
Under **Remote network**, select Remote side address.

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

IPsec Peers		IPsec Tunnels		IPsec Cryptos		IPsec Certificates		IPsec Settings		Authentication Server		IPsec Status		PPTP		PPTP Status	
<b>IPsec Tunnels</b> <a href="#">(Help)</a>																	
These settings are called "Phase 2 settings" in some other IPsec products.																	
Edit Row	Peer	Local Network			Remote Network			IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row						
		Address Type	Network	NAT As	Address Type	Network											
<input type="checkbox"/>	+ Branch office	Local side address	-	-	Remote side address	-	-	-	AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>						

## SIP through IPsec



Additionally, for SIP to work over your IPsec connections, you require a tunnel under **IPsec tunnels** between the client and the **public** IP address of the unit, i.e. the Local side address under **IPsec Peers**. This requires a Phase 2 connection in the client (The Greenbow) also.

Example: if your DNS record sip.abc.com points to the WAN IP of the unit then you must have a tunnel between the client and this IP address.

This is so that all SIP and RTP media through the b2bua or proxy is permitted.

Ensure that:

- The remote (road warrior) client also has a tunnel/Phase2 to the external IP of the unit. This means "the same IP address as on the IPsec Peers page". Optionally, a tunnel to a network or subnet that includes the external IP of the unit, i.e. to a DMZ range.
- The external IP (or DMZ range) of the unit is a network in the **IPsec Networks** table. In the **IPsec Tunnels** table, select Network under **Address type** and select the network you just created under **IPsec Networks**.

## Networks and Computers

Go to **Networks and Computers** under **Network** to create a network group for the remote network that will use the VPN tunnel. This will be used to define which computers can use the relay that will forward traffic to the inside servers.

The network on the client side of the VPN tunnel must consist of the IP address that is used to NAT the traffic on that side. As this IP address is dynamic, all IP addresses need to be included in the

network.

Select "-" under **Interface/VLAN**.

Networks and Computers		Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Networks and Computers													
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row					
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address							
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>					

### Relays

Go to the **Relays** page and create relays to forward traffic from the IPsec tunnel to the inside servers.

Select to Listen to an IP address on the outside. This IP address must be listed among the IP addresses for which the client side makes the IPsec negotiation.

Enter the IP address and port for the server under **Relay to** and select the appropriate relay type. Select the **IPsec peer** under IPsec peer and the client network under **Network**.

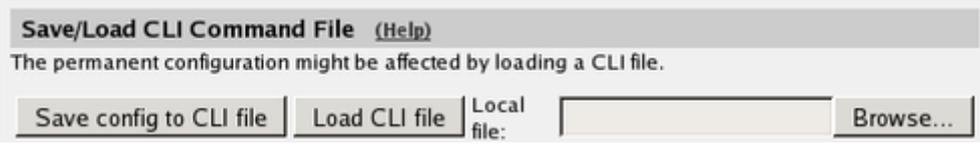
Relays (Help)												
Edit	Listen To ...		Relay To ...			Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class	Log Class	Delete
	IP Address	Port	DNS Name or IP Address	IP Address	Port		Network	IPsec Peer				
<input type="checkbox"/>	Internet (88.131.69.205)	110	192.168.0.33	192.168.0.33	110	TCP port forwarding	All	Branch office	-	24/7	Local	<input type="checkbox"/>

### Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

Save/Load Configuration	Show Configuration	User Administration	U
<b>Test Run and Apply Conf (Help)</b>			
Duration of limited test mode:			
<input type="text" value="30"/>	seconds		
<input type="button" value="Apply configuration"/>			

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



# 21.9. IPsec Connection With NAT, Server Side has a Dynamic IP Address

You might want to NAT the traffic through an IPsec tunnel. A reason for wanting this could be that the networks on each side of the tunnel clash, thus making routing decisions tricky.

In this example we assume that computers on one side (client side) wants to contact servers on the other side of the tunnel (server side), and that the IPsec peer of the server side has a dynamic IP address. The configuration needed for this is presented here.

NB! If the IPsec peer is not an Ingate unit, some settings might differ from what is shown here. The primary setting which will not look the same is which networks are involved in the IPsec negotiation. The local networks (sharing the same IP interval) will never be used in the negotiation; instead the IP addresses used to NAT the traffic are used.

## 21.9.1. Server Side

On the server side, the IPsec connection must be defined, and relays to forward the received traffic to the servers on the inside.

As the server side has a dynamic public IP address, it is not possible to make the client side use this address when contacting servers. Instead, you need to set up an extra IP network on the inside, just for forwarding traffic to the inside servers.

In this example, the common network for both sides is 192.168.0.0/24, and the extra IP network on the server side is 172.16.20.0/24.

### Interface

Go to **Interface** and create a new network for the traffic forwarding in the **Directly Connected Networks** table.

Directly Connected Networks (Help)										
Edit Row	Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
<input type="checkbox"/>	LAN	Static	192.168.0.1	192.168.0.1	24	192.168.0.0	192.168.0.255		-	<input type="checkbox"/>
<input type="checkbox"/>	Relay Net	Static	172.16.20.1	172.16.20.1	24	172.16.20.0	172.16.20.255		-	<input type="checkbox"/>

In the **Alias** table, add alias IP addresses for the server that should be reachable over the IPsec connection.

**Alias** (Help)

Below are the ranges from which you can select aliases.

172.16.20.1-172.16.20.254

192.168.0.1-192.168.0.254

Edit Row	Name	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	FTP Server	172.16.20.34	172.16.20.34	<input type="checkbox"/>
<input type="checkbox"/>	pop3 Server	172.16.20.33	172.16.20.33	<input type="checkbox"/>

**Certificates**

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.

**Private Certificates** (Help)

Name	Certificate			Information	Delete
VPN cert	Create New	Import	View/Download	Subject: /CN=home.ingate.com Issuer: /CN=home.ingate.com MDS Fingerprint: CD:6F:19:99:1C:4E:3C:94:C0:9B:F8:37:AD:5B:41:E0 Valid to: 2009-07-24 11:53:57	<input type="checkbox"/>

Enter information about the unit in the form, and press **Create a self-signed X.509 certificate**.

**Create Certificate or Certificate Request**

Fill in the certificate data for "VPN cert" below, then create either a certificate or a certificate request.

After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the firewall.

Expire in (days): \* 365      Country code (C):      Organization (O):

Common Name (CN): \* home.ingate.com      State/province (ST):      Organizational Unit (OU):

Email address      Locality/town (L):

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number: \* 0

Fields marked with "\*" are mandatory.

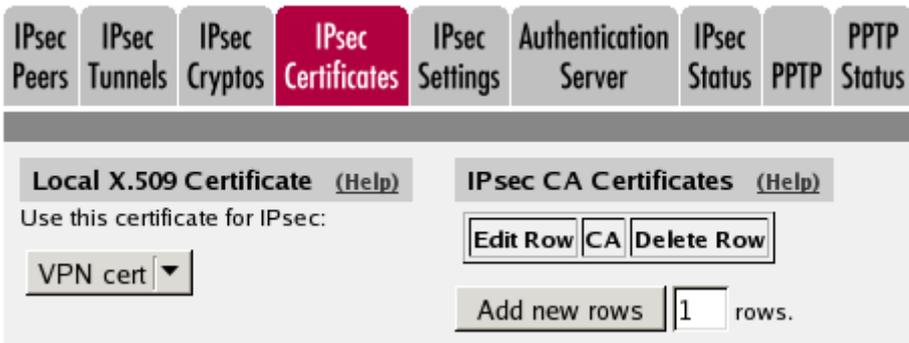
Below you can enter an optional challenge password for certificate requests.

Challenge password:      Challenge password again:     

When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

**IPsec Certificates**

Go to **IPsec Certificates** under **Virtual Private Networks** and select that the unit should use the newly created certificate for IPsec negotiations.



## IPsec Peers

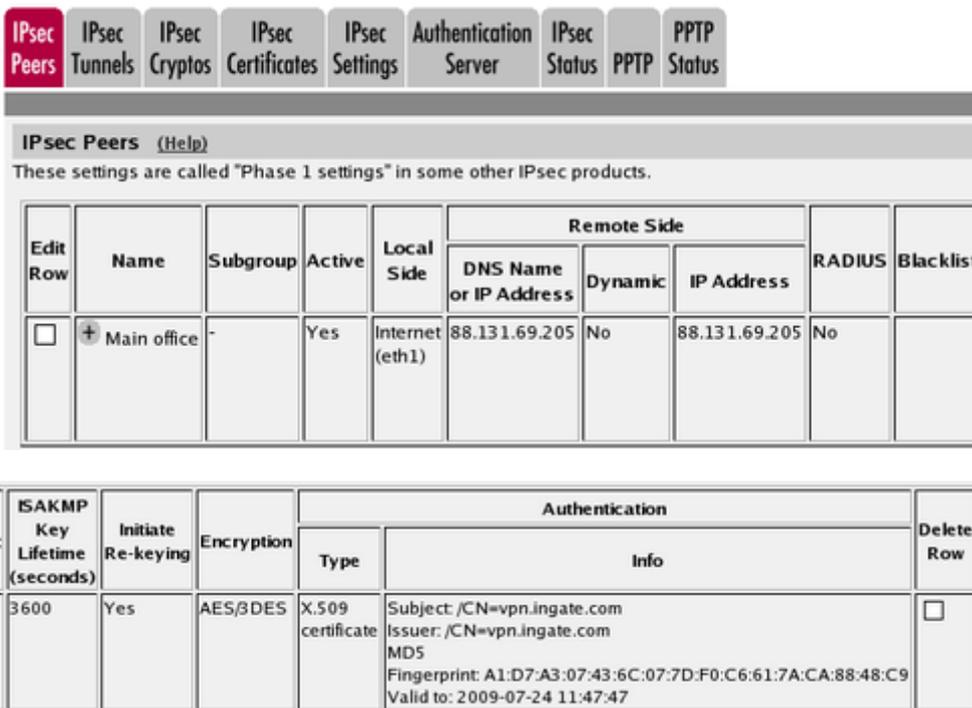
Go to the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the IPsec connection should be established. You also define how the IPsec peers should authenticate themselves to each other.

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the other unit's certificate.

Under **Local side**, select the interface with the dynamic IP address, and enter a public IP address of the other IPsec gateway under **Remote side**.

Select On under Status, select Off under RADIUS, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both IPsec peers.



## IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. Define the extra network that was created for the servers.

As the two office networks clash, you can't define the remote network directly here. Instead, the IP address from which the traffic seems to be sent will be used directly in the **IPsec Tunnels** table.

IPsec Networks <a href="#">(Help)</a>					
Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
<input type="checkbox"/>	Relay network	172.16.20.0	172.16.20.0	24	<input type="checkbox"/>

Then, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Network as the **Address type** and the server network that you defined below under Network.

Under **Remote network**, select Remote side address.

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

IPsec Tunnels <a href="#">(Help)</a>										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Main office	Network	Relay network	-	Remote side address	-		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

### 21.9.2. Networks and Computers

Go to **Networks and Computers** under **Network** to create a network group for the remote network that will use the IPsec tunnel. This will be used to define which computers can use the relay that will forward traffic to the inside servers.

The network on the client side of the IPsec tunnel must consist of the IP address(es) that are used to NAT the traffic on that side. This network must have "-" selected under **Interface/VLAN**.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
------------------------	------------------	----------------	-----	------	------	------	------	------	------	------	------------------	-------

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ LAN	-	192.168.0.0	192.168.0.0	192.168.0.255	192.168.0.255	Ethernet2 (eth2 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Remote IP	-	88.131.69.205	88.131.69.205			-	<input type="checkbox"/>

## Relays

Go to the **Relays** page and create relays to forward traffic from the IPsec tunnel to the inside servers.

Select to Listen to an IP address on the server network. This IP address must be listed among the IP addresses for which the client side makes the IPsec negotiation.

Enter the IP address and port for the server under **Relay to** and select the appropriate relay type. Select the **IPsec peer** under IPsec peer and the client network under **Network**.

Rules	Relays	DHCP Relay	Services	Protocols	Time Classes
-------	--------	------------	----------	-----------	--------------

Edit Row	Listen To ...		Relay To ...			Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class	Log Class	Delete Row
	IP Address	Port	DNS Name or IP Address	IP Address	Port		Network	IPsec Peer				
<input type="checkbox"/>	FTP Server (172.16.20.34)	21	192.168.0.34	192.168.0.34	21	FTP relay	Remote IP	Main office	-	24/7	Local	<input type="checkbox"/>
<input type="checkbox"/>	pop3 Server (172.16.20.33)	110	192.168.0.33	192.168.0.33	110	TCP port forwarding	Remote IP	Main office	-	24/7	Local	<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply** configuration.

Save/Load Configuration	Show Configuration	User Administration
-------------------------	--------------------	---------------------

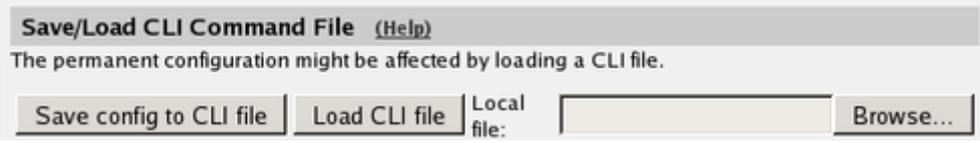
  

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.



### 21.9.3. Client Side

On the client side, the IPsec connection must be defined, and rules to allow traffic going through the tunnel to the server side.

#### Certificates

As one of the IPsec peers has a dynamic IP address, the IPsec authentication must be performed with X.509 certificates. Create a certificate on the **Certificates** page.

Add a new row to the **Private Certificates** table and enter a name for this certificate. Press **Create new**.



Enter information about the unit in the form, and press **Create a self-signed X.509 certificate**.



When the certificate has been created, download it as a PEM or DER certificate. This certificate should then be uploaded on the **IPsec Peers** page of the other unit.

#### IPsec Certificates

Go to **IPsec Certificates** under **Virtual Private Networks** and select that the unit should use the newly created certificate for IPsec negotiations.

[IPsec Peers](#)
[IPsec Tunnels](#)
[IPsec Cryptos](#)
[IPsec Certificates](#)
[IPsec Settings](#)
[Authentication Server](#)
[IPsec Status](#)
[PPTP](#)
[PPTP Status](#)

---

[Local X.509 Certificate](#) [\(Help\)](#)
[IPsec CA Certificates](#) [\(Help\)](#)

Use this certificate for IPsec:

rows.

## IPsec Peers

Go to the **IPsec Peers** page under **Virtual Private Networks**, where you define the IP addresses between which the IPsec connection should be established. You also define how the IPsec peers should authenticate themselves to each other.

Under **Authentication:Type**, select X.509 certificates.

Under **Info**, upload the *other* unit's certificate.

Under **Local side**, select the interface with the public IP address. Under **Remote side**, enter "\*", which means that the peer has a dynamic IP address.

Select On under **Status**, select Off under **RADIUS**, and enter a lifetime for the ISAKMP (IKE) keys. The lifetime must be the same on both IPsec peers.

[IPsec Peers](#)
[IPsec Tunnels](#)
[IPsec Cryptos](#)
[IPsec Certificates](#)
[IPsec Settings](#)
[Authentication Server](#)
[IPsec Status](#)
[PPTP](#)
[PPTP Status](#)

---

[IPsec Peers](#) [\(Help\)](#)

These settings are called "Phase 1 settings" in some other IPsec products.

Edit Row	Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist
					DNS Name or IP Address	Dynamic	IP Address		
<input type="checkbox"/>	+ Branch office	-	Yes	Internet (88.131.69.205)	*	No	*	No	*

ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
			Type	Info	
3600	Yes	AES/3DES	X.509 certificate	Subject: /CN=vpn.ingate.com Issuer: /CN=vpn.ingate.com MD5 Fingerprint: A1:D7:A3:07:43:6C:07:7D:F0:C6:61:7A:CA:88:48:C9 Valid to: 2009-07-24 11:47:47	<input type="checkbox"/>

## IPsec Tunnels

Next, go to the **IPsec Tunnels** page and enter the networks which will use the IPsec tunnel.

In the **IPsec Networks** table, define the networks that will connect through the IPsec tunnel. You must define the local office network as well as the remote server network.

IPsec Networks (Help)					
Edit	Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete
<input type="checkbox"/>	LAN	192.168.0.0	192.168.0.0	24	<input type="checkbox"/>
<input type="checkbox"/>	Servers	172.16.20.0	172.16.20.0	24	<input type="checkbox"/>

Then, create a new row in the **IPsec Tunnels** table. Under **Peer**, select the newly created IPsec peer.

Under **Local network**, select Network as the **Address type** and the local network (connected to the unit) that you defined below under **Network**.

Under **Remote network**, select Network and the network defined below, which consists of the IP address(es) connected to the remote VPN gateway.

The IPsec key lifetime is optional, but if you enter a lifetime, it must be the same on both IPsec peers.

Select AES/3DES as encryption algorithm.

IPsec Peers	IPsec Tunnels	IPsec Cryptos	IPsec Certificates	IPsec Settings	Authentication Server	IPsec Status	PPTP	PPTP Status		
IPsec Tunnels (Help)										
These settings are called "Phase 2 settings" in some other IPsec products.										
Edit Row	Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
		Address Type	Network	NAT As	Address Type	Network				
<input type="checkbox"/>	+ Branch office	Network	LAN	Internet (88.131.69.205)	Network	Servers		AES/3DES	Same as Phase 1 DH	<input type="checkbox"/>

## Networks and Computers

Go to **Networks and Computers** under **Network** to create network groups for the networks that will use the IPsec tunnel. These are used for building rules for the IPsec traffic.

The network on the server side of the IPsec tunnel must be the extra server network. This network must have "-" selected under **Interface/VLAN**.

Networks and Computers	Default Gateways	All Interfaces	NAT	VLAN	Eth0	Eth1	Eth2	Eth3	Eth4	Eth5	Interface Status	PPPoE
Networks and Computers												
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row				
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address						
<input type="checkbox"/>	+ LAN	-	192.168.0.0	192.168.0.0	192.168.0.255	192.168.0.255	Ethernet0 (eth0 untagged)	<input type="checkbox"/>				
<input type="checkbox"/>	+ Server network	-	172.16.20.0	172.16.20.0	172.16.20.255	172.16.20.255	-	<input type="checkbox"/>				

## Rules

Go to the **Rules** page and create rules to let traffic through the IPsec tunnel. If there are no rules, no traffic will be let through, even if the tunnel is established.

Select the local network under **Client**. Select the IPsec peer under **To IPsec peer** and the peer's network under **Server**. Create rules like this for the services that should be allowed to the server side.

Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	LAN	-	Server network Branch office	Branch office	Ethernet0 -> (VPN)	pop3	Allow	24/7	Local		<input type="checkbox"/>
<input type="checkbox"/>	2	Yes	LAN	-	Server network Branch office	Branch office	Ethernet0 -> (VPN)	ftp	Allow	24/7	Local		<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** Show Configuration User Administration U

**Test Run and Apply Conf** (Help)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** (Help)

The permanent configuration might be affected by loading a CLI file.

Local file:

## 21.10. How To Configure PPTP Passthrough

Sometimes, you might want to let PPTP traffic through the unit instead of using it as a PPTP endpoint. If the PPTP traffic is not NATed between the unit inside and outside, this will be a simple setting. Usually, some inside networks are NATed, and the settings then become more advanced.

In this example, you find settings for letting NATed PPTP through for an inside as well as an outside PPTP client.

## 21.10.1. PPTP client on the inside

Sometimes you have a few PPTP clients on the unit inside, which should be allowed to access PPTP servers on the Internet. It could be that you have guests who want to access their office. Here, settings for this are shown.

### Networks and Computers

First, create a network for the inside computers on the **Networks and Computers** page under **Network** (see the "Guest network" in the screen shot below).

Networks and Computers								
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>
<input type="checkbox"/>	+ Guest network	-	10.7.0.1	10.7.0.1	10.7.0.100	10.7.0.100	Guests (eth3 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>
<input type="checkbox"/>	+ Office network	-	10.10.0.0	10.10.0.0	10.10.0.255	10.10.0.255	Internal (eth0 untagged)	<input type="checkbox"/>
<input type="checkbox"/>		-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>

### Services

Then, go to the **Services** page under **Rules and Relays** and define the service to manage the NATed PPTP traffic. Use TCP as the **Protocol**, Dynamic PPTP management as the **Firewall type**, and **Server ports** 1723. Give the new service a descriptive name.

Services								
Edit row	Name	Subgroup	Protocol	Firewall type	Client ports	Server ports	ICMP type	Delete row
<input type="checkbox"/>	+ PPTP passthrough	-	TCP	Dynamic PPTP management	1-65535	1723		<input type="checkbox"/>

### Rules

Go to the **Rules** page and create a rule to let the PPTP traffic through from the inside to the Internet. Use the newly created service. You don't need a rule for the return traffic - the service will automatically set up rules for this.

Make sure that this rule is placed before other rules that might allow traffic from the clients to the PPTP server, like a general rule which lets through all traffic from the inside. You might have to renumber the rule to move it higher up in the list.

Rules													
Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	Guest network	-	Internet	-	Guests -> External (NAT:ed)	PPTP passthrough	Allow	24/7	Local		<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** | **Show Configuration** | **User Administration** | **U**

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

**Apply configuration**

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** [\(Help\)](#)

The permanent configuration might be affected by loading a CLI file.

**Save config to CLI file** | **Load CLI file** | Local file:  **Browse...**

## 21.10.2. PPTP client on the outside

For various reasons, you might want to use a separate PPTP server behind the unit instead of the built-in unit server. If the PPTP server is located on a non-NATed network, this is very simple. If NAT is involved, some more settings are required. Here, such a setup is shown.

### Networks and Computers

First, create a network for the PPTP server on the **Networks and Computers** page under **Network**.

Networks and Computers									
Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row	
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	+ All	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	-	<input type="checkbox"/>	
<input type="checkbox"/>	+ Internet	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	External (eth1 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ Office network	-	10.10.0.0	10.10.0.0	10.10.0.255	10.10.0.255	Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>		-	10.47.0.0	10.47.0.0	10.47.255.255	10.47.255.255	Internal (eth0 untagged)	<input type="checkbox"/>	
<input type="checkbox"/>	+ PPTP server	-	172.16.0.5	172.16.0.5			DMZ (eth2 untagged)	<input type="checkbox"/>	

## Relays

Go to the **Relays** page under **Rules and Relays** and create a TCP relay which should listen to port 1723 on the unit outside and forward the traffic to the PPTP server. Select TCP port forwarding as the **Relay type**.

The client should connect to the outside unit IP address.

Relays											
Edit row	Listen to ...		Relay to ...			Relay type	Allow access from ...		Time class	Log class	Delete row
	IP address	Port	DNS name or IP address	IP address	Port		Network	IPsec peer			
<input type="checkbox"/>	Outside (193.12.253.115)	1723	172.16.0.5	172.16.0.5	1723	TCP port forwarding	Internet	-	24/7	Local	<input type="checkbox"/>

## Services

Then, go to the **Services** page under **Rules and Relays** and define the service to manage the NATED PPTP traffic. Use TCP as the **Protocol**, Dynamic PPTP management as the **Firewall type**, and **Server ports** 1723. Give the new service a descriptive name.

Services								
Edit row	Name	Subgroup	Protocol	Firewall type	Client ports	Server ports	ICMP type	Delete row
<input type="checkbox"/>	+ PPTP passthrough	-	TCP	Dynamic PPTP management	1-65535	1723		<input type="checkbox"/>

## Rules

Go to the **Rules** page and create a rule to let the PPTP traffic through from the PPTP server to the Internet. Use the newly created service. This is needed to let the GRE traffic through.

Note that this rule must be higher up in your rule list than any other rules allowing traffic from the network where the PPTP server is located.

Edit Row	Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
<input type="checkbox"/>	1	Yes	PPTP server	-	Internet	-	DMZ -> External (NAT:ed)	PPTP passthrough	Allow	24/7	Local		<input type="checkbox"/>

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** | Show Configuration | User Administration | U

**Test Run and Apply Conf** (Help)

Duration of limited test mode:

seconds

When the configuration has been applied, you should save a backup to file. Press **Save config to CLI file** to save the configuration.

**Save/Load CLI Command File** (Help)

The permanent configuration might be affected by loading a CLI file.

Local file:

## 21.11. VPN between Ingate and AWS (Amazon Web Services)

This How-To will describe how to create a VPN connection between an Ingate and your VPC on the Amazon cloud service.

As an example, the Ingate will have the public IP address 192.0.2.119 assigned to eth1 and the private network 10.10.10.0/24 connected to eth2. Furthermore, the AWS VPN endpoints are 192.0.2.200 and 192.0.2.210. The network in the VPC is 10.20.20.0/24.

### 21.11.1. Amazon

Please follow [this guide](#) how to setup the VPN connection on the Amazon end.

In short, the following steps need to be taken in order to create a VPN connection via the AWS Management Console:

1. Login to the *AWS Management Console*.
2. Go to the *VPC* service.
3. Create a new *Customer Gateway*.
  - a. **Name tag:** CG\_ingate
  - b. **Routing:** Static
  - c. **IP address:** 192.0.2.119
4. Create a new *Virtual Private Gateway* and attach it to VPC.
  - a. **Name tag:** VPG\_ingate
5. Create a new *VPN Connection*.
  - a. **Name tag:** VPN\_ingate
  - b. **Virtual Private Gateway:** VPG\_ingate
  - c. **Customer Gateway:** GG\_ingate
  - d. **Routing Options:** Static
  - e. **Static IP Prefixes:** 10.10.10.0/24
6. When the connection is created choose *Download Configuration* and select Vendor *Generic*.

The downloaded configuration will contain the necessary information to setup the tunnels on the Ingate side. It will contain two IPsec Peer addresses and two preshared keys together with connection setup details.

**NOTE** In this How-To, example information will be used instead of the information found in the downloaded configuration.

## 21.11.2. Ingate

The following Ingate configuration will complete the setup of the VPN connection.

### IPsec Peers

Go to the **IPsec Peers** page.

Name	Subgroup	Active	Local Side	Remote Side				ISAKMP Key Lifetime (seconds)	Initiate Re-keying	Encryption	Authentication		Delete Row
				DNS Name or IP Address	Dynamic	IP Address	RADIUS				Type	Info	
Amazon-IKE-vpn-7		Yes	eth1 (192.0.2.119)	192.0.2.200	<input type="checkbox"/>	192.0.2.200	No	28800	Yes	AES	Preshared secret	Change/View	<input type="checkbox"/>
		Yes	eth1 (192.0.2.119)	192.0.2.210	<input type="checkbox"/>	192.0.2.210	No	28800	Yes	AES	Preshared secret	Change/View	<input type="checkbox"/>

For Tunnel 1:

#### Name

Select a suitable name. E.g. *Amazon-IKE-vpn-74d6a73f-0*.

### Local Side

Choose interface *eth1* (192.0.2.119).

### Remote Side

Enter IP address 192.0.2.200 (Virtual Private Gateway for Tunnel 1 in *Downloaded Configuration*).

### ISAKMP Key Lifetime (seconds)

Enter 28800.

### Encryption

Select AES.

### Authentication

Select **Type** *Preshared secret* and enter the preshared key for Tunnel 1 found in the *Downloaded Configuration*.

Click the + sign (left to the name *Amazon-IKE-vpn-74d6a73f-0*) and create Tunnel 2:

### Local Side

Choose interface *eth1* (192.0.2.119).

### Remote Side

Enter IP address 192.0.2.210 (Virtual Private Gateway for Tunnel 2 in *Downloaded Configuration*).

### ISAKMP Key Lifetime (seconds)

Enter 28800.

### Encryption

Select AES.

### Authentication

Select **Type** *Preshared secret* and enter the preshared key for Tunnel 2 found in the *Downloaded Configuration*.

## IPsec Tunnels

Go to page **IPsec Tunnels**. In the table **IPsec Networks** add the **lan** 10.10.10.0/24 and the **lan\_vpc** 10.20.20.0/24.

IPsec Networks <a href="#">(Help)</a>				
Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
lan	10.10.10.0	10.10.10.0	24	<input type="checkbox"/>
lan_vpc	10.20.20.0	10.20.20.0	24	<input type="checkbox"/>

Add new rows  rows.

In the **IPsec Tunnels** table add a new IPsec tunnel.

**IPsec Tunnels** [\(Help\)](#)  
 These settings are called "Phase 2 settings" in some other IPsec products.

Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
	Address Type	Network	NAT As	Address Type	Network				
+ Amazon-IKE-vpn-74d6a73f-0	Network	lan	.	Network	lan_vpc	3600	AES	Same as Phase 1 DH	<input type="checkbox"/>

Add new rows  groups with  rows per group.

*Peer*

Select the peer you created on the **IPsec Peers** page.

*Local Network*

Select **Address Type** *Network* and select the **Network** *lan*.

*Remote Network*

Select **Address Type** *Network* and select the **Network** *lan\_vpc*.

*IPsec Key Lifetime (seconds, optional)*

Enter *3600*.

*Encryption*

Select *AES*.

*PFS Group*

Select *Same as Phase 1 DH*

**IPsec Advanced**

Go to the page **IPsec Advanced** and create a new entry in the **IPsec Peers** table.

IPsec Peers | IPsec Tunnels | **IPsec Advanced** | IPsec Cryptos | IPsec Certificates | IPsec Settings | Authentication Server | IPsec Status | PPTP | PPTP Status

**IPsec Peers** [\(Help\)](#)  
 Here you can define advanced settings for **IPsec Peers** .

Peer	NAT Traversal	Dead Peer Detection				Delete Row
		Enabled	Delay	Timeout	Action	
Amazon-IKE-vpn-74d6a73f-0	Force	Yes	10	30	Restart	<input type="checkbox"/>

Add new rows  rows.

*Peer*

Select the peer you created on the **IPsec Peers** page.

*NAT Traversal*

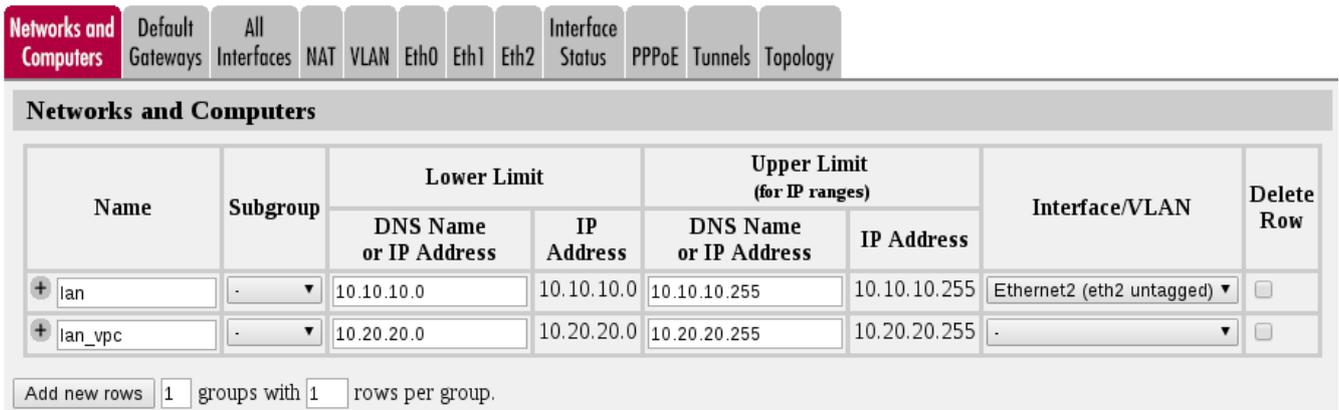
Select *Force*.

*Dead Peer Detection*

Select **Enabled** Yes. Enter **10** in **Delay** and **30** in **Timeout**. Select **Action Restart**.

## Networks and Computers

Go to the page **Networks and Computers** and add two networks, *lan* 10.10.10.0-10.10.10.255 on interface Ethernet2 (eth2 untagged) and *lan\_vpc* 10.20.20.0-10.20.20.255.

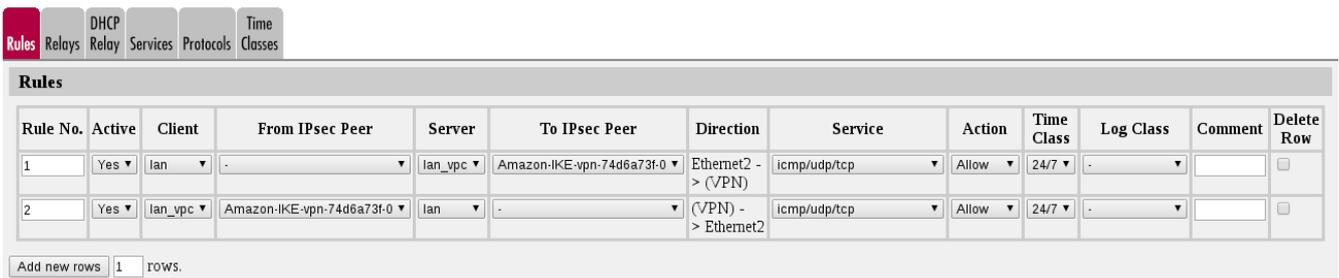


Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
lan	-	10.10.10.0	10.10.10.0	10.10.10.255	10.10.10.255	Ethernet2 (eth2 untagged)	<input type="checkbox"/>
lan_vpc	-	10.20.20.0	10.20.20.0	10.20.20.255	10.20.20.255	-	<input type="checkbox"/>

Add new rows 1 groups with 1 rows per group.

## Rules

Go to page **Rules** and create two rules to allow traffic from and to the Amazon VPN tunnel. These rules will allow all TCP, UDP and ICMP traffic to and from the tunnel.

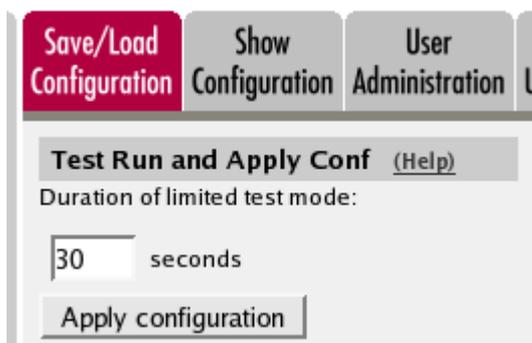


Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
1	Yes	lan	-	lan_vpc	Amazon-IKE-vpn-74d6a73f-0	Ethernet2 -> (VPN)	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>
2	Yes	lan_vpc	Amazon-IKE-vpn-74d6a73f-0	lan	-	(VPN) -> Ethernet2	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>

Add new rows 1 rows.

## Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



**Save/Load Configuration** | Show Configuration | User Administration

**Test Run and Apply Conf (Help)**

Duration of limited test mode:

30 seconds

Apply configuration

When the configuration is applied you should under page **IPsec Status** see that one of the two tunnels for peer *Amazon-IKE-vpn-74d6a73f-0* is up.

