

Ingate Firewall & SIParator Product Training

SIP Trunking Focused

Common SIP Applications

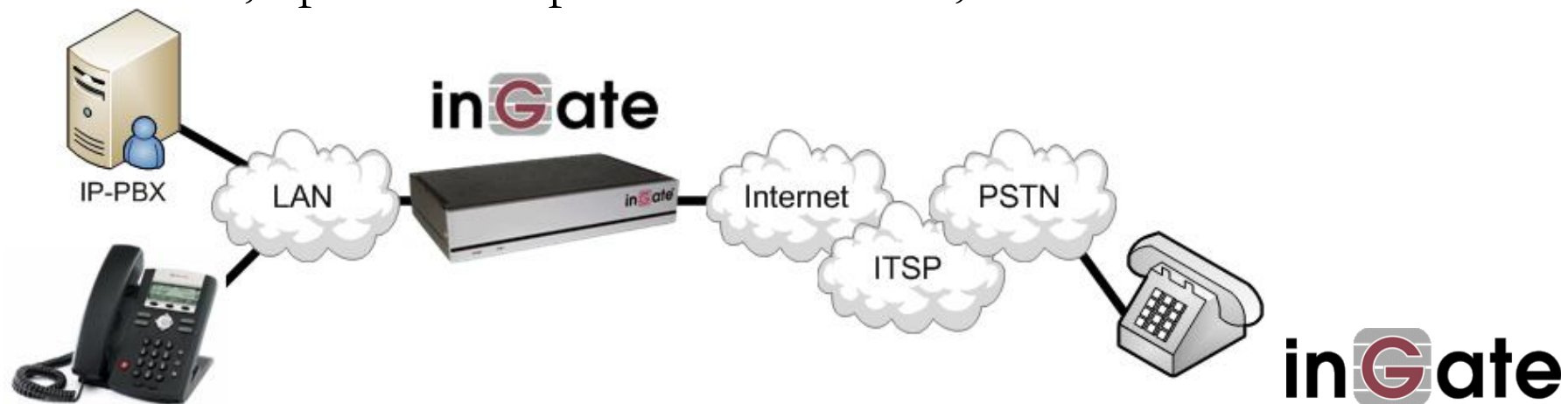
SIP Trunking
Remote Desktop

Ingate Product Training

Common SIP Applications

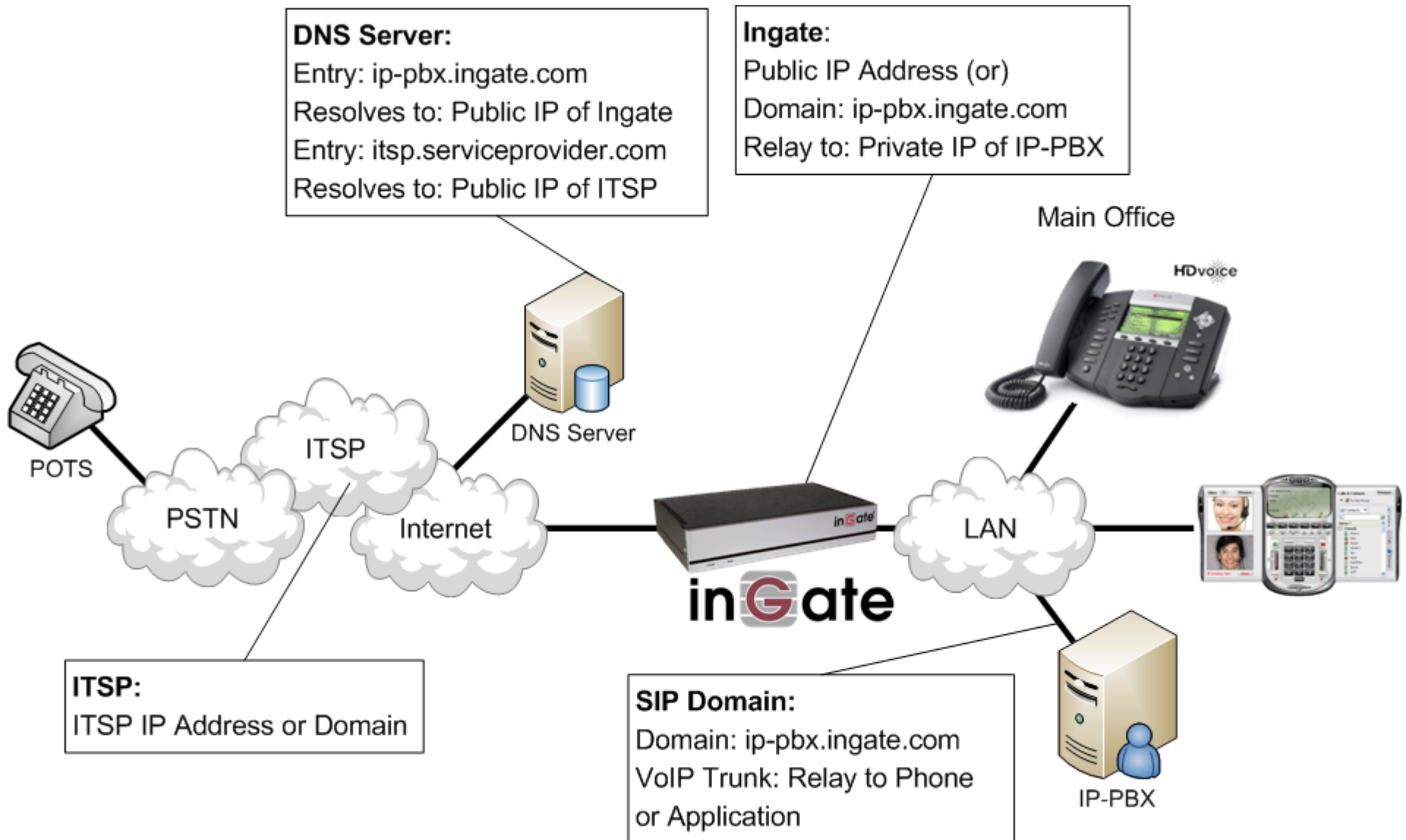
■ SIP Trunking

- A SIP Trunk is a concurrent call that is routed over the IP backbone of a carrier (ITSP) using VoIP technology.
- SIP Trunks are used in conjunction with an IP-PBX and are thought of as replacements for traditional PRI or analog circuits.
- The popularity of SIP Trunks is due primarily to the cost savings; due to a true convergence of voice and data infrastructure, Increased ROI, the maximizing of bandwidth utilization, open source protocol standards, and more.



Ingate Product Training

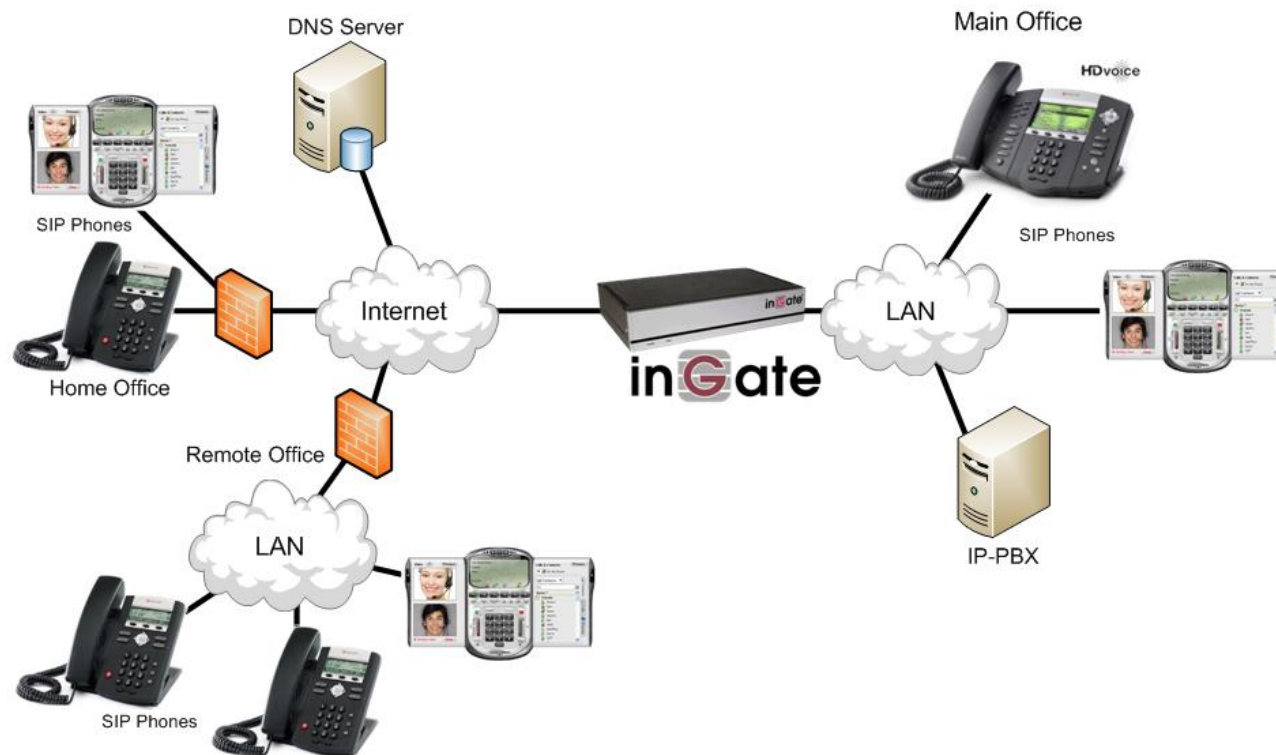
Common SIP Applications



Ingate Product Training

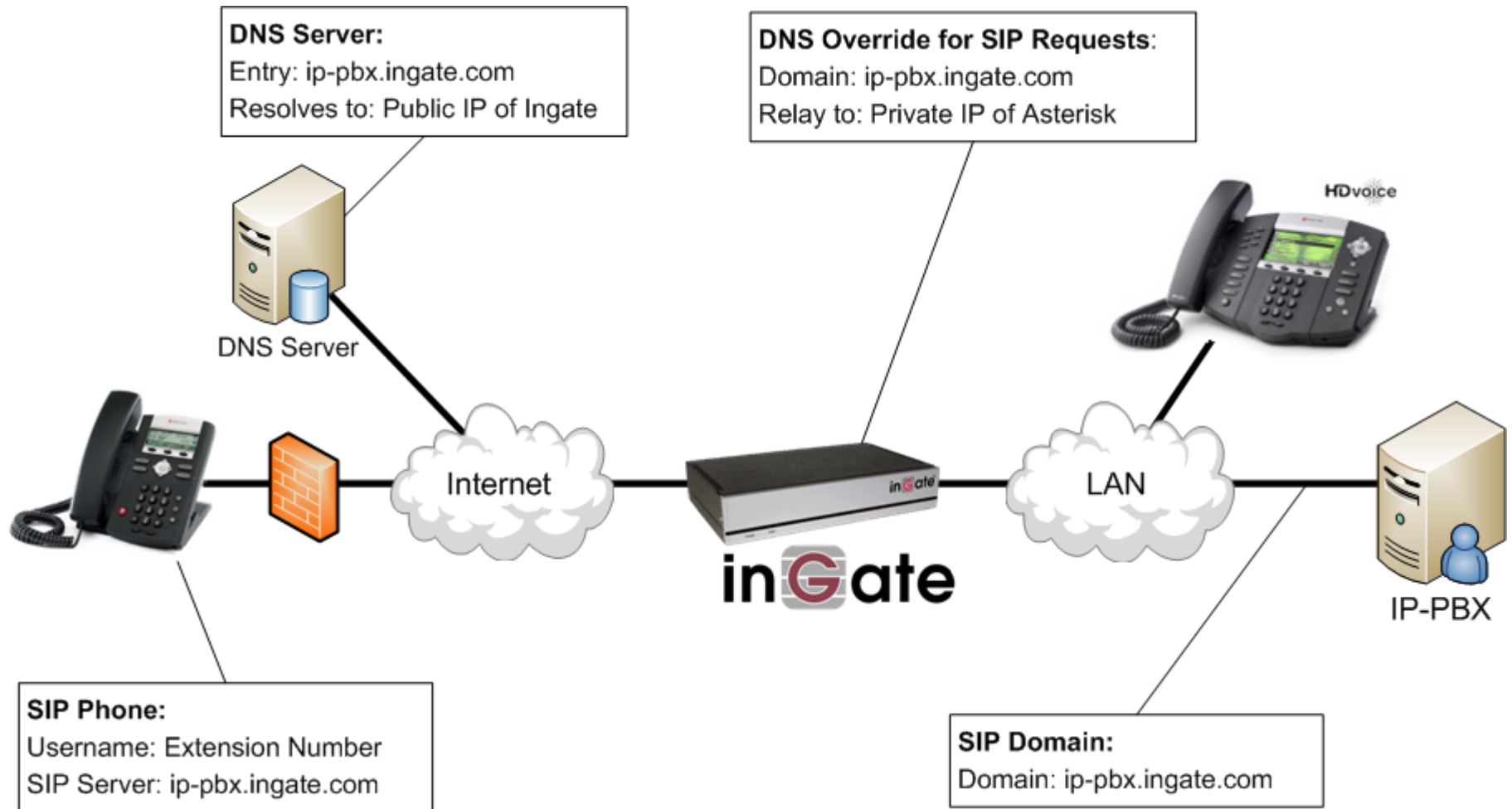
Common SIP Applications

- Remote Desktop
 - Extending SIP communications to Remote & Home Offices.
 - Extension of IP-PBX services using Open Source standardized Protocol
 - Use of off-the-self SIP Phones and Soft SIP Clients.



Ingate Product Training

Common SIP Applications

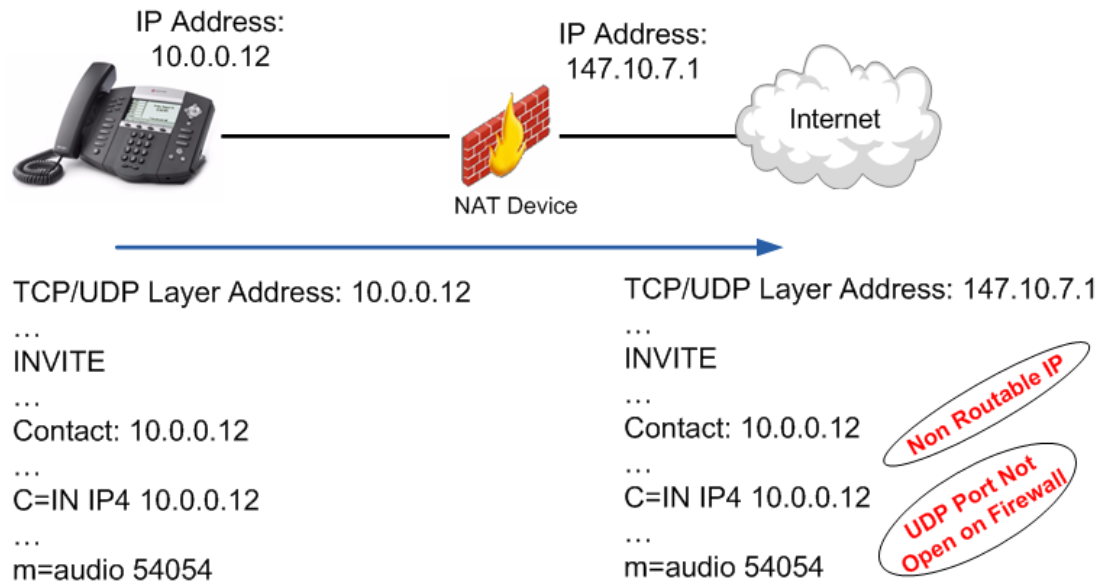


Common SIP Deployment Issues

Ingate Product Training

Common Deployment Issues

- **Problem #1 - “NAT BREAKS SIP”**
 - SIP Protocol is an Application Layer Protocol
 - Network Address Translation (NAT) resides at the Transport Layer (TCP/IP)
 - NAT will not change the SIP addressing within the TCP/UDP datagram
 - Firewalls are a NATing device and BLOCK all Incoming SIP Traffic to the LAN
 - Any NAT device, either Far End (remote) or Near End (on prem) can effect the call



Ingate Product Training

Common Deployment Issues

■ Before NAT

- TCP/IP Header is Private Space
- SIP Headers are Private Space

```
⊕ Internet Protocol, sr 10.51.77.60 (10.51.77.60), Dst: 10.51.77.1 (10.51.77.1)
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊖ Session Initiation Protocol
⊕ Request-Line: INVITE sip:1613963093@10.51.77.1 P/2.0
⊖ Message Header
⊕ Via:SIP/2.0/UDP 10.51.77.60:5060;rport;branch=z9hg4bkeda59e3
⊕ From:"Scott Beer" <sip:6139630933@10.51.77.1>;tag=484d0eda-186-6c1b36c8
⊕ To:<sip:16139630933@10.51.77.1>
⊕ Contact:"Scott Beer" <sip:613963093@10.51.77.60;transport=UDP>
  Call-ID:eda0000-2da6d41@10.51.77.1
⊕ CSeq:701887483 INVITE
  User-Agent:Mitel-5340-SIP-Phone FW.07.41.02 08000F314048
  Allow:INVITE,ACK,CANCEL,BYE,OPTIONS,REFER,NOTIFY,PRACK,UPDATE
  Allow-Events:talk,hold,conference
  Supported:timer,100rel,replaces
  Session-Expires: 1800
  Max-Forwards: 70
  Content-Type:application/sdp
  Content-Length: 249
⊖ Message Body
⊖ Session Description Protocol
  Session Description Protocol version (v): 0
⊕ Owner/Creator, Session Id (o): 6139630933 1213010017 1213010016 IN IP4 10.51.77.60
  Session Name (s): SIP Call
⊕ Connection Information (c): IN IP4 10.51.77.60
⊕ Time Description, active time (t): 0 0
  Session Attribute (a): sendrecv
⊕ Media Description, name and address (m): audio 20282 RTP/AVP 0 8 18 101
```