## 21.12. IPsec with road warriors using extended authentication

This How-To will describe how to set up an Ingate for road warriors using extended authentication (XAUTH) and IKE Mode Configuration (MODECFG). It will also cover a scenario where the road warriors want to utilize SIP for communication with local resources (e.g. PBX and local phones).

As an example, the Ingate will have the public IP address 192.0.2.119 assigned to eth1 and the private network 10.10.10.0/24 connected to eth0. Furthermore, the virtual address pool from which the road warriors are assigned IP addresses is 10.20.20.0/24.

### 21.12.1. Networks and Computers

Go to the **Networks and Computers** table found under the **Network** tab. Here, we will define a range for the virtual address pool with an upper and a lower limit in the network 10.20.20.0/24. We will also define our local net (10.10.10.0/24) and an outside network.

Networks and Computers							
Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ LocalNetwork	-	10.10.10.0	10.10.10.0	10.10.10.255	10.10.10.255	Ethernet0 (eth0 untagged)	<input type="checkbox"/>
+ Outside	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	Ethernet1 (eth1 untagged)	<input type="checkbox"/>
+ RemotePool	-	10.20.20.1	10.20.20.1	10.20.20.254	10.20.20.254	-	<input type="checkbox"/>

For the address pool enter the following:

#### *Name*

Select a suitable name. E.g. *RemotePool*.

#### *Lower Limit*

Enter the first address in the pool (10.20.20.1).

#### *Upper Limit*

Enter the last address in the pool (10.20.20.254).

### 21.12.2. Local Extended Authentication Database

Go to the **Local Extended Authentication Database** table found under the tab **Virtual Private Networks** → **IPsec Settings**. Here we will add users that should be able to authenticate via XAUTH.

## Local Extended Authentication Database [\(Help\)](#)

Here you add local users available for extended authentication (XAUTH).

Username	Password	Peer	Enabled	Delete Row
<input type="text" value="alice"/>	<input type="button" value="Change Password"/>	- ▾	Yes ▾	<input type="checkbox"/>
<input type="text" value="john"/>	<input type="button" value="Change Password"/>	- ▾	Yes ▾	<input type="checkbox"/>

In this example we add two users, alice and john.

### Username

Select a suitable user name. E.g. *alice*.

### Password

Enter a password for the user.

### Peer

For now, leave it '-'. Here we will reference the **IPsec Peer** created later in this howto.

## 21.12.3. IKE Mode Configuration (MODECFG)

Go to the **IKE Mode Configuration (MODECFG)** table found under the tab **Virtual Private Networks** → **IPsec Settings**. Here we will define the settings that will be sent to the clients.

### IKE Mode Configuration (MODECFG) [\(Help\)](#)

Here you add settings for client configuration via IKE Mode Configuration.

Name	IP Range	DNS 1		DNS 2		Domain	Banner	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address			
<input type="text" value="RemoteConfig"/>	<input type="text" value="RemotePool"/>	<input type="text" value="10.10.10.5"/>	<input type="text" value="10.10.10.5"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

### Name

Select a suitable name. E.g. *RemoteConfig*.

### IP Range

Select the range *RemotePool* that we created in [Networks and Computers](#). This is the address pool from which the clients will be assigned IP addresses.

### DNS 1

Enter a DNS server that will be assigned to clients (optional).

## 21.12.4. Phase 1 & 2 encryption proposals

Go to the the tab **Virtual Private Networks** → **IPsec Cryptos**. Here we will define encryption proposals for phase 1 and 2.

### IKE/ISAKMP (Phase 1) Encryption Proposals

In this example we want the road warriors to use the following phase 1 cryptographic algorithms.

<input type="checkbox"/>	+ RemoteProposals	1	AES256-SHA256	MODP1536 (Group 5)	<input type="checkbox"/>
<input type="checkbox"/>		2	AES256-SHA256	MODP2048 (Group 14)	<input type="checkbox"/>
<input type="checkbox"/>		3	AES256-SHA256	MODP4096 (Group 16)	<input type="checkbox"/>

### Encryption

AES-256

### Authentication/hash

SHA256

### Diffie-Hellman Groups

MODP1536 (group 5), MODP2048 (group 14) and MODP4096 (group 16)

## ESP/IPsec (Phase 2) Encryption Proposals

In this example we want the road warriors to use the following phase 2 cryptographic algorithms.

<input type="checkbox"/>	+ RemoteProposals	1	AES256-SHA256	<input type="checkbox"/>
--------------------------	-------------------	---	---------------	--------------------------

### Encryption

AES-256

### Authentication/hash

SHA256

#### NOTE

Diffie-Hellman Groups (PFS) for phase 2 will be chosen later.

## 21.12.5. IPsec Peers (Phase 1)

Go to the **IPsec Peers** table found under the tab **Virtual Private Networks** → **IPsec Peers**. Here we will create and configure a *phase 1* peer.

IPsec Peers (Help)															
These settings are called "Phase 1 settings" in some other IPsec products.															
Name	Subgroup	Active	Local Side	Remote Side			RADIUS	Blacklist	ISAKMP Key Lifetime (seconds)	Initiate Re-keying	IKEv2	Encryption	Authentication		Delete Row
				DNS Name or IP Address	Dynamic	IP Address							Type	Info	
+ RemoteWorkers	-	Yes	eth1 (192.0.2.119)	*	<input type="checkbox"/>	*	No		3600	No	Disallow	RemoteProposals	XAUTH+PSK	Change/View	<input type="checkbox"/>

### Name

Select a suitable name. E.g. *RemoteWorkers*.

### Local Side

Choose interface *eth1* (192.0.2.119).

### Remote Side

Enter "\*" (an asterisk).

### ISAKMP Key Lifetime (seconds)

Enter 3600.

### Initiate Re-keying

Select *No*.

### IKEv2

Select *Disallow*.

### Encryption

Select *RemoteProposals* that we created in [IKE/ISAKMP \(Phase 1\) Encryption Proposals](#).

### Authentication

Select **Type** *XAUTH+PSK* and enter a preshared key (click *Change/View*).

## 21.12.6. IPsec Tunnels (Phase 2)

Go to the **Virtual Private Networks** → **IPsec Tunnels** tab. Here we will create and configure a *phase 2* tunnel for our *phase 1* peer.

### IPsec Networks

In the table **IPsec Networks** add the *any* network *0.0.0.0/0*.

IPsec Networks <a href="#">(Help)</a>				
Name	DNS Name or Network Address	Network Address	Netmask / Bits	Delete Row
any	0.0.0.0	0.0.0.0	0	<input type="checkbox"/>

#### NOTE

If you don't want to route all the traffic from the clients over the tunnel, create a network that matches your local network. In this howto it would be *10.10.10.0/24*.

### IPsec Tunnels

In the **IPsec Tunnels** table, add a new tunnel.

IPsec Tunnels <a href="#">(Help)</a>									
These settings are called "Phase 2 settings" in some other IPsec products.									
Peer	Local Network			Remote Network		IPsec Key Lifetime (seconds, optional)	Encryption	PFS Group	Delete Row
	Address Type	Network	NAT As	Address Type	Network				
+ RemoteWorkers	Network	any	-	Remote/private address	-	3600	RemoteProposals	Same as Phase 1 DH	<input type="checkbox"/>

#### Peer

Select the peer *RemoteWorkers* that you created in [IPsec Peers \(Phase 1\)](#).

### Local Network

Select **Address Type** *Network* and select the **Network** *any*.

### Remote Network

Select **Address Type** *Remote/private address*.

### IPsec Key Lifetime (seconds, optional)

Enter 3600.

### Encryption

Select *RemoteProposals* that we created in [ESP/IPsec \(Phase 2\) Encryption Proposals](#).

### PFS Group

Select *Same as Phase 1 DH*. This setting will use the same Diffie-Hellman groups that were specified for *phase 1*.

## 21.12.7. Associate IPsec Peer with XAUTH users

Go to the **Local Extended Authentication Database** table found under the tab **Virtual Private Networks** → **IPsec Settings**. Now we want to associate the **IPsec Peer** that we created in [IPsec Peers \(Phase 1\)](#) to the users created in [Local Extended Authentication Database](#).

In the column **Peer** select *RemoteWorkers*. This specifies that the users *alice* and *john* only will be able to authenticate using this peer.

Local Extended Authentication Database <small>(Help)</small>				
Here you add local users available for extended authentication (XAUTH).				
Username	Password	Peer	Enabled	Delete Row
alice	Change Password	RemoteWorkers ▼	Yes ▼	<input type="checkbox"/>
john	Change Password	RemoteWorkers ▼	Yes ▼	<input type="checkbox"/>

## 21.12.8. Associate Mode Configuration with IPsec Peer

Go to the **IPsec Peers** table found under the tab **Virtual Private Networks** → **IPsec Advanced**. Here we want to associate the client configuration that we created in [IKE Mode Configuration \(MODECFG\)](#) to the **IPsec Peer** that we created in [IPsec Peers \(Phase 1\)](#). Furthermore, we also want to enable DPD (Dead Peer Detection).

IPsec Peers <small>(Help)</small>												
Here you can define advanced settings for IPsec Peers .												
Peer	NAT Traversal	Dead Peer Detection				Mode Configuration	Local ID		Remote ID		IKEv2 ESN	Delete Row
		Enabled	Delay	Timeout	Action		Type	Value	Type	Value		
RemoteWorkers ▼	Auto ▼	Yes ▼	30	120	Clear ▼	RemoteConfig ▼	- ▼		- ▼		No ▼	<input type="checkbox"/>

### Peer

Select *RemoteWorkers*.

### Dead Peer Detection

Set **Enabled** to *Yes*. Enter 30 in **Delay**, 120 in **Timeout** and select *Clear* in **Action**.

## Mode Configuration

Select *RemoteConfig*.

### 21.12.9. Create firewall rules

Go to the **Rules** table found under the tab **Rules and Relays** → **Rules**. Here we create firewall rules that allows traffic to flow between different entities.

Rules												
Rule No.	Active	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete Row
1	Yes	RemotePool	RemoteWorkers	LocalNetwork	-	(VPN) - > Ethernet0	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>
2	Yes	LocalNetwork	-	RemotePool	RemoteWorkers	Ethernet0 - > (VPN)	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>
3	Yes	RemotePool	RemoteWorkers	RemotePool	-	(VPN) - > Indeterminate interface	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>
4	Yes	RemotePool	-	RemotePool	RemoteWorkers	Indeterminate interface - > (VPN)	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>
5	Yes	RemotePool	RemoteWorkers	Outside	-	(VPN) - > Ethernet1	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>
6	Yes	Outside	-	RemotePool	RemoteWorkers	Ethernet1 - > (VPN)	icmp/udp/tcp	Allow	24/7	-		<input type="checkbox"/>

#### Rule Number 1-2

If you want to allow TCP, UDP and ICMP traffic between the road warriors and the local network (both directions).

#### Rule Number 3-4

If you want to allow TCP, UDP and ICMP traffic between the road warriors.

#### Rule Number 5-6

If you used the network *any* (0.0.0.0/0) when you created the *phase 2* tunnel in [IPsec Tunnels \(Phase 2\)](#), rule 5 and 6 are necessary if you want to allow TCP, UDP and ICMP traffic between the road warriors and the outside (internet).

### 21.12.10. NAT and outside traffic

If you added rule number 5 and 6 in the previous section and want to do NAT from the virtual address pool to the outside interface you need to add a NAT entry. In our example the outside interface is *eth1* and the address pool is *10.20.20.0/24*. The NAT table is found under the tab **Network** → **NAT**.

NAT										
Select if packets that originate from a unit behind the <b>From</b> interface should be NAT:ed when they are sent to a unit behind the <b>To</b> interface. Optionally you can also select specific networks to be NAT:ed, as well as the address to use.										
No.	Interface	From			To			NAT As (optional)	Delete Row	
		Network (optional)			Network (optional)					
		DNS Name or Network Address	Network Address	Netmask / Bits	Interface	DNS Name or Network Address	Network Address	Netmask / Bits		
1	Ethernet1 (eth1)	10.20.20.0	10.20.20.0	24	Ethernet1 (eth1)				eth1 (192.0.2.119)	<input type="checkbox"/>

In the **From** columns:

#### Interface

Select *eth1*.

*Network Address*

Enter *10.20.20.0*.

*Netmask*

Enter *24*.

In the **To** columns:

*Interface*

Select *eth1*.

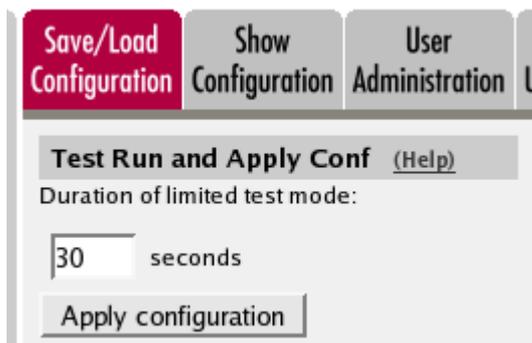
And finally:

*NAT As (optional)*

Select *eth1 (192.0.2.119)*.

### 21.12.11. Save/Load Configuration

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



When the configuration is applied you can see tunnel status on the page **Virtual Private Networks** → **IPsec Status**.

### 21.12.12. Troubleshooting

If you encounter problems with the tunnels, please consider the following.

- Ensure that the configured encryption algorithms (both phase 1 & 2) on the clients match the ones configured on the Ingate unit.
- Ensure that the configured ISAKMP Key Lifetime on the clients match the one configured on the Ingate unit.
- Ensure that the configured IPsec Key Lifetime on the clients match the one configured on the Ingate unit.
- Issues might be due to rekeying. Try with the setting **Initiate Re-keying** set to *Yes* (found in the **IPsec Peers** table) or set ISAKMP Key Lifetime and IPsec Key Lifetime to a lower value on the clients than configured on the Ingate unit.
- Disable Dead Peer Detection or increase the DPD **Timeout**.

- If IPsec is up and running but you experience issues with connectivity, try to set the **NAT Traversal** setting to *Force* (the setting is found in the table IPsec Advanced → IPsec Peers).

### 21.12.13. SIP communication and road warriors

If you want the road warriors to be able to communicate with local phones, local PBX and the outside world via SIP the following steps need to be taken.

**NOTE** The scenario described here is a general one and your setup and requirements may vary.

### 21.12.14. Assumptions

One PBX is located on the local network (10.10.10.0/24) with the IP address 10.10.10.10. One phone is located on the local network with the IP address 10.10.10.15. The local phone and the road warriors have outbound SIP proxy set to the PBX. The PBX has the Ingate unit's local address 10.10.10.1 set as outbound proxy. The Ingate unit has a default route on the outside interface (eth1) and DNS servers are configured. The local sip domain is sip.example.com.

### 21.12.15. SIP setup

#### Enable SIP

On the **Basic** page under **SIP Services**, you make the unit SIP-aware.

The screenshot shows the 'SIP Module' configuration page. The 'Basic' tab is active. Below the tabs, the 'SIP Module (Help)' section contains two radio buttons: 'Enable SIP module' (selected) and 'Disable SIP module'.

Go to the **SIP Traffic** → **Filtering** page. SIP requests from the internal network should always be processed. Enter a Proxy rule for this. All other requests should only be processed if they are directed to a local domain. To ensure this, select **Local only** as the **Default policy for requests**.

The screenshot shows the 'Sender IP Filter Rules (Help)' configuration page. The 'Filtering' tab is active. A table lists filter rules:

No.	From Network	Action	Delete Row
1	LocalNetwork ▼	Process all ▼	<input type="checkbox"/>

Below the table, there is a button 'Add new rows' and a text field '1 rows'. To the right, the 'Default Policy For SIP Requests' section has three radio buttons: 'Process all', 'Local only' (selected), and 'Reject all'.

Enter the SIP domain handled by the unit on the **Local Registrar** page. Usually, the SIP domain

looks just like the ordinary Internet domain for the company.

This setup should be enough for basic SIP processing. Note, for more comprehensive information regarding SIP setup please take a look at the [SIP](#) howtos.

### Enable SIParator functionality and select type

In order to enable SIParator functionality in Firewall mode go to the page **Basic Configuration** → **SIParator Type**. Select *Enable SIParator* and choose the type *Manual*.

### Configure Surroundings for the Manual type

When using the **Manual** configuration, the unit can be connected to one or more networks. All the networks that you want to handle must be added to the **Surroundings** table (found on the page **Network** → **Topology**). If you have default gateways defined, the outside world will be automatically configured. More information on [Surroundings](#).

The networks are defined on the **Networks and Computers** page and networks that can reach each other without going through your unit should be grouped together.

In our scenario we will group the *LocalNetwork* and the *RemotePool* together in a new group called *Surroundings* and reference that group in the surroundings table.

Networks and Computers							
Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ LocalNetwork	-	10.10.10.0	10.10.10.0	10.10.10.255	10.10.10.255	Ethernet0 (eth0 untagged)	<input type="checkbox"/>
+ Outside	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	Ethernet1 (eth1 untagged)	<input type="checkbox"/>
+ RemotePool	-	10.20.20.1	10.20.20.1	10.20.20.254	10.20.20.254	-	<input type="checkbox"/>
+ Surroundings	LocalNetwork					-	<input type="checkbox"/>
	RemotePool					-	<input type="checkbox"/>

Add the *Surroundings* group in the **Surroundings** table (found on the page **Network** → **Topology**).

Networks and Computers | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Eth3 | Interface Status | PPPoE | Tunnels | **Topology**

**Surroundings** [\(Help\)](#)

If your firewall type is not set to **DMZ** or **Manual**, the settings in this table cannot be used.

Network	Additional Negotiators	Delete Row
Surroundings	-	<input type="checkbox"/>

Add new rows  rows.

By using this configuration, road warriors in the *RemotePool* and clients in the *LocalNetwork* will be treated alike (SIP-wise).

### 21.12.16. Save/Load Configuration

Go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

**Save/Load Configuration** | Show Configuration | User Administration | U

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

# Chapter 22. Cloud Environment

## 22.1. Amazon Web Services (AWS)

### 22.1.1. Connect To an Instance

Launched instances are reached via HTTPS. The HTTPS certificate should have the Common Name (CN) set to the serial number of the instance.

### 22.1.2. Default Admin Password

The default *admin* password is set to the *instance-id* of the running instance. Please change the password after the first login.

## 22.2. Openstack

### 22.2.1. Connect To an Instance

Launched instances are reached via HTTPS. The HTTPS certificate should have the Common Name (CN) set to the serial number of the instance.

### 22.2.2. Default Admin Password

The default *admin* password is set to the *uuid/ID* of the instance (found in the overview page for the running instance, e.g. 7c84c36e-6a58-4023-b471-e4c023e0ce6a). If you fail to login with the uuid try to use the instance-id instead (it can be found if you launch the instance console via Horizon. It will show e.g. instance-00000015 in the top of the console window. In this case the password is i-00000015). Please change the password after the first login.

## 22.3. Azure

### 22.3.1. Connect To an Instance

Launched instances are reached via HTTPS. The HTTPS certificate should have the Common Name (CN) set to the serial number of the instance.

### 22.3.2. Default Admin Password

The *admin* password is set to the password that you entered when you created the instance. Note, the username that was set when you created the instance has no effect. The *admin* account will be used.

## 22.4. Google Cloud Platform (GCP)

## 22.4.1. Connect To an Instance

Launched instances are reached via HTTPS. The HTTPS certificate should have the Common Name (CN) set to the serial number of the instance.

## 22.4.2. Default Admin Password

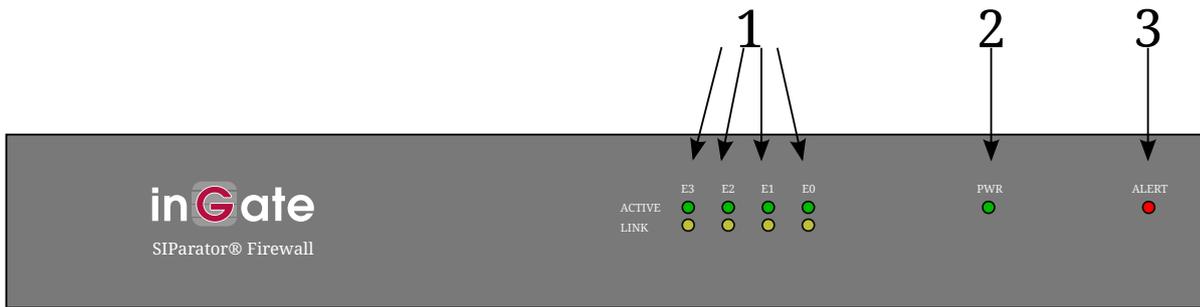
The default *admin* password is set to the *ID* of the instance. The ID can be found by entering the *Cloud Shell*. Enter the shell by clicking the >\_ icon in the upper right. Enter the following command in order to retrieve the id:

```
$ gcloud compute instances describe <<name_of_instance>> --zone <<zone>> | grep "id: "
```

where <<name\_of\_instance>> is the name of the instance and <<zone>> is where the instance was started. Please change the password after the first login.

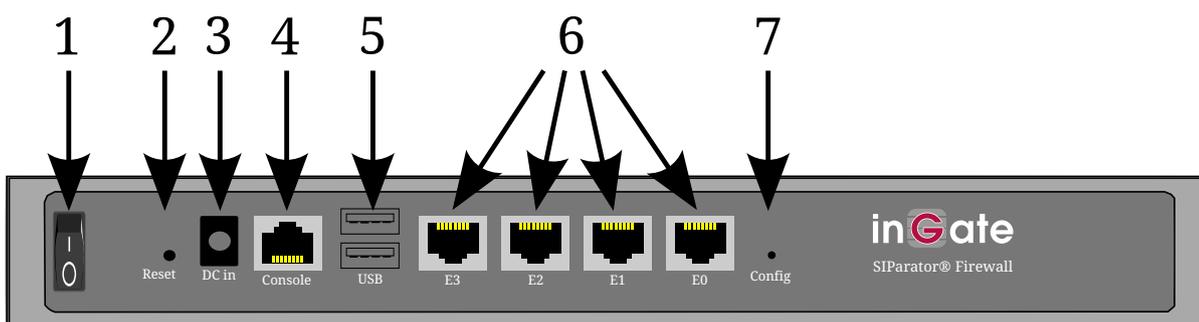
# Part V. Hardware Models

# Chapter 23. Ingate SIParator/Firewall S21 rev A



1. **Active / Link leds.** These leds show link and active status. The active led is green when there is link on the port and it flashes when there is network activity. The link led indicate the speed of the network, amber led indicate 1000Mbit network, green led indicate 100Mbit and when the led is off there is a 10 Mbit network.
2. **Power LED.** This LED is lit when the unit is connected to a power outlet and switched on.
3. **ALERT.** The ALERT LED indicates that something prevents the unit from working correctly. States are indicated thus:
  - The LED is **continuously lit**. Indicates one of the following states:
    - The unit boots.
    - The unit applies a new configuration.
    - The unit warns about a minor error which affects the network traffic.
  - The LED **blinks**. Indicates one of the following states:
    - The unit checks (during boot) if the **Config** button is pressed.
    - The unit is the standby unit of a failover team.
    - The unit warns about a major error, e.g. a hardware error.
  - The LED **double blinks** (two blinks followed by a short pause).
    - The unit waits for configuration through the installation program or *magic ping*. See also [Installation](#).

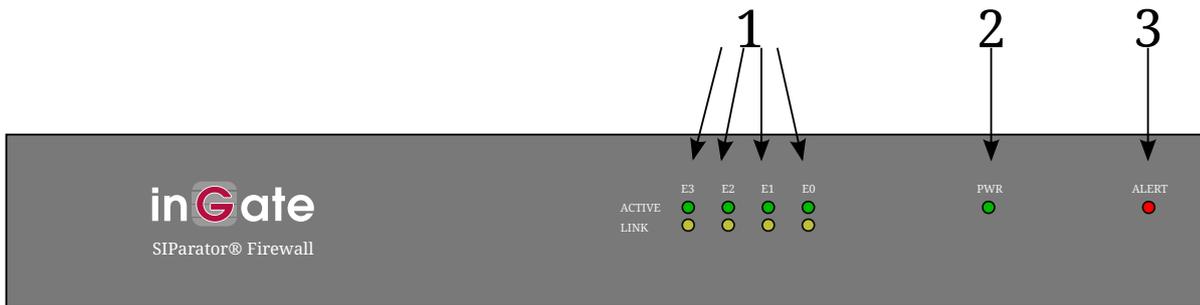
If the unit indicates an error, you will find an error message when you log on the configuration interface. At the top of each administration web page there will be a link to a page where you find an explanation of the error.



1. **Power button.** Press this button to turn off or on the unit.
2. **RESET button.** Press this button (a bent steel paper clip or other thin device is needed) to restart the unit.
3. **Power connection.** Connection for the power cord.
4. **Serial port.** Serial port for connecting the unit to a workstation. This is needed when installing the unit (see also [Installation](#)).
5. **Usb ports.** USB 2.0/1.1 Ports. These ports are currently unutilized.
6. **Ethernet ports.** Ethernet ports with 10/100/1000 Mbit led on the right side of the ethernet ports and link led on the left side of the ethernet ports. The link led is green when there is link and it flashes when there is network activity on the port. The Mbit led indicate the speed of the network, a unlit led indicate 10 Mbit network, a green led indicate 100 Mbit network and amber led indicate 1000 Mbit network.
7. **Config Button.** Press this button (a pencil or other thin device is needed) during boot to make the unit erase the current password and enter wait mode. In this mode, it waits for a reconfiguration made by a *magic ping* or the installation program (see <Installation>>). Before one of these is performed, no traffic will be let through the unit.

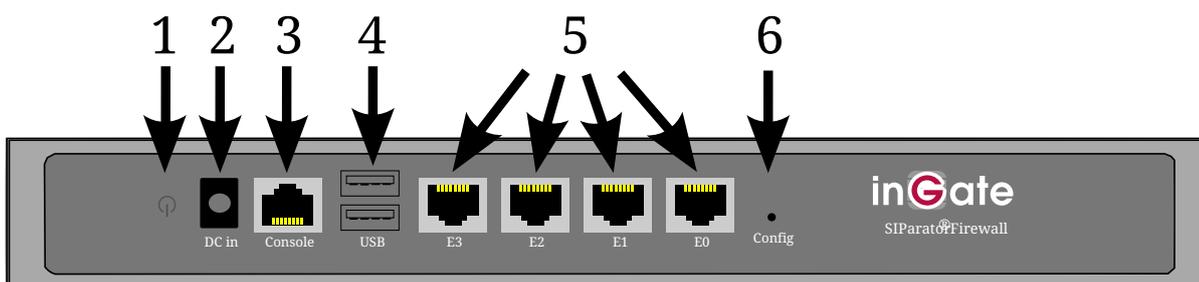
The unit logs when the button is pressed according to the **Logclass for administration and configuration** set on the **Logging Configuration** page under **Logging and Tools**.

# Chapter 24. Ingate SIParator/Firewall S21 rev B



1. **Active / Link leds.** These leds show link and active status. The active led is green when there is link on the port and it flashes when there is network activity. The link led indicate the speed of the network, amber led indicate 1000Mbit network, green led indicate 100Mbit and when the led is off there is a 10 Mbit network.
2. **Power LED.** This LED is lit when the unit is connected to a power outlet and switched on.
3. **ALERT.** The ALERT LED indicates that something prevents the unit from working correctly. States are indicated thus:
  - The LED is **continuously lit**. Indicates one of the following states:
    - The unit boots.
    - The unit applies a new configuration.
    - The unit warns about a minor error which affects the network traffic.
  - The LED **blinks**. Indicates one of the following states:
    - The unit checks (during boot) if the **Config** button is pressed.
    - The unit is the standby unit of a failover team.
    - The unit warns about a major error, e.g. a hardware error.
  - The LED **double blinks** (two blinks followed by a short pause).
    - The unit waits for configuration through the installation program or *magic ping*. See also [Installation](#).

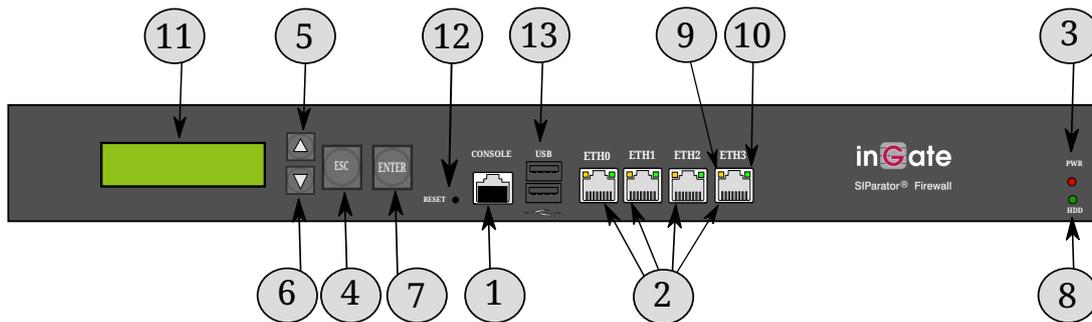
If the unit indicates an error, you will find an error message when you log on the configuration interface. At the top of each administration web page there will be a link to a page where you find an explanation of the error.



1. **Power button.** Press this button to turn off or on the unit.
2. **Power connection.** Connection for the power cord.
3. **Serial port.** Serial port for connecting the unit to a workstation. This is needed when installing the unit (see also [Installation](#)).
4. **Usb ports.** USB 2.0 Ports. These ports are currently unutilized.
5. **Ethernet ports.** Ethernet ports with 10/100/1000 Mbit led on the right side of the ethernet ports and link led on the left side of the ethernet ports. The link led is green when there is link and it flashes when there is network activity on the port. The Mbit led indicate the speed of the network, a unlit led indicate 10 Mbit network, a green led indicate 100 Mbit network and amber led indicate 1000 Mbit network.
6. **Config Button.** Press this button (a pencil or other thin device is needed) during boot to make the unit erase the current password and enter wait mode. In this mode, it waits for a reconfiguration made by a *magic ping* or the installation program (see [Installation](#)). Before one of these is performed, no traffic will be let through the unit.

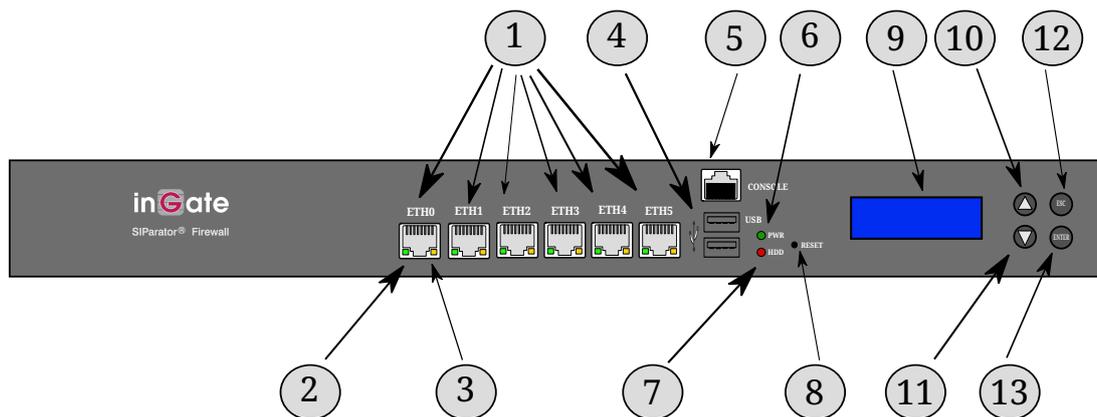
The unit logs when the button is pressed according to the **Logclass for administration and configuration** set on the **Logging Configuration** page under **Logging and Tools**.

# Chapter 25. Ingate SIParator/Firewall S51



1. **Serial port.** Serial port for connecting the unit to a workstation. This is needed when installing the unit (see also [Installation](#)).
2. **Ethernet ports.** Ethernet ports for connecting the unit to the network. Use Ethernet cables only, with RJ-45 connectors.
3. **Power LED.** This LED is lit when the unit is connected to a power outlet and switched on.
4. **ESC button.** When the unit is restarted, the display will show when to press the ESC button to make the unit erase the current password and enter wait mode. In this mode, it waits for a reconfiguration made by a *magic ping* or the installation program (see [Installation](#)). Before one of these is performed, no traffic will be let through the unit.
5. **Up button.** The Up button is used for going up in the menu on the display.
6. **Down button.** The Down button is used for going down in the menu on the display.
7. **Enter button.** The Enter button is used to select a setting in the menu shown on the LCD display.
8. **HDD LED.** This LED indicates that the hard drive is written to or read from.
9. **Activity LEDs.** A blinking yellow LED indicates activity on the port.
10. **10/100/1000 MBit LEDs.** The LEDs indicate what kind of network the port is connected to. The LEDs light green for 10/100/1000 MBit.
11. **Display.** The display shows status for the unit and also indicates when to press the ESC button during boot to enter wait mode. In wait mode, the unit waits for a new password and can also receive a new IP address.  
  
Via the LCD display and the buttons, simple configuration is also possible, when the unit is in unconfigured mode. The settings available is to assign an IP address and to make the unit the standby unit in a failover team, or to break it out from a failover team.
12. **RESET button.** Press this button (a pencil or other thin device is needed) for 3 sec in order to reboot the unit.
13. **USB 2.0/1.1 Ports.** These ports are currently unutilized.