LAN IP Address and Port Information

LAN IP Address

LAN IP Address

LAN IP Address

Ingate Product Training

Common Deployment Issues

■ After NAT

- TCP/IP Header is Public Space
- SIP Headers are Private Space

```
⊕ Internet Protocol (207.112.18.164 (207.112.18.164), 9.249.3.59 (209.249.3.59))
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊖ Session Initiation Protocol
⊕ Request-Line: INVITE sip:1613963093@10.51.77.1 P/2.0
⊖ Message Header
⊕ Via:SIP/2.0/UDP 10.51.77.60:5060;rport;branch=z9hg4bkeda59e3
⊕ From:"Scott Beer" <sip:6139630933@10.51.77.1>;tag=484d0eda-186-6c1b36c8
⊕ To:<sip:16139630933@10.51.77.1>
⊕ Contact:"Scott Beer" <sip:613963093@10.51.77.60;transport=UDP>
  Call-ID:eda0000-2da6d41@10.51.77.1
⊕ CSeq:701887483 INVITE
  User-Agent:Mitel-5340-SIP-Phone Fw.07.41.02 08000F314048
  Allow:INVITE,ACK,CANCEL,BYE,OPTIONS,REFER,NOTIFY,PRACK,UPDATE
  Allow-Events:talk,hold,conference
  Supported:timer,100rel,replaces
  Session-Expires: 1800
  Max-Forwards: 70
  Content-Type:application/sdp
  Content-Length: 249
⊖ Message Body
⊖ Session Description Protocol
  Session Description Protocol version (v): 0
⊕ Owner/Creator, Session Id (o): 6139630933 1213010017 1213010016 IN IP4 10.51.77.60
  Session Name (s): SIP Call
⊕ Connection Information (c): IN IP4 10.51.77.60
⊕ Time Description, active time (t): 0 0
  Session Attribute (a): sendrecv
⊕ Media Description, name and address (m): audio 20282 RTP/AVP 0 8 18 101
```

WAN IP Address

LAN IP Address

LAN IP Address

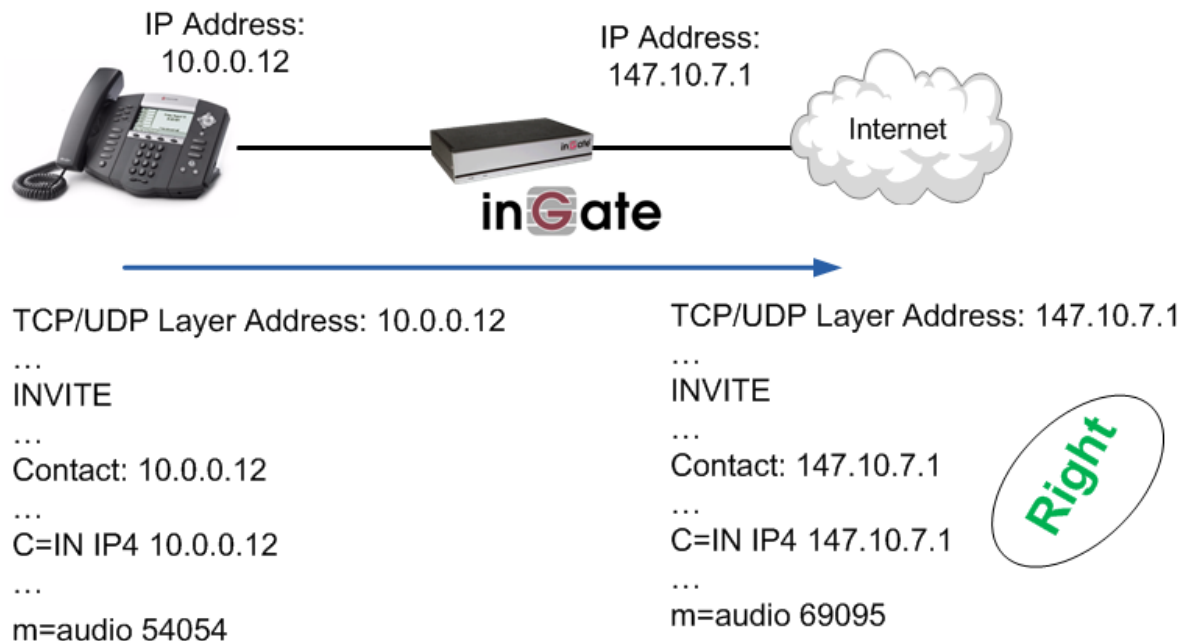
LAN IP Address

Ingate Product Training

Common Deployment Issues

■ Resolution #1 - “NAT BREAKS SIP”

- SIP Protocol requires a SIP Proxy or Application Layer Gateway and NAT
- SIP Proxy (SIP-Aware Firewall) will correct IP Addresses and Port allocation in SIP Protocol from Private LAN addresses to Public WAN address.
- SIP Proxy monitors all SIP Traffic IN and OUT and can apply routing rules



Ingate Product Training

Common Deployment Issues

- After NAT & Ingate
 - TCP/IP Header is Public Space
 - SIP Headers are Private Space

```
⊕ Internet Protocol 207.112.18.164 (207.112.18.164), 9.249.3.59 (209.249.3.59)
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊖ Session Initiation Protocol
⊕ Request-Line: INVITE sip:16139630933@209.249.3.59/2.0
⊖ Message Header
⊕ Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hg4bkb42dfb3914946b8801d52bd5732dc849.0
  Session-Expires: 14400
⊕ Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hg4bk793e9c7e89e6185d673ce730c431ec1e.oshxzb9xTBBjo-novQajpa__
⊕ To: <sip:16139630933@209.249.3.59>
⊕ From: <sip:6037694384@209.249.3.59>;tag=62b412e7
  Call-ID: 30a1d9e8-484d471bd3fc8-2e238874@sigpt-46d4aefa
⊕ CSeq: 1297043244 INVITE
⊕ Contact: <sip:esFNgzVDMneyw5XnKdkvXP2V7noiz_TLY5YXi_JTyGVdcqX80_w4C25fKksdpe:207.112.18.164
  Supported: timer, replaces
  Allow-Events:talk,hold,conference
  Min-SE: 90
  Max-Forwards: 68
  Content-Type:application/sdp
  Content-Length: 249
  Record-Route: <sip:997a280734e1769@207.112.18.164;lr>
⊖ Message Body
⊖ Session Description Protocol
  Session Description Protocol version (v): 0
⊕ Owner/Creator, Session Id (o): 6139630933 1213010017 1552 IN IP4 207.112.18.164
  Session Name (s): SIP Call
⊕ Connection Information (c): IN 207.112.18.164
⊕ Time Description, active time (t): v v
  Session Attribute (a): sendrecv
⊕ Media Description, name and address (m): audio 58534 RTP/AVP 0 8 18 101
```

WAN IP Address

WAN IP Address

WAN IP Address

WAN IP Address

Ingate Product Training

Common Deployment Issues

- **Ingate Benefits - “NAT BREAKS SIP”**
 - Ingate products are ICSA Certified VoIP Firewalls
 - Ingate have a SIP Proxy, SIP B2BUA and NAT working together
 - Ingate SIParator can bring enhance the SIP capabilities and SIP security of an existing Firewall
 - Ingate can provide “Far End NAT Traversal” functionality
- What Other IP-PBXs Vendors Do
 - Most all IP-PBX vendors recommend the use of some sort of “SIP-Aware Firewall” for deployment
 - Other recommend the use of Port Forwarding, to forward Port 5060 and a thousand other Ports to the IP-PBX –
HUGE SECURITY RISK!!



Ingate Product Training

Common Deployment Issues

■ Problem #2 – SIP Interoperability

- Not all SIP is the same
 - One vendors implementation may not be the same as another
 - There are many SIP components and extensions that may be supported on one vendors equipment and not on another
 - SIP Protocol is an open standard and can be left to interpretation by each vendor
- Examples
 - Use of REFER Method is not typically supported by ITSP
 - Use of INVITE with Replaces Header is not typically supported by ITSP
 - Some ITSPs don't like SDP with "a=Inactive" attribute
 - ENUM SIP URI Delivery is supported by some and not by others
 - Various TO and FROM Header conformances
 - Alternate SIP Domain routing requirements

Ingate Product Training

Common Deployment Issues

- **Resolution #2 – SIP Interoperability**
 - Testing and Development for each Vendor
 - Extensive Testing and Development time devoted to each vendor integration to ensure complete interoperability – a huge undertaking
 - Customization and Flexibility development for each Vendor integration
 - SIP Connect Compliance
 - Adherence to SIP Forum – SIP Connect Compliance, governing body of SIP Trunking deployments and standards

Ingate Product Training

Common Deployment Issues

■ Ingate Benefits – SIP Interoperability

- In General,
 - Can rewrite headers commonly needing changed between vendors
 - Provide SIP Protocol error checking and fixes Protocol non-conformances
 - Routing Rules and Policies to direct traffic
 - Contains extensive list of features devoted to SIP non-conformances customization
- Ingate contains a B2BUA
 - Separates the call between the two parties, helping separate two different implementations of SIP
 - Provides Client or Server User Accounts for Registration and Authentication
 - Separate SIP Method Handling between two parties

Ingate Product Training

Common Deployment Issues

■ Problem #3 – SIP Security

- SIP is written in clear text within the datagram of a UDP or TCP Transport.
- Confidential User/SIP URI Information
 - A SIP URI is like an Email Address, once someone has it, they know who you are and where you are located.
 - The malicious person or software can send SIP Request after SIP Request to your SIP URI. Some malicious uses like DoS Attacks, SPIT Attacks, Intrusion of Services, Toll Fraud, Tele-marketers and more.
 - Called and Calling Party Number Information
- Private LAN Network Address Scheme
 - Giving away the confidential Private IP Address scheme of the internal LAN network, gives malicious attackers knowledge of the internal configuration of the Enterprise.
 - The Port being used on the device, gives malicious attackers where to direct traffic
- Media Attributes
 - Easy to see what Media is being negotiated and where its going

Ingate Product Training

Common Deployment Issues

■ Why is SIP Insecure?

- Written in clear text within the datagram of a UDP or TCP Transport.

```
⊕ Internet Protocol (207.112.18.164 (207.112.18.164), 9.249.3.59 (209.249.3.59))
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊖ Session Initiation Protocol
  ⊕ Request-Line: INVITE sip:1613963093@10.51.77.1 P/2.0
  ⊖ Message Header
    ⊕ Via:SIP/2.0/UDP 10.51.77.60:5060;rport;branch=z9hG4bKeda59e3
  From:"Scott Beer" <sip:6139630933@10.51.77.1>184d0eda-186-6c1b36c8
  To:<sip:16139630933@10.51.77.1>
    ⊕ Contact:"Scott Beer" <sip:613963093@10.51.77.60;transport=UDP>
      Call-ID:eda0000-2da6d41@10.51.77.1
    ⊕ CSeq:701887483 INVITE
      User-Agent:Mitel-5340-SIP-Phone Fw.07.41.02 08000F314048
      Allow:INVITE,ACK,CANCEL,BYE,OPTIONS,REFER,NOTIFY,PRACK,UPDATE
      Allow-Events:talk,hold,conference
      Supported:timer,100rel,replaces
      Session-Expires: 1800
      Max-Forwards: 70
      Content-Type:application/sdp
      Content-Length: 249
  ⊖ Message Body
    ⊖ Session Description Protocol
      Session Description Protocol version (v): 0
      ⊕ Owner/Creator, Session Id (o): 6139630933 1213010017 1213010016 IN IP4 10.51.77.60
      Session Name (s): SIP Call
      ⊕ Connection Information (c): IN IP4 10.51.77.60
      ⊕ Time Description, active time (t): 0 0
      Session Attribute (a): sendrecv
      ⊕ Media Description, name and address (m): audio/20282 TP/AVP 0 8 18 101
```

Confidential User Information

Confidential SIP URI of the User

Confidential Equipment

MIME Content

LAN IP Address and Port Information

Media Attributes

Ingate Product Training

Common Deployment Issues

■ Common SIP Attacks

■ Intrusion of Services

- Devices attempting Register with a IP-PBX in an attempt to look like an IP-PBX extension and gain IP-PBX services
- SPIT (SPAM over Internet Telephony)

■ Toll Fraud

- A form of an Intrusion of Service, where malicious attempts to send INVITEs to an IP-PBX to gain access to PSTN Gateways and SIP Trunking to call the PSTN

■ Denial of Service

- INVITE (or any SIP Request) Flood in an attempt to slow services or disrupt services
- Or any UDP or TCP traffic directed at a SIP Service on SIP Ports

■ Indirect Security Breaches

- Private LAN IP Address and infrastructure are now made public, and can be used in attacks to other non-SIP areas

Ingate Product Training

Common Deployment Issues

■ Resolution #3 – SIP Security

- Dynamic Encryption of SIP URI
 - Using the SIP Specification, enforce an Encrypted SIP URI where possible
- Dynamic Port Allocation
 - Dynamically change ports on every call.
- Hide LAN IP Address Scheme
 - Apply LAN to WAN Network Address Translation within the SIP Signaling
- TLS and SRTP
 - TLS Transport provides complete encryption of SIP Signaling
 - SRTP provides encryption of RTP Media
- IDS/IPS for SIP Protocol
 - SIP Protocol specific Intrusion Detection Systems and Intrusion Prevention Systems allow for monitoring and statistics of all SIP Traffic, and apply rules and policies based on the traffic
- Traffic Routing Rules and Policies
 - IP Address Authentication, SIP URI Validation, and Routing Rules

Ingate Product Training

Common Deployment Issues

■ How to make SIP Secure

```
⊕ Internet Protocol, src(207.112.18.164) dst(207.112.18.164)
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊕ Session Initiation Protocol
  ⊕ Request-Line: INVITE sip:+1613963093@216.82.225.202 IP/2.0
  ⊕ Message Header
    ⊕ Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hG4bkbde001c8359d69da57625a8c701c6b3f.0
      Session-Expires: 14400
    ⊕ Via: SIP/2.0/UDP 207.112.18.164:5060;branch=z9hG4bke799f42397fe6b4dd98fcb5892ff0108.37100MV
    ⊕ To: <sip:+16139630933@216.82.225.202>
  From: "Scott Beer" <sip:6139630933@216.82.225.202>;i=4cabc24e
  Call-ID: 7f07a097-48b85d747273e-19d93dab@sipgate-2210018d
  ⊕ CSeq: 150055158 INVITE
  User-Agent: Ingate-Firewall/4.6.2
Contact: <sip:Eawid3EuJ5irvUuqE@207.112.18.164>
  Supported: timer, replaces
  Subject: sip phone call
  Allow-Events: talk, hold, conference
  Min-SE: 90
  Max-Forwards: 68
  Content-Type: application/sdp
  Content-Length: 248
  Record-Route: <sip:6b8f8d674fe4888@207.112.18.164;lr>
⊕ Message Body
  ⊕ Session Description Protocol
    Session Description Protocol Version (v): 0
    ⊕ Owner/Creator, Session Id (o): 6139630933 1220028525 305 IN IP4 207.112.18.164
    Session Name (s): SIP Call
    ⊕ Connection Information (c): IN I 207.112.18.164
    ⊕ Time Description, active time (t): 0 0
    Session Attribute (a): sendrecv
    ⊕ Media Description, name and address (m): audio 58200 RTP/AVP 0 8 18 101
    ⊕ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊕ Media Attribute (a): rtpmap:8 PCMA/8000
    ⊕ Media Attribute (a): rtpmap:18 G729/8000
    ⊕ Media Attribute (a): rtpmap:101 telephone-event/8000
```

TLS to Encrypt
all SIP Signaling

Hidden IP in User
Information

Hidden Internal
Vendor

Encrypted
SIP URI

Firewall Filters on
MIME Content

Hidden LAN IP
Information

SRTP to Encrypt
all RTP Media

Dynamic Port
Allocation

Ingate Product Training

Common Deployment Issues

- **Ingate Benefits – SIP Security**
 - Dynamic Encryption of SIP URI
 - Dynamic Port Allocation
 - Hide LAN IP Address Scheme
 - TLS and SRTP
 - IDS/IPS for SIP Protocol
 - Traffic Routing Rules and Policies

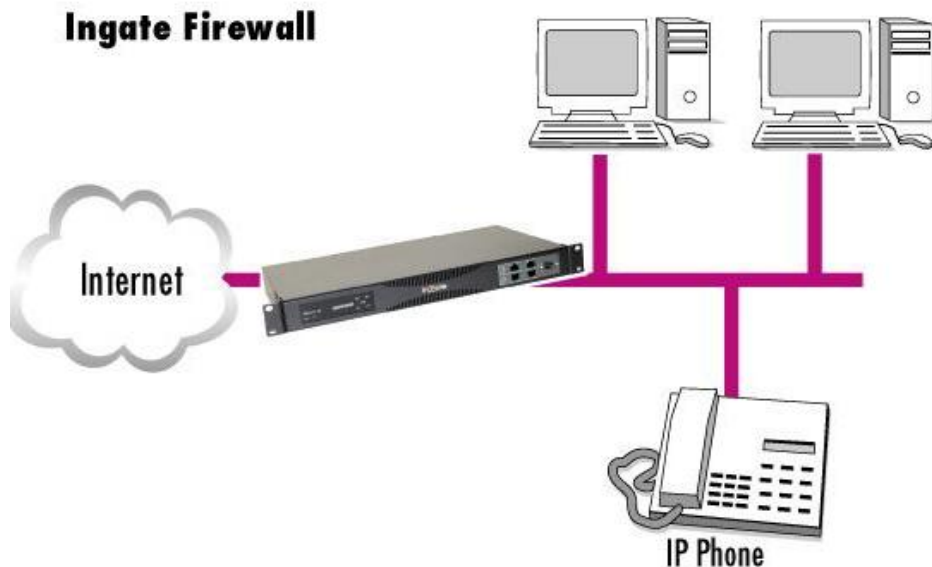
- Ingate products are ICSA Certified VoIP Firewall
- Ingate is focused on providing SIP Security

Introduction to Ingate Products

Ingate products

Firewalls

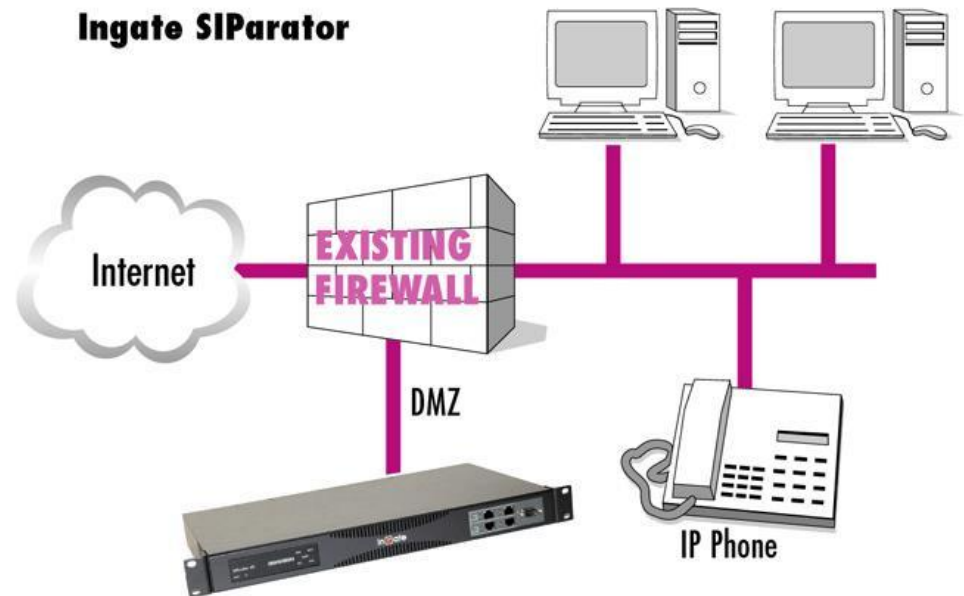
SIP-capable firewalls for computer security and communication



New and replacement installations

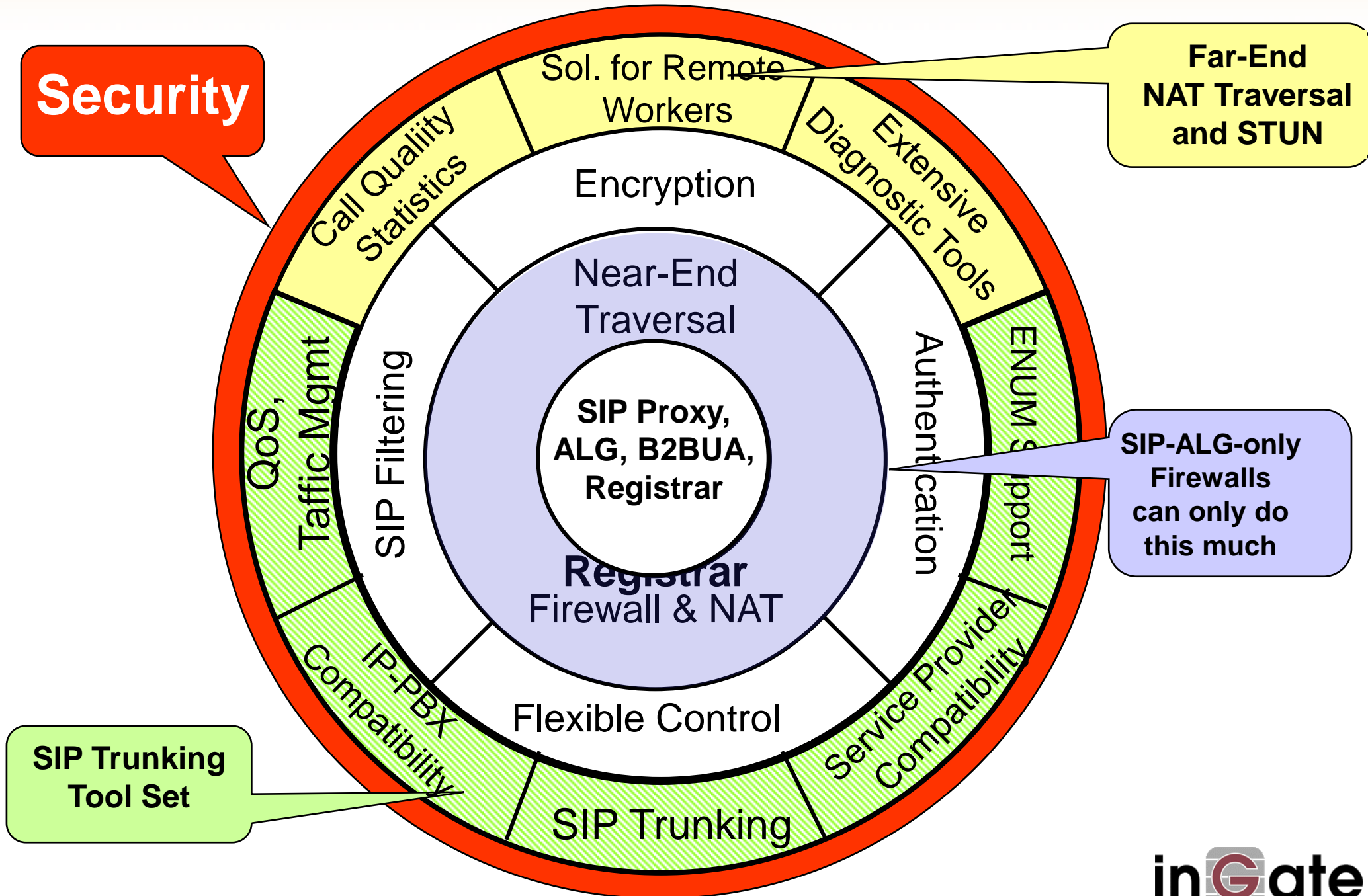
SIParator™

SIParator™ - Add-on to existing firewalls to enable SIP communication

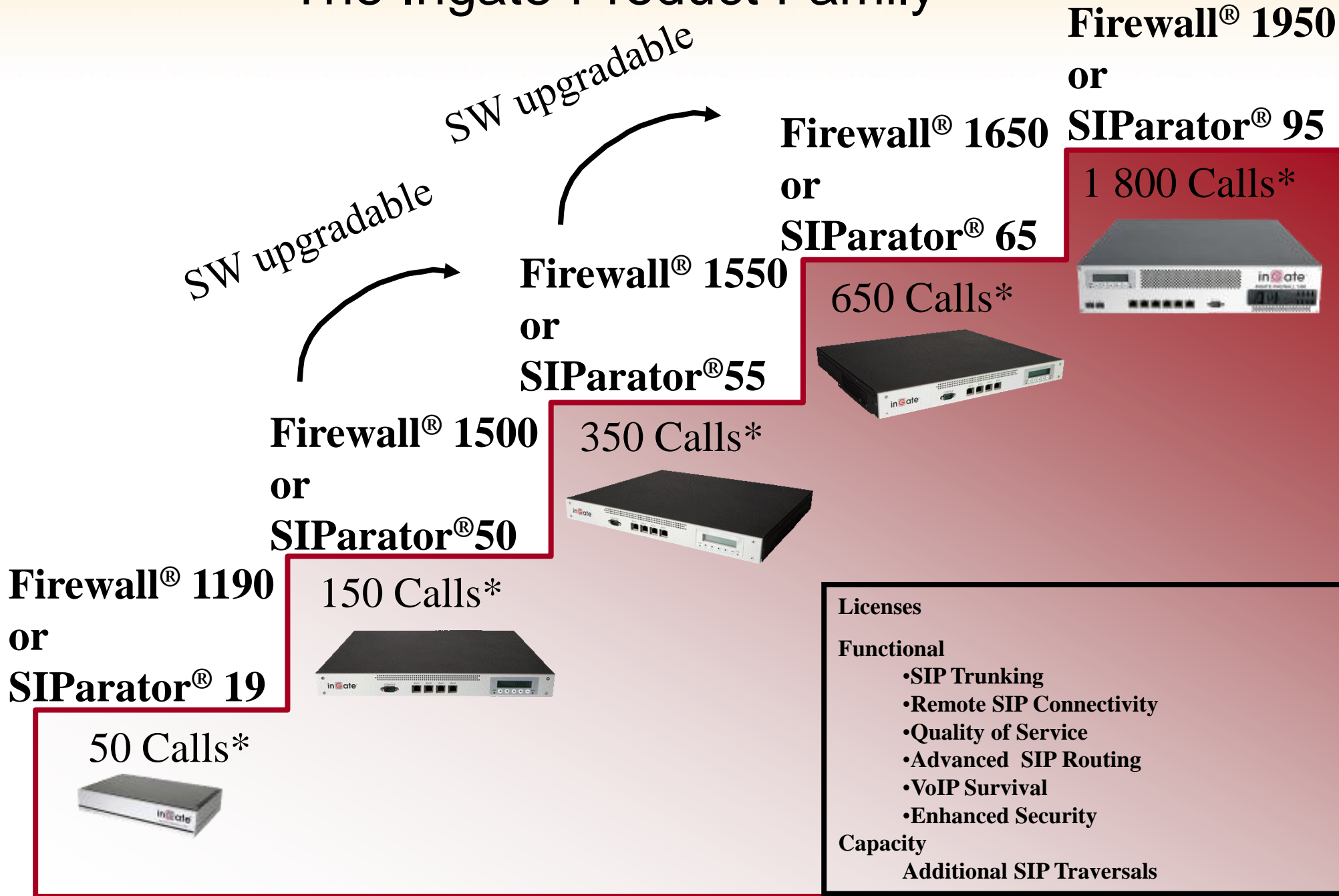


Preserve firewall investment and keep established security policies

Extensive SIP Feature Set



The Ingate Product Family

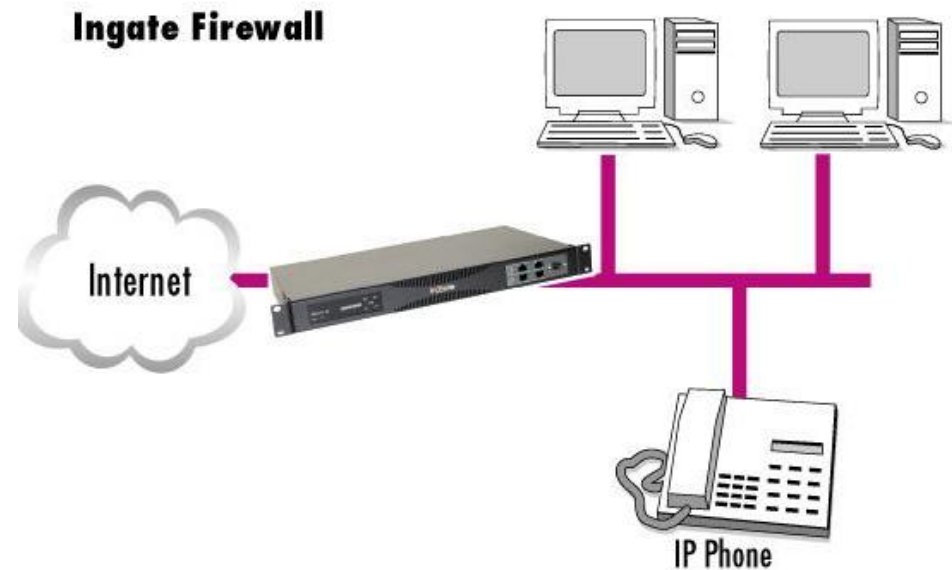


- Licenses**
- Functional**
- SIP Trunking
 - Remote SIP Connectivity
 - Quality of Service
 - Advanced SIP Routing
 - VoIP Survival
 - Enhanced Security
- Capacity**
- Additional SIP Traversals

* Calls = Maximum Concurrent RTP Sessions = SIP Trunks

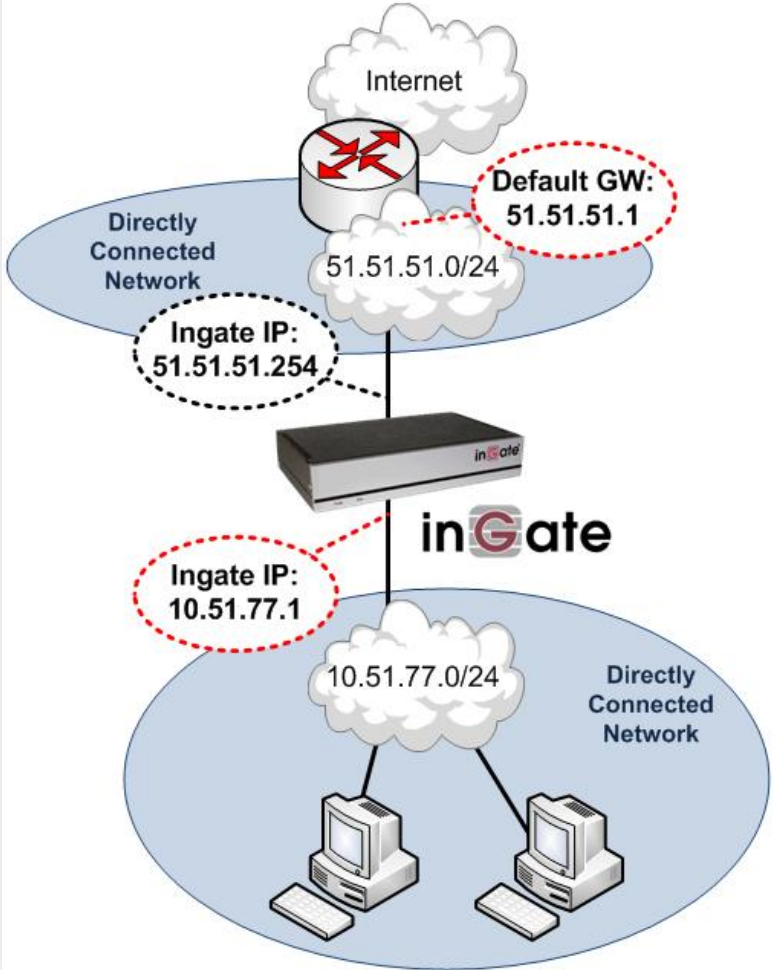
Connecting the Firewall

- Ingate Firewall
 - Handles All Data Traffic
 - Provides NAT
 - Protocol Service Rules
 - Data Traffic Relays
 - VPN (IPsec) Tunnels
 - PPTP Tunnels
 - DMZ Networks (multiple networks)
 - Default Gateway of the LAN
 - DHCP Server
 - SIP Session Border Controller