# Chapter 26. Ingate SIParator/Firewall S52



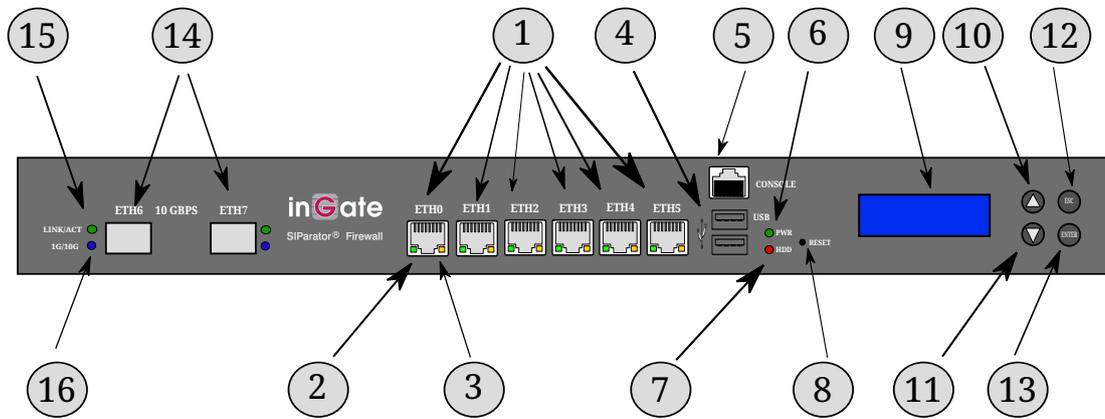
1. **Ethernet ports.** Ethernet ports for connecting the unit to the network. Use Ethernet cables only, with RJ-45 connectors.
2. **LINK/ACT LED.** The LED shows link and active status of the port. The LED is green when the port is connected to a network and it flashes when there is network activity.
3. **10/100/1000 MBit LED.** The LED indicates what kind of network the port is connected to. An unlit LED indicate 10 Mbit network, a green LED indicate 100 Mbit network and amber LED indicate 1000 Mbit network.
4. **Usb ports. USB 2.0 Ports.** These ports are currently unutilized.
5. **Serial port.** Serial port for connecting the unit to a workstation. This is needed when installing the unit (see also [Installation](#)).
6. **Power LED.** This LED is lit when the unit is connected to a power outlet and switched on.
7. **HDD LED.** This LED indicates that the hard drive is written to or read from.
8. **RESET button.** Press this button (a bent steel paper clip or other thin device is needed) to restart the unit.
9. **Display.** The display shows status for the unit and also indicates when to press the Enter and ESC buttons during boot to enter wait mode. In wait mode, the unit waits for a new password and can also receive a new IP address.

Via the LCD display and the buttons, simple configuration is also possible, when the unit is in unconfigured mode. The settings available is to assign an IP address and to make the unit the standby unit in a failover team, or to break it out from a failover team.

10. **Up button.** The Up button is used for going up in the menu on the display.
11. **Down button.** The Down button is used for going down in the menu on the display.
12. **ESC button.** The ESC button is only used in combination with the Enter button. When the unit is restarted, the display will show when to press the buttons to make the unit erase the current password and enter wait mode. In this mode, it waits for a reconfiguration made by a *magic ping* or the installation program (see [Installation](#)). Before one of these is performed, no traffic will be let through the unit.
13. **Enter button.** The Enter button is used to select a setting in the menu shown on the LCD display.

The Enter button is also used in combination with the ESC button. When the unit is restarted, the display will show when to press the buttons to make the unit erase the current password and enter wait mode. In this mode, it waits for a reconfiguration made by a *magic ping* or the installation program (see [Installation](#)). Before one of these is performed, no traffic will be let through the unit.

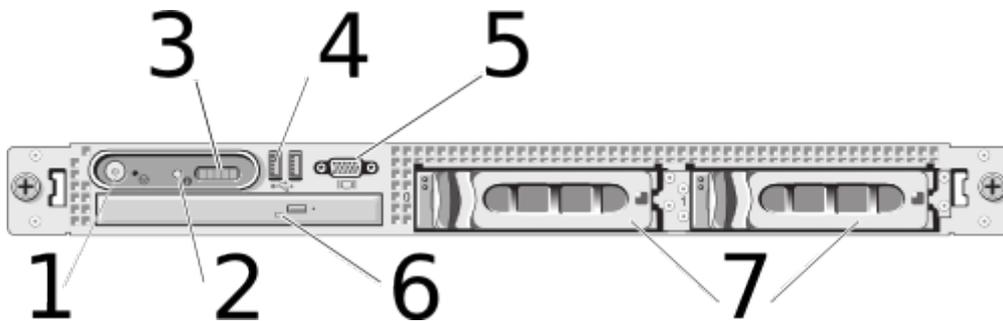
Optional variant with two 10Gbps Ethernet ports:



14. **10 Gbps Ethernet ports.** 10 Gbps Ethernet ports for connecting the unit to the network. Connect an SFP+ transceiver to adapt to your cables.
15. **LINK/ACT LED.** The LED shows link and active status of the port. The LED is green when the port is connected to a network and it flashes when there is network activity.
16. **1/10 GBit LED.** The LED indicates what kind of network the port is connected to. An amber LED indicate 1 Gbit network and a blue LED indicates 10 Gbit network.

# Chapter 27. Ingate SIParator/Firewall S95/S96/S97/S98

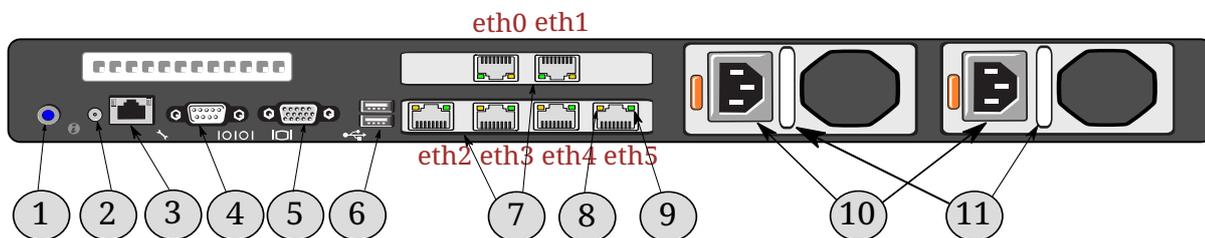
## 27.1. The front



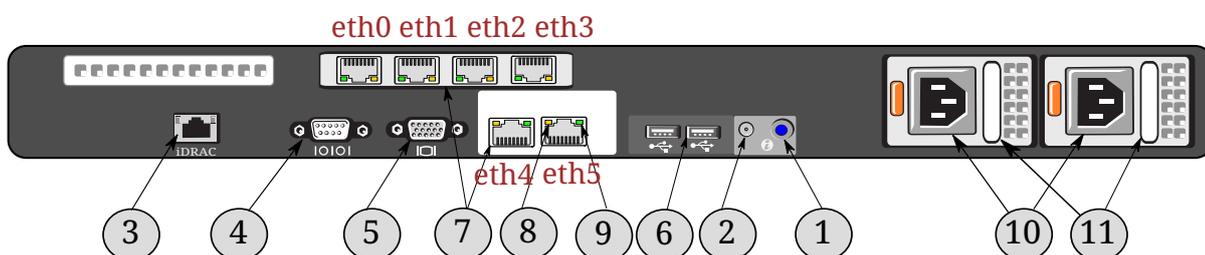
1. **Power.** depress to start the unit. Hold to power off the unit.
2. **System identification button.** Press to illuminate the system ID light. The identification buttons on the front and back panels can be used to locate a particular system within a rack.
3. **Hardware Status LCD.** reports hardware specific system health and status messages. Not used by the firmware.
4. **Usb ports.** USB 2.0 Ports. These ports are currently unutilized.
5. **Video connector.** Port for connection of a VGA display to the system. Currently not used.
6. **DVD drive.** Only used to boot the factory-reset CD. Simply (re)boot the unit with the factory-reset CD in the drive during boot sequence. The admin password is erased and the unit is placed into an UNCONFIGURED state. Note: eject the CD before next reboot.
7. **RAID bay.**

## 27.2. The back

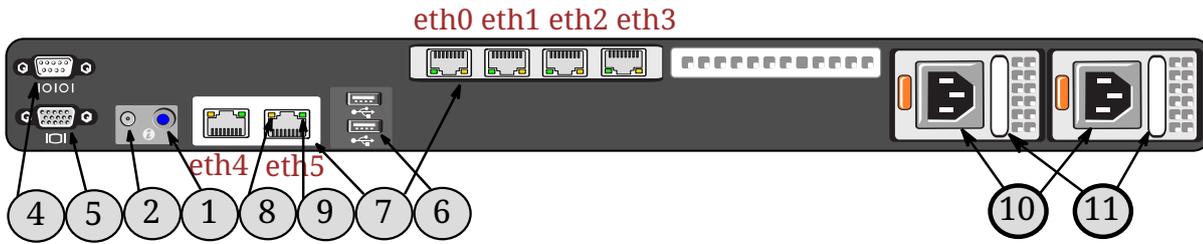
The back side of your Ingate SIParator/Firewall looks like this



or



or



1. **System identification button.** Press to illuminate the system ID light. The identification buttons on the front and back panels can be used to locate a particular system within a rack.
2. **System identification connector.** Connects the optional system status indicator assembly through the optional cable management arm.
3. **iDRAC port.** Dedicated management port. Currently not used. On some hardware it is not present.
4. **Serial port.** Serial port for connecting the unit to a workstation. This is needed when installing the unit (see also [Installation](#)).
5. **Video connector.** Port for connection of a VGA display to the system. Currently not used.
6. **Usb ports.** USB 2.0 Ports. These ports are currently unutilized.
7. **Ethernet ports.** Ethernet ports for connecting the unit to the network. Use Ethernet cables only, with RJ-45 connectors.
8. **10/100/1000 MBit LED.** The LED indicates what kind of network the port is connected to. An unlit LED indicate 10 Mbit network, a green LED indicate 100 Mbit network and amber LED indicate 1000 Mbit network.
9. **LINK/ACT LED.** The LED shows link and active status of the port. The LED is green when the port is connected to a network and it flashes when there is network activity.
10. **Power connection.** Connection for the power cord.
11. **Power supply status indicator.** When the handle/LED indicator isn't lit the power is not connected. When the handle/LED indicator lights green indicating that a valid power source is connected to the power supply and that the power supply is operational. When the handle/LED indicator is flashing amber it indicates a problem with the power supply.

# Appendix A: IP Firewall

## General

An IP firewall consists of: Two or more networks, basic filters for the different networks, and rules for the connections between the networks. In addition, there may be a NAT function that hides the inner network from the outside.

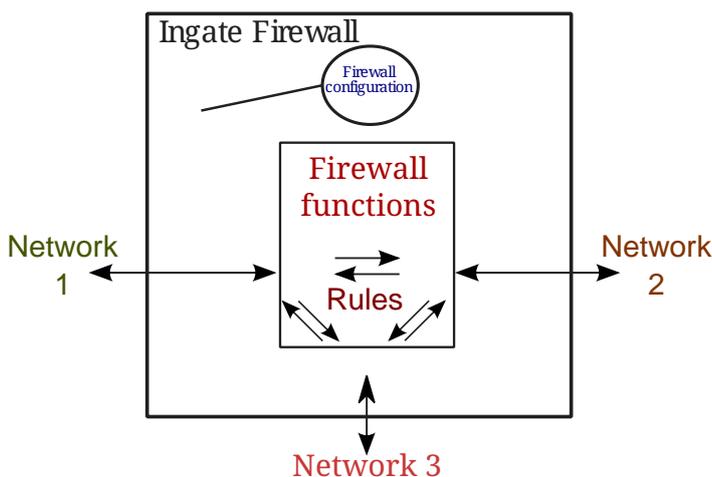
The unit also has various relays.

To handle firewall rules and relays, you need to group machines and networks for each network connected to the unit. These are defined on the **Networks and Computers** page.

The network interfaces in the unit are Ethernet cards.

## Traffic Configuration

You set separate rules and relays between each pair of network interfaces in the unit. The figure below shows a unit with three network interfaces. You can configure the unit from one or more computers on network 1.



The firewall rules work this way: Traffic comes in from one of the networks. The firewall looks for the IP address where the traffic originates. If the IP address belongs to a network that shouldn't be connected to this interface, the firewall discards or rejects all traffic from this source. This protects you against address spoofing. Next, the firewall examines the port and IP address to determine if the traffic should be allowed to continue to the second network. This also considers the direction from which a connection is made.

The order of the rules determines what rule is used. The first rule matching the packet in question is applied. For example, if a rule rejecting certain traffic comes before a rule allowing the same kind of traffic, the first rule will apply, rejecting the packets.

The process of rule matching is different, depending on which protocol is used. Basic features are:

- Packets must use the protocol defined in **Services**

- The IP address of the sender must be in the client group
- The IP address of the receiver must be in the server group

To match ICMP packets, the following also applies:

- The ICMP type used must be defined in **Services**

To match UDP packets, the following also applies:

- The sender port must be included in the definition of client ports in **Services**
- The receiver port must be included in the definition of server ports in **Services**

ICMP and UDP are connectionless traffic, where messages are just sent from one computer to another. So, if you want to let ICMP traffic through the unit, you must make a rule to allow the ICMP messages in one direction and another to allow the reply traffic in the other direction.

One example is *ping*, which is used to see if a computer is running. To send a ping packet from a computer on one network to a computer on another network, switch on ICMP type 8 (echo) in the direction from the client machine sending the signal to the server, and ICMP type 0 (echo reply) in the opposite direction for the response.

TCP packets are treated in a special way, since TCP is a connection oriented protocol. The first packet, the connection establishing packet, is matched the same way as a UDP packet. The unit also adds firewall rules for the reply packets from server to client.

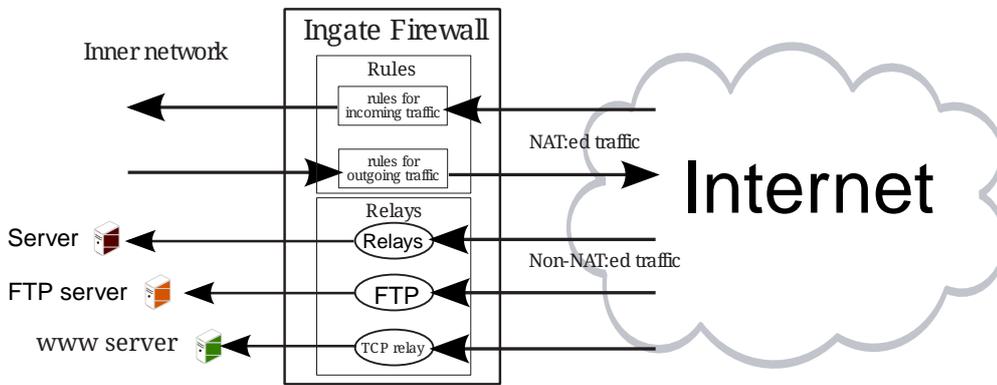
If NAT is used (see Masquerading), the unit will keep track of all current connections; only reply packets for active sessions are allowed.

If NAT is not used, the unit will do one of the following:

- If the service in question uses **Packet filter**, fixed firewall rules will be created which will allow all reply packets of allowed TCP connections, for all ports in the service definition and for all networks.
- If the service in question uses **Dynamic session management**, dynamic firewall rules will be created when a connection is established, and be discarded when the connection is closed. These rules only apply to server and client ports used by this particular connection.
- If the service in question uses **Dynamic FTP management**, dynamic firewall rules will be created when an FTP connection is established. The unit will also create shadow rules for the FTP data traffic, monitoring the FTP traffic to determine whether a rule for active or passive FTP should be used. If **Dynamic FTP management** is used, no rule for FTP data traffic is needed.

The unit rejects or discards all packets which do not match a firewall rule. This function works as if the last rule in the unit rules list were a rule which discards or rejects every single packet. By blocking all packets not accounted for in the rules list, you control the traffic more securely. It is easier to block everything and then let some through, than the other way round.

The figure shows how the firewall functions work in an example with one connection to the Internet and one to an internal network.



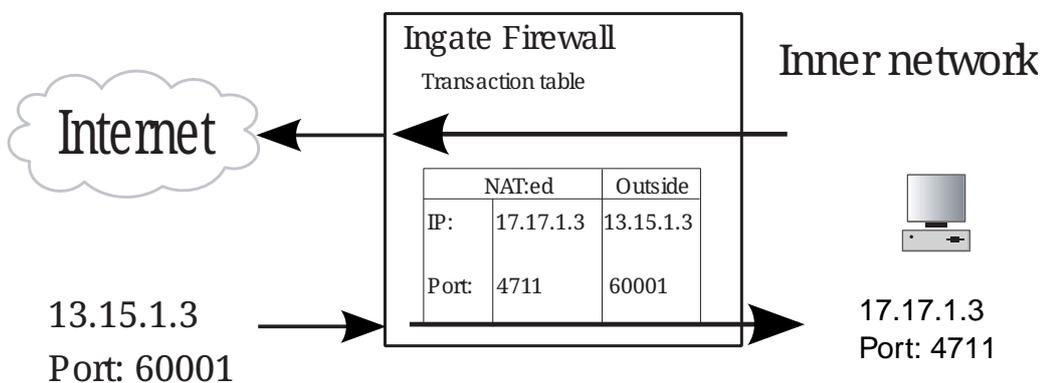
## NAT

You can masquerade the traffic between different network interfaces. NAT (Network Address Translation) hides the computers and networks behind the unit. For example, if network interface eth1 is connected to the Internet and eth0 is connected to an internal network, you can use NAT between eth0 and eth1 to hide the computers and networks connected to eth0 from outside eyes. From the Internet, only the IP addresses at eth1 is visible.

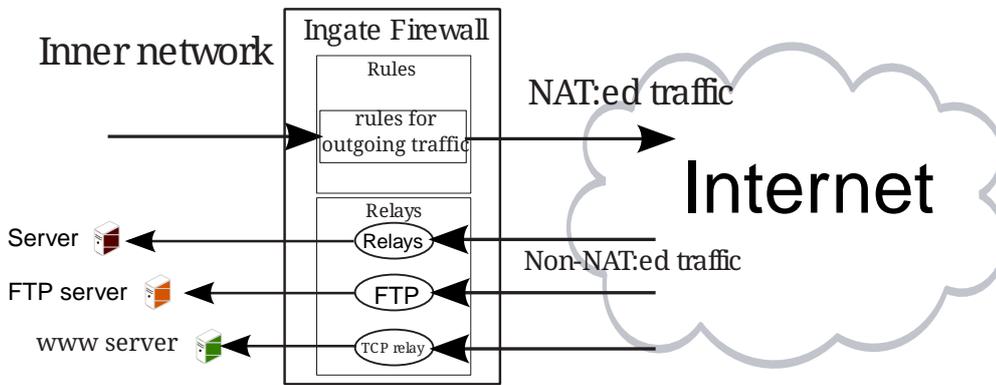
To access a server on the internal network in the above example, a further link is needed, a relay. All computers on the outer network believe that all servers in the organization are on the firewall machine, because that is the only visible computer.

When NAT is on, FTP, Real Audio and IRC work a little differently. When a client program on the internal network opens a connection with an external server, the unit converts the client computer's port and IP address. The new port number becomes one in the series 61000-65096, and the IP address becomes the same as the unit's external number. This is what the external server sees for the FTP, Real Audio and IRC services.

The unit uses a table to store the IP and port numbers of all established connections. In the example below, the inner network is hidden from the Internet. Traffic from a computer on the internal network is translated to the IP address and port on the inside of the unit. Reply traffic in the other direction is translated back to the IP address and port of the computer on the internal network.



The figure below shows how the firewall functions work in an example with one connection to the Internet and one to an internal network.



## Relays

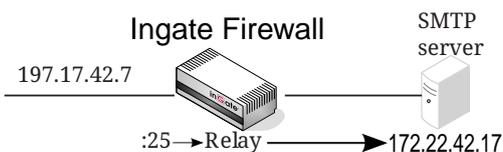
The unit has a number of relays: TCP relay, UDP relay, address rewriting HTTP relay, FTP relay, and DHCP relay. All relays (except for the DHCP relay) have access control, meaning that they can be configured to allow traffic only from certain IP addresses. Relays can also be configured to be active only for certain time intervals, such as only working hours or only during the weekend. This is accomplished by defining and using time classes for the relays.

### Relays

A relay performs a simple forwarding of traffic from one address to another. The relay receives traffic that comes to a certain port at a certain IP address of the unit, and sends it on to a specific port on a specific computer. You set the IP addresses and ports for each relay.

One example of using a relay is if there is a mail server on the internal network when NAT is on. The name server, which will be used by everyone on the external network, directs all e-mail to 197.17.42.7.

Now we create an alias for the IP address 197.17.42.7 in the unit and set up a relay to receive connections on port 25 for this IP address. We specify that all e-mail should be sent on to port 25 of the computer with the IP address 172.22.42.17, the mail server's IP address on the internal network.



Another typical area of use is a web server on the internal network. We have set up www.company.se on a name server, with an IP address which our unit has on the outside. In the unit, we set up a relay that sends WWW traffic on to the web server on the inside.

Suppose an organization has two web servers. One is for internal use and the other is available from the outside. Both servers are running on a computer with IP address 172.22.10.17 on the internal network. The internal server uses port 80 and the external one uses port 8080. By configuring a TCP relay to listen to port 80 on the external interface of the unit, and relaying the traffic to port 8080 at 172.22.10.17, the web server is available from the outside.

## TCP and UDP relays

With a TCP relay, the client machine connects to an IP address and a port in the unit. The client machine only sees the unit. The TCP relay receives a TCP packet, generates a new TCP packet with the same content and forwards the traffic to the server. What the server sees is a connection from the unit; it does not see the actual client.

A UDP relay works in the same way as the TCP relay, but forwards UDP traffic.

## Port forwarding

With regular TCP port forwarding, the client machine connects to an IP address and a port in the unit. The client machine only sees the unit. The TCP relay forwards the traffic to the server after rewriting the sender address to that of the unit. What the server sees is a connection from the unit; it does not see the actual client.

UDP port forwarding works in the same way as the TCP port forwarding, but forwards UDP traffic.

## Semi-transparent port forwarding

With semi-transparent TCP port forwarding, the client machine connects to an IP address and a port in the unit. The client machine only sees the unit. The TCP relay forwards the traffic to the server without rewriting the sender address to that of the unit. What the server sees is a connection from the actual client. The exception from this is when the client and the server are connected to the unit via the same interface; then, the sender address is rewritten just as for the regular port forwarding.

Semi-transparent UDP port forwarding works in the same way as the semi-transparent TCP port forwarding, but forwards UDP traffic.

## Address rewriting HTTP relay

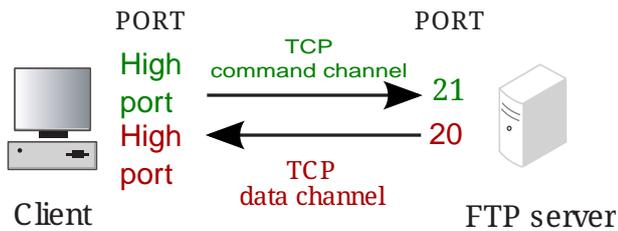
The address rewriting HTTP relay works in approximately the same way as a standard relay, except that the relay looks at all outgoing traffic from the web server on the inside. The relay replaces the web server's IP address with the IP address that the unit has on the outside for this relay in all outgoing traffic. This relay is somewhat slower than a standard relay. The relay does not understand HTTP or HTML and can sometimes exchange too much data, so it is usually better to use a standard relay for WWW traffic.

## FTP relay

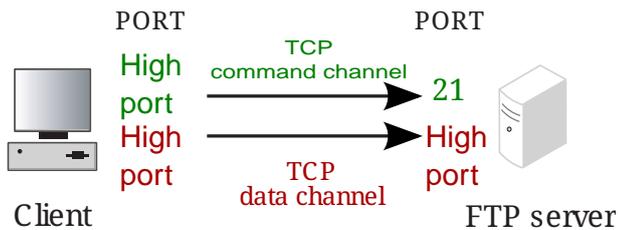
Another relay is FTP, which manages connections to an FTP server. For the client computer the FTP relay acts like an FTP server. The relay tries to establish contact with the FTP server just like a standard client. The FTP server only sees the relay and interprets it as a client.

FTP has two types of connections, active and passive. In an active connection, the client connects to the command port on the server, usually port 21. When a file is transferred, the server connects to the client for data transfer. For active FTP, the FTP relay assumes that FTP data is the port number under the one for FTP commands. This applies both to the port the FTP relay is listening to and the **Relay to Port**. Usually, the server uses port 21 for FTP commands and 20 for FTP data.

Arrows indicate in which direction the connections are set up. The direction of the data flow is independent of this.



In a passive connection, the client connects to the command port on the server. To send a file, the client connects again to a port with a number over 1023 on the server for the data transfer.



Active and passive FTP are both supported by the unit's FTP relay.

### DHCP relay

The DHCP relay handles DHCP requests between a client and a DHCP server. This makes it possible to let one single server support clients on several networks, thereby simplifying the IP address distribution.

DHCP requests are BOOTP packets sent from a client who wants to obtain an IP address. Since the client has no IP address and doesn't know about the network configuration, it just broadcasts the request. One or more DHCP servers reply, sending packets addressed to the client. The packets could grant an IP address or reject the request if no IP addresses are available.

Most DHCP servers are configured to hand out dynamically allocated addresses, which means that the client leases an address and must ask for new leases regularly. The server always checks an address before handing it out, to be sure that it really is available. This could be performed using ping, which means that ping also must be let through to the networks that the server supports. The client also checks the newly received address, e.g. using ARP, which means that you also must open for ARP communication between the networks.

### Relay limitations

There are some limitations for the unit's relays. These are mostly of the form that some ports can't be used for some of the unit IP addresses (this renders the error message The same local IP address/port combination is listened to more than once).

In these limitation descriptions, all references to "relays" means relays, port forwardings and semitransparent port forwardings unless otherwise stated.

### TCP relay on port 80 or 443

You can't make a TCP relay listen to port 80 (http) or 443 (https) on the IP address used for unit

configuration, i. e. the IP address which you connect to to make configurations on your unit. This is because these ports are locked for the configuration traffic and can't be used for anything else.

To relay traffic through the unit to servers on your local network, you must create an **Alias** on the interface holding the configuration IP address. Then, use this alias for the relays.

### **UDP relay on port 500**

You can't make a UDP relay listen to port 500 (IKE) on any unit IP address when VPN is installed. This is because these ports are locked for the unit's own IKE traffic and can't be used for anything else.

The best way to work around this is to terminate VPN tunnels in the unit.

### **UDP relay on port 514**

You can't make a UDP relay listen to port 514 (syslog) on any unit IP address. This is because these ports are locked for the unit's own syslog traffic and can't be used for anything else.

If you need to send syslog traffic through the unit, try to make the syslog message senders send to a different port.

### **Relays and VPN**

If you haven't entered a **Default gateway** on the **Default Gateways** page, you have to select an **IPsec peer** under **Allow access from** on the **IPsec Peers** page if computers should be allowed to use the relay through a IPsec connection. If no IPsec peer is selected, traffic through IPsec connections won't be allowed to use the relay.

If you want to allow computers to use the relay regardless of their using IPsec, you have to configure a default gateway for the unit.

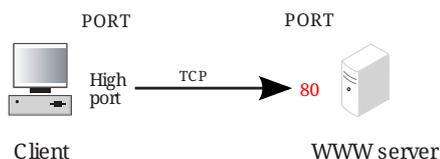
# Appendix B: Common services

The following is a description of some of the most common services and how they can be managed in the unit.

The following descriptions use the term 'high port' for a port with a high number (1024-65535).

## HTTP

HTTP stands for HyperText Transfer Protocol and is primarily used for transferring web pages. HTTP is a simple protocol to manage and does not require much comment. We describe it here because it is common and can serve as an example for similar services.



HTTP usually uses a high port number on the client, port 80 on the server, and the TCP protocol. This corresponds to the following service definition:

Table 2. Services

Name	Protocol	Firewall type	Client ports	Server ports
http	TCP	Dynamic session management	1024-65535	80

## Outgoing HTTP

Allow the http service as defined above from the computers that are allowed to use WWW (for example, the entire network on the inside), to the addresses to which they have access (for example the Internet, everything on the outside), using the firewall rules. Example:

Table 3. Rules

Client	Server	Services	Action
Inside	Internet	http	Allow
Inside	Internet	dns	Allow
Internet	Inside	dns-reply	Allow

DNS must work so that you can use a domain name (such as www.ingate.com) in URLs. If you accidentally block DNS, you can only surf with IP addresses in the URLs.

## Incoming HTTP

To allow outside computers to access web servers on an internal network, there are two alternatives: either use firewall rules or a relay. The relay solution can be used regardless of whether NAT is used or not. Forwarding with firewall rules can be used only if NAT isn't used.

## Using Rules

Allow the http service as defined above from the computers that are allowed to visit your web server (such as the Internet, everything on the outside) to the address of your web server. Example:

Table 4. Rules

Client	Server	Services	Action
Internet	Web server	http	Allow

## Using Relays

Use a relay to forward HTTP connections to the correct computer. Example (assuming that 192.168.1.17 is the internal IP address of the web server):

Table 5. Relays

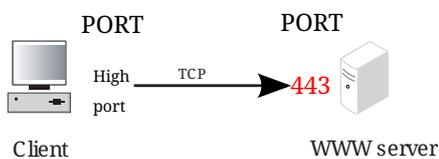
IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	80	192.168.1.17	80	TCP relay	Internet

The address in **IP address** is the one that visitors should point their browsers at.

If the web server on the inside insists on sending back its internal IP address in the web pages, problems will occur, since external web browsers can only access the web server via the relay. If this happens, you can use the Address rewriting HTTP relay type instead of a TCP relay to modify the outgoing web pages when they pass through the unit. See [IP Firewall](#).

## HTTPS

HTTPS is used for encrypted connections to a web server. It is a simple protocol to handle from the unit point of view. Everything works the same way as with HTTP, except that HTTPS uses port 443 on the server instead of port 80.



This corresponds to the following service definition:

Table 6. Services

Name	Protocol	Firewall type	Client ports	Server ports
https	TCP	Dynamic session management	1024-65535	443

Firewall rules configuration is the same as for HTTP, with the exception that the service https is used instead of http.

The http and https services are included in the predefined www service.

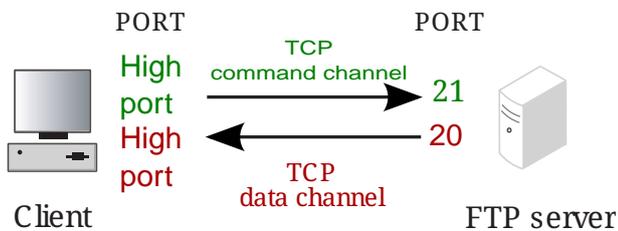
## FTP

The FTP file transfer protocol is not particularly attractive from the unit point of view, mainly because it was designed long before security became an important consideration. The more modern HTTP protocol does have some other problems, but it is much easier to handle for firewalls. Another complication is that there are two variants of the FTP protocol: active and passive FTP. The following is a somewhat simplified description of these alternatives:

### Active FTP

A transfer starts with the opening of a command channel from the client (high port) to the server (port 21).

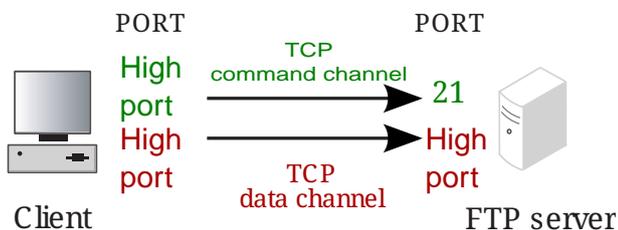
When data is to be transferred, the client opens another high port and sends a command over the command channel to convey the port number. The server opens a connection from port 20 to the new client port.



The problem from the unit point of view is mainly that the server connection is from the wrong direction. The connection is from the outside, but it is really the client that controls the connection. Dynamic FTP management allows the unit to create a shadow rule for the data channel connection.

### Passive FTP

Like active FTP, a command channel is opened from the client (high port) to the server (port 21). When data is to be transferred, the client sends the command PASV, which asks the server to open a high port and send back the port number. Then the client can open a connection from a high port of its own to the high port on the server.



The problem from a firewall point of view is mainly that the connection for data transfer is made from one high port to another, and we do not know either of the port numbers beforehand.

Some FTP clients can only manage active FTP, while others can only manage passive FTP. Some try passive first, then go to active if this fails. Also, it is not certain that all FTP servers in the world can manage passive FTP. Dynamic FTP management allows the unit to create a shadow rule for the data channel connection.

## Outgoing FTP configuration

Regardless of whether NAT is used or not, and whether the server supports active or passive FTP, this will be the FTP configuration.

To manage the command channel and the computer connection, we set up the following service:

Table 7. Services

Name	Protocol	Firewall type	Client ports	Server ports
ftp	TCP	Dynamic FTP management	1024-65535	21

The ftp service is let through in the usual way in **Rules**. If we assume that everyone on the inside can run FTP against the entire Internet:

Table 8. Rules

Client	Server	Services	Action
Inside	Internet	ftp	Allow

No firewall rule for the data channel connection is needed when dynamic FTP management is used.

## Incoming FTP configuration

To allow FTP traffic from the outside to servers within the protected network, there are two alternatives: use firewall rules or use the FTP relay.

### Using Rules (no NAT)

The following service is used in the rules below:

Table 9. Services

Name	Protocol	Firewall type	Client ports	Server ports
ftp	TCP	Dynamic FTP management	1024-65535	21

To allow active and passive FTP from the entire Internet to the FTP server, the following configuration is needed in **Rules**:

Table 10. Rules

Client	Server	Services	Action
Internet	FTP server	ftp	Allow

There are no troubling holes in this set of rules.

### Using Relays (NAT/no NAT)

To manage active and passive FTP in this way, set up a relay from the unit to the computer on the

inside that manages FTP:

Table 11. Relays

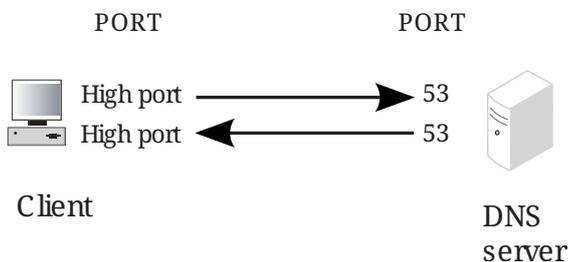
IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	21	192.168.1.42	21	FTP relay	Internet

In this example, we assume that the FTP server on the inner network has the address 192.168.1.42. Please note that clients on the outside should connect to the IP address 1.2.3.4 (or a DNS name for the outside), not 192.168.1.42. To use a different IP address than the usual one for the outside of the unit, we use an alias.

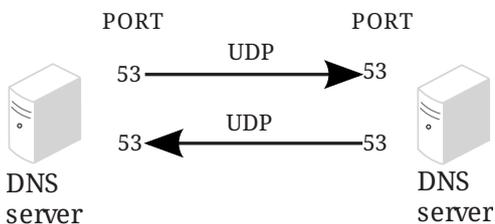
## DNS

DNS is used to look up names and IP addresses. It usually uses a high port on the client and port 53 on the server. When two DNS servers send data from one to the other, both usually use port 53. UDP is used for individual queries and TCP to transfer entire zones. Transferring of zones are, for example, used when a secondary name server gets information from a primary name server.

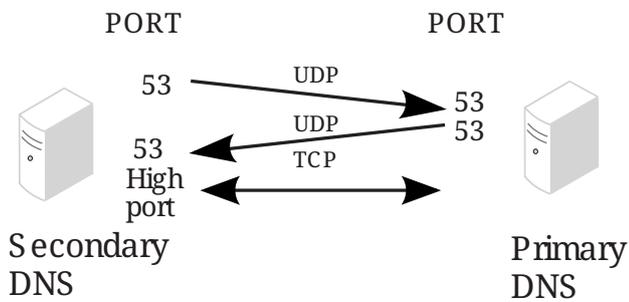
Some examples of clients are web browsers; Netscape, Internet Explorer, Lynx, etc. The client usually uses a high port and the server usually port 53. They use UDP as the protocol for transferring questions and answers. A query might also originate from a DNS server forwarding a query from a client program to another DNS server.