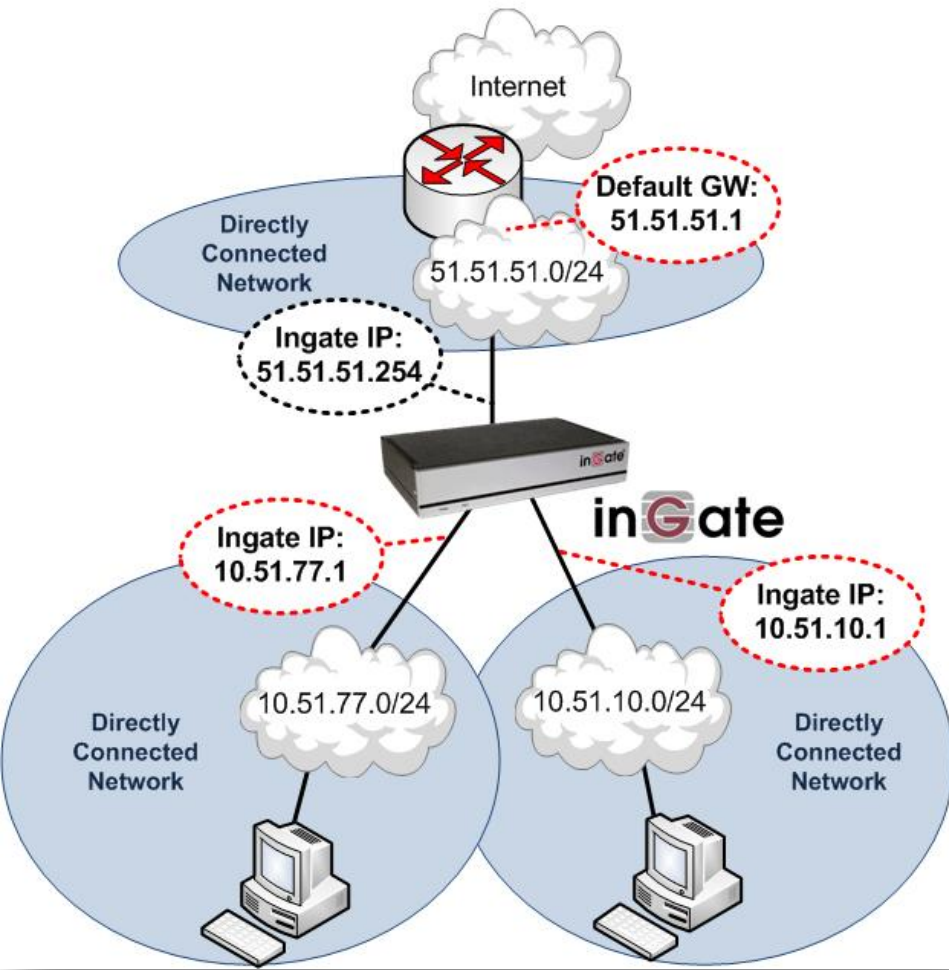


Connecting the Firewall

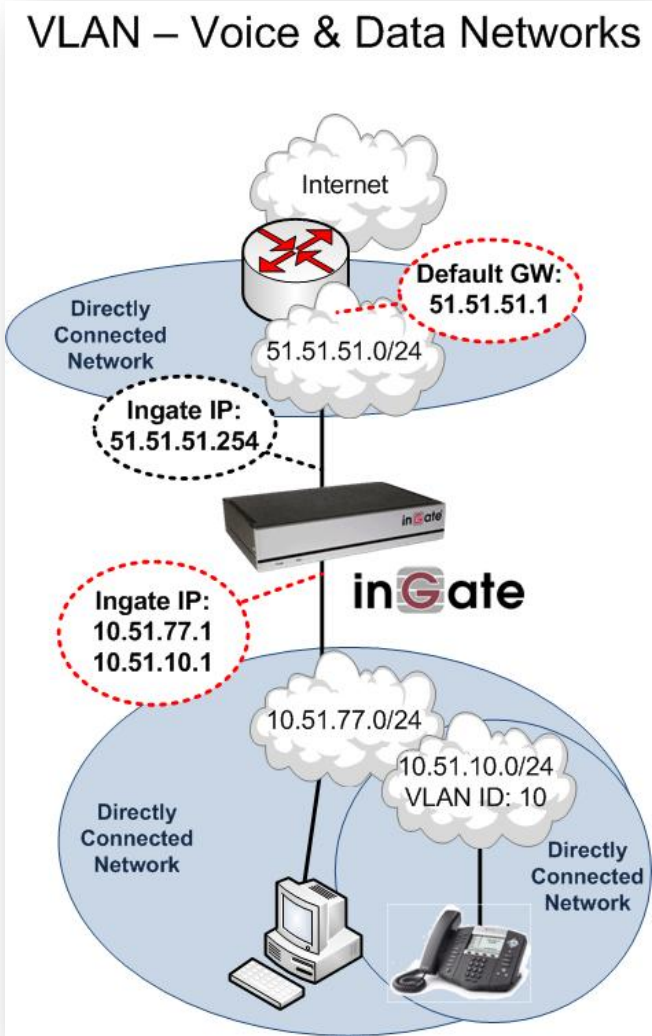
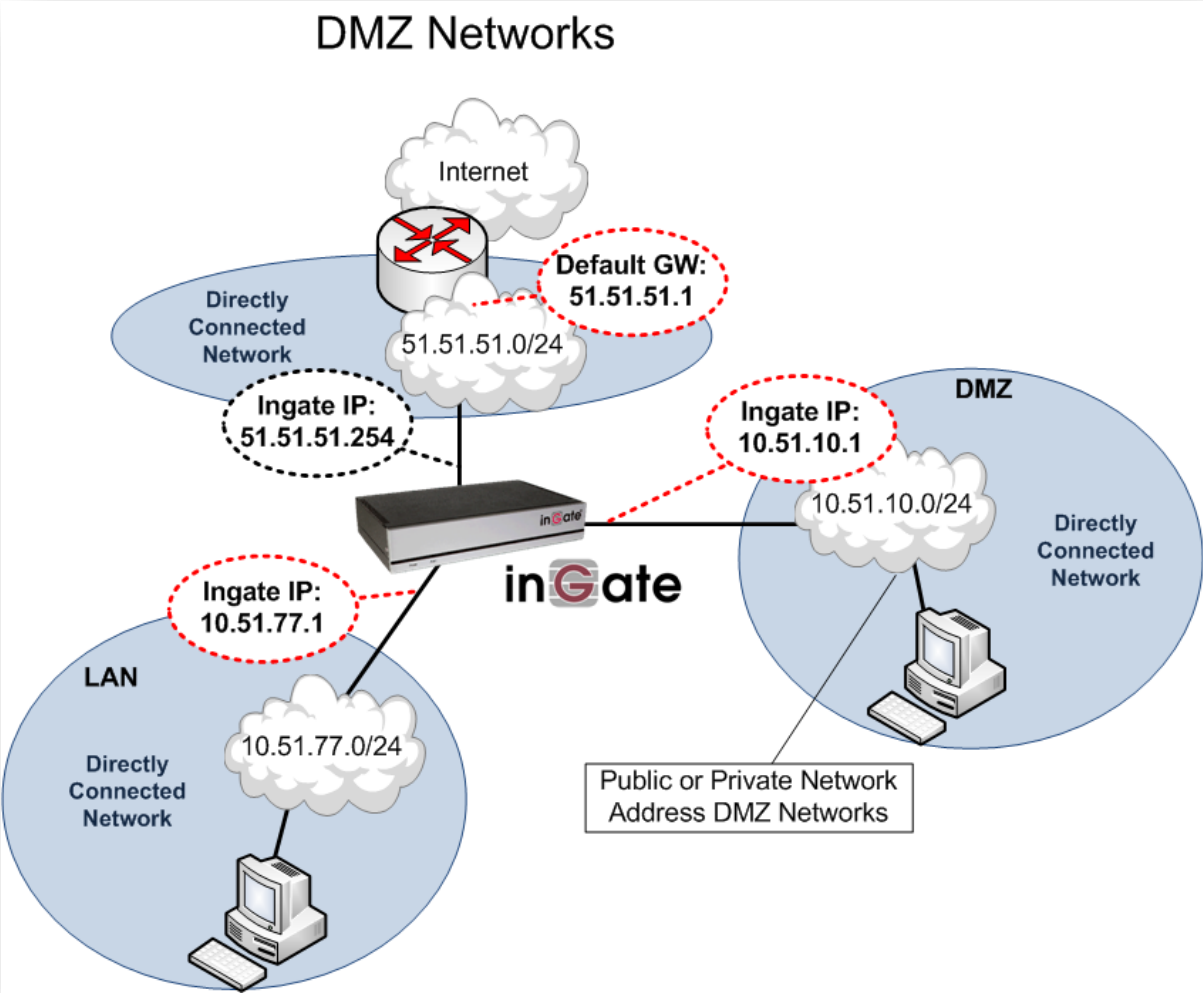
Network Address Translation (NAT)



Firewall Two LAN Networks

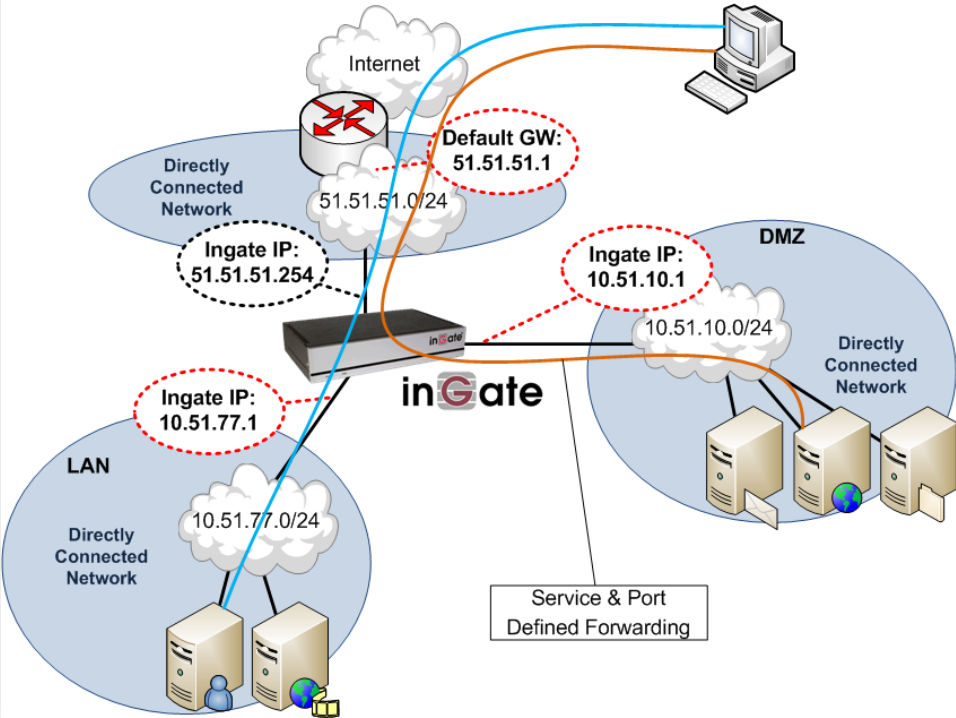


Connecting the Firewall

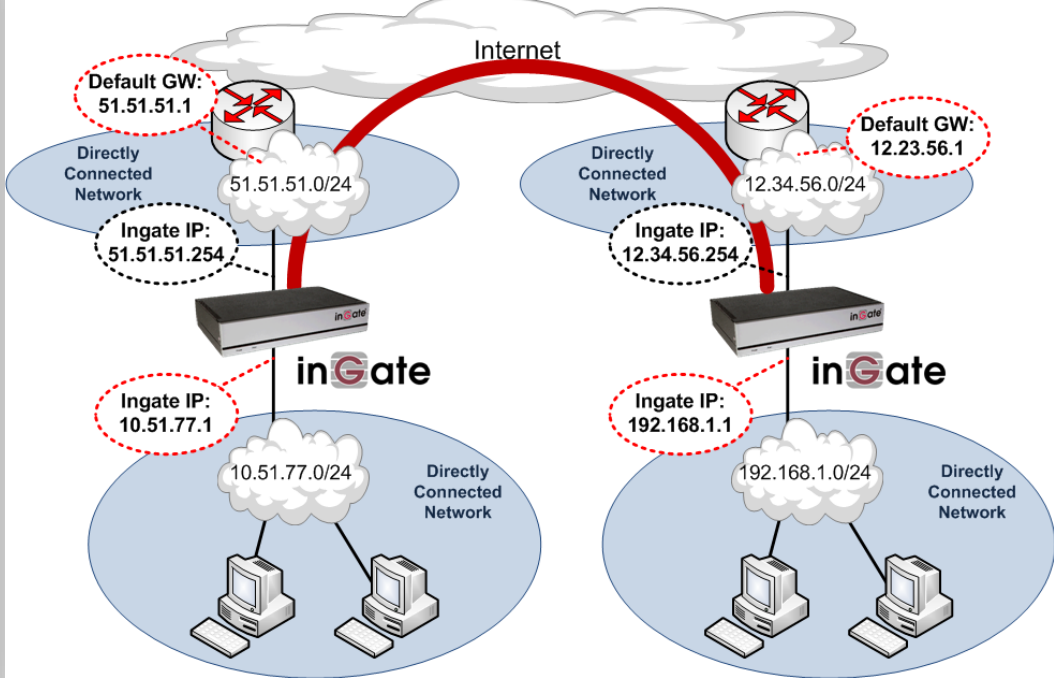


Connecting the Firewall

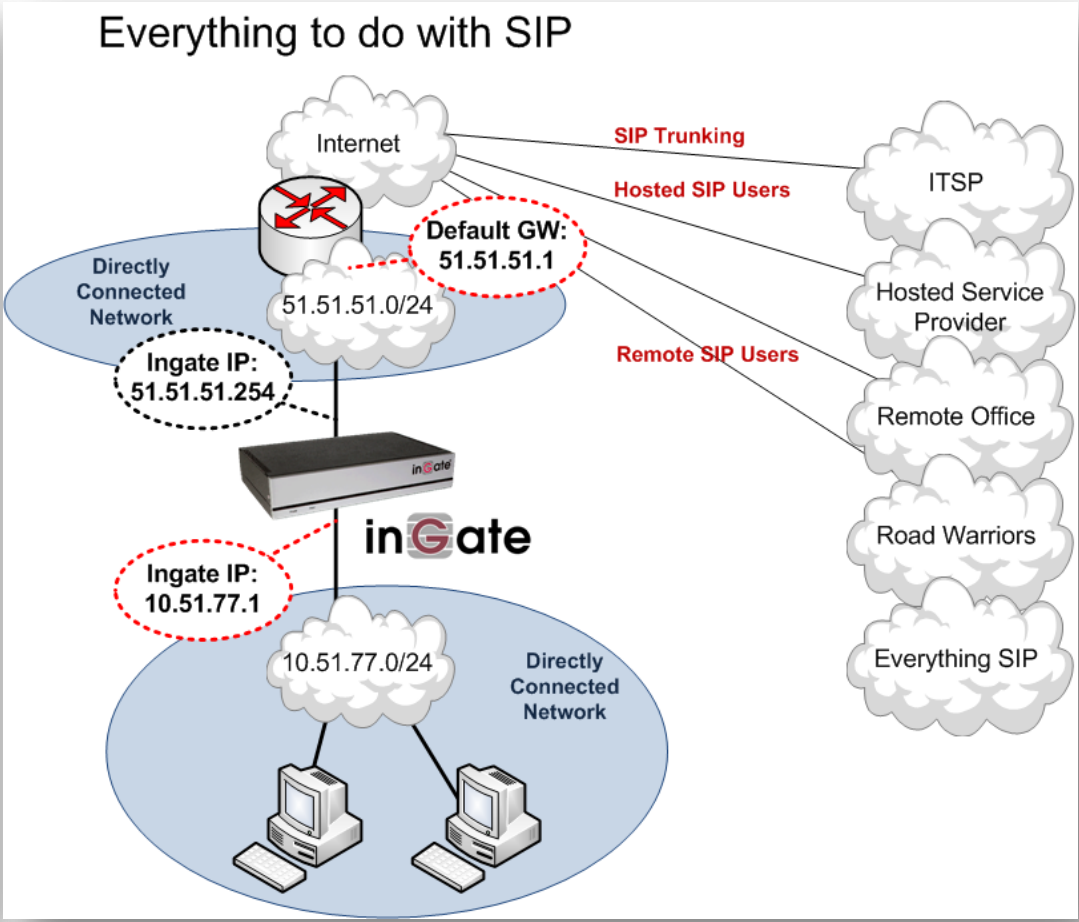
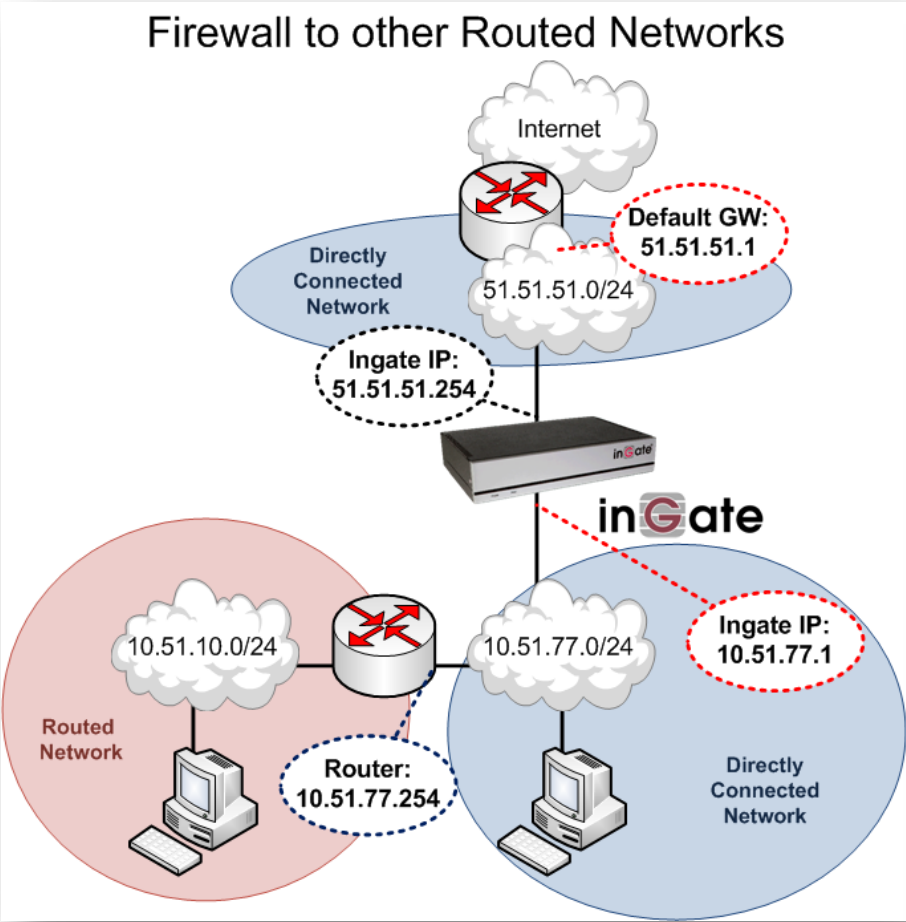
Rules & Relays



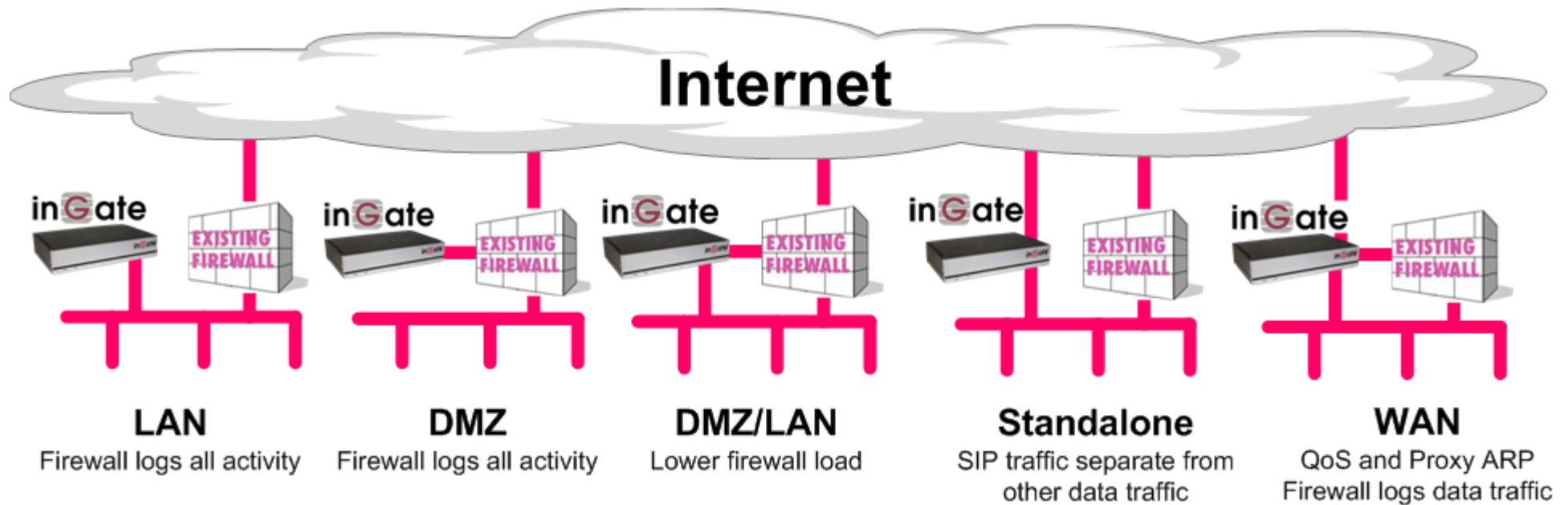
VPN Tunnel



Connecting the Firewall



Connecting the SIParator®

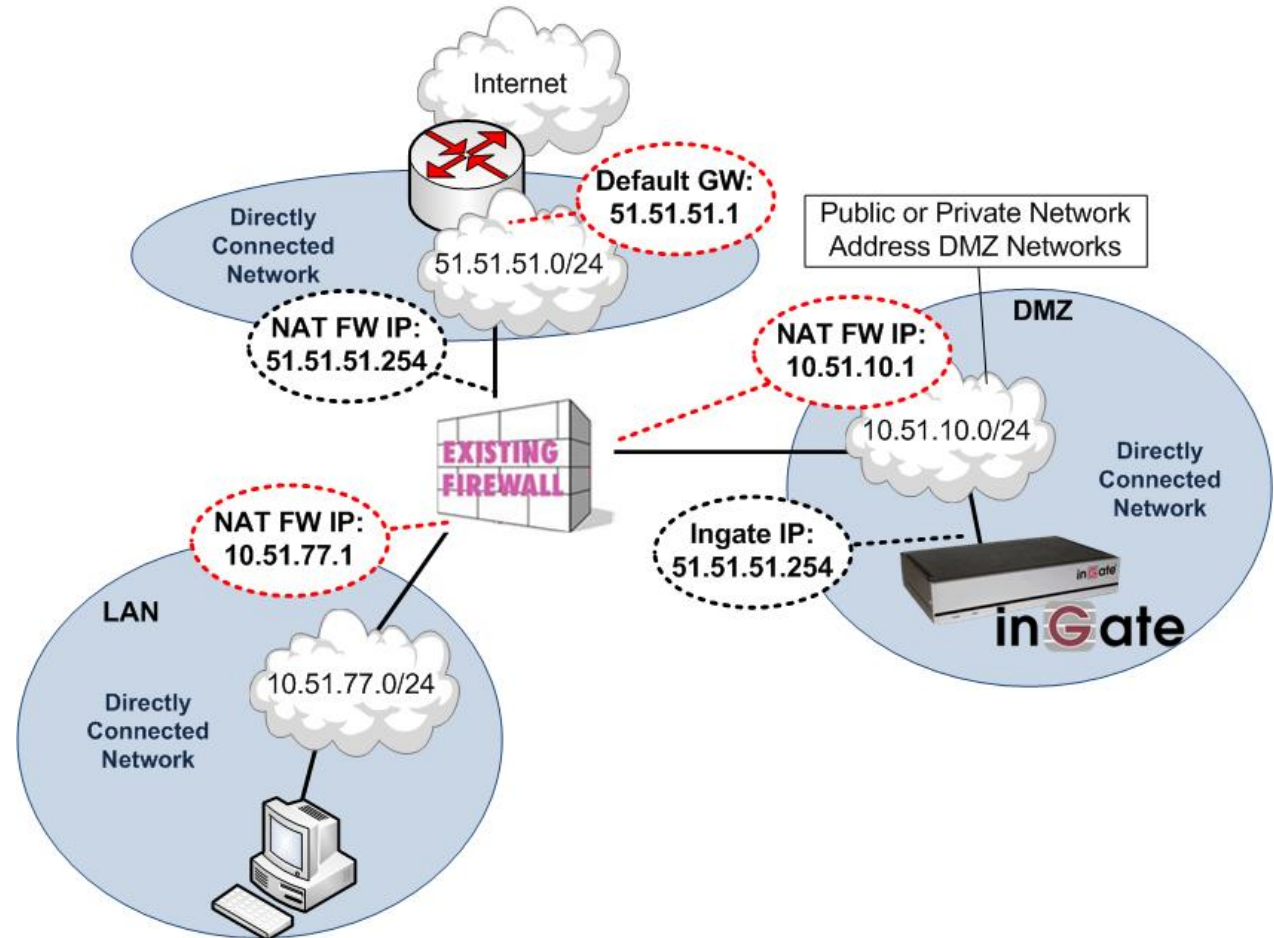


- Existing Firewall
 - Port Forward 5060
 - Port Forward Media Port range

Connecting the SIParator®

SIParator Deployment: DMZ

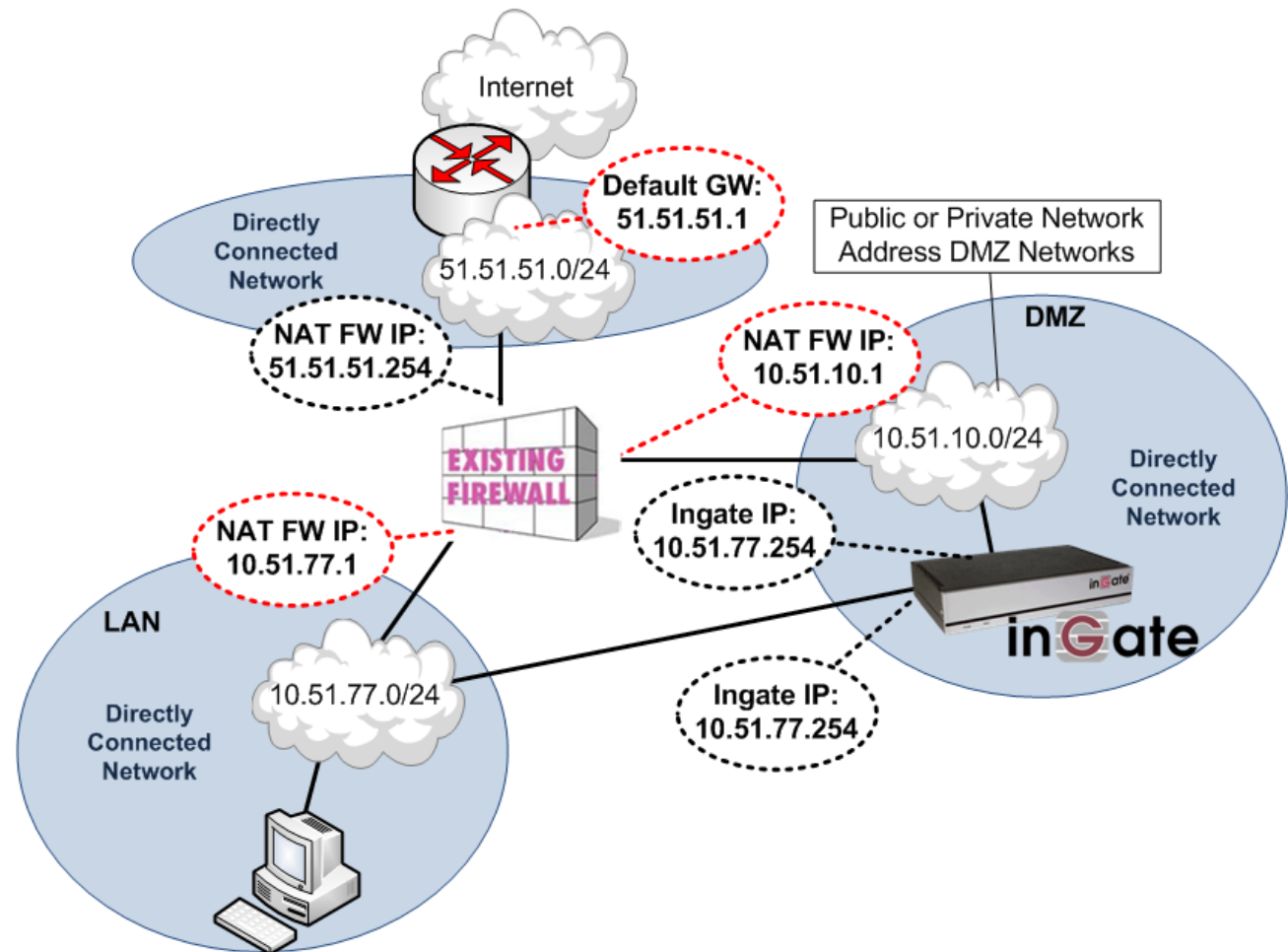
- NAT FW needs to Port FWD from Internet to DMZ and again from DMZ to LAN
- Increases number of Network hops
- Very Secure
- Ingate needs to know WAN IP address



Connecting the SIParator®

- NAT FW needs to Port FWD from Internet to DMZ
- Decreases Network hops
- Very Secure
- Ingate needs to know WAN IP address

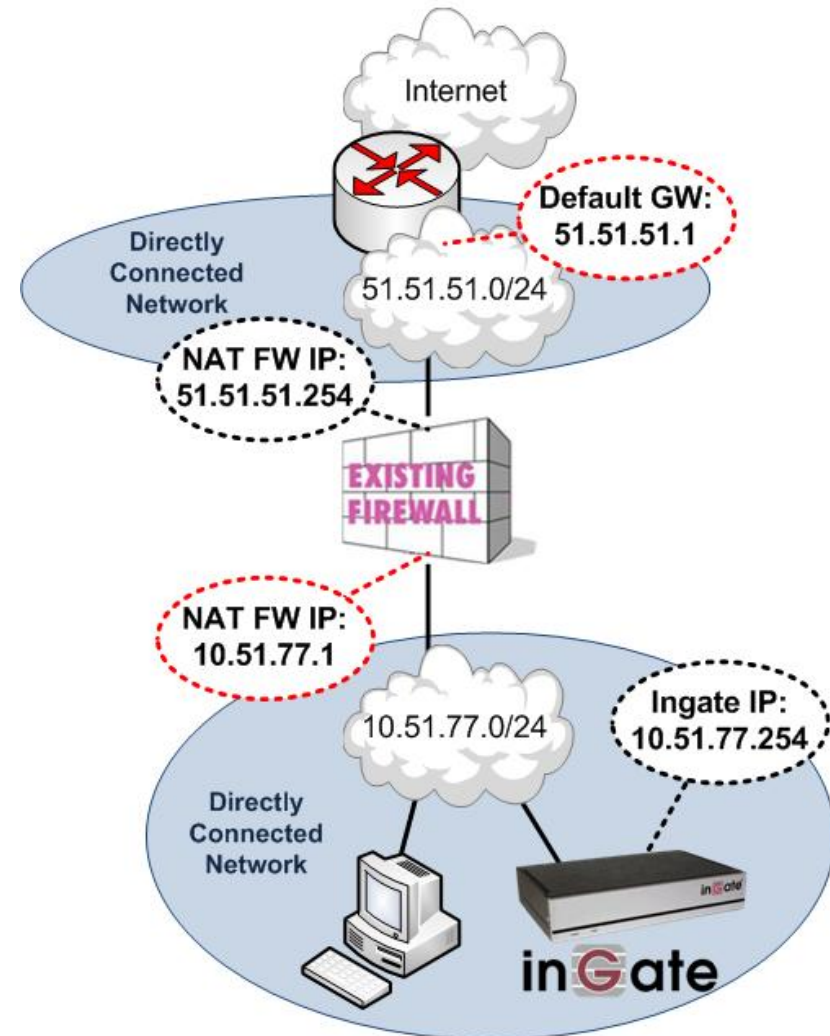
SIParator Deployment: DMZ-LAN



Connecting the SIParator®

- NAT FW needs to Port FWD from Internet to LAN
- Decreases Network hops
- Least Secure
- Ingate needs to know WAN IP address

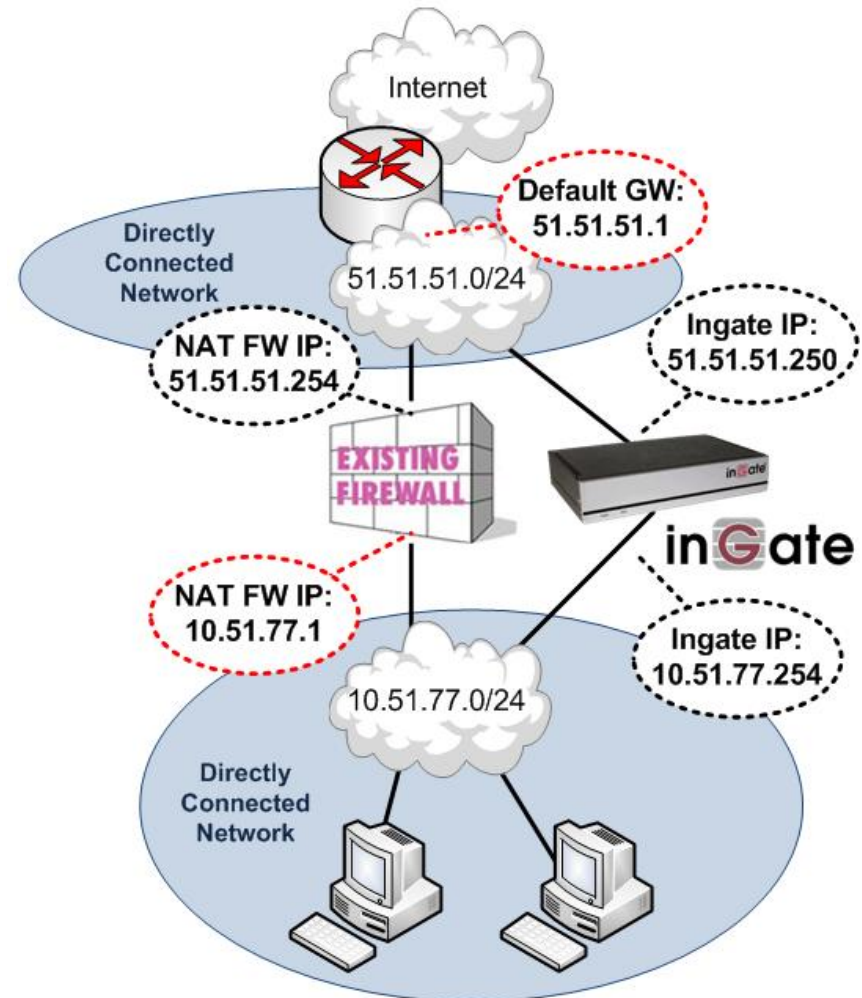
SIParator Deployment: LAN



Connecting the SIParator®

- Ingate has its own Public IP address
- One Network hop
- Very Secure
- Reduces impact to NAT FW
- No NAT FW setup required

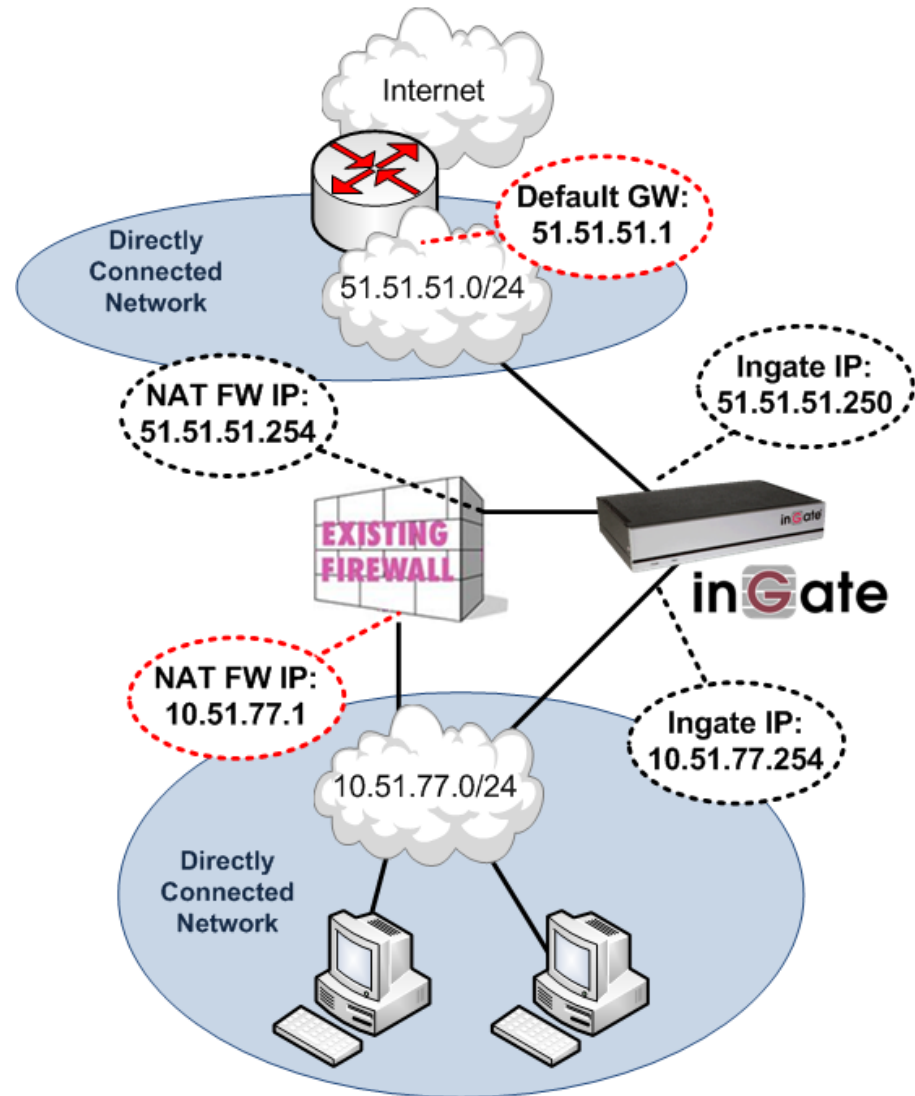
SIParator Deployment: Stand-alone



Connecting the SIParator®

- Ingate has its own Public IP address
- NAT FW has its own IP address
- Ingate adds QoS and Traffic Shaping
- Very Secure
- No NAT FW setup required

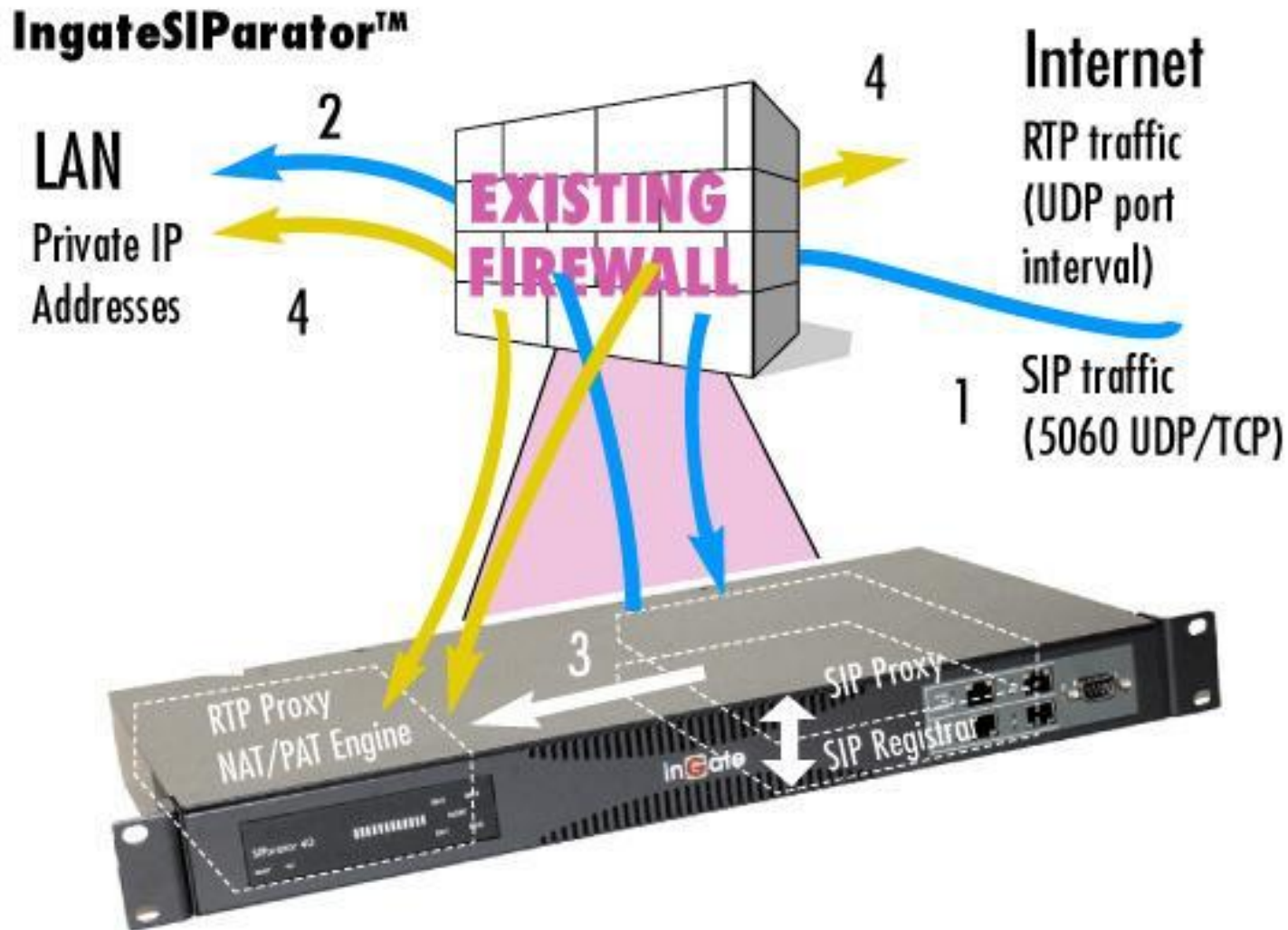
SIParator Deployment: WAN



How Does It Work?