When a client program queries a name server and the name server has to query another name server, the queries and data are sent with UDP from port 53 to port 53.



Both UDP and TCP are used for zone transfers. First, a little data is sent with UDP in the same way as when a name server asks another name server for a name or IP address. Then, a TCP connection is made from a high port on the secondary name server to port 53 on the primary name server.



Some versions of Windows contain programs that send DNS queries from port 137. If you use such programs you have to change 53, 1024-65535 to 53,137, 1024-65535 in the examples below.

## DNS (no NAT)

Set up the following services for DNS:

Table 12. Services

Name	Protocol	Firewall type	Client ports	Server ports
dns	UDP	Packet filter	53, 1024-65535	53
dns-reply	UDP	Packet filter	53	53, 1024-65535
dns-tcp	TCP	Dynamic session management	1024-65535	53

DNS requires rules for both directions through the unit. See the figure on the previous page.

### Incoming DNS configuration

To allow DNS queries to come in from the outside and a secondary DNS server on the outside to retrieve parts of or the entire database, enter the following rules for the internal server. Add a rule to allow the replies to get through:

Table 13. Rules

Client	Server	Services	Action
Internet	DNS server	dns	Allow
Internet	DNS server	dns-tcp	Allow
DNS server	Internet	dns-reply	Allow

### Outgoing DNS configuration

To allow DNS queries to come out from the inside and a secondary DNS server on the inside to retrieve parts of or the entire database of an external primary DNS server, enter the following rules for external servers. Add a rule for incoming traffic to allow the replies to get through:

Table 14. Rules

Client	Server	Services	Action
DNS server	Internet	dns	Allow
DNS server	Internet	dns-tcp	Allow

Client	Server	Services	Action
Internet	DNS server	dns-relpy	Allow

## DNS (NAT)

### Incoming DNS configuration

It is not common to allow DNS queries into a NAT:ed network, as the computers on this network are supposed to be hidden from the outside network. However, this is how to let the queries through.

For DNS queries from the outside to an internal DNS server, a UDP relay is needed (UDP relays can also be used when NAT isn't used). Define the relay under **Relays**:

Table 15. Relays

IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	53	DNS server	53	UDP relay	Internet

The relay does not need a firewall rule for traffic in the other direction.

### Outgoing DNS configuration

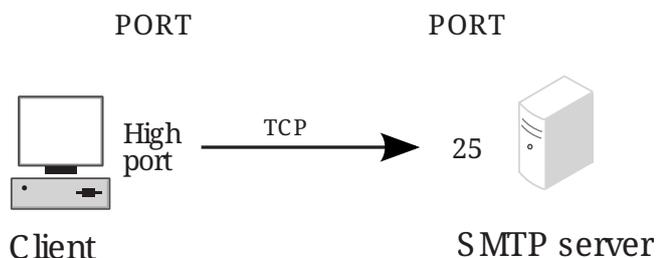
To query an external DNS server from the inside, firewall rules for outgoing traffic are needed. Since NAT is used, no rules for the reply traffic are needed.

Table 16. Rules

Client	Server	Services	Action
DNS server	Internet	dns	Allow
DNS server	Internet	dns-tcp	Allow

## SMTP

SMTP stands for Simple Mail Transfer Protocol and is used to transfer e-mail between mail servers. SMTP usually uses a high port number on the client, port 25 on the server, and the TCP protocol.



This corresponds to the following service definition:

Table 17. Services

Name	Protocol	Firewall type	Client ports	Server ports
smtp	TCP	Dynamic session management	1024-65535	25

## Outgoing SMTP

Allow the SMTP service as defined above from the computers that can forward e-mail to computers outside the unit (for example, a server on an internal network), to one or more mail servers (for example, the Internet, everyone on the outside). Example:

Table 18. Rules

Client	Server	Services	Action
Mail server	Internet	smtp	Allow

DNS must work (see the DNS section) so that you can use a domain name (such as mail.ingate.se). E-mail will not work properly if you accidentally block DNS.

## Incoming SMTP

To allow outside SMTP servers to connect to servers on an internal network, there are two alternatives: use firewall rules or use a relay. The relay solution works regardless of whether NAT is used or not, while the first solution only works when NAT isn't used.

### Using Rules

Allow the SMTP service as defined above from the computers that are allowed to visit your mail server (such as the Internet, everything on the outside) to the address of your mail server. Example:

Table 19. Rules

Client	Server	Services	Action
Internet	Mail server	smtp	Allow

### Using Relays

Use a relay to forward SMTP connections to the correct computer. Example (assuming that 192.168.1.17 is the internal IP address to the mail server):

Table 20. Relays

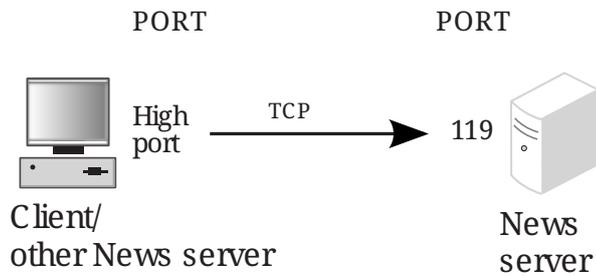
IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	25	Mail server	25	TCP relay	Internet

The outer name (the unit's outer address if you have not entered other outer names) is the address mail servers on the outside should use.

# Nntp

Nntp stands for Network News Transfer Protocol and is used to handle Usenet News over Internet. Far from being located on a single server, Usenet News texts are distributed to all News servers around the world. Most larger organizations have a News server of their own, the server being configured to receive certain parts of the News hierarchy from one or more other News servers.

Nntp uses TCP from a high port to port 119 on the News server. The connecting computer could be another News server or a News client.



This corresponds to the following service definition:

Table 21. Services

Name	Protocol	Firewall type	Client ports	Server ports
nntp	TCP	Dynamic session management	1024-65535	119

See the SMTP or HTTP section for information on how to create firewall rules and relays.

# Telnet

Telnet is used to establish terminal connections to other computers. Telnet enables you to log on to another computer. Telnet sends all traffic, including passwords, unencrypted, which means that anybody who can access the cables between the two computers can eavesdrop on the communication. Therefore, it is not advisable to allow telnet to the internal network of your organization from an insecure network such as Internet. We recommend only allowing telnet on networks that you control, and maybe from your network out to the insecure network.

Telnet usually uses a high port on the client, port 23 on the server and the TCP protocol.

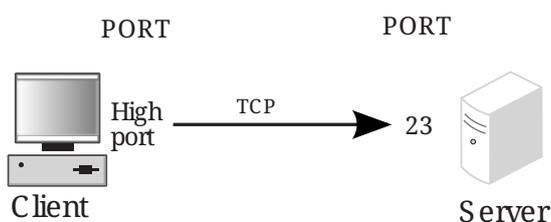


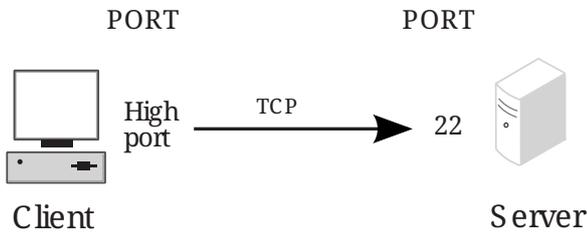
Table 22. Services

Name	Protocol	Firewall type	Client ports	Server ports
telnet	TCP	Dynamic session management	1024-65535	23

See the SMTP or HTTP section for information on how to create firewall rules and relays.

## SSH

SSH (Secure SHell) is used to establish terminal connections to other computers. SSH enables you to log on to another computer. SSH sends all traffic, including passwords, encrypted. SSH usually uses a high port on the client, port 22 on the server and the TCP protocol.



This corresponds to the following service definition:

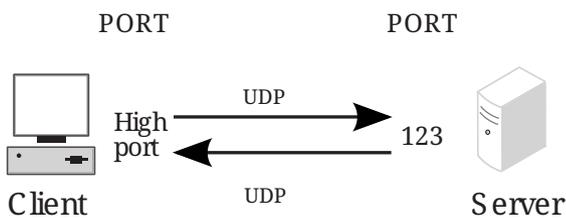
Table 23. Services

Name	Protocol	Firewall type	Client ports	Server ports
ssh	TCP	Dynamic session management	1024-65535	22

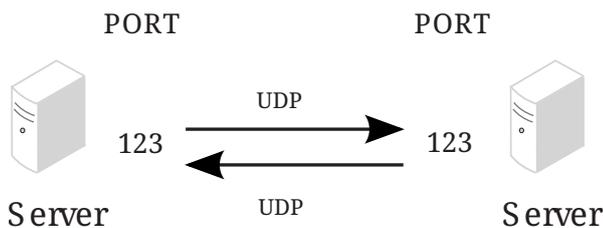
## NTP

NTP stands for Network Time Protocol. NTP is used for synchronizing computer clocks. The synchronization normally uses a computer with a very accurate clock, e.g., a computer with an atomic clock.

A client computer wanting to synchronize with a server via NTP usually uses a high port on the client, port 123 on the server and the UDP protocol. The server returns data using UDP from port 123 to a high port on the client computer.



Two NTP servers communicating with each other use port 123 and the UDP protocol.



This corresponds to the following service definitions:

Table 24. Services

Name	Protocol	Firewall type	Client ports	Server ports
ntp	UDP	Packet filter	123, 1024-65535	123
ntp-reply	UDP	Packet filter	123	123, 1024-65535

## Outgoing NTP configuration

### Using Rules (no NAT)

For the client and the server to be able to communicate, you need two rules, one for each direction. Allow the ntp service from the Inside to the Internet and the ntp-reply service from the Internet to the Inside. N. B.: By doing this, you open all high ports for UDP traffic from the Internet to the Inside. You will have to block services that should not be available by creating firewall rules rejecting the traffic. These rejecting rules must come before the ntp rules in the firewall table. It is advisable to block SMB, NFS and X.

Table 25. Rules

Client	Server	Services	Action
Inside	Internet	ntp	Allow
Internet	Inside	ntp-reply	Allow

### Using Rules (NAT)

For the client and the server to be able to communicate, you need one rule from the Inside to the Internet. The replies need no rules as the NAT system handles this automatically.

Table 26. Rules

Client	Server	Services	Action
Inside	Internet	ntp	Allow

## Incoming NTP configuration

### Using Rules (no NAT)

For the client and the server to be able to communicate, you need two rules, one for each direction. Allow the ntp service from the Internet to the ntp server and the ntp-reply service from the ntp server to the Internet.

Table 27. Rules

Client	Server	Services	Action
Internet	NTP server	ntp	Allow
NTP server	Internet	ntp-reply	Allow

### Using Relays (NAT/no NAT)

Use a relay to forward ntp connections to a computer. Example (supposing the internal ntp server

has the IP address 192.168.1.17):

Table 28. Relays

IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	123	192.168.1.17	123	UDP relay	Internet

If you want the server to know the IP addresses of the clients you should change the UDP relay to a semitransparent UDP port forwarding.

N.B.: The visitors should connect to the outside address of the unit - addresses inside a NAT:ed network aren't visible on the outside.

## Traceroute

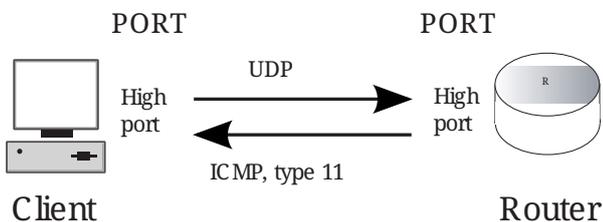
Traceroute is a service used for examining the routing from a client computer to a server. Traceroute is an excellent tool for tracing errors in a computer network. Traceroute finds failures and loops in the network. As traceroute often is used to examine the structure of a network, it is not advisable to allow this service into an internal network.

To explore the route to a server, traceroute first sends a packet to the first router or other network equipment in the network. The router sends a reply packet to the client computer. Then traceroute sends a packet to the second router, which also replies to the client. This is repeated until traceroute reaches the server, which also sends a reply packet to the client.

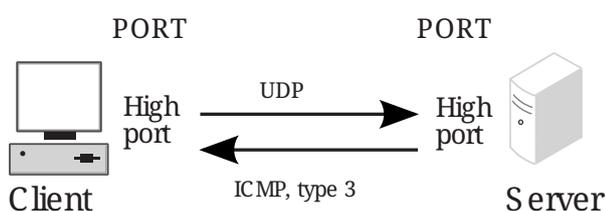
For traceroute to be able to query names in a DNS, services and rules for DNS traffic is required, see the DNS section. The name queries are made by the client.

Traceroute sends data using the UDP protocol. Client and server ports differ from different versions of traceroute, but usually both are high ports (a number higher than 32768), and the server port with few exceptions is in the interval 33434 to 33523, inclusive.

Routers and other network equipment reply by sending a type 11 ICMP packet.



The destination server replies with a type 3 ICMP packet.



This corresponds to the following service definition for UDP traffic:

Table 29. Services

Name	Protocol	Firewall type	Client ports	Server ports
tracert	UDP	Packet filter	1024-65535	33434-33523

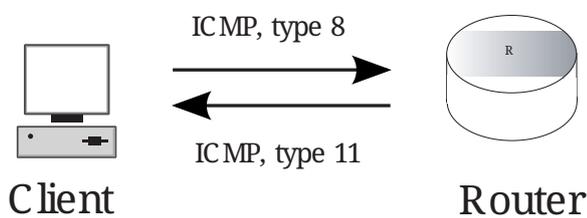
The reply traffic will need this service definition:

Table 30. Services

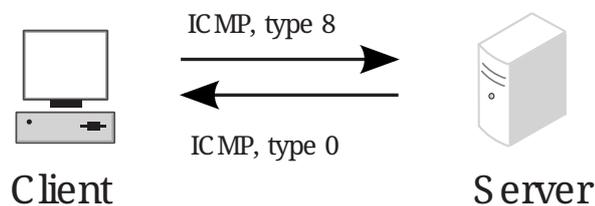
Name	Protocol	Firewall type	ICMP type
tracert-reply	ICMP	Packet filter	3, 11

## Tracert in Windows

In Microsoft Windows and some other operating systems tracert works differently. The client computer sends ICMP packets of type 8, echo-request, instead of UDP packets. Routers reply with type 11 ICMP packets as before.



The destination server replies with an ICMP packet of type 0, echo-reply, the same type as ping uses.



This corresponds to the following service definitions:

Table 31. Services

Name	Protocol	Firewall type	ICMP type
tracert	ICMP	Packet filter	8
tracert-reply	ICMP	Packet filter	0, 11

The tracert service defined above is usually called echo-request, but to simplify we use the name tracert for this service.

## Outgoing tracert configuration

### Using Rules (no NAT)

Allow the tracert service from the computers which should be able to run tracert (e. g., the Inside) to the computers whose route you want to examine (e.g., Internet). A firewall rule allowing tracert-reply in the opposite direction is needed for the replies to reach the client computers.

Table 32. Rules

Client	Server	Services	Action
Inside	Internet	traceroute	Allow
Internet	Inside	traceroute-reply	Allow

### Using Rules (NAT)

Allow the traceroute service from the computers which should be able to run traceroute (e. g., the Inside) to the computers whose route you want to examine (e.g., Internet). The replies need no rules as the NAT system handles this automatically.

Table 33. Rules

Client	Server	Services	Action
Inside	Internet	traceroute	Allow

## Incoming traceroute configuration

### Using Rules (no NAT)

Allow the traceroute service from the computers which should be able to run traceroute (e.g., Internet) to the computers whose route you want to examine (e.g., the Inside). A firewall rule allowing traceroute-reply in the opposite direction is needed for the replies to reach the client computers.

As traceroute often is used to examine the structure of a network, it is not advisable to allow this service into an internal network.

Table 34. Rules

Client	Server	Services	Action
Internet	Inside	traceroute	Allow
Inside	Internet	traceroute-reply	Allow

There is no alternative for incoming traceroute to a NAT:ed network, as it is supposed to be hidden for the outside network.

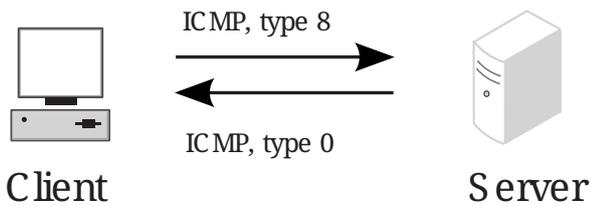
## Ping

Ping is used to examine whether a computer works and is accessible over a network. Ping sends ICMP traffic to the computer in question, and the target computer replies with a reply ICMP packet if it is running and reachable from the network.

You can also ping a whole network, and thereby use ping to examine which computers exist on a certain network. Therefore it is not advisable to allow ping into an internal network.

The client computer sends a type 8 ICMP packet, echo-request, to find out whether the target computer is working and accessible. The target computer ("server" in the picture below) replies

with a type 0 ICMP packet, echo-reply, to tell it is working and accessible over the network.



This corresponds to the following service definitions:

Table 35. Services

Name	Protocol	Firewall type	ICMP type
echo-request	ICMP	Packet filter	8
echo-reply	ICMP	Packet filter	0

## Outgoing ping configuration

### No NAT

Allow the echo-request service from the computers which should be able to run ping (e.g., the Inside) to the computers you want to ping (e.g., Internet). A firewall rule allowing echo-reply in the opposite direction is needed for the replies to reach the client computers. Example:

Table 36. Rules

Client	Server	Services	Action
Inside	Internet	echo-request	Allow
Internet	Inside	echo-reply	Allow

### NAT

Allow the echo-request service from the computers which should be able to run ping (e.g., the Inside) to the computers you want to ping (e.g., Internet). The replies need no rules as the NAT system handles this automatically. Example:

Table 37. Rules

Client	Server	Services	Action
Inside	Internet	echo-request	Allow

## Incoming ping configuration

### No NAT

Ping from the Internet to an internal network is not advisable (see above), but this is how to do it. Allow the echo-request service from the computers which should be able to run ping (e.g., Internet) to the computers you want to ping (e.g., the Inside). A firewall rule allowing echo-reply in the opposite direction is needed for the replies to reach the client computers. Example:

Table 38. Rules

Client	Server	Services	Action
Internet	Inside	echo-request	Allow
Inside	Internet	echo-reply	Allow

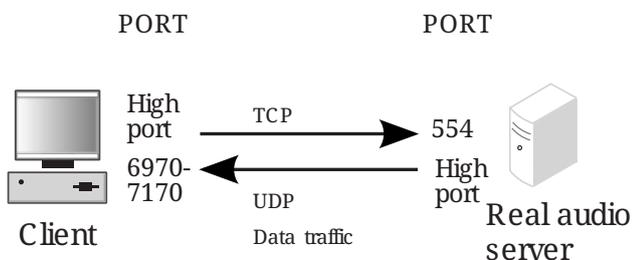
## NAT

Incoming ping through the unit using NAT for the outgoing traffic is not possible as there is no way to let the traffic into a NAT:ed network.

## Real Audio/Video

Real Audio/Video can be used for transferring sound and/or moving pictures.

When using Real Audio/Video, the client establishes a TCP connection from a high port to port 554 on the server. The server sends data from a high port to a port in the interval 6970-7170, inclusive, on the client. The data is sent using the UDP protocol.



This corresponds to the following service definitions:

Table 39. Services

Name	Protocol	Firewall type	Client ports	Server ports
real-audio	TCP	Dynamic session management	1024-65535	554
real-audio-data	UDP	Packet filter	1024-65535	6970-7170

## Outgoing Real Audio/Video configuration

### Using Rules (no NAT)

Allow the real-audio service from the computers which should be able to run Read Audio/Video (e.g., the Inside) to the servers you want to visit (e.g., Internet). A firewall rule allowing real-audio-data in the opposite direction is needed for the data to reach the client computers. Example:

Table 40. Rules

Client	Server	Services	Action
Inside	Internet	real-audio	Allow
Internet	Inside	real-audio-data	Allow

## Using Rules (NAT)

Allow the real-audio service from the computers which should be able to run Read Audio/Video (e.g., the Inside) to the servers you want to visit (e.g., Internet). The data traffic needs no rules as the NAT system handles this automatically.

Table 41. Rules

Client	Server	Services	Action
Inside	Internet	real-audio	Allow

## Incoming Real Audio configuration

When admitting incoming Real Audio to servers behind the unit, you have two options: using firewall rules or a relay. The relay option works regardless of NAT, but the rules will only work when NAT isn't used.

## Using Rules (no NAT)

Allow the real-audio service from the computers which should be able to run Read Audio/Video (e.g., Internet) to your server. A firewall rule allowing real-audio -data in the opposite direction is needed for the data to reach the client computers. Example:

Table 42. Rules

Client	Server	Services	Action
Internet	R/A server	real-audio	Allow
R/A server	Internet	real-audio-data	Allow

## Using Relays (NAT/no NAT)

Define a relay to forward Read Audio/Video connections to the server. Example (supposing 192.168.1.17 is the internal IP address of the Real Audio/Video server):

Table 43. Relays

IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	7070	192.168.1.17	7070	TCP relay	Internet

If you want the server to know the IP addresses of the clients you should change the TCP relay to a semitransparent TCP port forwarding.

N.B.: The visitors should connect to the outside address of the unit - addresses inside a NAT:ed network aren't visible on the outside.

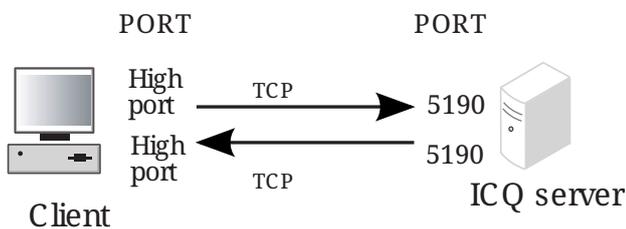
For more information on Real Audio/Video related traffic, see [Real Audio/Video](#).

# ICQ

ICQ is a popular service for communication with other people via Internet. The user client program connects to a server, enabling the user to communicate to other users via this server.

From a security point of view, ICQ traffic through a firewall is not advisable. ICQ clients and servers are notorious for having bugs and safety holes. The protocol is too insecure, sending all traffic, including passwords, unencrypted. The protocol design also makes it easier for a third party to intercept a connection without the client's noticing. The ICQ clients disclose a lot of information, such as the real IP address of the client computer - regardless of NAT being used - and which communication software is available on the client computer.

The ICQ client establish a connection from a high port to port 5190 on the server, using the TCP protocol. The server sends data from port 5190 to the same high port on the client. ICQ might also use other services, e.g., Real Audio/Video (see separate section on that).



This corresponds to the following service definitions:

Table 44. Services

Name	Protocol	Firewall type	Client ports	Server ports
icq	TCP	Dynamic session management	1024-65535	5190

## Outgoing ICQ configuration

### Using Rules (NAT/no NAT)

For the client and the server to be able to communicate, only one rule is needed, as the unit automatically creates shadow rules for TCP reply traffic. Allow the icq service from the Inside to the Internet.

Table 45. Rules

Client	Server	Services	Action
Inside	Internet	icq	Allow

## Incoming ICQ configuration

### Using rules (no NAT)

For the client and the server to be able to communicate, only one rule is needed, as the unit automatically creates shadow rules for TCP reply traffic. Allow the icq service from the Internet to the ICQ server.

Table 46. Rules

Client	Server	Services	Action
Internet	ICQ server	icq	Allow

## Using Relays (NAT/no NAT)

Use a relay to forward ICQ connections to a computer. Example (assuming the internal ICQ server has the IP address 192.168.1.17):

Table 47. Relays

IP address	Port	DNS name or IP address	Port	Relay type	Allow Access from
Outside (1.2.3.4)	5190	192.168.1.17	5190	TCP relay	Internet

If you want the server to know the IP addresses of the clients you should change the TCP relay to a semitransparent TCP port forwarding.

N.B.: The visitors should connect to the outside address of the unit - addresses inside a NAT:ed network aren't visible on the outside.

# Appendix C: More About SIP

## The SIP Protocol

SIP (Session Initiation Protocol), defined in RFC 3261 (with various extensions), handles creation, modification and termination of various media stream sessions over an IP network. It is for example used for Internet telephone calls and distribution of video streams.

SIP also supports user mobility by allowing registration of a user and proxying or redirecting requests to the user's current location. This is performed by the user registering his presence at a machine with the central registrar. The SIP registrar keeps track of the user, but doesn't hold any information about which media streams the computers or clients can manage. This is negotiated between the parts when initiating a SIP session.

### Why use SIP?

Today, two protocols for transmitting IP telephony exist; SIP and H.323. The H.323 protocol was originally designed for video conferences over ISDN and is a mix of several protocols and standards for performing the various phases of a connection. The SIP protocol was designed for general session initialization over the Internet.

Both protocols have the disadvantage (from a firewall point of view) of needing dynamically allocated ports for the data transmission, but today no protocol supports tunneling random media streams.

When comparing the two protocols, there is one major drawback to the H.323 protocol: its lack of scalability. H.323 is mostly used in small LANs. When extending to world-wide IP networks, SIP has many advantages:

- Loop detection

When trying to locate a user over several domains, loops can occur. H.323 has no support for loop detection, which can cause network overload.

Loops are easily detected using SIP headers, as they specify all proxies that have handled the SIP packet.

- Distributed control

H.323 uses gatekeepers, which are devices used for handling call states and redirecting calls to aliases. As every call is carried out statefully, the gatekeepers must keep a call state during the entire call. This of course makes the gatekeepers a major bottleneck in the system.

There is also a need for a central point when performing multi-user calls, which means that someone must provide this central point, and that this machine must be dimensioned for the size of the call.

SIP sessions are completely distributed, making the need of these central points disappear.

- Small connection overhead

Establishing a connection using H.323 takes about three times the data and turnarounds compared to when using SIP.

Apart from this, there are some more disadvantages with H.323. As it uses many protocols, more ports need to be opened in a firewall to enable H.323 signaling through. SIP is a single protocol, which means that only one port has to be opened for SIP signaling. For both protocols, however, more ports must be opened for the data traffic.

SIP runs on both TCP and UDP (and, in fact, can be extended to run on almost any transport protocol), making it possible to use UDP for large servers, thereby enabling stateless sessions. H.323 only runs on TCP, which as already stated loads the servers by requiring state management.

## **SIP and Firewalls**

When trying to use SIP through a firewall, there are some problems.

SIP initiates sessions of other protocols. This means that when a SIP session has been started, various other protocols are used as well, usually transmitted over TCP or UDP on some port. For a firewall, this is a problem, as it often opens up certain protocols and ports in advance, but now you don't know which ports to open. To handle SIP through a firewall which doesn't understand the SIP concept, all ports must be open all the time, which would make the firewall somewhat unnecessary. A firewall that understands SIP can open up the ports for the right protocols just when the SIP traffic needs it.

In the SIP headers there is a lot of information concerning what IP addresses the session participants use. This is a problem if a SIP session should be established through a firewall using NAT. The IP address on the hidden side (which appears in the SIP headers) won't be the same as the one that clients on the outside should use.

## **Managing Your Own SIP Domain**

If you want to use your own SIP domain, there are some things you need to configure in order to make everything work nicely.

- The unit needs to be configured to handle the SIP domain.
- If you use a separate PBX/registrar, this must also be configured to handle the SIP domain.
- The DNS server managing your main domain should be updated with records for the SIP domain.
- The SIP clients used by users on this domain need to be configured.

## **Configuring the unit**

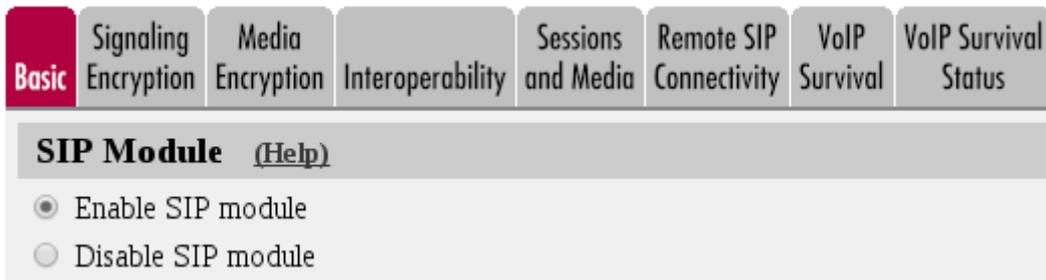
The unit needs configuration regardless of if it is used as registrar or not, although it needs more configuration when used as the registrar for your domain.

## Not Used As Registrar

When the unit is not used as the registrar for your domain, it only needs configuration to forward SIP requests to your registrar. This configuration guide assumes that the PBX is located on your LAN.

You can do this by using the Ingate Startup Tool, which can be downloaded from [http://www.ingate.com/Startup\\_Tool\\_TG.php](http://www.ingate.com/Startup_Tool_TG.php). Below you find the configuration that should be made manually if you do not use the Tool.

Go to the **Basic** page under **SIP Services** and switch the SIP module on.

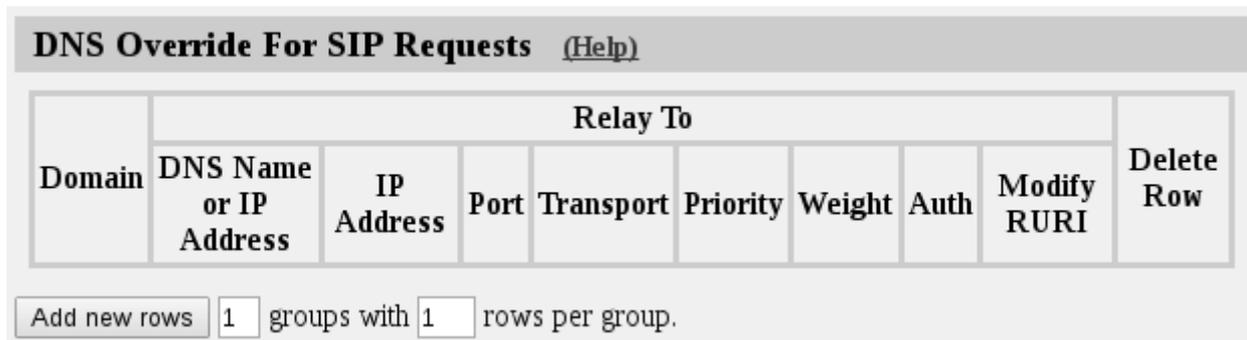


**Basic** Signaling Encryption Media Encryption Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival VoIP Survival Status

**SIP Module** [\(Help\)](#)

- Enable SIP module
- Disable SIP module

Go to the **Routing** page under **SIP Traffic**. In the **DNS Override For SIP Requests** table, add a row where you enter your SIP domain as the Domain, and enter your PBX/registrar IP address and port. You can also select which transport should be used when forwarding SIP requests to the PBX.



**DNS Override For SIP Requests** [\(Help\)](#)

Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	

Add new rows  groups with  rows per group.

If you have remote users behind NAT boxes, you also need to configure **Remote SIP Connectivity** under **SIP Services**. Use the built-in STUN server and/or the Remote NAT Traversal. It is recommended to use the Remote NAT Traversal, as it works for more clients and more NAT types.

**Remote NAT Traversal** [\(Help\)](#)

Enable Remote NAT Traversal  
 Disable Remote NAT Traversal

IP address for remote clients:   
 Forward signaling from IP address:

IP port for remote clients:

NAT keepalive method:  
 Use OPTIONS  
 Use short registration times  
 Use both OPTIONS and short registration times

Media Route:  
 Route media directly between clients behind the same NAT  
 Always route media through the firewall

NAT timeout for UDP:  
 seconds

NAT timeout for TCP:  
 seconds

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.

[Save/Load Configuration](#)
[Show Configuration](#)
[User Administration](#)

**Test Run and Apply Conf** [\(Help\)](#)

Duration of limited test mode:

seconds

## Used As Registrar

When you use the unit itself as the registrar, there are more settings to be made.

Go to the **Basic** page under **SIP Services** and switch the SIP module on.

[Basic](#)
[Signaling Encryption](#)
[Media Encryption](#)
[Interoperability](#)
[Sessions and Media](#)
[Remote SIP Connectivity](#)
[VoIP Survival](#)
[VoIP Survival Status](#)

**SIP Module** [\(Help\)](#)

Enable SIP module  
 Disable SIP module

Go to the **Local Registrar** page under **SIP Traffic** and enter the name of your SIP domain in the **Local SIP Domains** table.

SIP Methods	Filtering	<b>Local Registrar</b>	Authentication and Accounting	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status
-------------	-----------	------------------------	-------------------------------	--------------	-----------	---------	------------	---------	----------------

---

**Local SIP Domains** [\(Help\)](#)

Edit Row	Domain	Delete Row
<input type="checkbox"/>	ingate.com	<input type="checkbox"/>

There are two ways of listing your SIP users for this domain; either you enter them in the **Local SIP User Database** table on the same page, or you use a RADIUS server for keeping the user database.

If you use the Local SIP User Database table, it can look like this:

**Local SIP User Database** [\(Help\)](#)

Edit Row	Username	Domain	Authentication Name	Password	Register From	Delete Row
<input type="checkbox"/>	arthur	ingate.com	arth789		All	<input type="checkbox"/>
<input type="checkbox"/>	harry	ingate.com	harry456		All	<input type="checkbox"/>
<input type="checkbox"/>	helen	ingate.com	helen123		All	<input type="checkbox"/>
<input type="checkbox"/>	mark	ingate.com			All	<input type="checkbox"/>
<input type="checkbox"/>	test	ingate.com			Office network	<input type="checkbox"/>

The unit should be configured to require authentication for all users trying to register. You do this on the **Authentication and Accounting** page.

SIP Methods	Filtering	Local Registrar	<b>Authentication and Accounting</b>	SIP Accounts	Dial Plan	Routing	SIP Status	IDS/IPS	IDS/IPS Status	SIP Test	SIP Test Status
-------------	-----------	-----------------	--------------------------------------	--------------	-----------	---------	------------	---------	----------------	----------	-----------------

---

**Brute Force Authentication Protection** [\(Help\)](#)

Maximum amount of attempts:

Time interval:  seconds

Stop responding after interval:  seconds

Max number of clients:

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication (enabled below).