- **SIP Proxy**
 - Stateful Proxy redirects calls
 - NAT/PAT for UDP/TCP/TLS and SIP
- **SIP B2BUA**
 - Rewrites Request URIs, Domains, and other Headers
- **SIP Registrar / Client**
 - Can Register to ISTRP, and provide a Registrar for SIP Clients
- **SIP Media Relay**
 - Can ensure media is directed in/out
 - Dynamically open and close ports for security

Ingate SIParator®



Optional Modules

- The SIP functionality in Ingate Firewalls and SIParators has several software extension modules.
 - Remote SIP Connectivity
 - SIP Trunking
 - Advanced SIP Routing
 - VoIP Survival
 - Extended SIP Security
 - Quality of Service

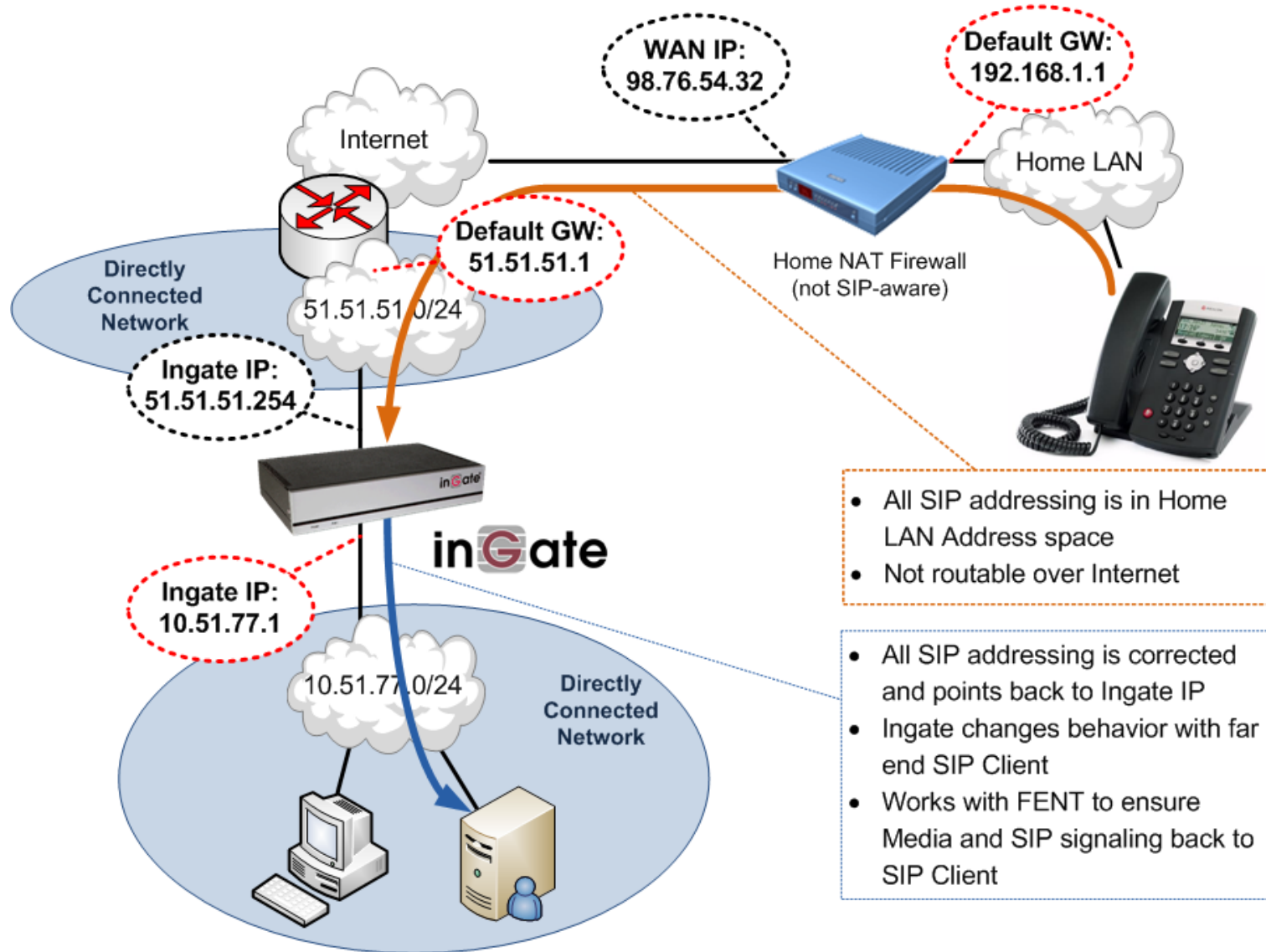
Optional Modules

Remote SIP Connectivity

- Manages SIP clients behind NAT boxes which are not SIP-aware
- Solves far-end NAT traversal
- Includes a STUN server

Optional Modules

Remote SIP Connectivity Far End NAT Traversal (FENT)



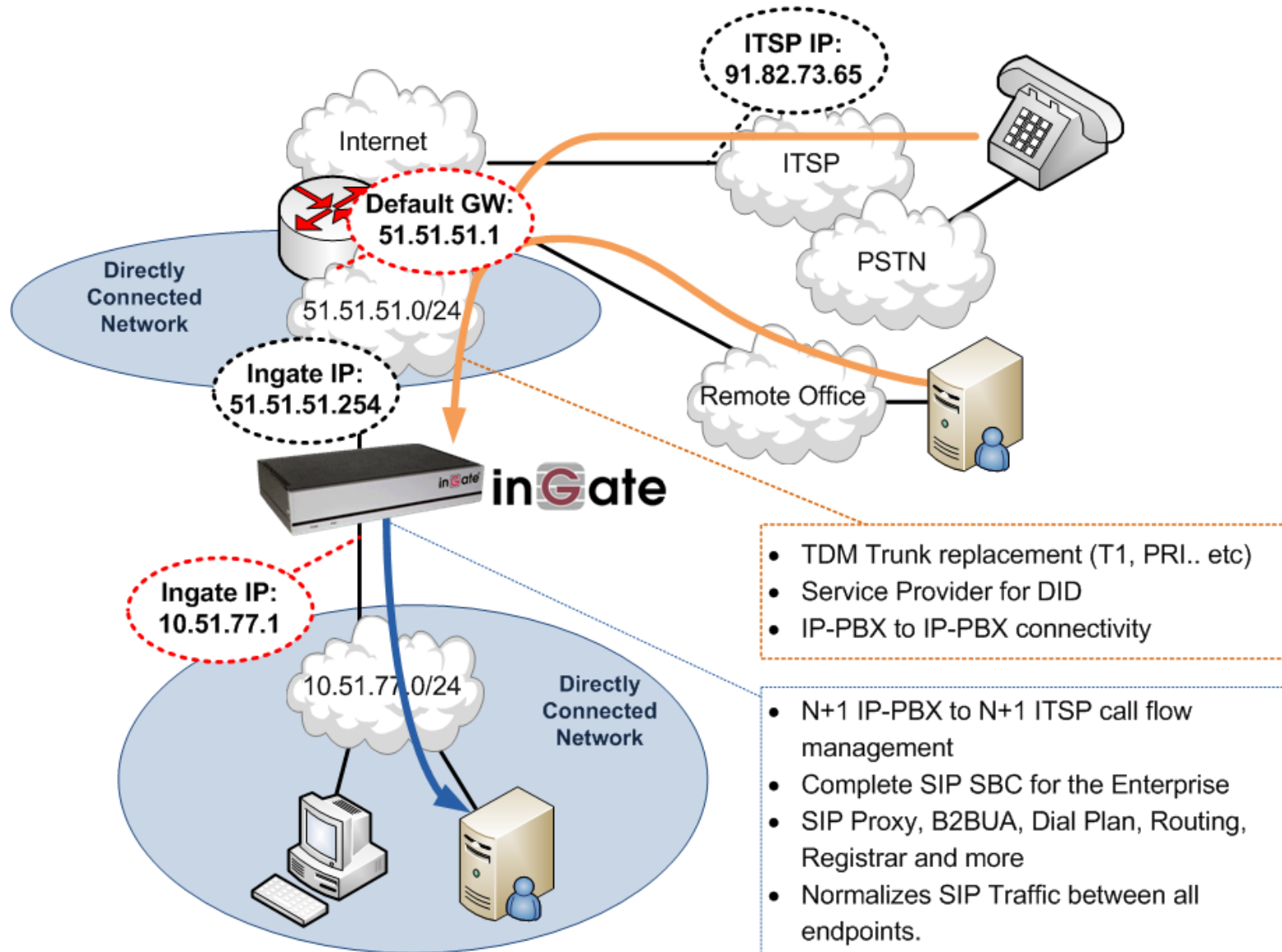
Optional Modules

SIP Trunking

- Lets the administrator rewrite the entire or part of a SIP URI before the request is passed on
- Redirects requests based on From header, Request-URI and originating network
- Adds features to make the firewall register on behalf on clients
 - Local Registrar, B2BUA, Proxy, extensive Dial Plan & Routing features.

Optional Modules

SIP Trunking



Optional Modules

VoIP Survival

- Monitors one or more remote SIP servers
- Useful for branch offices which uses a SIP server at the main office
- When the remote SIP server is down, the firewall:
 - Acts as registrar for the monitored SIP domain
 - Manages local calls
 - Redirects PSTN calls to a local PSTN gateway
 - Manages outgoing calls to other SIP domains

Optional Modules

Extended SIP Security

- Contains features such as:
 - IDS/IPS
 - Makes it possible to block SIP traffic due to various conditions
 - Traffic exceeds a given rate limit
 - Packets match specified criteria
 - TLS and SRTP

Advanced SIP Routing

- Create hunt groups, aliases and other user-based features

Break – 10 minutes

Ingate Startup Tool

Ingate Startup Tool

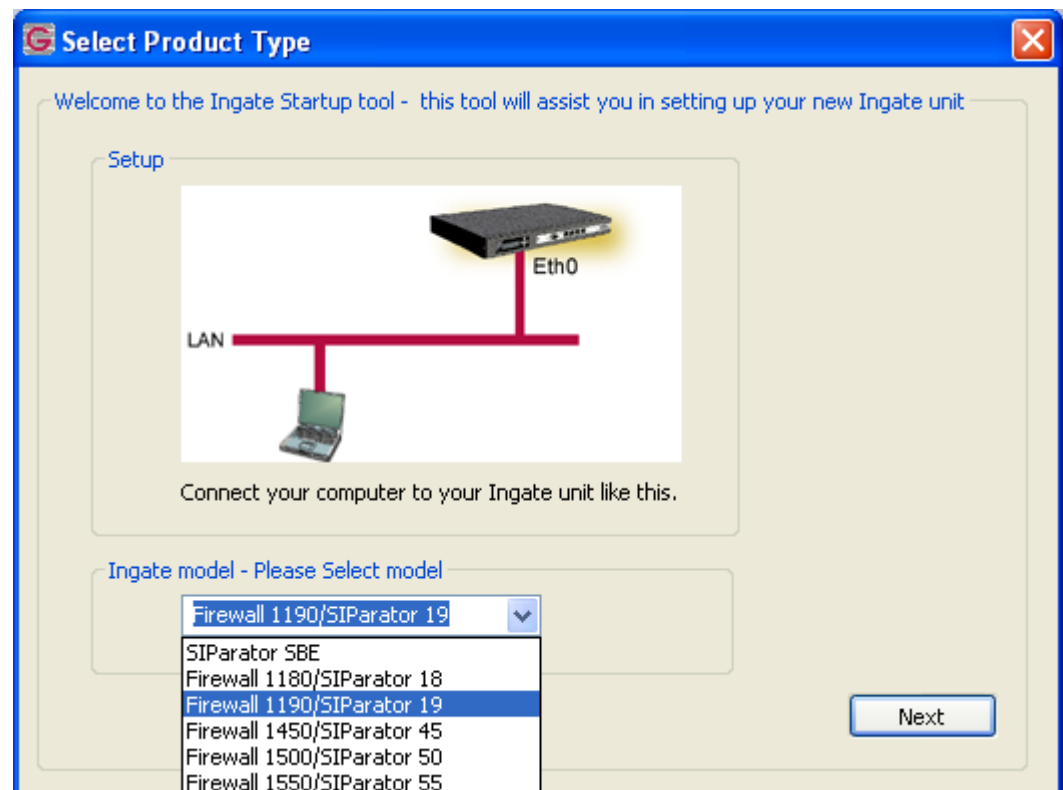
Startup Tool

- “Out of the Box” setup and commissioning of the Firewall and SIParator products
- Update current configuration
- Product Registration and unit Upgrades, including Software and Licenses.
- Automatic selection of ITSP and IP-PBX
- Backup of Startup Tool database
- Located at www.ingate.com **FREE!**

Ingate Startup Tool

Startup Tool - Product Type

- Select the Ingate Model



Ingate Startup Tool

Startup Tool Title Reference

- Configure the unit for the first time
- Change or update configuration
- Register the unit
- Backup the config

- IP/MAC Address
- Password

The screenshot shows the 'Ingate Startup Tool' window with the following sections:

- Ingate Startup Tool Version:** You are running the latest version of this tool.
- Help:** A 'Help' button is present.
- First select what you would like to do:**
 - Configure the unit for the first time
 - Change or update configuration of the unit
 - Check SIP configuration and logs
 - Register this unit with Ingate
 - Upgrade this unit
 - Enable SIP module
 - Configure Remote SIP Connectivity
 - Configure SIP trunking
 - Backup the created configuration
 - Create a config without connecting to a unit
 - This tool remembers passwords
- Establish contact:**
 - Inside (Interface Eth0):** IP Address: 0 . 0 . 0 . 0
 - Enter the password:** Password: []
 - Contact:** A 'Contact' button is present.
- Status:** Ingate Startup Tool Version 2.3.6, connected to: Ingate Firewall 1190, IG-092-719-5012-4
- Configuration Summary:**
 - Remote SIP Connectivity
 - VPN
 - QoS
 - Enhanced Security
 - 15 SIP Traversal Licenses
 - 20 SIP User Registration Licenses
 - Software Version: 4.6.2
 - Error: Please enter an IP address to your provider.
 - Error: Please enter an IP address to your provider.