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

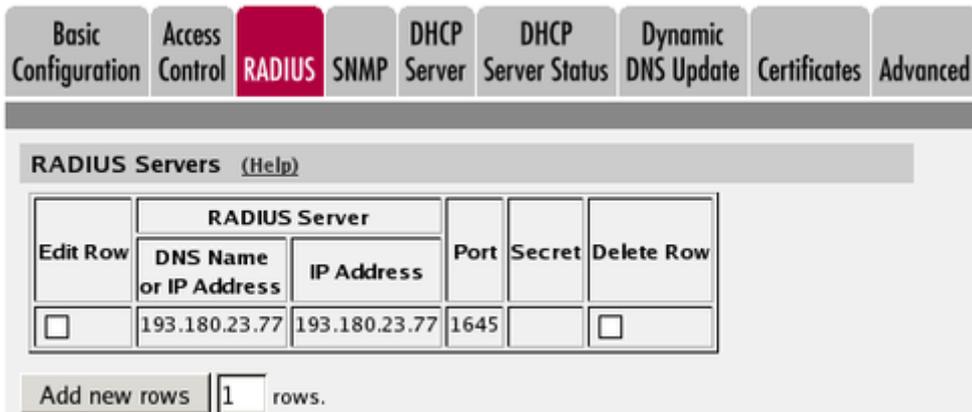
If you use a RADIUS server for the user database, you select this on the **Authentication and Accounting** page.

When you do this, you must also select a network from which the users are allowed to register. If they will register from different networks, you need to select a network group (from the **Networks and Computers** page) which contains all IP addresses.



The screenshot shows the 'RADIUS Database Settings' section. It includes a 'Select SIP User Database' header with a '(Help)' link. Below it, there are radio buttons for 'Local' and 'RADIUS', with 'RADIUS' selected. To the right, under 'RADIUS Database Settings', there is a label 'RADIUS users register from:' followed by a dropdown menu currently showing 'Office network'.

If you use a RADIUS server, you also need to configure which server to use on the **RADIUS** page under **Basic Configuration**.



The screenshot shows the 'RADIUS Servers' configuration page. At the top, there is a navigation bar with tabs: 'Basic Configuration', 'Access Control', 'RADIUS' (highlighted in red), 'SNMP', 'DHCP Server', 'DHCP Server Status', 'Dynamic DNS Update', 'Certificates', and 'Advanced'. Below the tabs is the 'RADIUS Servers' section with a '(Help)' link. It contains a table with the following structure:

Edit Row	RADIUS Server		Port	Secret	Delete Row
	DNS Name or IP Address	IP Address			
<input type="checkbox"/>	193.180.23.77	193.180.23.77	1645		<input type="checkbox"/>

Below the table, there is a button 'Add new rows' followed by an input field containing '1' and the text 'rows'.

You need to select which SIP methods should be authenticated. This is done on the **SIP Methods** page under **SIP Traffic**.

It is recommended that you only authenticate REGISTER messages for the local domain - the domain that this unit handles. If you allow REGISTER messages to other domains to pass through without authentication, users will be able to register to other domains if they need to.

You can also select to use authentication for INVITE requests to other domains. This means that your registered users can call anyone (as they can authenticate), and anyone can call users on your domain, but people from other domains can't use your unit to call to other domains.

**SIP Methods** [\(Help\)](#)

Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.

Edit Row	Method	Traffic To	Allow	Auth	Delete Row
<input type="checkbox"/>	BYE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	DO	Both	No	No	<input type="checkbox"/>
<input type="checkbox"/>	INFO	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	INVITE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	MESSAGE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	NOTIFY	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	OPTIONS	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	PRACK	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REFER	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Local domains	Yes	Yes	<input type="checkbox"/>
<input type="checkbox"/>	REGISTER	Other domains	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SERVICE	Both	Yes	No	<input type="checkbox"/>
<input type="checkbox"/>	SUBSCRIBE	Both	Yes	No	<input type="checkbox"/>

Add new rows  rows.

If you have remote users behind NAT boxes, you also need to configure **Remote SIP Connectivity** under **SIP Services**. Use the built-in STUN server and/or the Remote NAT Traversal. It is recommended to use the Remote NAT Traversal, as it works for more clients and more NAT types.

**Remote NAT Traversal** [\(Help\)](#)

Enable Remote NAT Traversal  
 Disable Remote NAT Traversal

IP address for remote clients:

Forward signaling from IP address:

IP port for remote clients:

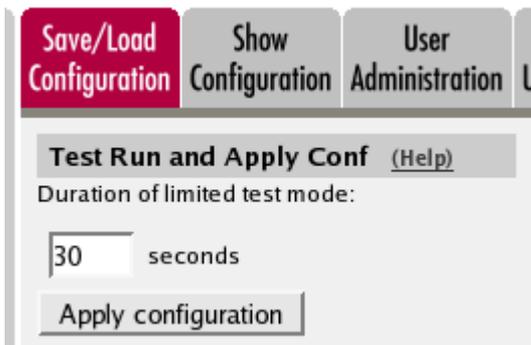
NAT keepalive method:  
 Use OPTIONS  
 Use short registration times  
 Use both OPTIONS and short registration times

Media Route:  
 Route media directly between clients behind the same NAT  
 Always route media through the firewall

NAT timeout for UDP:  seconds

NAT timeout for TCP:  seconds

Finally, go to the **Save/Load Configuration** page under **Administration** and apply the new settings by pressing **Apply configuration**.



## Configuring the PBX

The PBX must be configured to accept registrations for your SIP domain. How you do this depends on the PBX you are using. Some PBX:s accept all domains.

## Configuring the DNS Server

To make other SIP users find your SIP domain, you need to configure your DNS (or rather, the DNS managing the domain).

One way of doing this is to add an A record for the domain, and point it to the unit. With this solution, you need to have a SIP domain that is not used for anything else. An example of a SIP-specific domain would be **sip.ingate.com**.

If you want to use the same domain for all your communication (like **ingate.com**), you need to add an SRV record to the DNS server instead, and point it to the unit. The SRV record is used specifically by SIP devices.

This is an example of an SRV record:

```
_sip._udp      SRV      100      0        5060     tess
_sip._tcp      SRV      100      0        5060     tess
_sips._tcp     SRV      100      0        5061     tess
```

This SRV record is entered into the zone file for the SIP domain. It points to the host tess, which is supposed to be a computer under the same domain (tess.ingate.com) - in this case the unit.

If you don't want to use all transports, you can enter just the lines for the transport you want to allow (like only the TCP line).

## Configuring the SIP Clients

SIP clients that can be configured to use a domain name only need to use the DNS which handles the domain.

SIP clients that need to be configured with an (additional) IP address should use the IP address of the registrar when located on the LAN, and the outside IP address of the unit when located anywhere else.

# SIP Sessions

## Establishing a SIP session

You start a call (a session) by sending a request to the address of the person you want to communicate with. The format of the address is <sip:user@host>, where user can be a user name or a telephone number, and host can be a domain name (e.g. example.com) or a numerical IP address (e.g. 172.15.253.12). This means that it usually looks a lot like a standard email address. In this request information about which media streams the client wants to send/receive and what ports should be used is also included.

The SIP client sends this request to its default SIP proxy. This proxy resolves the SIP domain in DNS, and sends the request to the SIP registrar for that domain. The proxy also adds information stating that the request was routed through the proxy, thus ensuring that the reply will be routed the same way.

The registrar for the domain looks up the user to see where he is registered, and forwards the request to the machine in question. The SIP client on this machine alerts the user, indicating that someone wants to initiate a SIP session. The user confirms that he, too, wants the SIP session. The client sends a reply with necessary information about what ports should be used by this client for sending and receiving media streams.

The first client receives the reply and sends a confirmation packet. After this, the media streams can be sent.

## SIP in Ingate SIParator/Firewall

### SIP Routing Order

Here, the order for SIP routing decisions is listed. Sometimes you need to know this in order to configure the unit to make it work the way you want. The unit searches for the first matching setting in the list.

1. The unit checks that the SIP method in the packet is allowed according to the settings under **SIP Methods**.
2. The unit checks that the SIP packet is allowed according to the settings under **Sender IP Filter Rules**.
3. The unit checks that the SIP packet is allowed according to the settings under **Header Filter Rules**.
4. The unit checks if the SIP packet contains a Route header which determines the next destination.
5. If VoIP Survival is enabled and active, the unit checks if the SIP packet is addressed to a user under a monitored domain.
6. The unit checks for the SIP domain of the Request-URI in the **DNS Override For SIP Requests** table.

7. The unit checks for the SIP user from the Request-URI among locally registered users and users listed in the **Static Registrations** table.
8. The unit checks if there is a matching row in the **Dial Plan** table.
9. The unit checks if the SIP packet Request-URI contains one of its **Local SIP Domains**. If so, and no match was found in the above list, the unit returns a SIP packet with error code 404 (Not Found) to the sender.

After finding something to guide it in routing the packet, the unit proceeds to the next list, which tells it where to send the packet (if it hasn't already sent a 404 reply). This list is also searched until a match is found.

1. The unit sends the SIP packet to the **Outbound Proxy** if one has been entered.
2. The unit checks for the SIP domain of the Request-URI in the **DNS Override For SIP Requests** table.
3. If there are still unresolved domain names, the unit makes an ordinary DNS lookup.

## SIP Packet Headers

This is a list of the more common SIP packet headers, and advice on how to modify them using different settings in the unit.

### Request-URI

The Request-URI (RURI) of the SIP packet can be found in the first line, right after the name of the SIP method used. The RURI tells the destination of the packet.

When the unit acts as registrar for the domain of the RURI, it rewrites the RURI from user@domain into whatever the user gave as its Contact when it registered.

When the incoming RURI is one that the unit has previously substituted in a Contact header, the RURI is also rewritten.

When an XF account is used, the domain part of the incoming RURI will be changed into the domain of the XF account.

### From

The From header contains the SIP user who sent the SIP request.

The unit only changes the From header when the built-in b2bua is used, like when an XF account is used.

### To

The To header contains the SIP user who should receive the SIP request.

The unit only changes the To header when an XF account is used.

## Contact

The Contact header tells on which address the SIP client wants to be contacted.

The unit always rewrites the Contact when a SIP request is forwarded through, if the unit NATs traffic in that direction. To prevent this rewriting, the **URI Encoding** and **Preserve Username For All Requests** settings can be used.

## Via

The Via header is used to keep track of which route the SIP request was sent. The response is sent back the same route.

The Via header is always rewritten by the unit when the SIP signaling crosses a NAT border (when the IP addresses change).

The unit can remove Via headers, when the server receiving the SIP request will not accept requests with more than one Via header. This is done using the **Remove Via Headers** setting.

## Record-Route

The Record-Route header is used to make subsequent signaling for this request to be sent via the unit.

The Record-Route header is always rewritten by the unit when the SIP signaling crosses a NAT border (when the IP addresses change).

You can force the unit to add Record-Route headers using the **Force Record-Route for Outbound Requests** and **Force Record-Route for All Requests** settings.

## Route

The Route header is used to send SIP signaling via a predefined route. All Record-Route headers added to the original SIP request will be converted into Route headers in later SIP requests within the same SIP session.

The Route header is always rewritten by the unit when the SIP signaling crosses a NAT border (when the IP addresses change).

## Content-Type

The Content-Type header is used when the SIP packet has a body. A body is used to convey information about something, like call parameters when a voice call is set up. The Content-Type header defines the body type to help the client read the content correctly.

Some content types are automatically allowed through the unit, but most types must be allowed by configuration. For this, the **Content Types** table is used.

If a SIP packet is not allowed because of the content type, this error message is shown in the log: SIP unaccepted content - deny.

# Appendix D: More About VPN

## VPN protocols

### IPsec

IPsec (Internet Protocol Security protocol) handles authentication and encryption of data packets. Authentication is the process of making sure that the message you receive really originates from the right sender, and that it hasn't been corrupted during transmission. Authentication also protects against resending of packets. Encryption is the process of distorting data so that only the desired receiver can read the message.

A thorough description of IPsec can be found in RFC 2401.

### IKE (ISAKMP)

IKE is a protocol for handling key exchanges between peers. IKE is an adaption for IPsec of the general key exchange protocol ISAKMP. Thorough descriptions of ISAKMP and IKE can be found in RFC 2408 and RFC 2409, respectively.

The key exchange has two phases; first, a secure channel for key management is created, and second, the peers exchange parameters for IPsec. The result is an SA (Security Association).

Phase one is performed in either Main Mode or Aggressive Mode. Aggressive Mode is slightly faster, but will reveal the identities of the parts involved. Main Mode requires more traffic during the connection phase, but the identities of both parts will remain concealed. Both modes generate the same level of secure encryption of the message. The unit always uses Main Mode.

## VPN interoperability

Ingate SIParator/Firewall's VPN interoperability has been tested with several of the market leading firewalls and security gateways. These tests show that Ingate VPN works with all products meeting the requirements listed below.

### General requirements

- The IETF standards IPsec and IKE must be supported.
- *Preshared keys* or *X.509 certificates* must be used as the authentication method (VPN clients must use X.509 certificates). Methods using digital signatures also exist, but are not supported by Ingate VPN.
- *Main Mode* must be supported. Ingate SIParator/Firewall does not support *Aggressive Mode*.
- The *3DES* encryption algorithm or the *AES* encryption algorithm must be supported. 3DES performs encryption with 168 bits, and some countries do not allow export of products with such a strong encryption algorithm. For AES, Ingate SIParator/Firewall supports a 128, 192 or 256 bit encryption.

- ESP must use encryption of the traffic. The ESP standard permits authentication only, but Ingate VPN will not permit this for security reasons.
- At least one of the *MD5*, *SHA-1*, *SHA2-256* or *SHA2-512* authentication algorithms must be supported. Almost all security products support these methods.
- *Tunnel mode* must be used. Transport mode is not supported.
- *PFS (Perfect Forward Secrecy)*, group 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 23 or 24 must be supported. PFS is turned off as default in some products.

## VPN connections

### Establishing a VPN connection

When establishing a VPN connection, the unit starts with negotiating a key for the encrypted connection. The negotiation is performed by sending several UDP packets from port 500 on the unit to port 500 on the remote firewall. When the negotiation is done, the encrypted VPN tunnel is established. This tunnel is used later on for connecting the different networks communicating with each other.

After that, an IPsec connection is established through the tunnel. IPsec also uses UDP packets to port 500. Now a complete encrypted VPN tunnel has been created. N.B.: VPN does not encrypt the data traffic within the local networks, only through the tunnel between the different networks.

The encrypted traffic is handled using the ESP protocol. This protocol uses the IP protocol, just as TCP and UDP do.

### VPN connections in the log

An established IKE connection may look like this:

```
>>> VPN: ISAKMP SA established: 130.236.128.2 === 147.52.114.5
```

The following IPsec connection may look like this:

```
>>> VPN: IPsec SA established: office---130.236.128.2  
=== juliet@home --- 147.52.114.5
```

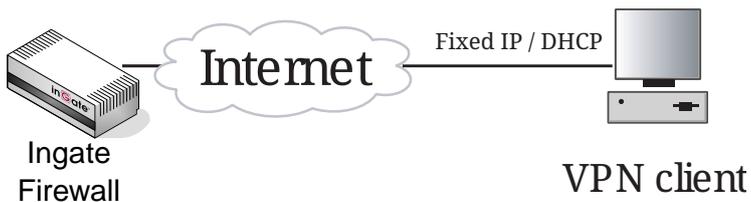
The encrypted traffic is shown as ESP packets.

## VPN clients

This is a description of various scenarios for connecting a VPN client to a VPN gateway (such as a firewall with VPN support). For each scenario you also find configuration details for the unit.

## Client with a public IP address

In this scenario, the VPN client has a public IP address, visible for the entire Internet.



### Unit configuration

The unit's VPN configuration has the following details:

#### 1. IPsec Peers

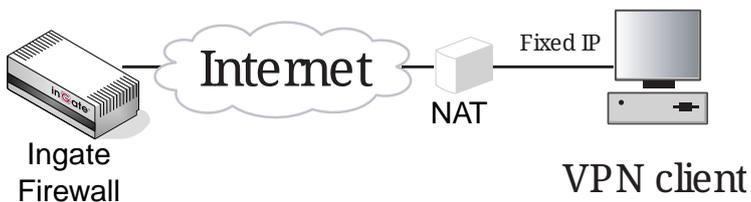
**Remote side** should be set to "\*".

#### 2. IPsec Tunnels

- **Remote network: Address type** should be set to "Remote side address".
- **Remote side: Network** should be left empty.

## Client with NAT:ed, fixed IP address

In this scenario, the VPN client is located behind a NAT device, which means that its real IP address can't be seen on the Internet. This makes it trickier for IPsec, though, since the real IP address inside the packet does not match the NAT:ed IP address which the unit sees as the sender of the packet.



### Unit configuration

The unit's VPN configuration has the following details:

#### 1. IPsec Peers

**Remote side** should be set to "\*".

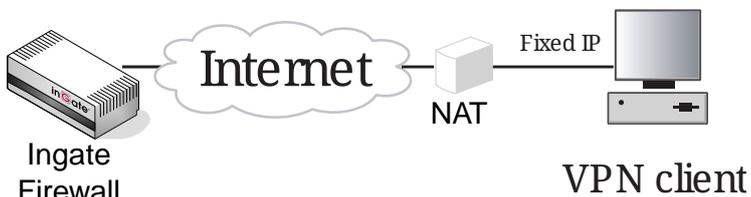
#### 2. IPsec Tunnels

- In the **IPsec Networks** table, create a new row. Enter the real client IP address (not the NAT address) and netmask 32.
- In the **IPsec Tunnels** table; select Network under **Remote network: Address type**.
- Select under **Remote network: Network** the network you just created.

## Client with NAT:ed DHCP IP address

In this scenario, the VPN client is located behind a NAT device, which means that its real IP address can't be seen on the Internet. The client acquired its IP address via DHCP.

The settings below require that the client IP address belong to one of the standardized private IP address ranges.



### Unit configuration

The unit's VPN configuration has the following details:

#### 1. IPsec Peers

**Remote side** should be set to "\*".

#### 2. IPsec Tunnels

- **Remote network: Address type** should be set to "Any private address".
- **Remote side: Network** should be left empty.

If the DHCP IP address range is not within the standardized private networks, you need to do this instead:

#### 1. IPsec Peers

**Remote side** should be set to "\*".

#### 2. IPsec Tunnels

- In the **IPsec Networks** table, create a new row. Enter the network number and netmask for the IP range from which the client obtains its DHCP IP address.
- In the **IPsec Tunnels** table; select "Network, allow subset" under **Remote network: Address type**.
- Select under **Remote network: Network** the network you just created.

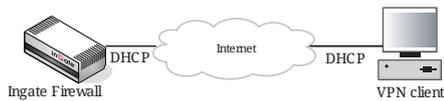
## Client with dynamic IP addresses

In this scenario, the unit as well as the VPN client have acquired their IP addresses via DHCP/PPPoE.

This is a problem, since none of the IP addresses is known in advance, which makes it difficult to define a connection point for either device.

One solution is to let the unit report its IP address to DynDNS.org, where the client can look it up. This requires settings on the **Dynamic DNS update** page under **Basic Configuration**. It also

requires that you acquire an account at DynDNS.org.



## Unit configuration

The unit's VPN configuration has the following details:

### 1. Dynamic DNS update

- **DynDNS.org status** should be set to On.
- Select which **DynDNS.org service** you use.
- Enter your DynDNS.org **Username** and **Password**
- Select the **IP address for updates**. This should be the IP address of the unit outside - the one that get its address via DHCP/PPPoE.
- Under **DNS names to update at DynDNS.org**, enter the host/domain name for the unit. This is the name which the client should use to connect to the unit.

### 2. IPsec Peers

- **Remote side** should be set to "\*".
- **IPsec Tunnels**
- **Remote network: Address type** should be set to "Any private address".
- **Remote side: Network** should be left empty.

# Appendix E: More about security

## Some of the most common types of attacks

The primary task of a firewall is to prevent illicit connections to services from an insecure network. One common attack is to try to connect to servers and use them to break into the network. By only allowing the insecure network to access the allowed services, they are blocked from accessing other services. For example, the services on ports 139 and 1035 on the internal network are to be protected from the Internet. Set up a firewall that does not allow connection to these ports, which makes sure that no one uses these services incorrectly.

The unit usually blocks everything. You set up rules and relays only for the traffic you want to receive.

### Address spoofing

One common attack is address spoofing. This means that a computer on an insecure network uses an IP number that belongs to the internal, secure network. This computer pretends to be part of the internal, secure network. Since the unit detects which interface a connection originates from, it blocks this type of attack, preventing any packets from coming in from the wrong interface.

### Denial of Service

Denial of Service, DoS, is a class of attacks that prevents or interrupts a service. SYN flooding is an example of this. Most server computers have a limited number of simultaneous connections for a given service. Starting many half-connections to a service prevents others from accessing it. The unit can prevent SYN flooding of the unit itself to a certain degree, but the usual firewall rules do not prevent SYN flooding of the computers on an internal network. For good protection even for computers on an internal network, use relays for the traffic that passes through the unit.

Another type of attack is the ‘ping of death.’ A ping is a signal to detect if a computer is up and running. The ping sends an ‘echo request’ ICMP packet and receives an ‘echo reply’ ICMP packet in response. Receiving a ping packet that is larger than the usually accepted size can make a computer crash. The unit does not fall for the ping of death. To protect computers on a network, you should not allow ICMP echo requests to pass through the unit into your internal networks, only ICMP echo replies.

Another type of attack is to send packets with incorrect out-of-bounds data to a server. This can crash a server computer that has certain broken programs. The relays in the unit will not forward out-of-bounds data, which gives some protection from some attacks, but the firewall rules do not protect against incorrect out-of-bounds data.

### Using bugs

The most common type of attack is using bugs in some server software. Always make sure that you have the latest versions of all server software that you use. Another safety measure is not to allow the entire Internet access to all servers on your internal network unless absolutely necessary. This is easy to do with the unit.

The above examples describe a few of the attacks you may fall prey to. A small list like this cannot be complete. New attacks and counter-attacks are constantly being developed. To keep abreast of developments, we recommend that you join some of the mailing lists and news groups listed in the next section.

## Security resources on the Internet

### BUGTRAQ

A mailing list about security in general and UNIX in particular. Go to <http://www.securityfocus.com/> and select Bugtraq.

### NT-BUGTRAQ

A mailing list about security in Windows NT, Windows 2000 and Windows XP. Go to <http://www.ntbugtraq.com/>.

### DARPA

In 1988, DARPA (Defense Advanced Research Projects Agency) created CERT, Computer Emergency Response Team. CERT works with computer and computer network-related security issues. For more information on CERT, see <http://www.cert.org/>.

CERT also has several mailing lists and news groups that may be of interest.

Table 48. Security resources

Name	Subject	Type	Where
unix-security	General security	M	<a href="mailto:security@cpd.com">security@cpd.com</a>
security-misc	General security	G	comp.security.misc
virus-list	Computer viruses	G	comp.virus
sgi-bugs	IRIX bugs	G	comp.sys.sgi.bugs
hpux-list	General about HP-UX	G	comp.sys.hp.hpux
solaris-list	Solaris 2.X	G	comp.unix.solaris
sun-managers	Sun managers	M	<a href="mailto:sun-managers-request@eecs.nwu.edu">sun-managers-request@eecs.nwu.edu</a>
cert-tools	New security tools	M	<a href="mailto:cert-tools-request@cert.org">cert-tools-request@cert.org</a>
cert-advisory	Recommendations from CERT	G	comp.security.announce

M means mailing list, G means news group.

## Encryption

## Encrypted data

PGP (Pretty Good Privacy) is a tool for data encryption. PGP is good to use for e-mails containing sensitive information. PGP can be downloaded from WWW and FTP at <http://www.pgpi.com/>.

An open source version of PGP is GPG (GNU Privacy Guard), which can be found at <http://www.gnupg.org/>.

## Encrypted connections

There are primarily two tools for encrypted computer connections over the Internet: Kerberos and SSH.

Kerberos uses a central server that other computers use for verification. You must specify whether or not to encrypt files in each program that uses Kerberos. For more information on Kerberos, see <http://web.mit.edu/kerberos/www/>.

SSH does not use a central server; everything occurs on the two computers that are connected. An SSH connection encrypts everything; the password and all other traffic. X-Window System and Open-windows connections can be run with an SSH connection. For more information on SSH, see <http://www.datafellows.com/products/>.

An open source version of SSH is OpenSSH, which can be found at <http://www.openssh.com/>.

You can also purchase the extension module Ingate VPN to your unit. Ingate VPN enables you to create secure encrypted connections on an insecure network. See also <http://www.ingate.com/vpn/>.

# Appendix F: Troubleshooting

Troubleshooting the unit largely consists of checking the hardware (the unit, the network connectors, ...) and checking the unit log. The log is usually an excellent tool in finding out why the unit does not do what you wanted it to do.

Below is some general advice to help you troubleshoot, almost regardless of which problem you have.

- Check that the events you look for are really logged (on the **Logging Configuration** page).
- Check that the configuration has been applied properly, either by applying it (on the **Save/Load Configuration** page) or by checking the Permanent Configuration (on the **Show Configuration** page).
- Check that you display the log you want to look for. The correct date and time (or no date or time) should be filled in, the desired log entries should be checked on the righthand side of the page, and the three boxes concerning which IP packets to show should be filled in accordingly.

## Network troubleshooting

### No traffic shown in the log

- Check that the interface is turned on on the corresponding interface page.
- Check that the unit has a correct default gateway (on the **Basic Configuration** page).
- Check that the client computer has a correct default gateway.

### Traffic discarded as spoofed

When traffic is blocked and the reason given is Spoofed, there is a mismatch between the network that the unit is configured for and the network that the client is configured for. The unit regards an IP address as spoofed if it detects traffic from that IP address on an interface where the IP address should not be.

An example of a situation where this occurs is when you move a computer from one unit interface to another without changing its IP address and netmask.

Another example is if the unit has been configured to use a network with a netmask of 255.255.255.128, but the network really is larger, like 255.255.254.0. The IP addresses outside the smaller IP interval will be regarded as spoofed by the unit.

## Firewall troubleshooting

No traffic through the unit (traffic discarded/rejected) ^^^^^^^^^^^^^^^^^^^^^ \* Check that there is a rule for this type of traffic (on the Rules page). Check that the client network contains the sender computer and that the server network contains the receiver computer, that the service contains the ports you want to use, and that the timeclass includes the time when you want the traffic let through. \* If www traffic from an inside network does not appear in the log, check if the web clients have a DNS

server, and if the unit is configured to let DNS traffic through.

## No reply traffic through the unit

- Check that rules for the reply traffic exist, if NAT or TCP services are not used.
- If NAT is not used, check that the inside network are public IP addresses. If you don't use public IP addresses, you must use NAT for traffic to the Internet.

## SIP troubleshooting

Before going into the different error descriptions below, check that the SIP module is turned on and the configuration applied.

### SIP users can't register on the unit

- Check that the SIP domain that the users try to register on is listed in the **Local SIP Domains** table.
- If you do not use RADIUS authentication, check that the SIP user which tries to register is listed in the **Local SIP User Database** table.
- If you do not use RADIUS authentication, check in the **Local SIP User Database** table that the SIP user which tries to register is allowed to register from the network where the SIP client is located. If you use RADIUS authentication, check on the **Authentication and Accounting** page that the SIP user which tries to register is allowed to register from the network where the SIP client is located.
- If local SIP authentication is used, check that the SIP user uses the correct password.

### SIP users can't register through the unit

- Check that the SIP domain that the users try to register on is not listed in the **Local SIP Domains** table.
- Check that SIP authentication is not used. If you want the unit to perform SIP authentication, make sure that the unit and the SIP registrar uses the same SIP realm.
- If the client sends the REGISTER request to the unit itself and the unit is supposed to redirect it to the registrar, check on the **Routing** page that this is configured correctly.
- Check that there are **Sender IP Filter Rules** to allow the registration through the unit. For the network from where the registration was sent (or as **Default Policy For SIP Requests**), you must select **Process all**.

### SIP Trunking (calls via SIP operator)

- If your operator requires registration, check that the unit registered successfully. A successful registration is indicated in the **Registered Users** table on the **SIP Status** page. If you find the operator user listed in that table, the registration was successful.
- If you do not get a ring tone in the calling phone, there is probably something wrong in the SIP signaling. Check the log to see that the unit can connect to the operator. Also check that the

Request-URI of the incoming INVITE request looks like you expected. For incoming calls, you might have to change your Dial Plan to match what the operator sends out, like a "+" first in the phone number. For outgoing calls, some operators require the phone number to start with a "+". Contact your operator to find out the details about the dial scheme.

## VPN troubleshooting

### No IPsec tunnel established

- Check that VPN negotiation packets (UDP port 500) reach the unit. The other end could be located behind a NATing device which changes the sender port.
- Check that packets from the other end can reach the unit and vice versa. A failure to do so could indicate a faulty routing somewhere between the two VPN units or that some blocking device is located between them.
- Check that the VPN negotiation packets to the unit are addressed to the correct IP address (the one selected on the **IPsec Peers** page).
- If preshared secrets are used, check that both units share the same secret. If certificates are used, check that the right certificates are used.
- If the unit in the other end is no Ingate SIParator/Firewall, make sure that it uses PFS (Perfect Forward Secrecy). Ingate SIParator/Firewall always uses PFS.
- If the unit in the other end is no Ingate SIParator/Firewall, make sure that it uses 3DES or AES. Ingate SIParator/Firewall accepts both encryption algorithms.
- Check that the networks to use the VPN tunnel are the same on both VPN units.

### IPsec tunnel established, no traffic

- Check that the networks, between which the traffic should be sent, are allowed to use the IPsec tunnel. They must be configured for that peer on the **IPsec Tunnels** page.
- Check that there is a rule to let this traffic through. Check that the rule uses a proper network, service, IPsec peer and time class.

### IPsec tunnel established, no traffic after some time

- Check that the key lifetime for the ISAKMP key is the same for both VPN units.
- Check that the key lifetime for the IPsec key is the same for both VPN units.

## Administration troubleshooting

This section describes problems that can arise when administrating the unit.

### The unit reverts to the old version when trying to upgrade

- Check the release note for new error checks, which will make some part of your configuration invalid with the new software version.

## The unit is inaccessible for some time when trying to apply a configuration

There is something in the new configuration that does not allow you to access the web configuration interface.

- Check the log to see if your access attempts reached the unit.
- Check that the configuration IP address (**Configuration Transport** on the **Access Control** page) is the one you use when trying to access the unit. Note that if you apply a configuration which changes the configuration IP address, your web browser will not automatically be redirected to the new IP address.
- Check that configuration traffic is allowed via the interface your web browser is located behind (**Configuration Allowed Via Interface** on the **Access Control** page).
- Check that configuration traffic is allowed from the computer where you run your web browser (**Configuration Computers** on the **Access Control** page).

## Log Messages

Here is a presentation of many common log messages that can be found in the unit log.

In many messages, information about IP addresses, usernames and other changing parameters will be displayed in the log messages. In the listing, such information will be presented contained in angle brackets. The listed log message "<Username> logged on" will mean that the real message in your log will look like "admin logged on" or "Charlie logged on", that is, the <Username> will be replaced by a username on your system.

### SIP errors

These log messages can appear when the SIP errors box has been checked on the **Display Log** page.

#### **SIP send failure -1 on socket -1 <event number>**

Something went wrong when the unit tried to send a SIP packet to another SIP device. Maybe there was no TLS connection (if TLS should be used), or the device is known not to reply, or the unit has no network connection at all on the interface facing the other device. The event number is an internal parameter to keep track of different SIP events.

#### **Destination <IP address>:<port> is known bad. Skipping.**

The SIP device on <IP address> has been blacklisted by the unit. This happens when the other SIP device has sent an ICMP type 3 packet in response to a SIP packet, or when the other SIP device has not responded at all to previous SIP signaling. For the latter event, you can avoid the blacklisting by setting the **SIP blacklist interval** on the **Sessions and Media page** to zero(0). If the interval is set to zero (0) neither blacklisting nor monitoring will be done.

#### **Parse error at <character> in message from <IP address>, at line: <SIP line>**

Something on the referred line in the SIP message does not comply with the SIP standard or is something else that the unit does not recognize as valid SIP syntax.

### **No answer from destination <IP address>:<port>**

The unit sent a SIP packet to the IP address, but it hasn't responded before the message timed out. If this was a message to a SIP domain, the unit will try next server handling this domain.

### **sipfw: SIP <response code> response from <IP address> rejected, no state**

Something in the received SIP response was unexpected. It could be a very late response to a SIP request, or a message where the topmost Via header does not indicate the unit, or something else that does not make it an invalid SIP packet in itself, but it doesn't match what has happened in the unit.

### **Starting SIP TCP server at port 5060**

This message will be shown when the SIP module is started. This can happen when you apply settings where the SIP module just has been activated, or when you boot the unit or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the unit is now ready to receive SIP signaling over TCP.

### **Starting SIP UDP server at port 5060**

This message will be shown when the SIP module is started. This can happen when you apply settings where the SIP module just has been activated, or when you boot the unit or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the unit is now ready to receive SIP signaling over UDP.

### **Stopped SIP TCP server**

This message will be shown when the SIP module is stopped. This can happen when you apply settings where the SIP module just has been deactivated, or when you boot the unit or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the unit can no longer receive SIP signaling over TCP.

### **Stopped SIP UDP server**

This message will be shown when the SIP module is stopped. This can happen when you apply settings where the SIP module just has been deactivated, or when you boot the unit or after you have pressed the **Restart the SIP module** button on the **Restart** page. It means that the unit can no longer receive SIP signaling over UDP.

## **IPsec key negotiations**

These log messages can appear when the IPsec key negotiations box has been checked on the Display Log page.

### **IPsec: "<peer name>-<tunnel number>" #<event number>: ignoring informational payload, type <payload type>**

The IPsec peer <peer name> sent a message during negotiation which the unit ignores, because it can't use it. The payload type (like IPSEC\_RESPONDER\_LIFETIME) will give you a hint about what is

the matter. The event number is a counter for how many negotiation attempts has been performed for this peer.

**IPsec: "<peer name>-<tunnel number>" <IP address> #<event number>: Issuer CRL not found**

The unit has no Certification Revocation List for the CA of the peer's certificate. This is not an error, but is perfectly normal. You only need a Certification Revocation List when you want to make some certificates invalid.

## Configuration server logins

These log messages can appear when the Configuration server logins box has been checked on the Display Log page.

**<Username> [<IP address>] (<privileges>) logged on to the configuration server using local password**

The user <Username> logged on to the web user interface. You can also see the IP address the user came from and which privileges this user has in the web interface.

**<Username> [<IP address>] (<privileges>) was logged out from the configuration server due to inactivity**

The user <Username> has not saved any configuration, changed page in the web interface or done any other changes for the last ten minutes. Next time this user tries to do anything in the web interface, he will be prompted for his password again.

## Performance Enhancements

Here is some advice regarding how to get the best performance from your unit.

### Networks and Computers

#### Entire subnets

Networks should, where possible, be constructed to be entire subnets. This means that the IP interval should also be possible to write as a network address and a netmask.

Example: If you have the network interval 192.168.0.1-192.168.0.254, it can easily be changed into 192.168.0.0-192.168.0.255, which can be written as 192.168.0.0/24, which is a network address and a corresponding netmask. Note that on the Networks and Computers page, you always write the first and last IP address of the interval. You never use netmasks.

#### Select interface

You should select an interface for the networks where possible. Otherwise, a large IP interval (like 0.0.0.0-255.255.255.255) will generate internal rules for all directly connected networks of the unit when the network is used.

## Rules

### Frequently used rules on top

The unit searches the rule table from top to bottom when trying to find a matching rule for the received traffic. This means that performance can be notably better if frequently used rules are placed on top in the table, especially for large rule tables.

# Appendix G: Regular Expressions

In this section, you will get a short introduction to regular expressions and their usage in Ingate SIParator/Firewall. More extensive information and tutorials can be found at <http://www.regular-expressions.info/>.

## Matching Characters

In regular expressions, you want to match certain characters or types of characters. There is a number of ways to denote various types.

Table 49. Regular expressions

Type	Description
.	Any character
\d	Any digit
\w	Any letter
\	Makes the next character mean exactly the character written. If you want to match any of the characters that have a special meaning, like ".", you can't just enter . in your regular expression, as this means "any character". When you enter \. instead, you make the engine match a full stop instead of any character.

If you want to match any US phone number (as dialed on a regular phone), you can use the expression `\d\d\d\d\d\d\d\d\d\d`.

Usually, a regular expression engine tries to match expressions anywhere in a string, which means that the above expression would also match the string `abc1234567890`, as this string also contains ten digits, although other characters are present, too. This might not be what you really want. To prevent this, you can add the "start of string" and "end of string" matchers, to make sure that nothing but ten-digit strings match: `^\d\d\d\d\d\d\d\d\d\d$`.

## Modifiers and Operators

If you should try to match strings with expressions where every character in the string must have its correspondent in the expressions, they will get rather long and tedious to write. Instead, you use a number of modifiers and operators to build more powerful - and usually shorter - expressions.

Table 50. Regular expressions

Type	Description
()	Grouping of characters

Type	Description
[]	One character in the set ([adef] means "one of a, d, e and f"). You can also form ranges ([ad-f] means "a or on in the range d-f" which is the same as "one of a, d, e and f").
{n}	The previous character/group n number of times
{n,}	The previous character/group at least n number of times
{n,m}	The previous character/group between n and m number of times
*	The previous character/group 0 or more times
+	The previous character/group 1 or more times
?	The previous character/group 0 or 1 times
a b	a or b

Now, you can start creating short expressions to match SIP URIs.

**.+@ingate.com** will match any user with SIP domain ingate.com.

**202[0-9]+@ingate.com** will match any Washington phone number where ingate.com was used as the SIP domain. This will, however, also match any Egypt phone number (country code 20) where the area code+local phone number is 2 followed by at least one digit.

## Using Regular Expressions

Here are some expressions that will often be of use when you use the Dial Plan regular expressions to match SIP URIs.

In the Dial Plan, "(" are used to build references as well as groups. This is not necessarily true for all regular expression engines.

### NOTE

The User part of the expression (the part before the "@" character) is matched on case, but the Domain part is not.

### Match all users on all domains

Matching all users on all domains is done with the expression **.+@.+**. This will match any URI with a username of at least one character, and a domain name of at least one character.

In most situations, though, you want to refer to a part of this expression later, which means that we write **(.+ )@(.+)** instead. The only change is the grouping of the user name and domain name within parentheses. When referring to the user part later, we use "\$1" (the content of the first pair of parentheses), and the domain part is referred to as "\$2" (the content of the second pair of parentheses).

If all calls through the unit should be rewritten as going to the same user, but at the domain

ingate.com, it would look like this:

Regular expression in **Matching Request-URI**:

```
(.+)+@.+
```

Regular expression in **Forward To**:

```
$1@ingate.com
```

# Appendix H: Format Descriptions

## Log File Format

The unit can currently export logs in three formats: WELF, comma separated and tab separated. The WELF format is documented at <http://www.webtrends.com/>.

The comma separated and tab separated formats are basically the same. Only the separator character differs.

This document specifies the export formats used by version 4.6.1. It is expected that future versions of Ingate products will log new types of events. The new events will be given a new event code.

Ingate Systems AB will try to avoid changing the format of logged events, but we may do so, e.g. to allow more information to be logged. If that happens, the new format of the event will be given a new event code, so that log parsing utilities can distinguish between the old and the new log format.

## Log File Structure

Most events in the log are stored as a single line of text (exceptions for events that are logged using the TXT- format). Each line is terminated by a single linefeed (0x0A). The charset is UTF-8.

Each event contains several fields, separated by the separator (tab (0x09) or comma (",", 0x2C)). The first field is an event code that determines the type of the event, such as "an IP packet was received" or "the clock was set by the operator". All event codes are documented below, together with information about the fields that accompanies them.

The backslash character ("\", 0x5C) is used to quote the separator if it occurs inside a field. It is also used to quote a backslash.

The following example illustrates the syntax of the log files when comma is used as the separator:

```
DEMO,2000-03-03 18:13:27,Testing\, testing,y\x
```

This event is logged with four fields:

DEMO is the event code.

- 2000-03-03 18:13:29 is the second field. Most events store the time in the second field, but see CLKSET for an exception.
- The third field has the value Testing, testing. Note the embedded comma.
- The fourth and final field has the value y\x. Note that the backslash is quoted.

The fields can contain control characters.

## The IP Event Type

The IP event type is used for logged IP packets. Below is a list of the fields of this type.

Table 51. IP Event Types

Field	Description
Event code	The code field is set to IP.
Time	The timestamp for this event (see below).
Protocol	The IP protocol. This can be one of the strings TCP, UDP, ICMP, IGMP, IPIP, GRE , ESP, AH, SKIP, or a decimal number.
From Iface	The name of the source interface, such as eth0 or ipsec1. If empty, the source of the IP packet was the unit itself.
From IP Address	The source IP address, such as 10.0.3.4.
From Port	The source port number, such as 53. Only used for TCP and UDP packets; blank otherwise.
To Iface	The name of the destination interface, such as eth0 or ipsec1. The interface can be empty.
To IP Address	The destination IP address, such as 10.0.3.4.
To Port	The destination port number, such as 53. Only used for TCP and UDP packets; blank otherwise.
Type	The ICMP type field, such as 8. Only used for ICMP and IGMP packets; blank otherwise.
Code	The ICMP code field, such as 0. Only used for ICMP and IGMP packets; blank otherwise.

Field	Description
Flags	<p>The TCP flags, as a string. This string consists of one character for each TCP flag that is set:</p> <ul style="list-style-type: none"> <li>• S SYN Request for connection</li> <li>• A ACK Response to a previous packet</li> <li>• U URG Contains out-of-band data</li> <li>• P PUSH Packets that must be delivered quickly</li> <li>• F FIN Disconnect request</li> <li>• R RST Reset - response to incorrect packet</li> </ul> <p><i>If no flags were set, or if the packet was not a TCP packet, the field is blank.</i></p>
Decision	<p>The action that was taken for this packet. The content of this field is language-dependent.</p> <ul style="list-style-type: none"> <li>• Blacklisted (discarded)</li> <li>• Discarded</li> <li>• Blacklisted (rejected)</li> <li>• Rejected</li> <li>• Accepted</li> <li>• NAT</li> <li>• DNAT</li> </ul> <p><i>More actions may be added in the future.</i></p>

Field	Description
Reason	<p>The reason for this action. The content of this field is language-dependent.</p> <ul style="list-style-type: none"> <li>• Rule x</li> <li>• Relay</li> <li>• IP policy</li> <li>• SIP signaling</li> <li>• Broadcast</li> <li>• IPsec</li> <li>• Ping policy</li> <li>• Config server</li> <li>• Local ICMP</li> <li>• SNMP</li> <li>• DNS</li> <li>• NTP</li> </ul>
Text message	There may be an additional text message in some rare cases.

## The VPN Event Type

When the status of a VPN tunnel changes, a message of this type is logged.

*Table 52. VPN Event Types*

Field	Description
Event code	The code field is set to VPN.
Time	The timestamp for this event (see below).

Field	Description
Event type	<p>The event type. The content of this field is language-dependent.</p> <ul style="list-style-type: none"> <li>• ISAKMP SA established</li> <li>• ISAKMP SA replaced</li> <li>• ISAKMP SA deleted</li> <li>• ISAKMP SA expired</li> <li>• ISAKMP SA failed</li> <li>• Timeout (re)establishing ISAKMP SA</li> <li>• Peer unknown</li> <li>• IPsec SA established</li> <li>• IPsec SA replaced</li> <li>• IPsec SA deleted</li> <li>• IPsec SA expired</li> <li>• IPsec SA failed</li> <li>• Timeout (re)establishing IPsec SA</li> <li>• Unknown connection</li> </ul> <p><i>More event types may be added in the future.</i></p>
Local security gateway	The IP address of the local security gateway (that is, one of the IP addresses of the unit that generates this log).
Local identity	This may be an IP address or a string, depending on how the tunnel is configured.
Local network	The local network that is tunneled through this IPsec connection, as a network address and a netmask. Example: 10.41.0.0/16. This field is blank for ISAKMP SA events.
Remote security gateway	The IP address of the remote security gateway.
Remote identity	The remote identity, if known.
Remote network	The remote network that is tunneled through this IPsec connection, as a network address and a netmask. Example: 10.41.0.0/16. This field is blank for ISAKMP SA events.

## The TXT Event Type

The TXT event is a catch-all for various events that log a text message.

*Table 53. TXT Event Types*

<b>Field</b>	<b>Description</b>
Event code	The code field is set to TXT.
Time	The timestamp for this event (see below).

Field	Description
Category	<p>The category is a string that categorizes the message. The current categories are:</p> <ul style="list-style-type: none"> <li>• <b>CFG/AUTH</b> Messages regarding authentication of accesses to the configuration server.</li> <li>• <b>CFG/MGMT</b> Messages regarding configuration changes.</li> <li>• <b>DHCP/CLIENT</b> Messages about leases from the built-in DHCP client.</li> <li>• <b>HARDWARE/FAILOVER</b> Messages regarding failover activities (unit switching, contact established or lost with other unit).</li> <li>• <b>HARDWARE/FIRMWARE</b> Messages regarding firmware errors.</li> <li>• <b>HARDWARE/LOGDISK</b> Messages regarding the log disk (only for units with a hard drive).</li> <li>• <b>HARDWARE/PSU</b> Messages regarding the power supply.</li> <li>• <b>IDSIPS/RULES</b> Messages regarding SIP IDS/IPS.</li> <li>• <b>MAIL/ALERT</b> Messages regarding mail delivery problems.</li> <li>• <b>PPPOE/CLIENT</b> Messages regarding the built-in PPPoE client.</li> <li>• <b>RADIUS/ERROR</b> Messages regarding problems with RADIUS servers, such as no or broken responses (but not broken passwords or wrong Service-Type attribute).</li> <li>• <b>SIP/ERRORS</b> Error messages regarding the SIP functions.</li> <li>• <b>SIP/LICENSE</b> Messages regarding SIP license usage.</li> <li>• <b>SIP/MEDIA</b> Messages regarding SIP media streams</li> <li>• <b>SIP/MESSAGE</b> SIP messages (the entire contents).</li> <li>• <b>SIP/SIGNALING</b> The first line of a SIP message or the first packet of a media stream.</li> <li>• <b>SIP/VERBOSE</b> Messages regarding the SIP</li> </ul>

Field	Description
Facility	The syslog facility. This is only useful for some categories.
Priority	The syslog priority of the message.
Progname	The name of the program that logged this message. <ul style="list-style-type: none"> <li>• fuego_run</li> <li>• IPsec</li> <li>• net-snmp</li> <li>• sipfw</li> </ul>
Message	The message itself.

a road warrior VPN user authenticates himself (currently with the aid of a RADIUS server).

## The TXT- Event Type

The TXT- event is an extension to the TXT event type. TXT- indicates that the next line is part of the same log message as the current one. In all other respects, it is the same as the TXT event type.

*More categories may be added in the future.*

## The CLKSET Event Type

The CLKSET event is generated when the time is changed.

Table 54. CLKSET Event Types

Field	Description
Event code	The code field is set to CLKSET.
Old timestamp	The timestamp before the clock change.
New timestamp	The timestamp after the clock change.

## The CFGSET Event Type

The CFGSET event is generated when something happens to the permanent configuration, i.e. when a configuration is applied and when the unit is rebooted.

Table 55. CFGSET Event Types

Field	Description
Event code	The code field is set to CFGSET.

Field	Description
Time	The timestamp for this event (see below).
Reason	<p>The reason for this configuration change. The content of this field is language -dependent.</p> <ul style="list-style-type: none"> <li>• Restart</li> <li>• Effectuate (trialrun)</li> <li>• Effectuate (finalize)</li> <li>• Effectuate (timecontrol)</li> <li>• Effectuate (cancellation)</li> <li>• Effectuate (reload)</li> <li>• Effectuate (VPN update)</li> <li>• Effectuate (activate)</li> <li>• Effectuate (standby)</li> </ul> <p><i>More reasons may be added in the future.</i></p>

## Time Format

All timestamps are logged in a common format: YYYY-mm-dd HH:MM:SS.ttt.

Table 56. Time Format

Field	Description
YYYY	The year, with four digits.
mm	The month, with two digits. January is 01, and December is 12.
dd	The day of the month, with two digits. 01-31.
HH	The hour, with two digits. 00-23.
MM	The minute, with two digits. 00-59.
SS	The seconds, with two digits. Normally 00-59, but leap seconds may extend the range to 00-60.
ttt	The thousandths of a seconds, with three digits.

Example: one minute past 3 PM, December 24, 1997 would be logged as 1997-12-24 15:01:00.000.

# Ingate RADIUS Accounting

The unit supports RADIUS Accounting as described in RFC 2866.

RADIUS Accounting adds the ability to deliver accounting information about SIP calls from a unit to a RADIUS Accounting server.

RADIUS Accounting is enabled or disabled by a GUI setting. The configuration of RADIUS servers is shared with RADIUS authentication. This means that accounting and authentication uses the same list of servers, and that there is no way to use a specific server for only one or the other of the services. RADIUS Accounting always uses port 1813.

## Accounting attributes used by the unit

Table 57. Radius attributes

Attribute	No.	Format of value or text	Sample
User-name	1	String of UTF-8 characters	sip:alice@ingate.com
NAS-IP-Address	4	Four octet IP address	193.45.23.245
NAS-Identifier	32	One or more octets	
Acct-Session-Id	44	String of UTF-8 characters	ea1bba66464748908df9f7
Acct-Status-Type	40	Four octets (32 bit unsigned value) - Integer	2
Called-Station-Id	30	String of UTF-8 characters	sip:bob@ingate.com 10.17.244.14
Calling-Station-Id	31	String of UTF-8 characters	sip:alice@ingate.com 193.45.23.1
Acct-Session-Time	46	Four octets (32 bit unsigned value) - Integer	180
Acct-Terminate-Cause	49	Four octets (32 bit unsigned value) - Integer	1
Acct-Input-Octets	42	Four octets (32 bit unsigned value) - Integer	1800000 (number of octets to the calling endpoint, including the IP-header)

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
Acct-Output-Octets	43	Four octets (32 bit unsigned value) - Integer	1800000 (number of octets from the calling endpoint)
Acct-Input-Packets	47	Four octets (32 bit unsigned value) - Integer	9000 (number of packets to the calling endpoint)
Acct-Output-Packets	48	Four octets (32 bit unsigned value) - Integer	9000 (number of packets from the calling endpoint)
IG-Acct-Input-Jitter	128	Four octets (32 bit unsigned value) - Integer	1 (average jitter in msec)
IG-Acct-Output-Jitter	129	Four octets (32 bit unsigned value) - Integer	1
IG-Acct-Input-Missing	130	Four octets (32 bit unsigned value) - Integer	1 (total number of missing packets)
IG-Acct-Output-Missing	131	Four octets (32 bit unsigned value) - Integer	1
IG-Acct-Input-Missing-Max	132	Four octets (32 bit unsigned value) - Integer	1 (max. number of consecutive missing packets)
IG-Acct-Output-Missing-Max	133	Four octets (32 bit unsigned value) - Integer	1
IG-Acct-Output-Missing-Max	133	Four octets (32 bit unsigned value) - Integer	1
IG-Acct-Input-Est-Mos	134	Four octets (32 bit unsigned value, should be divided by 100)	440 (this means Mean Opinion Score = 4.40)
IG-Acct-Output-Est-Mos	135	Four octets (32 bit unsigned value, should be divided by 100)	393
IG-Acct-Input-Last-Payload-Type	136	Four octets (32 bit unsigned value) - Integer	0 (value of field .payload-type. in last seen RTP packet)

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
IG-Acct-Output-Last-Payload-Type	137	Four octets (32 bit unsigned value) - Integer	0
IG-Acct-Input-Reordered	138	Four octets (32 bit unsigned value) - Integer	3 (number of reordered packets)
IG-Acct-Output-Reordered	139	Four octets (32 bit unsigned value) - Integer	1
IG-Acct-Input-Comfort-Noise	140	String of UTF-8 characters	Yes (if there was any comfort noise packet with payload-type 13)
IG-Acct-Output-Comfort-Noise	141	String of UTF-8 characters	No
IG-Acct-Input-Codec-Name	142	String of UTF-8 characters	PCMU (codec name as present in SIP SDP; if sample rate is other than 8000, then this is also shown (e.g. .BV32/16000.))
IG-Acct-Output-Codec-Name	143	String of UTF-8 characters	PCMU
IG-Acct-Input-Jitter-Max	144	Four octets (32 bit unsigned value) - Integer	9 (max. jitter in msec)
IG-Acct-Output-Jitter-Max	145	Four octets (32 bit unsigned value) - Integer	3
IG-Acct-Remote-Party-Id	146	String of UTF-8 characters	"User" <sip:1989@example.com>
IG-Acct-P-Asserted-Identity	147	String of UTF-8 characters	<sip:1989>
IG-Acct-Diversion	148	String of UTF-8 characters	<sip:+123456789>
IG-Acct-Input-Jitter-Avg-Rtcp	149	String of UTF-8 characters	5.11 (average jitter . as reported from the endpoint via RTCP - in msec)

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
IG-Acct-Input-Jitter-Max-Rtcp	150	String of UTF-8 characters	10.11 (max. jitter . as reported from the endpoint via RTCP - in msec)
IG-Acct-Input-Missing-Rtcp	151	(32bit unsigned value)-Integer	43 (total number of missing packets, as reported from the endpoint via RTCP)
IG-Acct-Output-Jitter-Avg-Rtcp	152	String of UTF-8 characters	6.11
IG-Acct-Output-Jitter-Max-Rtcp	153	String of UTF-8 characters	10.11
IG-Acct-Input-Missing-Rtcp	154	(32bit unsigned value)-Integer	78
IG-Acct-Rtd-Avg-Rtcp	155	String of UTF-8 characters	39.6 (total round trip delay . calculated based on RTCP monitoring . in msec; obsolete, replaced by No. 156 and 157 below)
IG-Acct-Rtd-Avg-RtcpIn	156	String of UTF-8 characters	1.7 (round trip delay between Ingate and calling endpoint . calculated based on RTCP monitoring . in msec)
IG-Acct-Rtd-Avg-RtcpOut	157	String of UTF-8 characters	37.9 (round trip delay between Ingate and called endpoint . calculated based on RTCP monitoring . in msec)
IG-Acct-Input-DscpIn	158	Four octets (32 bit unsigned value) - Integer	16 (a value between 0 and 63, from the 6 DSCP bits in the IP header of the packets as they enter the Ingate box)

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
IG-Acct-Input-DscpOut	159	Four octets (32 bit unsigned value) - Integer	16 (a value between 0 and 63, from the 6 DSCP bits in the IP header of the packets as they leave the Ingate box)
IG-Acct-Output-DscpIn	160	Four octets (32 bit unsigned value) - Integer	16
IG-Acct-Output-DscpOut	161	Four octets (32 bit unsigned value) - Integer	16
IG-Acct-Input-IfIpIn	162	String of UTF-8 characters	192.168.4.13 (the IP adress of the interface on which the packets for this direction are entering the Ingate box)
IG-Acct-Input-IfIpOut	163	String of UTF-8 characters	211.111.111.111 (the IP adress of the interface on which the packets for this direction are leaving the Ingate box)
IG-Acct-Output-IfIpIn	164	String of UTF-8 characters	211.111.111.111
IG-Acct-Output-IfIpOut	165	String of UTF-8 characters	192.168.4.13
IG-Acct-Input-Mtype	166	String of UTF-8 characters	audio RTP/AVP (the media-type and -protocol, as in the SIP SDP)
IG-Acct-Output-Mtype	167	String of UTF-8 characters	audio RTP/AVP
IG-Acct-Video-Input-Octets	176	Four octets (32 bit unsigned value) - Integer	220000
IG-Acct-Video-Output-Octets	177	Four octets (32 bit unsigned value) - Integer	220000

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
IG-Acct-Video-Input-Packets	178	Four octets (32 bit unsigned value) - Integer	236
IG-Acct-Video-Output-Packets	179	Four octets (32 bit unsigned value) - Integer	236
IG-Acct-Video-Input-Jitter	180	Four octets (32 bit unsigned value) - Integer	0.9
IG-Acct-Video-Output-Jitter	181	Four octets (32 bit unsigned value) - Integer	2.1
IG-Acct-Video-Input-Jitter-Max	182	Four octets (32 bit unsigned value) - Integer	1.3
IG-Acct-Video-Output-Jitter-Max	183	Four octets (32 bit unsigned value) - Integer	3.6
IG-Acct-Video-Input-Missing	184	Four octets (32 bit unsigned value) - Integer	0
IG-Acct-Video-Output-Missing	185	Four octets (32 bit unsigned value) - Integer	4
IG-Acct-Video-Input-Missing-Max	186	Four octets (32 bit unsigned value) - Integer	0
IG-Acct-Video-Output-Missing-Max	187	Four octets (32 bit unsigned value) - Integer	2
IG-Acct-Video-Input-Last-Payload-Type	190	Four octets (32 bit unsigned value) - Integer	124
IG-Acct-Video-Output-Last-Payload-Type	191	Four octets (32 bit unsigned value) - Integer	124
IG-Acct-Video-Input-Reordered	192	Four octets (32 bit unsigned value) - Integer	0
IG-Acct-Video-Output-Reordered	193	Four octets (32 bit unsigned value) - Integer	1
IG-Acct-Video-Input-Codec-Name	194	String of UTF-8 characters	H264/90000

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
IG-Acct-Video-Output-Codec-Name	195	String of UTF-8 characters	H264/90000
IG-Acct-Video-Input-Jitter-Avg-Rtcp	196	String of UTF-8 characters	1.4
IG-Acct-Video-Input-Jitter-Max-Rtcp	197	String of UTF-8 characters	6.6
IG-Acct-Video-Input-Missing-Rtcp	198	Four octets (32 bit unsigned value) - Integer	0
IG-Acct-Video-Output-Jitter-Avg-Rtcp	199	String of UTF-8 characters	2.5
IG-Acct-Video-Output-Jitter-Max-Rtcp	200	String of UTF-8 characters	9.3
IG-Acct-Video-Output-Missing-Rtcp	201	Four octets (32 bit unsigned value) - Integer	6
IG-Acct-Video-Rtd-Avg-RtcpIn	202	String of UTF-8 characters	0.9 (in msec)
IG-Acct-Video-Rtd-Avg-RtcpOut	203	String of UTF-8 characters	5.4 (in msec)
IG-Acct-Video-Input-DscpIn	204	Four octets (32 bit unsigned value) - Integer	40
IG-Acct-Video-Input-DscpOut	205	Four octets (32 bit unsigned value) - Integer	40
IG-Acct-Video-Output-DscpIn	206	Four octets (32 bit unsigned value) - Integer	40
IG-Acct-Video-Output-DscpOut	207	Four octets (32 bit unsigned value) - Integer	40
IG-Acct-Video-Input-IfIpIn	208	String of UTF-8 characters	192.168.4.13
IG-Acct-Video-Input-IfIpOut	209	String of UTF-8 characters	211.111.111.111
IG-Acct-Video-Output-IfIpIn	210	String of UTF-8 characters	211.111.111.111
IG-Acct-Video-Output-IfIpOut	211	String of UTF-8 characters	192.168.4.13
IG-Acct-Video-Input-Mtype	212	String of UTF-8 characters	video RTP/AVP

<b>Attribute</b>	<b>No.</b>	<b>Format of value or text</b>	<b>Sample</b>
IG-Acct-Video-Output-Mtype	213	String of UTF-8 characters	video RTP/AVP
IG-Acct-Other-Input-Octets	224	Four octets (32 bit unsigned value) - Integer	2203
IG-Acct-Other-Output-Octets	225	Four octets (32 bit unsigned value) - Integer	45004
IG-Acct-Other-Input-Packets	226	Four octets (32 bit unsigned value) - Integer	40
IG-Acct-Other-Output-Packets	227	Four octets (32 bit unsigned value) - Integer	623
IG-Acct-Other-Input-DscpIn	228	Four octets (32 bit unsigned value) - Integer	24
IG-Acct-Other-Input-DscpOut	229	Four octets (32 bit unsigned value) - Integer	24
IG-Acct-Other-Output-DscpIn	230	Four octets (32 bit unsigned value) - Integer	24
IG-Acct-Other-Output-DscpOut	231	Four octets (32 bit unsigned value) - Integer	24
IG-Acct-Other-Input-IfIpIn	232	String of UTF-8 characters	192.168.4.13
IG-Acct-Other-Input-IfIpOut	233	String of UTF-8 characters	211.111.111.111
IG-Acct-Other-Output-IfIpIn	234	String of UTF-8 characters	211.111.111.111
IG-Acct-Other-Output-IfIpOut	235	String of UTF-8 characters	192.168.4.13
IG-Acct-Other-Input-Mtype	236	String of UTF-8 characters	image udptl (this is what you get for fax over T.38 connections)
IG-Acct-Other-Output-Mtype	237	String of UTF-8 characters	image udptl

The attributes follow RFC 2865 and RFC 2866, where more information can be found.

The Acct-Session-Time and Acct-Terminate-Cause are sent when the Acct-Status-Type is "Stop".

## RADIUS dictionary file with Ingate content example

```
#
# dictionary.ingate
#
#           Ingate Systems AB
#           "Marcus Sundberg" <marcus@ingate.com>
#
# Version:   $Id: dictionary.ingate,v 1.8 2009/10/15 12:32:58 erik Exp $
#

VENDOR      Ingate          13465
BEGIN-VENDOR Ingate

ATTRIBUTE   IG-Admin-Account 1 integer

#
# Type of administrator account.
#
VALUE       IG-Admin-Account Full-Access-Admin 1
VALUE       IG-Admin-Account Backup-Admin        2
VALUE       IG-Admin-Account Read-Only-Admin    3
VALUE       IG-Admin-Account VPN-Admin              4
VALUE       IG-Admin-Account SIP-Admin                  5
VALUE       IG-Admin-Account VPN-Reneg-Admin           6

#
# Accounting attributes.
#
ATTRIBUTE   IG-Acct-Input-Jitter 128 integer #start of
media stats for audio
ATTRIBUTE   IG-Acct-Output-Jitter 129 integer
ATTRIBUTE   IG-Acct-Input-Missing 130 integer
ATTRIBUTE   IG-Acct-Output-Missing 131 integer
ATTRIBUTE   IG-Acct-Input-Missing-Max 132 integer
ATTRIBUTE   IG-Acct-Output-Missing-Max 133 integer
ATTRIBUTE   IG-Acct-Input-Est-Mos 134 integer
ATTRIBUTE   IG-Acct-Output-Est-Mos 135 integer
ATTRIBUTE   IG-Acct-Input-Last-Payload-Type 136 integer
ATTRIBUTE   IG-Acct-Output-Last-Payload-Type 137 integer
ATTRIBUTE   IG-Acct-Input-Reordered 138 integer
ATTRIBUTE   IG-Acct-Output-Reordered 139 integer
ATTRIBUTE   IG-Acct-Input-Comfort-Noise 140 string
ATTRIBUTE   IG-Acct-Output-Comfort-Noise 141 string
ATTRIBUTE   IG-Acct-Input-Codec-Name 142 string
ATTRIBUTE   IG-Acct-Output-Codec-Name 143 string
ATTRIBUTE   IG-Acct-Input-Jitter-Max 144 integer
ATTRIBUTE   IG-Acct-Output-Jitter-Max 145 integer
ATTRIBUTE   IG-Acct-Remote-Party-Id 146 string
ATTRIBUTE   IG-Acct-P-Asserted-Identity 147 string
```

ATTRIBUTE	IG-Acct-Diversion	148	string
ATTRIBUTE	IG-Acct-Input-Jitter-Avg-Rtcp	149	string
ATTRIBUTE	IG-Acct-Input-Jitter-Max-Rtcp	150	string
ATTRIBUTE	IG-Acct-Input-Missing-Rtcp	151	integer
ATTRIBUTE	IG-Acct-Output-Jitter-Avg-Rtcp	152	string
ATTRIBUTE	IG-Acct-Output-Jitter-Max-Rtcp	153	string
ATTRIBUTE	IG-Acct-Output-Missing-Rtcp	154	integer
ATTRIBUTE	IG-Acct-Rtd-Avg-Rtcp	155	string #obsolete, replaced by 156 and 157
ATTRIBUTE	IG-Acct-Rtd-Avg-RtcpIn	156	string
ATTRIBUTE	IG-Acct-Rtd-Avg-RtcpOut	157	string
ATTRIBUTE	IG-Acct-Input-DscpIn	158	integer
ATTRIBUTE	IG-Acct-Input-DscpOut	159	integer
ATTRIBUTE	IG-Acct-Output-DscpIn	160	integer
ATTRIBUTE	IG-Acct-Output-DscpOut	161	integer
ATTRIBUTE	IG-Acct-Input-IfIpIn	162	string
ATTRIBUTE	IG-Acct-Input-IfIpOut	163	string
ATTRIBUTE	IG-Acct-Output-IfIpIn	164	string
ATTRIBUTE	IG-Acct-Output-IfIpOut	165	string
ATTRIBUTE	IG-Acct-Input-Mtype	166	string
ATTRIBUTE	IG-Acct-Output-Mtype	167	string
ATTRIBUTE	IG-Acct-Video-Input-Octets media stats for video	176	integer #start of
ATTRIBUTE	IG-Acct-Video-Output-Octets	177	integer
ATTRIBUTE	IG-Acct-Video-Input-Packets	178	integer
ATTRIBUTE	IG-Acct-Video-Output-Packets	179	integer
ATTRIBUTE	IG-Acct-Video-Input-Jitter	180	integer
ATTRIBUTE	IG-Acct-Video-Output-Jitter	181	integer
ATTRIBUTE	IG-Acct-Video-Input-Jitter-Max	182	integer
ATTRIBUTE	IG-Acct-Video-Output-Jitter-Max	183	integer
ATTRIBUTE	IG-Acct-Video-Input-Missing	184	integer
ATTRIBUTE	IG-Acct-Video-Output-Missing	185	integer
ATTRIBUTE	IG-Acct-Video-Input-Missing-Max	186	integer
ATTRIBUTE	IG-Acct-Video-Output-Missing-Max	187	integer
ATTRIBUTE	IG-Acct-Video-Input-Est-Mos	188	integer #not yet used
ATTRIBUTE	IG-Acct-Video-Output-Est-Mos	189	integer #not yet used
ATTRIBUTE	IG-Acct-Video-Input-Last-Payload-Type	190	integer
ATTRIBUTE	IG-Acct-Video-Output-Last-Payload-Type	191	integer
ATTRIBUTE	IG-Acct-Video-Input-Reordered	192	integer
ATTRIBUTE	IG-Acct-Video-Output-Reordered	193	integer
ATTRIBUTE	IG-Acct-Video-Input-Codec-Name	194	string
ATTRIBUTE	IG-Acct-Video-Output-Codec-Name	195	string
ATTRIBUTE	IG-Acct-Video-Input-Jitter-Avg-Rtcp	196	string
ATTRIBUTE	IG-Acct-Video-Input-Jitter-Max-Rtcp	197	string
ATTRIBUTE	IG-Acct-Video-Input-Missing-Rtcp	198	integer
ATTRIBUTE	IG-Acct-Video-Output-Jitter-Avg-Rtcp	199	string
ATTRIBUTE	IG-Acct-Video-Output-Jitter-Max-Rtcp	200	string
ATTRIBUTE	IG-Acct-Video-Output-Missing-Rtcp	201	integer
ATTRIBUTE	IG-Acct-Video-Rtd-Avg-RtcpIn	202	string
ATTRIBUTE	IG-Acct-Video-Rtd-Avg-RtcpOut	203	string

ATTRIBUTE	IG-Acct-Video-Input-DscpIn	204	integer
ATTRIBUTE	IG-Acct-Video-Input-DscpOut	205	integer
ATTRIBUTE	IG-Acct-Video-Output-DscpIn	206	integer
ATTRIBUTE	IG-Acct-Video-Output-DscpOut	207	integer
ATTRIBUTE	IG-Acct-Video-Input-IfIpIn	208	string
ATTRIBUTE	IG-Acct-Video-Input-IfIpOut	209	string
ATTRIBUTE	IG-Acct-Video-Output-IfIpIn	210	string
ATTRIBUTE	IG-Acct-Video-Output-IfIpOut	211	string
ATTRIBUTE	IG-Acct-Video-Input-Mtype	212	string
ATTRIBUTE	IG-Acct-Video-Output-Mtype	213	string
ATTRIBUTE	IG-Acct-Other-Input-Octets	224	integer #start of
	media stats for other apps		
ATTRIBUTE	IG-Acct-Other-Output-Octets	225	integer
ATTRIBUTE	IG-Acct-Other-Input-Packets	226	integer
ATTRIBUTE	IG-Acct-Other-Output-Packets	227	integer
ATTRIBUTE	IG-Acct-Other-Input-DscpIn	228	integer
ATTRIBUTE	IG-Acct-Other-Input-DscpOut	229	integer
ATTRIBUTE	IG-Acct-Other-Output-DscpIn	230	integer
ATTRIBUTE	IG-Acct-Other-Output-DscpOut	231	integer
ATTRIBUTE	IG-Acct-Other-Input-IfIpIn	232	string
ATTRIBUTE	IG-Acct-Other-Input-IfIpOut	233	string
ATTRIBUTE	IG-Acct-Other-Output-IfIpIn	234	string
ATTRIBUTE	IG-Acct-Other-Output-IfIpOut	235	string
ATTRIBUTE	IG-Acct-Other-Input-Mtype	236	string
ATTRIBUTE	IG-Acct-Other-Output-Mtype	237	string
END-VENDOR	Ingate		

## When Accounting Data is Generated

The unit generates accounting information when accounting is enabled in the configuration and at least one of the following conditions is true:

- Media is handled by the unit, i.e. every case when the media traverses through the unit, or when Remote SIP Connectivity is used for the specific call.
- The unit acts as a B2BUA. This requires that the SIP Trunking or the Advanced SIP Routing module is installed, and that at least one of the criteria below is met:
  - An XF or B2BUAWM account is used for the specific call.
  - Regular Expressions are used in the **Matching Request-URI** and **Forward To** tables, and the Regular Expression in the **Forward To** table ends with a ";b2bua".
  - **Local REFER Handling** is used for the call.
- **Force Record-Route for All Requests** is used.