Ingate Startup Tool

Startup Tool - Network Topology

- Firewall or SIParator deployment type
- Inside (Eth0) - Private
- Outside (Eth1) - Public
- Default Gateway
- DNS Server

The screenshot displays the 'Ingate Startup Tool' window with the 'Network Topology' tab selected. The interface includes the following sections:

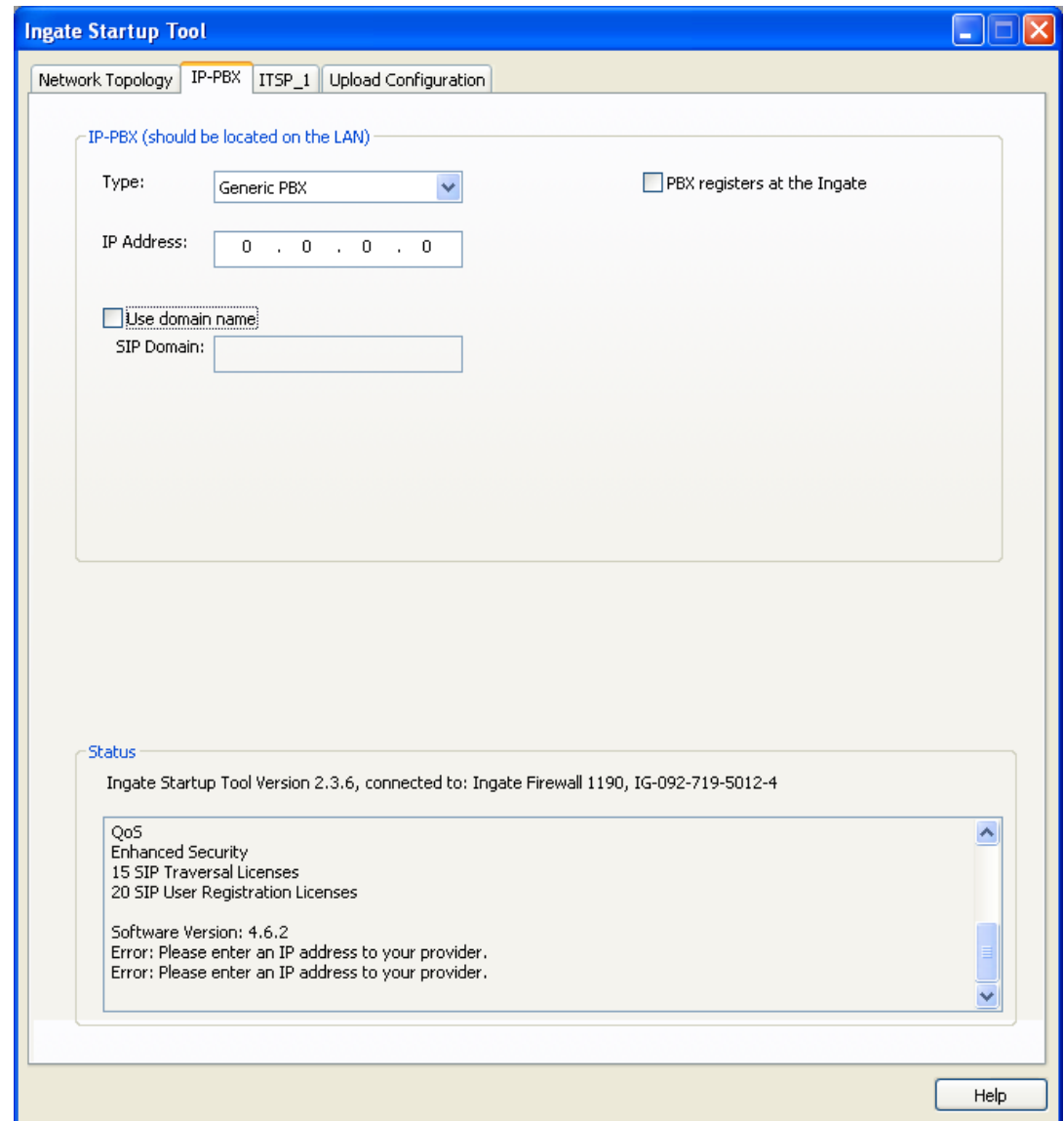
- Product Type:** Standalone SIParator
- Inside (Interface Eth0):**
 - IP address: 10 . 51 . 77 . 100
 - Netmask: 255 . 255 . 255 . 0
- Outside (Interface Eth1):**
 - Use DHCP to obtain IP
 - IP Address: 123 . 123 . 123 . 10
 - Netmask: 255 . 255 . 255 . 0
 - Allow https access to web interface from Internet
 - Gateway: 123 . 123 . 123 . 1
- DNS server:**
 - Primary: 4 . 2 . 2 . 2
 - Secondary (Optional): 4 . 2 . 2 . 1
- Status:** Ingate Startup Tool Version 2.3.2, connected to: Ingate SIParator 19, IG-092-702-2121-2
- Configuration List:**
 - VoIP Survival
 - VPN
 - QoS
 - Enhanced Security
 - 10 SIP Traversal Licenses
 - 10 SIP User Registration Licenses
 - Software Version: 4.6.2

The network topology diagram on the right shows an 'Internet' cloud connected to an 'Ingate SIParator' device and an 'Existing firewall'. Both are connected to a 'LAN' bus, which is also connected to an 'IP-PBX' device.

Ingate Startup Tool

Startup Tool – IP-PBX

- Select IP-PBX
 - Provide IP Address



The screenshot displays the 'Ingate Startup Tool' window with the 'IP-PBX' tab selected. The interface includes a title bar with standard window controls and a menu bar with options: 'Network Topology', 'IP-PBX', 'ITSP_1', and 'Upload Configuration'. The main content area is titled 'IP-PBX (should be located on the LAN)' and contains the following fields and controls:

- Type:** A dropdown menu set to 'Generic PBX'.
- IP Address:** A text input field containing '0 . 0 . 0 . 0'.
- Use domain name:** A checkbox that is currently unchecked.
- SIP Domain:** An empty text input field.
- PBX registers at the Ingate:** An unchecked checkbox.

Below the configuration fields is a 'Status' section with the following text:

Ingate Startup Tool Version 2.3.6, connected to: Ingate Firewall 1190, IG-092-719-5012-4

QoS
Enhanced Security
15 SIP Traversal Licenses
20 SIP User Registration Licenses

Software Version: 4.6.2
Error: Please enter an IP address to your provider.
Error: Please enter an IP address to your provider.

A 'Help' button is located at the bottom right of the window.

Ingate Startup Tool

Startup Tool – ITSP_1

- Select Trunking Provider
- Account Information

The screenshot displays the 'Ingate Startup Tool' window with the 'ITSP_1' tab selected. The interface is organized into several sections:

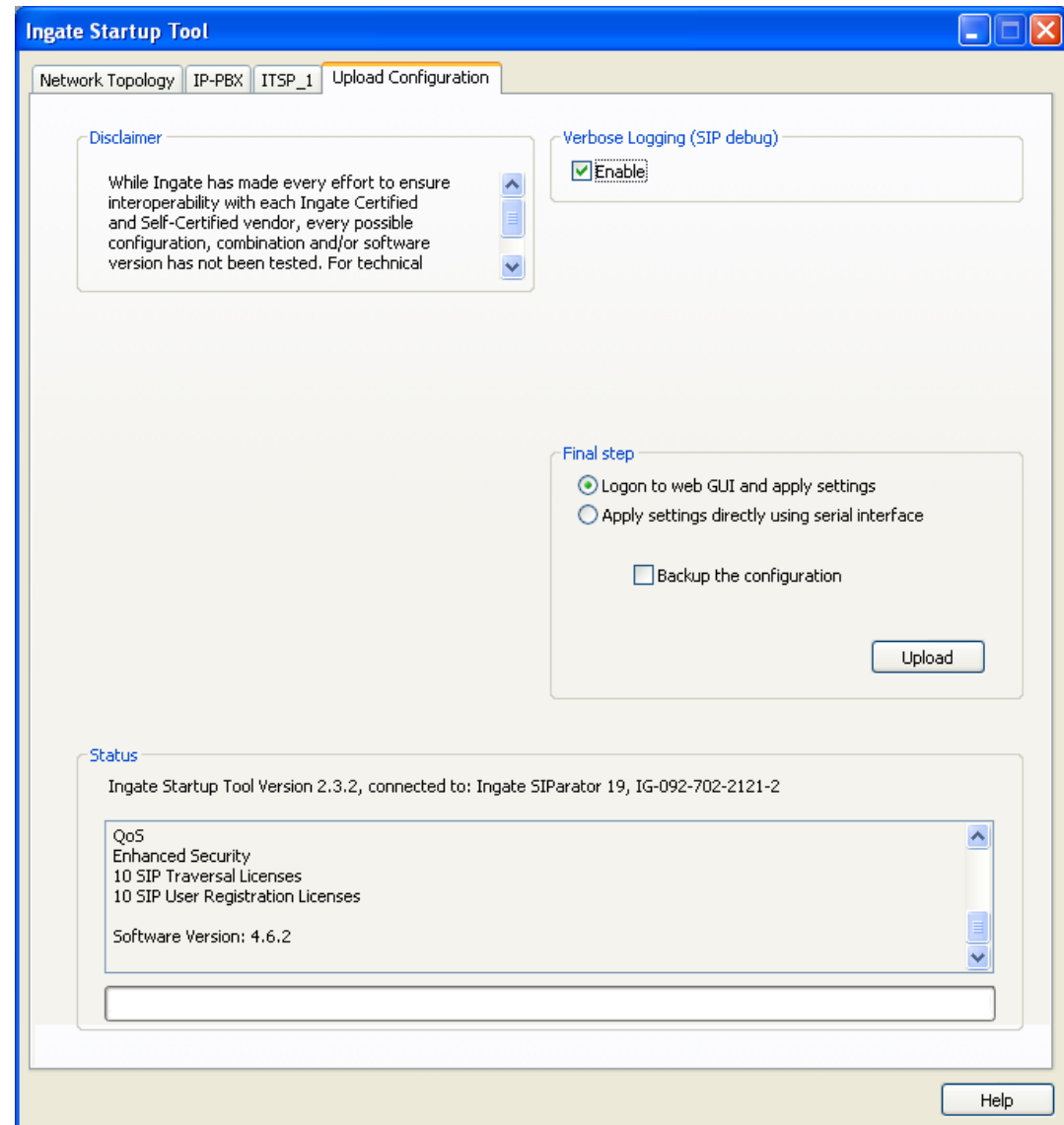
- Name:** A dropdown menu set to 'Generic ITSP'.
- Provider address:** Includes an 'IP Address' field with '0 . 0 . 0 . 0' and a checkbox for 'Use domain name'.
- Advanced:** Contains three sub-sections:
 - 'Prefix to match and remove from inbound calls' with a 'Prefix' input field.
 - 'Prefix to add to outbound calls' with a 'Prefix' input field.
 - 'Forward 3xx messages' with a checked 'Enable' checkbox.
- Account information:** Includes a 'DID/User name (start of range):' field, a 'Use account' checkbox, and fields for 'Authentication name', 'Domain', and 'Password'. A checkbox for 'Use user account on incoming call' is also present.
- Advanced: DID - Mapping to Local user:** Includes a 'DID range size' field set to '1', 'Local phone numbers (start of range):' and 'Password' fields, and a checkbox for 'PBX registers at the Ingate'.
- Status:** Displays 'Ingate Startup Tool Version 2.3.6, connected to: Ingate Firewall 1190, IG-092-719-5012-4' and a scrollable list of system details:
 - Remote SIP Connectivity
 - VPN
 - QoS
 - Enhanced Security
 - 15 SIP Traversal Licenses
 - 20 SIP User Registration Licenses
 - Software Version: 4.6.2

A 'Help' button is located in the bottom right corner of the window.

Ingate Startup Tool

Startup Tool – Upload Config

- Login to web GUI and apply settings
- Upload



Ingate Startup Tool

Startup Tool – Apply the Config

- The Startup Tool will launch a browser to have the installer Apply the Configuration.

The screenshot displays the Ingate Startup Tool web interface. At the top, there is a navigation menu with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a secondary menu with buttons for Save/Load Configuration, Show Configuration, User Administration, Upgrade, Table Look, Date and Time, Restart, and Change Language. The main content area is divided into several sections:

- Test Run and Apply Conf (Help)**: Contains a text input field for "Duration of limited test mode:" with the value "30" and the unit "seconds". Below it is a button labeled "Apply configuration".
- Show Message About Unapplied Changes**: Contains three radio button options: "On every page" (selected), "On the Save/Load Configuration page", and "Never".
- Backup (Help)**: Contains the text "The permanent configuration is not affected." and buttons for "Save to local file", "Load from local file", a text input field for "Local file:", and a "Browse..." button.
- Save/Load CLI Command File (Help)**: Contains the text "The permanent configuration might be affected by loading a CLI file." and buttons for "Save config to CLI file", "Load CLI file", a text input field for "Local file:", and a "Browse..." button.
- Abort All Edits (Help)**: Contains the text "The permanent configuration is not affected." and a button labeled "Abort all edits".
- Reload Factory Configuration (Help)**: Contains the text "The permanent configuration is not affected." and a button labeled "Load factory configuration".

Ingate Startup Tool

Startup Tool – Register & Upgrade

- Enter Ingate Web Account
- Create Ingate Web Account
- Connect to www.ingate.com
- Install Modules & Licenses by entering 12-digit Purchase Key
- Upgrade the software of the unit

The screenshot displays the 'Ingate Startup Tool' window with the 'Licenses and Upgrades' tab selected. The interface is divided into several sections:

- Your Ingate Web Account:** Includes input fields for 'User:' and 'Password:', and a 'Create' button.
- Connect and Register this unit with the Ingate Web:** Shows 'Model: Ingate SIParator 19' and 'Serial #: IG-092-719-5151-0', with a 'Connect' button.
- Download and install licenses and upgrades from the Ingate Web:** Contains a 'Purchase code:' field, an 'Install' button, and a checkbox for 'I have the license on my PC'. Below this is an 'Upgrade' button.
- Currently Installed Modules:** A list box showing 'SIP Trunking', 'Advanced SIP Routing', 'Remote SIP Connectivity', 'VoIP Survival', 'VPN', 'Enhanced Security', and '10 SIP Traversal Licenses'.
- Status:** Displays 'Ingate Startup Tool Version 2.3.6, connected to: Ingate SIParator 19, IG-092-719-5151-0' and a list of installed modules: 'VPN', 'Enhanced Security', '10 SIP Traversal Licenses', and '10 SIP User Registration Licenses'. It also shows 'Software Version: 4.6.2'.

A 'Help' button is located at the bottom right of the window.

Exercise #1

Startup Tool

Overall Training Setup

Training Station #2



Softphone
DID #: 6135552222
IP Address: 10.20.20.20

Laptop
IP Address: 10.20.20.20
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A9-7F-15
Eth0 (Inside) IP Address: 10.20.20.22
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.22
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #3



Softphone
DID #: 6135553333
IP Address: 10.30.30.30

Laptop
IP Address: 10.30.30.30
Mask: 255.255.255.0
Default GW: 10.30.30.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-63
Eth0 (Inside) IP Address: 10.30.30.33
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.33
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #1



Softphone
DID #: 6135551111
IP Address: 10.10.10.10

Laptop
IP Address: 10.10.10.10
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-39
Eth0 (Inside) IP Address: 10.10.10.11
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.11
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

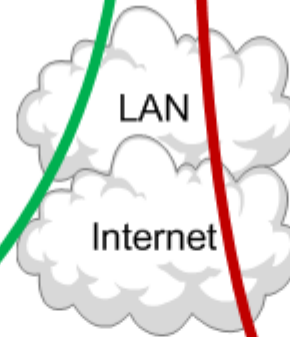
Training Station #4



Softphone
DID #: 6135554444
IP Address: 10.40.40.40

Laptop
IP Address: 10.40.40.40
Mask: 255.255.255.0
Default GW: 10.40.40.1
DNS: 65.175.129.149

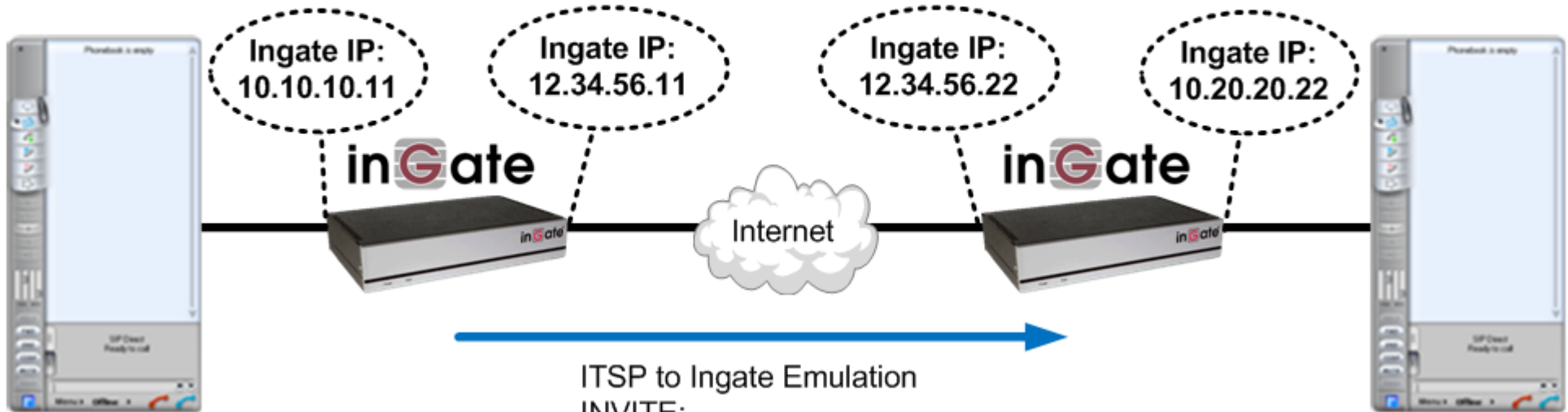
Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-AD-B5-02
Eth0 (Inside) IP Address: 10.40.40.44
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.44
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Exercise #1

Training Station #1

Training Station #2



IP-PBX to Ingate
INVITE:
6135552222@10.10.10.11

ITSP to Ingate Emulation
INVITE:
6135552222@12.34.56.22

Ingate to IP-PBX
INVITE:
6135552222@10.20.20.20

ITSP to Ingate Emulation
INVITE:
6135551111@12.34.56.11

Ingate to IP-PBX
INVITE:
6135551111@10.10.10.10

IP-PBX to Ingate
INVITE:
6135551111@10.20.20.22

Break - Lunch

Recap

Ingate Products

- Ingate Firewall and Ingate SIParator
- Scale by appliance giving more traversals
- Number of purchasable Options Modules

Deployments

- Ingate Firewall and Ingate SIParator

Startup Tool

- “Out of the Box” setup and commissioning
- Select IP-PBX and ITSP

Programming GUI

Programming GUI

Web Configuration

- Web into the Ingate
- Major Categories and separate Tabs



Networks and Computers

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ ITSP_IP	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>
+ LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)	<input type="checkbox"/>
+ PBX	-	10.51.77.20	10.51.77.20			-	<input type="checkbox"/>
+ WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)	<input type="checkbox"/>
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>

Programming: Network

Programming: Network

Networks & Computers

- Provides a view of the Network connected on each interface as a Routing Table.



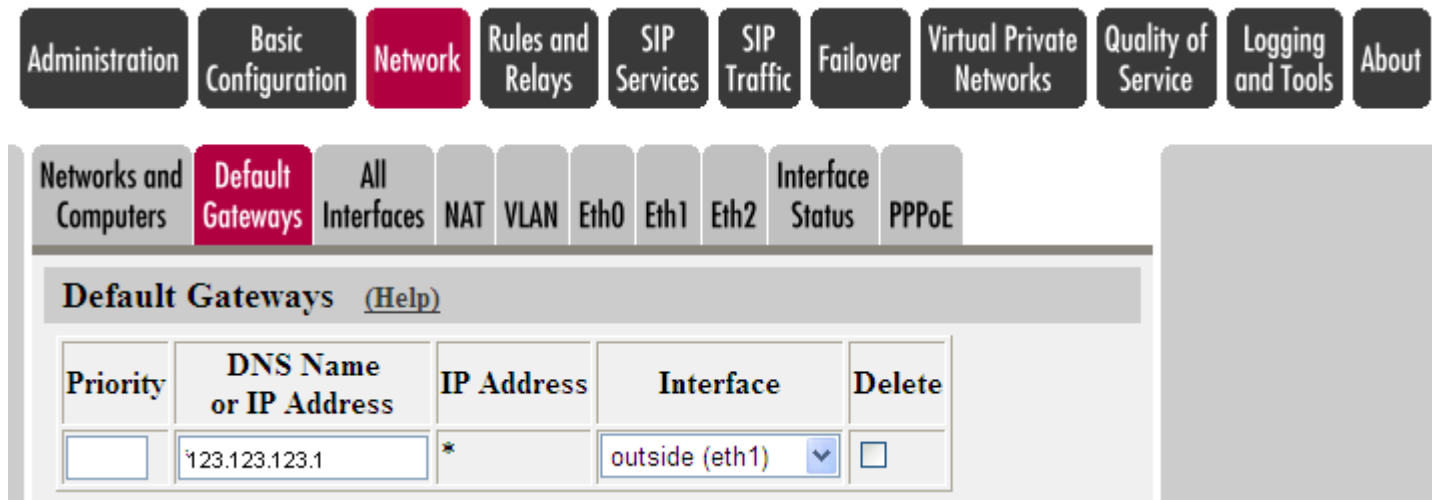
Networks and Computers

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ ITSP_IP	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>
+ LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)	<input type="checkbox"/>
+ PBX	-	10.51.77.20	10.51.77.20			-	<input type="checkbox"/>
+ WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)	<input type="checkbox"/>
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)	<input type="checkbox"/>

Programming: Network

Default Gateway

- The Default Gateway to the Internet, provided by the ISP.