To test RADIUS Accounting with the unit, [FreeRADIUS](#) or any commercial RADIUS server supporting RFC 2866 can be used.

# Appendix I: Definitions of terms

## *AFS, Andrew File System*

AFS is a more secure way of distributing file systems over a network. If files are mounted over the Internet, AFS is fairly secure. Normally, AFS uses Kerberos for security management.

## *ARP*

ARP, Address Resolution Protocol, is a protocol for mapping an IP address to a physical machine address in the local network. A thorough description of ARP can be found in RFC 826.

## *Broadcast*

Broadcast is a method of sending packets when you don't know the actual recipient. The packets are sent to all computers on the network.

Each network has a network address (the first address of the IP interval) and a broadcast address (the last address of the IP interval). On the network 192.168.0.0/24 (192.168.0.0-192.168.0.255), 192.168.0.255 is the broadcast address. When a computer wants to address all computers on the network, like when a Windows computer wants to map the resources, it sends a request to the broadcast address. All computers on the network receive this request and decides if they should reply.

## *Client program*

A client program is one that the user runs on her computer. A client program connects to a server. One example of a client program is Mozilla (a web browser). One benefit of dividing up a service into server and client programs is that the server program can be run on a larger computer with better resources, and the users do not have to make their own copies of the databases. This allows the client programs to be run on less powerful computers.

## *Cracker*

A person who breaks into computer systems and commits other criminal acts using a computer.

## *Daemon program*

A daemon program is a server program for a service. This kind of program waits for and manages external calls. A typical example is FTP. A user starts his FTP client. The client connects to the FTP server. Now the user can transfer files to his own computer or to the server. See Server.

## *Denial of Service, DoS*

A type of attack that tries to block a network service by overloading the server.

## *DHCP*

DHCP, Dynamic Host Configuration Protocol, is a protocol for handing out IP addresses and other configuration information to computers without having to log on to every single machine. Instead, the computers themselves send out requests about this information at boot, and gets appropriate configuration parameters from a DHCP server. A thorough description of DHCP can be found in RFC 2131.

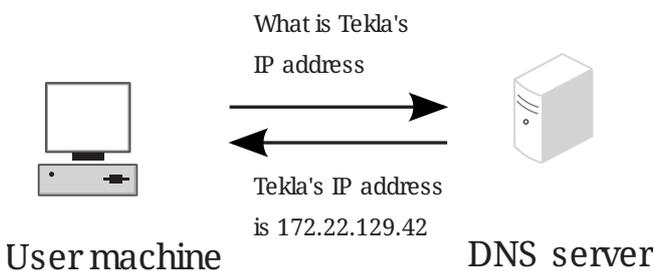
## DMZ

A DMZ is a computer network that is accessible from several other computer networks that have no direct contact with each other. Often, one of these networks is the Internet and the other is a local, internal network. There is no direct connection between the Internet and the local network, but both of them can access an intermediate network, a demilitarized zone.

DMZs are often used for special servers, such as web servers, which must be accessible from two separate networks.

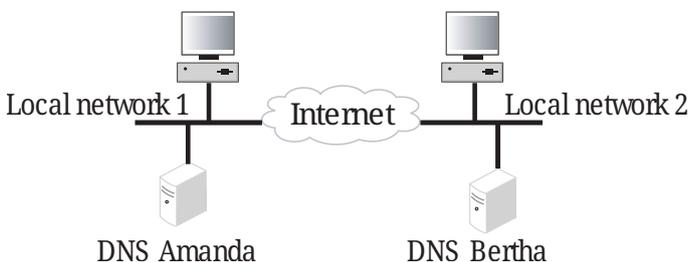
## DNS, Domain Name System

A DNS server is the Internet equivalent of dialing telephone information. If you know the name of a computer, you can access its IP address and vice versa. The server keeps track of names and IP addresses. Imagine that a user wants to connect to the computer "Tekla" through a Telnet (terminal) connection. The Telnet program asks the DNS server about Tekla and receives Tekla's IP address. If the DNS server does not know a name, it asks its nearest DNS server. See the figure.



DNS servers are usually named primary, secondary, or other. If you have several networks with several DNS servers, they can communicate with each other. It is a good idea to make them secondary DNS servers to each other. Secondary DNS servers work as extra DNS servers if the primary server is not working.

A secondary DNS server updates its information from the primary DNS server at regular intervals. You can specify how often. Only the manager of the DNS server can set it up as a secondary DNS server for someone else. In the figure below, we have two local networks with separate DNS servers. If DNS server Amanda does not work, a machine in network 1 may ask the DNS server in network 2, Bertha, if this server is set up as secondary DNS server for Amanda. Other DNS servers outside network 1 and 2 belong to the other category.



The DNS server responds to name queries on port 53. Both TCP and UDP are used for name queries.

## Domain

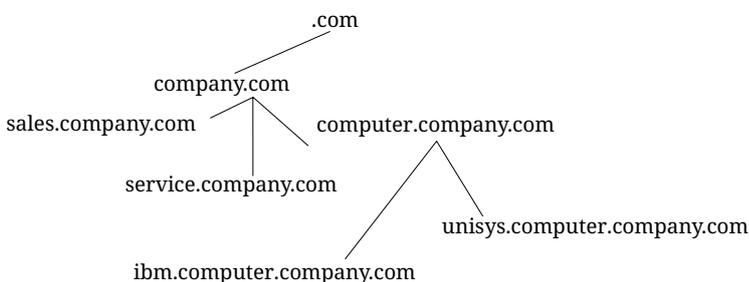
A domain is a country, organization, or subdivision. All countries have one top domain for the country, except for the United States, which is divided into a commercial domain (.com), a non-profit organizational domain (.org), a university domain (.edu), a military domain (.mil), a

governmental domain (.gov), and a network domain (.net). All domains are hierarchical and each domain is responsible for the domains directly under it.

A domain can have several sub-domains, which in turn can have sub-domains and so on. The structure combines the domain name of the organization with the overlying domain name.

For example, Stanford University has the domain name stanford, which is under the university domain of USA, .edu; together they form the domain stanford.edu. The university also has different departments under stanford.edu.

The departments of a company or organization can request a sub-domain from the domain manager. If the tech support people in the company's service division want their own domain, they can go to their domain manager and request a domain called, for instance, service. Below, we have 'Company Inc.,' which consists of three departments: A sales department, a service department, and a computer department. The computer department is divided into an IBM section and a Unisys section.



Contact your internet service provider to register a domain.

### *Dynamic routing*

Dynamic routing is used when the traffic between two computers have several routes available. The route for the packets can be changed if a connection is broken or a router is turned off. RIP is a protocol handling dynamic routing.

### *Firewall*

A device that prevents unauthorized access to a computer network.

### *Forwarding*

See Relay.

### *FTP (File Transfer Protocol)*

Imagine that you have an account on a UNIX machine. You can retrieve and store files on the UNIX machine with FTP. The program that manages this is called the FTP server. You can also establish an area of files that are accessible to others. Anyone can log in as user anonymous and enter his email address as a password. They can then access all files in this area, but nothing else. A computer with an FTP server and a freely available area is usually called an FTP site.

### *Gateway*

Gateway is an old name for a Router.

### *Hacker*

A person who is skilled and knowledgeable about computers and likes to examine the details of

a computer system and what can be done with it. A hacker is good at programming and achieves good results. A hacker is not to be confused with a computer criminal; see Cracker.

### *HTTPS*

HTTPS is WWW traffic (HTTP traffic) over an encrypted connection. The encrypted connection is established using the SSL protocol.

### *ICMP protocol*

ICMP is used to forward information, primarily error messages. To see if a computer is running, the 'ping' program sends an echo request, which is an ICMP packet. If a problem occurs with a connection, a response is sent using ICMP that something is not right (the computer is not responding, the network is down, etc). If there are two possible paths for a connection, a router along the way may tell the computer to use the other path. The router sends an ICMP redirect. ICMP uses the IP protocol to send data over the network.

### *IP address*

IP addresses are used to connect to computers, and are the Internet equivalent to telephone numbers. An IP address is divided into four groups, each of which is a number from 0 to 255. The groups are separated by dots. An example of an IP address is 192.165.122.42. Several IP addresses are required to connect several computers in a network; one for each computer.

IP addresses can be divided into public and private addresses. Public IP addresses are unique throughout the Internet, and can be reached by all computers connected to the Internet. Private IP addresses can be used on several local networks, but can't be reached from other networks. When a computer with a private IP address wants to connect to a computer on the Internet, the traffic must be NATed (see also NAT).

### *IP*

IP is short for Internet Protocol. This is a protocol that is used to send data between two computers on the same or different networks. IP performs no security checks. It works analogous to standard mail. Peter sends four postcards to Christy from the other side of the world. Christy gets postcard two first, then postcard one and postcard four. Postcard three disappears on the way. Peter and Christy know each other's addresses, and the post office knows how to read addresses and send postcards in the right direction. But Peter and Christy cannot know if all of their postcards will arrive, and Christy doesn't know what order the postcards were sent in.

For more information about IP addresses, see IP address.

### *Kerberos*

Kerberos is a system to secure connections between several computers over networks. The Kerberos system uses a Kerberos server to manage security. Connections that go through Kerberos are often encrypted.

### *Masquerading*

See NAT.

### *Name server*

See DNS.

### *NAT*

NAT (Network Address Translation), also known as masquerading, is a way to hide a network from outside computers. Used with firewalls to hide the computers on the internal network from the rest of the world.

### *Netmask*

See network mask.

### *Network mask*

A network mask tells what computers can be accessed locally without using a gateway, and what computers can only be reached through a gateway. The bits in the network mask determine what is a network and what is a computer. The total amount of bits is 32 and the "one-bits" are for networks. The network mask can be specified as the amount of one-bits grouped in the same way as IP addresses. For what formerly was called a class C network, the network mask is 24, which can also be expressed as 255.255.255.0 (i.e., 24 one-bits grouped in octets and then interpreted as binary numbers). If this network is divided into several parts, the network mask is different, depending on how the division is done. For example, the network mask 255.255.255.224 gives a network with 32 IP addresses in it. See also the table of network masks in appendix I, Lists of Reserved Ports, ICMP Types and Codes, and Internet Protocols.

### *News*

News is a distributed, loose conference system, which includes the entire Internet and more. News originated in email, so it has many similarities to email. It can also be called Usenet News and NetNews.

News is a conference system for exchange of ideas, questions and answers, and so on, just like in a BBS or COM system. What is written in News is not stored on a central computer; it is sent out all over the world and stored in several places. Your organization may choose to retrieve News and store all texts locally.

To keep track of everything, News is divided into news groups. A news group focuses on a specific area of interest. Each news group can have divisions and subgroups.

rec.motorcycles.harley is an example of a group name. rec is the main group, Recreational, which includes hobbies, recreation and the arts. A subgroup of rec is motorcycles, which is solely about motorcycles. A subgroup of rec.motorcycles is harley, which is only about Harley Davidson motorcycles. Another example is sci.geo.geology. Anyone can post articles to News; remember that several million people may be reading what you write. Make sure that all users are aware of this and are restrictive of what they write.

News servers use the NNTP protocol to communicate with each other. Many client programs also use NNTP to communicate with the news server. NNTP communication uses port 119.

### *NFS, Network File System*

NFS is a protocol for mounting disks from other computers over the network. NFS should be blocked against unsecure external networks. NFS uses port 2049.

NIS/YP is used to distribute central information to client machines in a network. Passwords and e-mail aliases are typical examples of such information. This also often used to allow users to sit at any work station, log in as themselves, and access their user accounts. NIS/YP should be blocked against unsecure external networks.

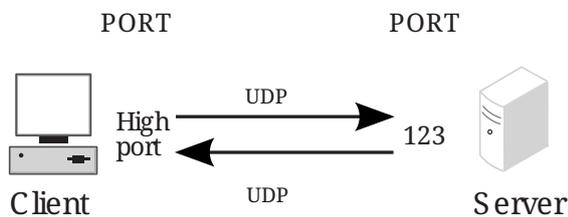
*Nntp*

See News.

*NTP*

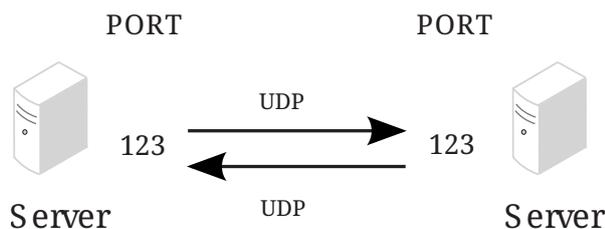
NTP is short for Network Time Protocol and is used for synchronizing computer clocks. The synchronization normally uses a computer with a very accurate clock, e.g., a computer with an atomic clock.

A client computer wanting to synchronize with a server via NTP usually uses a high port on the client, port 123 on the server and the UDP protocol. The server returns data using UDP from port 123 to a high port on the client computer.



The time interval between connections to the NTP server depends on the difference between the computer clock and the server clock. When NTP is started on a computer, it connects rather often to check that the time is correct and that it doesn't gain or lose time compared to the server clock. After that, it will connect with lower frequency just to check that it keeps the correct time.

Two NTP servers communicating with each other use port 123 and the UDP protocol.



*Open Windows*

Open Windows is a window system that is used by several work stations. A similar window system is the X Window System, which Open Windows is based on. The X Window System and Open Windows use ports 6000 and upward for traffic to the work stations. It is a good idea to block ports 6000-6010 for incoming traffic from an unsecure outside network.

*Packet*

When something is sent over a computer network, for example, a file or an email, it is divided up into sections. These sections are called packets. They make up a sort of jigsaw puzzle, each piece sent individually. The receiving computer has to reassemble the pieces.

## *Ping*

Ping is used to examine whether a computer works and is accessible over a network. Ping sends ICMP traffic to the computer in question, and the target computer replies with a reply ICMP packet if it is running and reachable from the network.

You can also ping a whole network, and thereby use ping to examine which computers exist on a certain network. Therefore it is not advisable to allow ping into an internal network.

The client computer sends a type 8 ICMP packet, echo-request, to find out whether the target computer is working and accessible. The target computer ("server" in the picture below) replies with a type 0 ICMP packet, echo-reply, to tell it is working and accessible over the network.

## *Ports*

When two computers use UDP or TCP to connect, ports are used. A client machine that wants access to a certain service on a server connects to the standard port for that particular service on the server. The programs on the client machine receive an available port over 1023. For example, if a user on the computer Tekla wants to run a Telnet session to the computer Winona, the user's Telnet client program receives an available port over 1023 to connect to port 23 on Winona. If two server programs contact each other, one can act as a client program, receiving an available port over 1023 on its local machine. However, many server programs have special definitions of how servers communicate with each other, where both servers use their standard port.

## *PPP*

PPP is short for Point-to-Point Protocol. This is usually used to send IP packets over modem connections. See also IP.

## *Protocols*

Protocols are sets of rules for how programs communicate with each other. For example, a web server can use the protocols HTTP and HTTPS.

## *Proxy*

Proxies are devices through which web pages, FTP files, and so on can be retrieved for a local network. This can be good to combine with a cache memory, which will store pages and files once fetched from the Internet site. When another user wants to look at a page already in the cache, it acts as a web server, sending the cached page instead of fetching a new copy through the Internet.

In your web browser, specify a computer and cache/proxy to be used to store this information.

## *Relay*

When the local network is connected to the Internet through a firewall, all types of services are usually blocked. It is as if the network is not connected to the Internet. Relays can then be set up to allow certain services, such as the WWW, to pass through under controlled circumstances. Think of it as a giant stone wall with a gate and a specialized gate keeper. The gate keeper only lets certain visitors pass. To allow others to pass through, you set up another gate with another specialized gate keeper.

### *Request-URI*

A Request-URI is used by the SIP protocol to indicate where a SIP request should be sent. The Request-URI can contain a username, a SIP domain or an IP address. It also contains the sip/sips parameter (sips if the request should be sent encrypted all the way, sip if not) and the SIP version (usually SIP/2.0).

### *RFC*

An RFC (Request For Comments) is a document which standardizes some aspect of the Internet traffic. RFC:s are available at <http://rfc.dotsrc.org/rfc-url.shtml>.

### *RIP*

RIP is a protocol that manages dynamic routing. Dynamic routing means that the path for traffic can be changed. RIP selects the path that goes through the least amount of routers, but does not consider the bandwidth or load on the network. RIP is only used in local networks. Fixed paths for traffic are called static routing.

### *Router*

A router is a machine that is used to connect several smaller and larger networks. Often, a router is used to connect a local network to the Internet. This router only lets traffic to the Internet out; all other traffic remains on the local network. A router can also be called a gateway.

### *Routing*

A routing is a path for the traffic between different computers.

### *Server*

A server can be a program that performs a service on a network or a computer that runs one or more server programs. One example is a computer that stores files centrally, which makes it a kind of server, usually called a file server. The program that manages traffic so that people from the outside can access an organization's web pages is a server program.

### *SIP*

SIP, Session Initiation Protocol, is a protocol for creating, maintaining and terminating various media stream sessions over an IP network. SIP is used to negotiate which media streams the parts can send and receive, and which parts should be involved in the exchange. When this is established, the media streams are sent according to their own protocols (e.g. HTTP). A thorough description of SIP can be found in RFC 2543.

### *SLIP*

SLIP is short for Serial Line IP. This is usually used to send IP packets over modem connections. See IP.

### *SLIRP*

SLIRP is a program that sends IP packets over serial connections, such a modem connections. SLIRP is run as a user program. SLIRP does not need its own IP address; it uses the server's IP address. The program works with both SLIP and PPP clients. See IP.

### *SMTP*

Simple Mail Transfer Protocol, a protocol for sending e-mail between e-mail servers. SMTP uses

port 25.

### *SNMP*

A protocol used for network monitoring. SNMP uses ports 161 and 162.

### *Sockets*

When two computers connect to each other, they use their IP addresses and port numbers. The combination of an IP address and a port number is called a socket. See IP addresses and Ports.

### *SSH, Secure SHell*

SSH is a system for secure, encrypted connections between two computers over a network. SSH uses one open and one secret key. In contrast to Kerberos, SSH does not use a central server for security. SSH uses port 22.

### *SSL*

SSL is short for Secure Sockets Layer. The SSL protocol handles establishing of encrypted computer connections. Usually HTTP and WWW traffic is sent on SSL. HTTP on SSL is called HTTPS.

### *Static Routing*

A fixed path for the contact between computers. With a static routing, traffic cannot be redirected to another path if the connection is broken. This would require dynamic routing, for example, with RIP.

### *Syslog*

Syslog is a service for logging data. In UNIX, regular programs do not log any information; they send all data to a syslog server that saves data in a log file. One example is a web server that sends data over the computers that connects to the server and sends error messages for web pages that it could not locate. Messages to a syslog server can also be sent over the network. Syslog uses the UDP protocol. A syslog server listens to port 514 for syslog messages.

### *TCP protocol*

TCP connects two computers and makes sure that all data gets through and in the right order. TCP uses IP. IP manages addresses and makes sure that data is sent out to the network. When TCP connects, it receives a response from the TCP protocol layer on the receiving end. The recipient sends a little data along with a confirmation that the sender's data arrived. When a connection is made, a confirmation is always sent with all data packets. This can be compared with Peter and Christy sending postcards and, along with their message, commenting that they received the other's postcard. TCP shortens this confirmation to ACK (acknowledgment).

You know if a TCP packet is a connection attempt if it does not have ACK.

TCP keeps track of connections for different services using different port numbers. See Ports.

### *UDP protocol*

UDP does not make a connection. It examines data that comes from outside for accuracy, by checksums. This is like examining a postcard to ensure that it has not been torn up. UDP does not keep track of whether or not all data gets through or if it is in the right order; this is the job

of the application. So the data does not have an ACK confirmation. Peter and Christy, sending postcards, have to keep track of their own postcards and Peter has to tell Christy the order in which they should be read. UDP keeps track of the contacts using port numbers, just like TCP.

### *UUCP*

UNIX to UNIX Copy, an old protocol for copying files between two UNIX computers. This is sometimes used to send e-mail between two computers.

### *WWW, World Wide Web*

The WWW is currently the best known Internet service. The World Wide Web consists of millions of documents that are interconnected all over the world. A document can contain text, pictures, sound, and even video sequences. The WWW is based on the client-server concept. This means that each document is in a database on a web server. The user runs a client program, such as Netscape or Internet Explorer, that connects to a server, which could be anywhere in the world, and request a document. This document is displayed on the user's screen and the user can use his client program to click on other documents to display them. WWW usually runs on the HTTP and HTTPS protocols, using ports 80 and 443, respectively.

### *X Window System*

A window system that is used by several work stations. A similar window system is Open Windows. The X Window System and Open Windows uses port numbers starting at 6000 and upward for traffic to the work stations. It is a good idea to block ports 6000-6010 from incoming traffic from an insecure outside network.

# Appendix J: License Conditions

The Ingate SIParator/Firewall contains third party software that is subject to the following license agreements.

To fulfill the license conditions, we must either attach the source code with the software, or send a written offer, valid at least three years, to give a copy of the source code to anyone who wants it. According to 3b) of the license, we are entitled to charge for the distribution of the source code.

To make the distribution easier and cheaper, both for Ingate Systems AB and you, we have an FTP server where you can download the GPL:ed source code. You find the FTP server at <ftp://ftp.ingate.com/pub/fuego/firewall/src/>.

We also have this offer:

Ingate Systems AB offer the source code for all third party software included in Ingate SIParator/Firewall and licensed under GPL. This offer is valid for this version of Ingate SIParator/Firewall and is valid for three years after deliverance of your Ingate SIParator/Firewall unit. Deliverance in Sweden C.O.D. The charge is 200 SEK, plus postage and C.O.D. fee, for CDROM. Ingate Systems AB reserves the right to change charge or medium without previous notice. Contact Ingate Systems AB for current information.

## GNU Lesser General Public License (LGPL) v 2.1

GNU LESSER GENERAL PUBLIC LICENSE  
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.  
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts  
as the successor of the GNU Library Public License, version 2, hence  
the version number 2.1.]

### Preamble

The licenses for most software are designed to take away your  
freedom to share and change it. By contrast, the GNU General Public  
Licenses are intended to guarantee your freedom to share and change  
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some  
specially designated software packages--typically libraries--of the  
Free Software Foundation and other authors who decide to use it. You  
can use it too, but we suggest you first think carefully about whether  
this license or the ordinary General Public License is the better  
strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the

entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE  
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that,

in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany

it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the Library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work

during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by

all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## Modules under this license

GeoIP 1.5.0	glibc 2.17	glibc-common 2.17
keyutils-libs 1.5.8	kmod-libs 20	libacl 2.2.51
libassuan 2.1.0	libattr 2.4.46	libblkid 2.23.2
libcap 2.22	libcap-ng 0.7.5	libdaemon 0.14
libgcc 4.8.5	libgcrypt 1.5.3	libgpg-error 1.12
libmicrohttpd 0.9.33	libmnl 1.0.3	libstdc++ 4.8.5
ppp 2.4.5	pptpd 1.3.4	procps-ng 3.3.10
pth 2.0.7	xz-libs 5.2.2	

## GNU General Public License (GPL) v 2

GNU GENERAL PUBLIC LICENSE  
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,  
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this

License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include

anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to

apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES

PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## Modules under this license

GeoIP 1.5.0	acpid 2.0.19	glibc 2.17
glibc-common 2.17	gmp 6.0.0	iproute 3.10.0
iputils 20160308	keyutils-libs 1.5.8	kmod 20
lrzsz 0.12.20	net-tools 2.0	pciutils 3.5.1
pciutils-libs 3.5.1	ppp 2.4.5	pptpd 1.3.4
procps-ng 3.3.10	psmisc 22.20	traceroute 2.0.22
busybox 1.23.2	MAKEDEV 3.24	SysVinit 2.84
dmiwriter 2.12	e2fsprogs 1.42.9	e2fsprogs-libs 1.42.9
ethtool 4.5	ipset 6.19	ipset-libs 6.19
iptables 1.4.21	kernel-fuego 3.10.105	libreswan 3.20
libreswan-kmod 3.20	lyspython 0.0.1	memtester 4.0.5
ndisc6 1.0.3	ntp 4.2.6p5	e1000e 3.3.5.3
igb 5.3.4.4	ixgbe 3.22.3	netxtreme2 7.10.73
tg3 3.136h		

## GNU Lesser General Public License (LGPL) v 3

GNU LESSER GENERAL PUBLIC LICENSE  
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

#### 0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

#### 1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

#### 2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

- a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs

whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

### 3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

### 4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

## 5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

## 6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

## Modules under this license

autogen-libopts 5.18

gmp 6.0.0

## GNU General Public License (GPL) v 3

### GNU GENERAL PUBLIC LICENSE Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>  
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

#### Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive

or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

## TERMS AND CONDITIONS

### 0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

#### 1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free

programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

## 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

## 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to

the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

#### 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

#### 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users

beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

## 6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

## 7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this

License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

#### 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

#### 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

## 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

## 11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a

party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

## 12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may

not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

### 13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

### 14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

### 15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF

ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

#### 16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### 17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

## Modules under this license

bash 4.2.46	cpio 2.11	diffutils 3.3
ed 1.9	findutils 4.5.11	gnupg2 2.0.22
grep 2.20	libassuan 2.1.0	libgcc 4.8.5
libstdc++ 4.8.5	procps-ng 3.3.10	readline 6.2
sed 4.2.2	tar 1.26	ndisc6 1.0.3

## GNU Library General Public License (LGPL) v 2

GNU LIBRARY GENERAL PUBLIC LICENSE  
Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.  
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is  
numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your

freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary

one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

#### GNU LIBRARY GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the

Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of

its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a

medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference

directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library

facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any

such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE

LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## Modules under this license

e2fsprogs-libs 1.42.9

libnl3 3.2.28

libroxml 2.3.0

## GNU Free Documentation License (GFDL) v 1.3

GNU Free Documentation License  
Version 1.3, 3 November 2008

Copyright (C) 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc.  
<<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the

software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available

drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use

technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

### 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

### 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under

the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements"

or to conflict in title with any Invariant Section.

#### 0. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

### 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled

"History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

## 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include

the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

## 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or

of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

## 11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

## Modules under this license

ed 1.9

## License exceptions for libgcc

libgcc contains this exception to the GNU General Public License (v2):

In addition to the permissions in the GNU General Public License, the Free Software Foundation gives you unlimited permission to link the compiled version of this file into combinations with other programs, and to distribute those combinations without any restriction coming from the use of this file. (The General Public License restrictions do apply in other respects; for example, they cover modification of the file, and distribution when not linked into a combine executable.)

Various assembler files contain this exception to the GNU General Public License:

As a special exception, if you link this library with files compiled with GCC to produce an executable, this does not cause the resulting executable to be covered by the GNU General Public License. This exception does not however invalidate any other reasons why the executable file might be covered by the GNU General Public License.

## Modules under this license

libgcc 4.8.5

## License exceptions for libstdc++

libstdc++ comes with the following so called "runtime exception" to GPLv2:

As a special exception, you may use this file as part of a free software library without restriction. Specifically, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other files to produce an executable, this file does not by itself cause the resulting executable to be covered by the GNU General Public License. This exception does not however invalidate any other reasons why the executable file might be covered by the GNU General Public License.

## Modules under this license

libstdc++ 4.8.5

## GCC RUNTIME LIBRARY EXCEPTION

GCC RUNTIME LIBRARY EXCEPTION

Version 3.1, 31 March 2009

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This GCC Runtime Library Exception ("Exception") is an additional permission under section 7 of the GNU General Public License, version 3 ("GPLv3"). It applies to a given file (the "Runtime Library") that bears a notice placed by the copyright holder of the file stating that the file is governed by GPLv3 along with this Exception.

When you use GCC to compile a program, GCC may combine portions of certain GCC header files and runtime libraries with the compiled program. The purpose of this Exception is to allow compilation of non-GPL (including proprietary) programs to use, in this way, the header files and runtime libraries covered by this Exception.

## 0. Definitions.

A file is an "Independent Module" if it either requires the Runtime Library for execution after a Compilation Process, or makes use of an interface provided by the Runtime Library, but is not otherwise based on the Runtime Library.

"GCC" means a version of the GNU Compiler Collection, with or without modifications, governed by version 3 (or a specified later version) of the GNU General Public License (GPL) with the option of using any subsequent versions published by the FSF.

"GPL-compatible Software" is software whose conditions of propagation, modification and use would permit combination with GCC in accord with the license of GCC.

"Target Code" refers to output from any compiler for a real or virtual target processor architecture, in executable form or suitable for input to an assembler, loader, linker and/or execution phase. Notwithstanding that, Target Code does not include data in any format that is used as a compiler intermediate representation, or used for producing a compiler intermediate representation.

The "Compilation Process" transforms code entirely represented in non-intermediate languages designed for human-written code, and/or in Java Virtual Machine byte code, into Target Code. Thus, for example, use of source code generators and preprocessors need not be considered part of the Compilation Process, since the Compilation Process can be understood as starting with the output of the generators or preprocessors.

A Compilation Process is "Eligible" if it is done using GCC, alone or with other GPL-compatible software, or if it is done without using any work based on GCC. For example, using non-GPL-compatible Software to optimize any GCC intermediate representations would not qualify as an Eligible Compilation Process.

## 1. Grant of Additional Permission.

You have permission to propagate a work of Target Code formed by combining the Runtime Library with Independent Modules, even if such propagation would otherwise violate the terms of GPLv3, provided that all Target Code was generated by Eligible Compilation Processes. You may then convey such a combination under terms of your choice, consistent with the licensing of the Independent Modules.

## 2. No Weakening of GCC Copyleft.

The availability of this Exception does not imply any general presumption that third-party software is unaffected by the copyleft requirements of the license of GCC.

## Modules under this license

libgcc 4.8.5

libstdc++ 4.8.5

## Mozilla Public License Version 2.0

### 1. Definitions

#### 1.1. "Contributor"

means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

#### 1.2. "Contributor Version"

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor's Contribution.

#### 1.3. "Contribution"

means Covered Software of a particular Contributor.

#### 1.4. "Covered Software"

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

#### 1.5. "Incompatible With Secondary Licenses"

means

a. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

b. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

#### 1.6. "Executable Form"

means any form of the work other than Source Code Form.

### 1.7. "Larger Work"

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

### 1.8. "License"

means this document.

### 1.9. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

### 1.10. "Modifications"

means any of the following:

a. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

b. any new file in Source Code Form that contains any Covered Software.

### 1.11. "Patent Claims" of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

### 1.12. "Secondary License"

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

### 1.13. "Source Code Form"

means the form of the work preferred for making modifications.

### 1.14. "You" (or "Your")

means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

## 2. License Grants and Conditions

### 2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

- a. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and
- b. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

## 2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

## 2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1 (b) above, no patent license is granted by a Contributor:

- a. for any code that a Contributor has removed from Covered Software; or
- b. for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or
- c. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

## 2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

## 2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

## 2.6. Fair Use

This License is not intended to limit any rights You have under applicable

copyright doctrines of fair use, fair dealing, or other equivalents.

## 2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

## 3. Responsibilities

### 3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

### 3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

- a. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and
- b. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

### 3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

### 3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known

factual inaccuracies.

### 3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

### 4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

### 5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

## 6. Disclaimer of Warranty

Covered Software is provided under this License on an “as is” basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

## 7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party’s negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

## 8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party’s ability to bring cross-claims or counter-claims.

## 9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

## 10. Versions of the License

### 10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new

versions of this License. Each version will be given a distinguishing version number.

#### 10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

#### 10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

#### 10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

##### Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at <https://mozilla.org/MPL/2.0/>.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

##### Exhibit B - "Incompatible With Secondary Licenses" Notice

This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.

## Modules under this license

nspr 4.13.1

nss 3.28.2

nss-softokn 3.16.2.3

nss-softokn-freebl 3.16.2.3

nss-tools 3.28.2

nss-util 3.28.2

## Python 2.7 license

This is the official license for the Python 2.7 release:

## A. HISTORY OF THE SOFTWARE

=====

Python was created in the early 1990s by Guido van Rossum at Stichting Mathematisch Centrum (CWI, see <http://www.cwi.nl>) in the Netherlands as a successor of a language called ABC. Guido remains Python's principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for National Research Initiatives (CNRI, see <http://www.cnri.reston.va.us>) in Reston, Virginia where he released several versions of the software.

In May 2000, Guido and the Python core development team moved to BeOpen.com to form the BeOpen PythonLabs team. In October of the same year, the PythonLabs team moved to Digital Creations (now Zope Corporation, see <http://www.zope.com>). In 2001, the Python Software Foundation (PSF, see <http://www.python.org/psf/>) was formed, a non-profit organization created specifically to own Python-related Intellectual Property. Zope Corporation is a sponsoring member of the PSF.

All Python releases are Open Source (see <http://www.opensource.org> for the Open Source Definition). Historically, most, but not all, Python releases have also been GPL-compatible; the table below summarizes the various releases.

Release	Derived from	Year	Owner	GPL-compatible? (1)
0.9.0 thru 1.2		1991-1995	CWI	yes
1.3 thru 1.5.2	1.2	1995-1999	CNRI	yes
1.6	1.5.2	2000	CNRI	no
2.0	1.6	2000	BeOpen.com	no
1.6.1	1.6	2001	CNRI	yes (2)
2.1	2.0+1.6.1	2001	PSF	no
2.0.1	2.0+1.6.1	2001	PSF	yes
2.1.1	2.1+2.0.1	2001	PSF	yes
2.2	2.1.1	2001	PSF	yes
2.1.2	2.1.1	2002	PSF	yes
2.1.3	2.1.2	2002	PSF	yes
2.2.1	2.2	2002	PSF	yes
2.2.2	2.2.1	2002	PSF	yes
2.2.3	2.2.2	2003	PSF	yes
2.3	2.2.2	2002-2003	PSF	yes
2.3.1	2.3	2002-2003	PSF	yes
2.3.2	2.3.1	2002-2003	PSF	yes
2.3.3	2.3.2	2002-2003	PSF	yes
2.3.4	2.3.3	2004	PSF	yes
2.3.5	2.3.4	2005	PSF	yes

2.4	2.3	2004	PSF	yes
2.4.1	2.4	2005	PSF	yes
2.4.2	2.4.1	2005	PSF	yes
2.4.3	2.4.2	2006	PSF	yes
2.5	2.4	2006	PSF	yes
2.7	2.6	2010	PSF	yes

Footnotes:

- (1) GPL-compatible doesn't mean that we're distributing Python under the GPL. All Python licenses, unlike the GPL, let you distribute a modified version without making your changes open source. The GPL-compatible licenses make it possible to combine Python with other software that is released under the GPL; the others don't.
- (2) According to Richard Stallman, 1.6.1 is not GPL-compatible, because its license has a choice of law clause. According to CNRI, however, Stallman's lawyer has told CNRI's lawyer that 1.6.1 is "not incompatible" with the GPL.

Thanks to the many outside volunteers who have worked under Guido's direction to make these releases possible.

B. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING PYTHON

=====

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

-----

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0  
-----

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at <http://www.pythonlabs.com/logos.html> may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

#### CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1

-----

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: <http://hdl.handle.net/1895.22/1013>".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2  
-----

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam,  
The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Modules under this license

python 2.7.5

python-crypto 2.6.1

python-libs 2.7.5

## The Vovida Software License, Version 1.0

Copyright (c) 2000 Vovida Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names "VOCAL", "Vovida Open Communication Application Library", and "Vovida Open Communication Application Library (VOCAL)" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [vocal@vovida.org](mailto:vocal@vovida.org).

Products derived from this software may not be called "VOCAL", nor may "VOCAL" appear in their name, without prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DAMAGES IN EXCESS OF \$1,000, NOR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Modules under this license

stund 0.92

## Software developed by Cisco Systems

Copyright (c) 2001-2006, Cisco Systems, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Modules under this license

srtp 1.5.3

libsrtp 1.5.3

## Software developed at University of California

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

Copyright (c) 1988 The Regents of the University of California. All rights reserved.

This code is derived from software written by Ken Arnold and published in UNIX Review, Vol. 6, No. 8.

vixie-cron 3.0.1

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Paul Vixie.

vixie-cron 3.0.1

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

Copyright (c) 1985, 1986 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by James A. Woods, derived from original work by Spencer Thomas and Joseph Orost.

ppp 2.4.5

Copyright (c) 1982, 1986, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2004

The Regents of the University of California. All rights reserved.

ftp 0.17

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

There are several licenses with the same terms, but different copyright notices. For each copyright notice, the modules under that license are listed. Below are the terms common for all these licenses.

Copyright (c) 2002 Google, Inc. All rights reserved.

ppp 2.4.5

Copyright (c) 1995 Eric Rosenquist. All rights reserved.

ppp 2.4.5

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

**zlib**

```
/* zlib.h -- interface of the 'zlib' general purpose compression library
   version 1.2.11, January 15th, 2017
```

Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly  
jloup@gzip.org

Mark Adler  
madler@alumni.caltech.edu

```
*/
```

## Modules under this license

zlib 1.2.7

ppp 2.4.5

## ISC

Copyright (c) 2004-2013 by Internet Systems Consortium, Inc. ("ISC")  
Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Systems Consortium, Inc.  
950 Charter Street  
Redwood City, CA 94063  
<info@isc.org>  
<https://www.isc.org/>

## Modules under this license

bind-libs-lite 9.9.4	dhcp 4.2.5	dhclient 4.2.5
dhcp-common 4.2.5	dhcp-libs 4.2.5	

## License for bzip2

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996-2010 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, [jseward@bzip.org](mailto:jseward@bzip.org)  
bzip2/libbzip2 version 1.0.6 of 6 September 2010

## Modules under this license

bzip2-libs 1.0.6

## License for lilo

LIinux LOader (LILO) program code, documentation, and auxiliary programs:

Copyright 1992-1998 Werner Almesberger  
Copyright 1999-2007 John Coffman  
Copyright 2009-2013 Joachim Wiedorn  
All rights reserved.

#### License

-----

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the names of the authors nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

#### Disclaimer

-----

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(Note: The above license is based on the BSD License at:  
<http://www.opensource.org/licenses/bsd-license.html>)

## Modules under this license

lilo 24.2

lilo32 24.2

## Software in the GNU C distribution

This file contains the copying permission notices for various files in the GNU C Library distribution that have copyright owners other than the Free Software Foundation. These notices all require that a copy of the notice be included in the accompanying documentation and be distributed with binary distributions of the code, so be sure to include this file along with any binary distributions derived from the GNU C Library.

All code incorporated from 4.4 BSD is distributed under the following license:

Copyright (C) 1991 Regents of the University of California.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. [This condition was removed.]
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The DNS resolver code, taken from BIND 4.9.5, is copyrighted by UC Berkeley, by Digital Equipment Corporation and by Internet Software Consortium. The DEC portions are under the following license:

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED ``AS IS'' AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The ISC portions are under the following license:

Portions Copyright (c) 1996-1999 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The Sun RPC support (from rpcsrc-4.0) is covered by the following license:

Copyright (c) 2010, Oracle America, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of the "Oracle America, Inc." nor the names of its

contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following CMU license covers some of the support code for Mach, derived from Mach 3.0:

Mach Operating System  
Copyright (C) 1991,1990,1989 Carnegie Mellon University  
All Rights Reserved.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS ``AS IS'' CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Carnegie Mellon requests users of this software to return to

Software Distribution Coordinator  
School of Computer Science  
Carnegie Mellon University  
Pittsburgh PA 15213-3890

or [Software.Distribution@CS.CMU.EDU](mailto:Software.Distribution@CS.CMU.EDU) any improvements or extensions that they make and grant Carnegie Mellon the rights to redistribute these changes.

The file `if_ppp.h` is under the following CMU license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY CARNEGIE MELLON UNIVERSITY AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following license covers the files from Intel's "Highly Optimized Mathematical Functions for Itanium" collection:

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR

A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The files inet/getnameinfo.c and sysdeps/posix/getaddrinfo.c are copyright (C) by Craig Metz and are distributed under the following license:

```
/* The Inner Net License, Version 2.00
```

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
1. All terms of the all other applicable copyrights and licenses must be followed.
2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. [The copyright holder has authorized the removal of this clause.]
5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

If these license terms cause you a real problem, contact the author. \*/

The file sunrpc/des\_impl.c is copyright Eric Young:

Copyright (C) 1992 Eric Young

Collected from libdes and modified for SECURE RPC by Martin Kuck 1994

This file is distributed under the terms of the GNU Lesser General Public License, version 2.1 or later - see the file COPYING.LIB for details. If you did not receive a copy of the license with this program, please see <<http://www.gnu.org/licenses/>> to obtain a copy.

The libidn code is copyright Simon Josefsson, with portions copyright The Internet Society, Tom Tromej and Red Hat, Inc.:

Copyright (C) 2002, 2003, 2004, 2011 Simon Josefsson

This file is part of GNU Libidn.

GNU Libidn is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

GNU Libidn is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with GNU Libidn; if not, see <<http://www.gnu.org/licenses/>>.

The following notice applies to portions of libidn/nfkc.c:

This file contains functions from GLIB, including gutf8.c and gunidecomp.c, all licensed under LGPL and copyright hold by:

Copyright (C) 1999, 2000 Tom Tromej  
Copyright 2000 Red Hat, Inc.

The following applies to portions of libidn/punycode.c and libidn/punycode.h:

This file is derived from RFC 3492bis written by Adam M. Costello.

Disclaimer and license: Regarding this entire document or any portion of it (including the pseudocode and C code), the author makes no guarantees and is not responsible for any damage resulting from its use. The author grants irrevocable permission to anyone to use, modify, and distribute it in any way that does not diminish the rights of anyone else to use, modify, and distribute it, provided that redistributed derivative works do not contain misleading author or version information. Derivative works need

not be licensed under similar terms.

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The file inet/rcmd.c is under a UCB copyright and the following:

Copyright (C) 1998 WIDE Project.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The file `posix/runtests.c` is copyright Tom Lord:

Copyright 1995 by Tom Lord

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of the copyright holder not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

Tom Lord DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL TOM LORD BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The `posix/rxspencer` tests are copyright Henry Spencer:

Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

The file `posix/PCRE.tests` is copyright University of Cambridge:

Copyright (c) 1997-2003 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. In practice, this means that if you use PCRE in software that you distribute to others, commercially or otherwise, you must put a sentence like this

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

somewhere reasonably visible in your documentation and in any relevant files or online help data or similar. A reference to the ftp site for the source, that is, to

`ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/`

should also be given in the documentation. However, this condition is not intended to apply to whole chains of software. If package A includes PCRE, it must acknowledge it, but if package B is software that includes package A, the condition is not imposed on package B (unless it uses PCRE independently).

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. If PCRE is embedded in any software that is released under the GNU General Purpose Licence (GPL), or Lesser General Purpose Licence (LGPL), then the terms of that licence shall supersede any condition above with which it is incompatible.

Files from Sun `fdlibm` are copyright Sun Microsystems, Inc.:

Copyright (C) 1993 by Sun Microsystems, Inc. All rights reserved.

Developed at SunPro, a Sun Microsystems, Inc. business.

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

Part of `stdio-common/tst-printf.c` is copyright C E Chew:

(C) Copyright C E Chew

Feel free to copy, use and distribute this software provided:

1. you do not pretend that you wrote it
2. you leave this copyright notice intact.

Various long double libm functions are copyright Stephen L. Moshier:

Copyright 2001 by Stephen L. Moshier <moshier@na-net.ornl.gov>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, see <<http://www.gnu.org/licenses/>>. \*/

## Modules under this license

glibc 2.17

glibc-common 2.17

## Apache License

Version 2.0, January 2004  
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity

on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
  - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
  - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or,

within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. **Submission of Contributions.** Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. **Trademarks.** This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.



```

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

```

Original SSLeay License

-----

```

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*

```

```

* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the routines from the library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

## Modules under this licence

openssl 1.0.1e

openssl-libs 1.0.1e

## License for ipmitool

Copyright (c) 2003 Sun Microsystems, Inc. All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sun Microsystems, Inc. or the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### Modules under this license

ipmitool 1.8.11

## License for libedit

Copyright (c) 1992, 1993

The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by  
Christos Zoulas of Cornell University.

Redistribution and use in source and binary forms, with or without  
modification, are permitted provided that the following conditions  
are met:

1. Redistributions of source code must retain the above copyright  
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright  
notice, this list of conditions and the following disclaimer in the  
documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors  
may be used to endorse or promote products derived from this software  
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND  
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE  
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE  
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL  
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS  
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT  
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY  
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF  
SUCH DAMAGE.

## Modules under this license

libedit 3.0

## License for libevent

Libevent is available for use under the following license, commonly known  
as the 3-clause (or "modified") BSD license:

=====

Copyright (c) 2000-2007 Niels Provos <provos@citi.umich.edu>

Copyright (c) 2007-2010 Niels Provos and Nick Mathewson

Redistribution and use in source and binary forms, with or without  
modification, are permitted provided that the following conditions  
are met:

1. Redistributions of source code must retain the above copyright  
notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

Portions of Libevent are based on works by others, also made available by them under the three-clause BSD license above. The copyright notices are available in the corresponding source files; the license is as above. Here's a list:

log.c:

Copyright (c) 2000 Dug Song <dugsong@monkey.org>  
Copyright (c) 1993 The Regents of the University of California.

strlcpy.c:

Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>

win32select.c:

Copyright (c) 2003 Michael A. Davis <mike@datanerds.net>

evport.c:

Copyright (c) 2007 Sun Microsystems

ht-internal.h:

Copyright (c) 2002 Christopher Clark

minheap-internal.h:

Copyright (c) 2006 Maxim Yegorushkin <maxim.yegorushkin@gmail.com>

=====

The arc4module is available under the following, sometimes called the "OpenBSD" license:

Copyright (c) 1996, David Mazieres <dm@uun.org>  
Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any

purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Modules under this license

libevent-2.0.21

## License for libuuid

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Modules under this license

libuuid 2.23.2

# License for net-snmp

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

----- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

----- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of the Networks Associates Technology, Inc nor the

names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2012, Sparta, Inc  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

\* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) ----

Copyright (c) 2009, ScienceLogic, LLC  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Modules under this license

net-snmp 5.7.2

net-snmp-agent-libs 5.7.2

net-snmp-libs 5.7.2

net-snmp-utils 5.7.2

# License for nginx

```
/*
 * Copyright (C) 2002-2016 Igor Sysoev
 * Copyright (C) 2011-2016 Nginx, Inc.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
```

## Modules under this license

nginx 1.10.1

## License for NTP

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this entire notice applies as if the text was explicitly included in the file.

```
*****
 *
 * Copyright (c) University of Delaware 1992-2015
 *
 * Permission to use, copy, modify, and distribute this software and
 * its documentation for any purpose with or without fee is hereby
 * granted, provided that the above copyright notice appears in all
```

```
* copies and that both the copyright notice and this permission *
* notice appear in supporting documentation, and that the name *
* University of Delaware not be used in advertising or publicity *
* pertaining to distribution of the software without specific, *
* written prior permission. The University of Delaware makes no *
* representations about the suitability this software for any *
* purpose. It is provided "as is" without express or implied *
* warranty. *
*
```

```
*****
```

Content starting in 2011 from Harlan Stenn, Danny Mayer, and Martin Burnicki is:

```
*****
```

```
* *
* Copyright (c) Network Time Foundation 2011-2015 *
* *
* All Rights Reserved *
* *
* Redistribution and use in source and binary forms, with or without *
* modification, are permitted provided that the following conditions *
* are met: *
* 1. Redistributions of source code must retain the above copyright *
* notice, this list of conditions and the following disclaimer. *
* 2. Redistributions in binary form must reproduce the above *
* copyright notice, this list of conditions and the following *
* disclaimer in the documentation and/or other materials provided *
* with the distribution. *
*
```

```
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS *
* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED *
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE *
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE *
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR *
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT *
* OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR *
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF *
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT *
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE *
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH *
* DAMAGE. *
```

```
*****
```

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. Takao Abe <takao\_abe@xurb.jp> Clock driver for JJY receivers
2. Mark Andrews <mark\_andrews@isc.org> Leitch atomic clock controller
3. Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
4. Viraj Bais <vbais@mailman1.intel.com> and Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
5. Michael Barone <michael,barone@lmco.com> GPSVME fixes

6. Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
8. Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
10. Nelson B Bolyard <nelson@bolyard.me> update and complete broadcast and crypto features in sntp
11. Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
12. Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
13. Steve Clift <clift@ml.csiro.au> OMEGA clock driver
14. Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
15. Sven Dietrich <sven\_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
16. John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
17. Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
18. Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
19. John Hay <jhay@icomtek.csiro.co.za> IPv6 support and testing
20. Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
21. Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
22. Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
23. Mike Iglesias <iglesias@uci.edu> DEC Alpha port
24. Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
25. Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
26. Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or <H.Lambermont@chello.nl> ntpsweep
27. Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
28. Frank Kardel <kardel (at) ntp (dot) org> PARSE <GENERIC> (driver 14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
29. Johannes Maximilian Kuehn <kuehn@ntp.org> Rewrote sntp to comply with NTPv4 specification, ntpq saveconfig
30. William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
31. Dave Katz <dkatz@cisco.com> RS/6000 AIX port
32. Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
33. George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
34. Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
35. Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
36. Danny Mayer <mayer@ntp.org> Network I/O, Windows Port, Code Maintenance
37. David L. Mills <mills@udel.edu> Version 4 foundation, precision kernel; clock drivers: 1, 3, 4, 6, 7, 11, 13, 18, 19, 22, 36
38. Wolfgang Moeller <moeller@gwdg1.dnet.gwdg.de> VMS port
39. Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
40. Tom Moore <tmoore@fieval.daytonoh.ncr.com> i386 svr4 port

41. Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
42. Derek Mulcahy <derek@toybox.demon.co.uk> and Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
43. Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
44. Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
45. Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
46. Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
47. Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
48. Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
49. Ray Schnitzler <schnitz@unipress.com> Unixware1 port
50. Michael Shields <shields@tembel.org> USNO clock driver
51. Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
52. Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
53. Kenneth Stone <ken@sdd.hp.com> HP-UX port
54. Ajit Thyagarajan <ajit@ee.udel.edu> IP multicast/anycast support
55. Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp> TRAK clock driver
56. Brian Utterback <brian.utterback@oracle.com> General codebase, Solaris issues
57. Loganaden Velvindron <loganaden@gmail.com> Sandboxing (libseccomp) support
58. Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
59. Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

## Modules under this license

ntp 4.2.6p5

## PCRE2 LICENCE

PCRE2 is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE2, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data in the testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the distribution is a just-in-time compiler that can be used to optimize pattern matching. This is an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

-----

Written by: Philip Hazel  
Email local part: ph10  
Email domain: cam.ac.uk

University of Cambridge Computing Service,  
Cambridge, England.

Copyright (c) 1997-2017 University of Cambridge  
All rights reserved.

#### PCRE2 JUST-IN-TIME COMPILATION SUPPORT

-----

Written by: Zoltan Herczeg  
Email local part: hzmester  
Email domain: freemail.hu

Copyright(c) 2010-2017 Zoltan Herczeg  
All rights reserved.

#### STACK-LESS JUST-IN-TIME COMPILER

-----

Written by: Zoltan Herczeg  
Email local part: hzmester  
Email domain: freemail.hu

Copyright(c) 2009-2017 Zoltan Herczeg  
All rights reserved.

#### THE "BSD" LICENCE

-----

Redistribution and use in source and binary forms, with or without  
modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice,  
this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright  
notice, this list of conditions and the following disclaimer in the  
documentation and/or other materials provided with the distribution.
- \* Neither the name of the University of Cambridge nor the names of any  
contributors may be used to endorse or promote products derived from this  
software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## **Modules under this license**

pcrc 8.32

## **Software developed by Carnegie Mellon University**

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.  
Redistribution and use in source and binary forms, with or without modification,  
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

Office of Technology Transfer  
Carnegie Mellon University  
5000 Forbes Avenue  
Pittsburgh, PA 15213-3890  
(412) 268-4387, fax: (412) 268-7395  
<tech-transfer@andrew.cmu.edu>

4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Modules under this license

ppp 2.4.5

## Software developed by Gregory M Christy

Copyright (c) 1991 Gregory M. Christy. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Gregory M. Christy. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

## **Modules under this license**

ppp 2.4.5

## **Software developed by Google, Inc**

By Frank Cusack <frank@google.com>. Copyright (c) 2002 Google, Inc. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that the above copyright notice appears in all copies. This software is provided without any warranty, express or implied.

## **Modules under this license**

ppp 2.4.5

## **Software developed in the GIE DYADE cooperation**

Copyright (c) 1995, 1996, 1997 <Francis.Dupont@inria.fr>, INRIA Rocquencourt, <Alain.Durand@imag.fr>, IMAG, <Jean-Luc.Richier@imag.fr>, IMAG-LSR.

Copyright (c) 1998, 1999 <Francis.Dupont@inria.fr>, GIE DYADE, <Alain.Durand@imag.fr>, IMAG, <Jean-Luc.Richier@imag.fr>, IMAG-LSR.

Ce travail a été fait au sein du GIE DYADE (Groupement d'Intérêt Économique ayant pour membres BULL S.A. et l'INRIA).

Ce logiciel informatique est disponible aux conditions usuelles dans la recherche, c'est-à-dire qu'il peut être utilisé, copié, modifié, distribué à l'unique condition que ce texte soit conservé afin que l'origine de ce logiciel soit reconnue.

Le nom de l'Institut National de Recherche en Informatique et en Automatique (INRIA), de l'IMAG, ou d'une personne morale ou physique ayant participé à l'élaboration de ce logiciel ne peut être utilisé sans son accord préalable explicite.

Ce logiciel est fourni tel quel sans aucune garantie, support ou responsabilité d'aucune sorte. Ce logiciel est dérivé de sources d'origine "University of California at Berkeley" et "Digital Equipment Corporation" couvertes par des copyrights.

L'Institut d'Informatique et de Mathématiques Appliquées de Grenoble (IMAG) est une fédération d'unités mixtes de recherche du CNRS, de l'Institut National Polytechnique de Grenoble et de l'Université Joseph Fourier regroupant sept laboratoires dont le laboratoire Logiciels, Systèmes, Réseaux (LSR).

This work has been done in the context of GIE DYADE (joint R & D venture between BULL S.A. and INRIA).

This software is available with usual "research" terms with the aim of retain credits of the software. Permission to use, copy, modify and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and the name of INRIA, IMAG, or any contributor not be used in advertising or publicity pertaining to this material without the prior explicit permission. The software is provided "as is" without any warranties, support or liabilities of any kind. This software is derived from source code from "University of California at Berkeley" and "Digital Equipment Corporation" protected by copyrights.

Grenoble's Institute of Computer Science and Applied Mathematics (IMAG) is a federation of seven research units funded by the CNRS, National Polytechnic Institute of Grenoble and University Joseph Fourier. The research unit in Software, Systems, Networks (LSR) is member of IMAG.

## Modules under this license

ppp 2.4.5

## Software developed by Tommi Komulainen

Copyright (c) 1999 Tommi Komulainen. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without specific prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Tommi Komulainen  
<Tommi.Komulainen@iki.fi>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Modules under this license

ppp 2.4.5

## Software developed by Paul Mackerras

Copyright (c) 1984, 1989-2002 Paul Mackerras. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without specific prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Paul Mackerras <paulus@samba.org>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## **Modules under this license**

ppp 2.4.5

## **Software developed by Pedro Roque Marques**

Copyright (c) 1995 Pedro Roque Marques. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Pedro Roque Marques  
<pedro\_m@yahoo.com>"

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## **Modules under this license**

ppp 2.4.5

## **Software developed by RSA Data Security, Inc**

Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

## Modules under this license

ppp 2.4.5

## Software developed by Sun Microsystems, Inc

Copyright (c) 2000 by Sun Microsystems, Inc. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that the above copyright notice appears in all copies.

SUN MAKES NO REPRESENTATION OR WARRANTIES ABOUT THE SUITABILITY OF THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SUN SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES.

## Modules under this license

ppp 2.4.5

## More software developed by Sun Microsystems, Inc

Copyright (c) 2001 by Sun Microsystems, Inc. All rights reserved.

Non-exclusive rights to redistribute, modify, translate, and use this software in source and binary forms, in whole or in part, is hereby granted, provided that the above copyright notice is duplicated in any source form, and that neither the name of the copyright holder nor the author is used to endorse or promote products derived from this software.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

## Modules under this license

ppp 2.4.5

## Software developed by Andrew Tridgell

Copyright (C) Andrew Tridgell 1999

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms AND provided that this software or any derived work is only used as part of the PPP daemon (pppd) and related utilities.

The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Note: this software is also available under the Gnu Public License version 2 or later

## Modules under this license

ppp 2.4.5

## License for dropbear

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston  
Portions copyright (c) 2004 Mihnea Stoenescu  
All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,  
Copyright (c) 1995 Tatu Ylonen <yl@cs.hut.fi>, Espoo, Finland  
All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c  
loginrec.h  
atomicio.h  
atomicio.c  
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed

under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

```
/* Copyright 2008, Google Inc.
```

```
* All rights reserved.
```

```
*
```

```
* Redistribution and use in source and binary forms, with or without  
* modification, are permitted provided that the following conditions are  
* met:
```

```
*
```

```
* * Redistributions of source code must retain the above copyright  
* notice, this list of conditions and the following disclaimer.
```

```
* * Redistributions in binary form must reproduce the above
```

```
* copyright notice, this list of conditions and the following disclaimer
```

```
* in the documentation and/or other materials provided with the
* distribution.
*   * Neither the name of Google Inc. nor the names of its
* contributors may be used to endorse or promote products derived from
* this software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
* "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
* LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
* A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
* OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
* DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
* THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
* OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
* curve25519-donna: Curve25519 elliptic curve, public key function
*
* http://code.google.com/p/curve25519-donna/
*
* Adam Langley <agl@imperialviolet.org>
*
* Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>
*
* More information about curve25519 can be found here
*   http://cr.yp.to/ecdh.html
*
* djb's sample implementation of curve25519 is written in a special assembly
* language called qhasm and uses the floating point registers.
*
* This is, almost, a clean room reimplementation from the curve25519 paper. It
* uses many of the tricks described therein. Only the crecip function is taken
* from the sample implementation.
*/
```

## Modules under this license

dropbear 2016.74

## License for kerberos

Please refer to [MIT Kerberos License information](#)

## Modules under this license

krb5-libs 1.14.1

## License for libcom\_err

This software component is released under LGPL and the following additional MIT attribution:

Copyright 1987, 1988 by the Student Information Processing Board of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T. and the M.I.T. S.I.P.B. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

M.I.T. and the M.I.T. S.I.P.B. make no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

## Modules under this license

libcom\_err 1.42.9

## License for libss

This software component is released under LGPL and the following additional MIT attribution:

Copyright 1987, 1988 by the Student Information Processing Board of the Massachusetts Institute of Technology

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the names of M.I.T. and the M.I.T. S.I.P.B. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

M.I.T. and the M.I.T. S.I.P.B. make no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

## Modules under this license

libss 1.42.9

## License for libcurl

### COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2017, Daniel Stenberg, daniel@haxx.se, and many contributors, see the THANKS file.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

## Modules under this license

libcurl 7.29.0

## License for libffi

libffi - Copyright (c) 1996-2014 Anthony Green, Red Hat, Inc and others.  
See source files for details.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ``Software''), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED ``AS IS'', WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Modules under this license

libffi 3.0.13

## License for libverto

Copyright 2011 Red Hat, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## **Modules under this license**

libverto 0.2.5

## **License for libxml2**

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## **Modules under this license**

libxml2 2.9.1

## **License for ncurses**

```

-----
-- Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.      --
--                                                                    --
-- Permission is hereby granted, free of charge, to any person obtaining a --
-- copy of this software and associated documentation files (the      --
-- "Software"), to deal in the Software without restriction, including --
-- without limitation the rights to use, copy, modify, merge, publish, --
-- distribute, distribute with modifications, sublicense, and/or sell copies --
-- of the Software, and to permit persons to whom the Software is furnished --
-- to do so, subject to the following conditions:                      --
--                                                                    --
-- The above copyright notice and this permission notice shall be included --
-- in all copies or substantial portions of the Software.            --
--                                                                    --
-- THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS --
-- OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF        --
-- MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN --
-- NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, --
-- DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR --
-- OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE --
-- USE OR OTHER DEALINGS IN THE SOFTWARE.                             --
--                                                                    --
-- Except as contained in this notice, the name(s) of the above copyright --
-- holders shall not be used in advertising or otherwise to promote the --
-- sale, use or other dealings in this Software without prior written --
-- authorization.                                                     --
-----

```

## Modules under this license

ncurses-libs 5.9

## License for dnspython

Copyright (C) 2001-2003 Nominum, Inc.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Modules under this license

python-dns-1.12.0

## License for pillow

The Python Imaging Library is

Copyright (c) 1997-2009 by Secret Labs AB  
Copyright (c) 1995-2009 by Fredrik Lundh

By obtaining, using, and/or copying this software and/or its associated documentation, you agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its associated documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies, and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Secret Labs AB or the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SECRET LABS AB AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL SECRET LABS AB OR THE AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Modules under this license

python-pillow 2.0.0

## License for wslay

The MIT License

Copyright (c) 2011, 2012, 2015 Tatsuhiro Tsujikawa

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Modules under this license

wslay-libs 1.0.0

## License for libpcap

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

## Modules under this license

libpcap 1.5.3

## License for radvd

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.
1. All terms of all other applicable copyrights and licenses must be followed.
2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.
3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software must display the following acknowledgement with the name(s) of the authors as specified in the copyright notice(s) substituted where indicated:

This product includes software developed by the authors which are mentioned at the start of the source files and other contributors.

5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Modules under this license

radvd 1.9.2

## License for tcpdump

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

## Modules under this license

tcpdump 4.5.1

## License for util-linux/agetty

```
/*
 * Alternate Getty (agetty) 'agetty' is a versatile, portable, easy to use
 * replacement for getty on SunOS 4.1.x or the SAC ttymon/ttyadm/sacadm/pmadm
 * suite on Solaris and other SVR4 systems. 'agetty' was written by Wietse
 * Venema, enhanced by John DiMarco, and further enhanced by Dennis Cronin.
 *
 * Ported to Linux by Peter Orbaek <poe@daimi.aau.dk>
 * Adopt the mingetty features for a better support
 * of virtual consoles by Werner Fink <werner@suse.de>
 *
 * This program is freely distributable.
 */
```

## Modules under this license

util-linux 2.23.2

## License for util-linux/uuidgen

```
/*
 * gen_uuid.c --- generate a DCE-compatible uuid
 *
 * Copyright (C) 1999, Andreas Dilger and Theodore Ts'o
 *
 * %Begin-Header%
 * This file may be redistributed under the terms of the GNU Public
 * License.
 * %End-Header%
 */
```

## Modules under this license

util-linux 2.23.2

## License for libselinux

This library (libselinux) is public domain software, i.e. not copyrighted.

### Warranty Exclusion

-----

You agree that this software is a non-commercially developed program that may contain "bugs" (as that term is used in the industry) and that it may not function as intended. The software is licensed "as is". NSA makes no, and hereby expressly disclaims all, warranties, express, implied, statutory, or otherwise with respect to the software, including noninfringement and the implied warranties of merchantability and fitness for a particular purpose.

### Limitation of Liability

-----

In no event will NSA be liable for any damages, including loss of data, lost profits, cost of cover, or other special, incidental, consequential, direct or indirect damages arising from the software or the use thereof, however caused and on any theory of liability. This limitation will apply even if NSA has been advised of the possibility of such damage. You acknowledge that this is a reasonable allocation of risk.

## Modules under this license

libselinux 2.5

## License for tzdata

Copyright (c) 2014 Lau Taarnskov

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.  
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Modules under this license

tzdata 2017b

## License for sqlite

## SQLite Is Public Domain

All of the code and documentation in SQLite has been dedicated to the public domain by the authors. All code authors, and representatives of the companies they work for, have signed affidavits dedicating their contributions to the public domain and originals of those signed affidavits are stored in a firesafe at the main offices of Hwaci. Anyone is free to copy, modify, publish, use, compile, sell, or distribute the original SQLite code, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

The previous paragraph applies to the deliverable code and documentation in SQLite - those parts of the SQLite library that you actually bundle and ship with a larger application. Some scripts used as part of the build process (for example the "configure" scripts generated by autoconf) might fall under other open-source licenses. Nothing from these build scripts ever reaches the final deliverable SQLite library, however, and so the licenses associated with those scripts should not be a factor in assessing your rights to copy and use the SQLite library.

All of the deliverable code in SQLite has been written from scratch. No code has been taken from other projects or from the open internet. Every line of code can be traced back to its original author, and all of those authors have public domain dedications on file. So the SQLite code base is clean and is uncontaminated with licensed code from other projects.

## Modules under this license

sqlite 3.7.17

## Licenses for mediafw

Copyright (c) Ingate Systems AB, 2013

```
/** src/ssl.c
 * Copyright (c) 2010 Daemotron <mail@daemotron.net>
 *
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this permission notice appear in all copies.
 *
 * THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
 * WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
 * MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
 * ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
 * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
 * ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
 * OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
 */

/** src/filters/dtls.c
 * Copyright (C) 2009 - 2012 Robin Seggelmann, seggelmann@fh-muenster.de,
 * Michael Tuexen, tuexen@fh-muenster.de
 *
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 * may be used to endorse or promote products derived from this software
 * without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *****/
```

## Modules under this license

mediafw 0.7.0

## Licenses for sipfw

turnserver/src:

```
/*
 * Copyright (C) 2011, 2012, 2013 Citrix Systems
 *
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 * may be used to endorse or promote products derived from this software
 * without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
```

ixlibc/src/http\_parser.c:

```
/* Based on src/http/nginx_http_parse.c from NGINX copyright Igor Sysoev
 *
 * Additional changes are licensed under the same terms as NGINX and
 * copyright Joyent, Inc. and other Node contributors. All rights reserved.
 *
 * Permission is hereby granted, free of charge, to any person obtaining a copy
 * of this software and associated documentation files (the "Software"), to
 * deal in the Software without restriction, including without limitation the
 * rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
```

```
* sell copies of the Software, and to permit persons to whom the Software is
* furnished to do so, subject to the following conditions:
*
* The above copyright notice and this permission notice shall be included in
* all copies or substantial portions of the Software.
*
* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
* FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
* AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
* LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
* FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
* IN THE SOFTWARE.
*/
```

```
ixlibc/src/cJSON.c
```

```
/*
```

```
Copyright (c) 2009 Dave Gamble
```

```
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:
```

```
The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.
```

```
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
```

```
*/
```

## Modules under this license

sipfw

# Appendix K: References

## Bibliography

### Books

*Applied Cryptography*, Bruce Schneier, John Wiley & Sons, 0-471-11709-9.

*Brandväggar vid anslutning till Internet [Firewalls in Internet Connections]*, Statskontoret, Stockholm.

*Building Internet Firewalls*, D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates Inc, 1-56592-124-0.

*Computer Security Basics*, Deborah Russel and G.T. Gangemi Sr, O'Reilly & Associates Inc.

*Practical Unix & Internet Security*, Simson Garfinkel and Gene Spafford, O'Reilly & Associates Inc, 1-56592-148-8.

*TCP/IP Network Administration*, Craig Hunt, O'Reilly & Associates Inc, 0-937175-82-X.

*Virtual Private Networks*, Charlie Scott, Paul Wolfe, and Mike Erwin, O'Reilly & Associates Inc, 1-56592-319-7.

### RFC:s

*RFC 793: Transmission Control Protocol*, J. Postel.

*RFC 826: An Ethernet Address Resolution Protocol*, David C. Plummer.

*RFC 1918: Address Allocation for Private Internets*, G. J. de Groot, D. Karrenberg, E. Lear, B. Moskowitz, and Y. Rekhter.

*RFC 2131: Dynamic Host Configuration Protocol*, R. Droms.

*RFC 2401: Security Architecture for the Internet Protocol*, S. Kent and R. Atkinson.

*RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)*, D. Maughan, M. Schertler, M. Schneider, and J. Turner.

*RFC 2409: The Internet Key Exchange (IKE)*, D. Carrel and D. Harkins.

*RFC 2865: Remote Authentication Dial In User Service (RADIUS)*, C. Rigney, A. Rubens, W. Simpson, and S. Willens.

*RFC 3261: SIP: Session Initiation Protocol*, M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, G. Camarillo, A. Johnston, J. Peterson, and R. Sparks.