The screenshot shows a network configuration interface with a top navigation bar containing buttons for Administration, Basic Configuration, Network (highlighted), Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-navigation bar with buttons for Networks and Computers, Default Gateways (highlighted), All Interfaces, NAT, VLAN, Eth0, Eth1, Eth2, Interface Status, and PPPoE. The main content area is titled "Default Gateways" with a "(Help)" link. It contains a table with the following structure:

Priority	DNS Name or IP Address	IP Address	Interface	Delete
<input type="text"/>	<input type="text" value="123.123.123.1"/>	*	outside (eth1) <input type="button" value="v"/>	<input type="checkbox"/>

Programming: Network

Eth0 Network Interface

- The IP Address/Mask of the NIC on the LAN.

The screenshot shows the Network Configuration page for the Eth0 interface. The 'Network' tab is selected, and the 'Eth0' sub-tab is active. The 'General' section shows the physical device as 'eth0' and the interface name as 'inside'. The 'Obtain IP Address Dynamically' section has 'OFF' selected. The 'Speed and Duplex' section has 'Automatic negotiation' selected. The 'Directly Connected Networks' table shows one entry for the 'inside' interface with IP 10.51.77.1 and netmask 255.255.255.0. The 'Alias' section shows a range of 10.51.77.1-10.51.77.254. The 'Static Routing' section is empty.

Name	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete
inside	10.51.77.1	10.51.77.1	255.255.255.0	10.51.77.0	10.51.77.255		-	<input type="checkbox"/>

Name	DNS Name or IP Address	IP Address	Delete

Routed Network			Router		Delete
DNS Name or Network Address	Network Address	Netmask / Bits	DNS Name or IP Address	IP Address	

- Static Routing – defines Router address for other network address on the LAN.

Programming: Network

Eth1 Network Interface

- The IP Address/Mask of the NIC on the WAN.

The screenshot shows the Mikrotik WinBox configuration page for the Eth1 network interface. The interface is divided into several sections:

- General:** Physical device: eth1. This interface is On. Interface name: outside.
- Obtain IP Address Dynamically:** OFF, DHCP client ON, PPPoE client ON.
- 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 table with columns: Name, DNS Name or IP Address, IP Address, Netmask/Bits, Network Address, Broadcast Address, VLAN Id, VLAN Name, Delete. One row is shown for 'outside'.
- Alias:** Below are the ranges from which you can select aliases. (An interface using dynamic IP may not have aliases.) A table with columns: Name, DNS Name or IP Address, IP Address, Delete. One row is shown.
- Static Routing:** A table with columns: Routed Network (DNS Name or Network Address, Network Address, Netmask/Bits), Router (DNS Name or IP Address, IP Address), Delete. One row is shown for 'default'.

- PPPoE or DHCP IP address assignment are possible.

Programming: Basic Configuration

Programming: Basic Configuration

Basic Configuration

- Provides DNS Server addresses.

The screenshot displays the InGate Firewall configuration interface. At the top, there is a navigation bar with tabs: Administration, Basic Configuration (selected), Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar includes: Basic Configuration (selected), Access Control, RADIUS, SNMP, DHCP Server, DHCP Server Status, Dynamic DNS Update, Certificates, and Advanced.

The main configuration area is divided into several sections:

- General**:
 - Name of this firewall: Office
 - Default domain: .
- Version of Ingate Firewall**:
 - Check for new versions of Ingate Firewall: Yes No
 - Date of last successful version check: 2008-02-12 10:30:12
 - Software version in use: 4.6.1
- IP Policy**:
 - Discard IP packets
 - Reject IP packets
- 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
- DNS Servers (Help)**:

No.	DNS Name or IP Address	IP Address	Delete
1	216.254.141.13	216.254.141.13	<input type="checkbox"/>
2	209.90.160.220	209.90.160.220	<input type="checkbox"/>

Programming: Basic Configuration

Access Control

- Provides configuration for HTTP and HTTPS access.

The screenshot shows the Cisco IOS configuration interface for Access Control. The top navigation bar includes tabs for Administration, Basic Configuration (selected), Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar shows Basic Configuration, Access Control (selected), RADIUS, SNMP, DHCP Server, DHCP Server Status, Dynamic DNS Update, Certificates, and Advanced.

The main configuration area is divided into several sections:

- Configuration Transport (Help)**
 - Configuration via HTTP**: Direct your web browser to this address: Port: inside (10.51.77.1) 80
 - Configuration via HTTPS**: Direct your web browser to this address: Port: outside (eth1) 443. Certificate to use: HTTPS_Prvt
 - Configuration via SSH**: Connect your SSH client to this address: Port: - 22
- Configuration Allowed Via Interface (Help)**: A table with columns for interface (Eth0, Eth1, Eth2) and status (On/Off).
- User Authentication For Web Interface Access (Help)**: Radio buttons for Local users (selected), RADIUS database, and Local users or RADIUS database.
- Configuration Computers (Help)**: A table with columns for No., DNS Name or Network Address, Network Address, Netmask/Bits, Range, Via IPsec Peer, SSH, HTTP, HTTPS, Log Class, and Delete.

No.	DNS Name or Network Address	Network Address	Netmask/Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	Log Class	Delete
1	10.51.77.0	10.51.77.0	255.255.255.0	10.51.77.0 - 10.51.77.255	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Local	<input type="checkbox"/>
2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0 -	-	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Local	<input type="checkbox"/>

Programming: NAT & Rules and Relays

Firewall Only

Programming: NAT

NAT

- Define when to apply NAT rules. Typically, From LAN network to WAN network, NAT as WAN address

The screenshot shows a web-based configuration interface. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network (highlighted in red), Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-menu with buttons for Networks and Computers, Default Gateways, All Interfaces, NAT (highlighted in red), VLAN, Eth0, Eth1, Eth2, Interface Status, and PPPoE. The main content area is titled 'NAT' and contains the following text: '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
	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	inside (eth0) ▾				outside (eth1) ▾				outside (eth1) ▾	<input type="checkbox"/>

Programming: Rules & Relays

Rules

- Define specific Service from Client to Server networks.



Rule No.	Rule State	Client	From IPsec Peer	Server	To IPsec Peer	Direction	Service	Action	Time Class	Log Class	Comment	Delete
1	On	LAN	-	WAN	-	inside - > outside (NAT:ed)	pptp	Allow	24/7	Local		<input type="checkbox"/>
2	On	LAN	-	WAN	-	inside - > outside (NAT:ed)	icmp/udp/tcp	Allow	24/7	Local		<input type="checkbox"/>

Programming: Rules & Relays

Relays

- Direct specific Traffic to specific locations



Listen To ...		Relay To ...			Relay Type	Allow Access From ...		Certificate for TLS/SSL	Time Class
IP Address	Port	DNS Name or IP Address	IP Address	Port		Network	IPsec Peer		
outside (eth1) ▾	80	10.51.77.58	10.51.77.58	80	UDP port forwarding ▾	WAN ▾	- ▾	- ▾	24/7 ▾

Programming: Quality of Service

Firewall Only

Programming: QoS

Quality of Service – Call Admission Control

- You can make the firewall reject SIP calls when there is not bandwidth enough left to get media streams through satisfactorily.
- Bandwidth for SIP Media - define BW Reservations
- Codec Bandwidth – define Codec BW

The screenshot shows the 'Call Admission Control' configuration page. At the top, there is a navigation bar with tabs for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service (highlighted), Logging and Tools, and About. Below this, there are sub-tabs for QoS and SIP, QoS Classes, QoS Eth0, QoS Eth1, QoS Eth2, TOS Modification, and All QoS Interfaces. The main content area is titled 'Call Admission Control' and includes a 'Call admission control' toggle set to 'On'. Below this is the 'Bandwidths For SIP Media' section, which contains a table with columns for Interface, Outgoing (kbit/s) Allowed for Media, Outgoing (kbit/s) Allowed for Emergency, Incoming (kbit/s) Allowed for Media, and Incoming (kbit/s) Allowed for Emergency. The table lists interfaces: inside (eth0), outside (eth1), and DMZ (eth2). The 'Codec Bandwidths' section follows, featuring a table with columns for Type, Codec Name, Bandwidth (kbit/s), This Codec Is Allowed, and Delete. The table lists various audio codecs such as g723, g726-16, g726-24, g726-32, g726-40, g729, g729a, gsm, ilbc, pcma, pcmu, speex, and video, each with a bandwidth value and a toggle for being allowed. At the bottom, there is a 'Codec Filtering' section with a 'Use codec filtering' toggle set to 'No' and 'Save' and 'Undo' buttons.

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)
inside (eth0)	200		200	
outside (eth1)	200		200	
DMZ (eth2)				

Type	Codec Name	Bandwidth (kbit/s)	This Codec Is Allowed	Delete
audio	g723	40	On	<input type="checkbox"/>
audio	g726-16	16	On	<input type="checkbox"/>
audio	g726-24	24	On	<input type="checkbox"/>
audio	g726-32	32	On	<input type="checkbox"/>
audio	g726-40	40	On	<input type="checkbox"/>
audio	g729	8	On	<input type="checkbox"/>
audio	g729a	8	On	<input type="checkbox"/>
audio	gsm	13	On	<input type="checkbox"/>
audio	ilbc	16	On	<input type="checkbox"/>
audio	pcma	64	On	<input type="checkbox"/>
audio	pcmu	64	On	<input type="checkbox"/>
audio	speex	44	On	<input type="checkbox"/>
audio	*	100	Off	<input type="checkbox"/>
video	*	100	Off	<input type="checkbox"/>

Programming: QoS

Quality of Service – QoS Classes

- Using Priority queues, you assign different priority to different types of traffic.
- Using Bandwidth allocation, you assign guaranteed bandwidth and bandwidth limits for different types of traffic.

The screenshot shows a web-based configuration interface for Quality of Service (QoS). The top navigation bar includes tabs for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service (highlighted), Logging and Tools, and About. Below this, a sub-menu shows QoS and SIP, QoS Classes (highlighted), QoS Eth0, QoS Eth1, QoS Eth2, TOS Modification, and All QoS Interfaces.

The main section is titled "Type of QoS" with a "(Help)" link. It contains two radio buttons: "Priority queues" (selected) and "Bandwidth allocation".

Below this is the "QoS Classes" section, also with a "(Help)" link. It contains a table with the following columns: No., Class Name, Client, Server, Service, SIP, Packet Size (bytes) (Min, Max), TOS Octet (TOS, DSCP), and Delete.

No.	Class Name	Client	Server	Service	SIP	Packet Size (bytes)		TOS Octet		Delete
						Min	Max	TOS	DSCP	
1	SIP Signaling	-	-	-	Signaling			-		<input type="checkbox"/>
2	SIP Media	-	-	-	Media			-		<input type="checkbox"/>
3	HTTP	-	-	http	Non-SIP			-		<input type="checkbox"/>
4	FTP	-	-	ftp	Non-SIP			-		<input type="checkbox"/>

Below the table, there is a button "Add new rows" followed by a text input field containing "1" and the word "rows".

The bottom section is titled "TOS Description" and lists three options: MD - Minimize Delay, MT - Maximize Throughput, and MR - Maximize Reliability. At the very bottom, there are "Save" and "Undo" buttons.

Programming: QoS

Quality of Service – Most Restricted Interface

- You specify how packets belonging to different classes should be handled by the interface
- The Priority field specifies in which priority queue to put the packets. Higher priority traffic will always be let through before lower priority traffic is allowed (but see also the Loose Priority setting).

The screenshot shows the configuration page for Quality of Service on the most restricted interface. The navigation menu at the top includes Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service (highlighted), Logging and Tools, and About. The sub-menu includes QoS and SIP, QoS Classes, QoS Eth0, QoS Eth1 (highlighted), QoS Eth2, TOS Modification, and All QoS Interfaces.

Loose Priority (global setting) (Help)
Save % for lower priority traffic

Outgoing Traffic

General (Help)
Outgoing QoS: Active Inactive

Bandwidths (Help)
Total bandwidth limit: kbit/s
Reserved for SIP media: 200 kbit/s
Available bandwidth: 2800 kbit/s

Classification (Help)

Class	Priority	Delete
SIP Signaling	1 (highest)	<input type="checkbox"/>
SIP Media	1 (highest)	<input type="checkbox"/>
HTTP	2	<input type="checkbox"/>
FTP	8 (lowest)	<input type="checkbox"/>

Add new rows rows.

Unclassified Traffic (Help)
Priority

Save Undo

Incoming Traffic

General (Help)
Incoming QoS: Active Inactive

Bandwidth (Help)
Total bandwidth limit: kbit/s
Reserved for SIP media: 200 kbit/s
Available bandwidth: 440 kbit/s

Classification (Help)

Class	Priority	Delete
SIP Signaling	1 (highest)	<input type="checkbox"/>
SIP Media	1 (highest)	<input type="checkbox"/>
HTTP	2	<input type="checkbox"/>
FTP	8 (lowest)	<input type="checkbox"/>

Add new rows rows.

Unclassified Traffic (Help)
Priority

Programming: QoS

Quality of Service – ToS Modification

- Modify the TOS octet of packets leaving the firewall. You can either specify a value for the (3 bit) TOS field (RFC 791), or you can specify a value for the (6 bit) Differentiated Services field (RFC 2474).

The screenshot shows the inGate configuration interface. At the top, there are navigation tabs: Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, and Quality of Service. Below these are sub-tabs for QoS and SIP, QoS Classes, QoS Eth0, QoS Eth1, QoS Eth2, TOS Modification (which is highlighted in red), and All QoS Interfaces.

The main content area is titled "TOS/DSCP Modification". It contains the following text: "You can modify the TOS octet of packets leaving the firewall. You can either specify a value for the (3 bit) TOS field (RFC 791), or you can specify a value for the (6 bit) Differentiated Services field (RFC 2474). Note that the DSCP value is entered in decimal form in this table."

Class	TOS Octet		Delete
	TOS	DSCP	
SIP Signaling	-	17	<input type="checkbox"/>

Below the table is a button "Add new rows" followed by a text input field containing "1" and the text "rows."

The section is titled "TOS Description" and lists the following options: MD - Minimize Delay, MT - Maximize Throughput, and MR - Maximize Reliability.

At the bottom of the section are "Save" and "Undo" buttons.

Programming: SIP Services

Programming: SIP Services

Basic

- Turn On SIP Module.
- Define Media Port Range.

The screenshot shows a web-based configuration interface for SIP Services. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services (highlighted in red), SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar includes Basic (highlighted in red), Signaling Encryption, Media Encryption, Interoperability, Sessions and Media, Remote SIP Connectivity, and VoIP Survival.

The main configuration area is titled "SIP Module (Help)". It contains a radio button control for "SIP module:" with "On" selected and "Off" unselected. Below this, there are two main sections:

- Additional SIP Signaling Ports (Help)**: This section includes a table with columns for Port, Transport, Comment, and Delete. Below the table is an "Add new rows" button and a text input field containing "1" followed by "rows".
- SIP Media Port Range (Help)**: This section has a "Ports:" label followed by two input fields containing "58024" and "60999" separated by a hyphen.

To the right of these sections is a "SIP Logging (Help)" section with four dropdown menus for log classes: "Log class for SIP signaling:", "Log class for SIP packets:", "Log class for SIP license messages:", and "Log class for SIP media messages:". Each dropdown menu currently shows "Local".

Programming: SIP Services

Interoperability

- Common deviations from the standard

The screenshot displays a web-based configuration interface for SIP services. The top navigation bar includes tabs for Administration, Basic Configuration, Network, Rules and Policy, SIP Services (highlighted), SIP Traffic, Firewall, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-menu highlights Interoperability. The main content area is divided into two columns of settings, each with a 'Help' link.

Loose Routing (Help)
 Use `*`
 Use `*` or `*`

Remove Via Headers (Help)
Table with columns: SIP Server, DNS Name or IP Address, IP Address, Delete. Includes an 'Add new rows' button.

Expires Header (Help)
 Never add Expires header
 Add Expires header if the request contained one
 Always add Expires header

URI Encoding (Help)
Recommended setting: Always encrypt URIs
 Always encrypt URIs
 Use shorter, encrypted URIs
 Escape URIs
 Keep username in URIs

Loose Username Check (Help)
 Use the username as authentication name
 Use the entire address as authentication name

Accept RTP/AVP With sdescriptions (Help)
Recommended setting: Accept RTP/AVP with sdescriptions offer
 Accept RTP/AVP with sdescriptions offer
 Only accept RTP/SAVP with sdescriptions offer

Force Record-Route for Outbound Requests (Help)
Recommended setting: No
Force Record-Route for outbound request: Yes No

Force Remote TLS Connection Reuse (Help)

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

Translation Exceptions (Help)
Table with columns: Except This From Translation, DNS Name or IP Address, IP Address, Delete. Includes an 'Add new rows' button.

Force Translation (Help)
 Always Translate This/Delete
Includes an 'Add new rows' button.

Delay URI Decryption (Help)
Recommended setting: Normal URI decryption
 Normal URI decryption
 Delayed URI decryption

User Matching (Help)
 Match only on username
 Match on username and domain

Transmit RTP/AVP With sdescriptions (Help)
Recommended setting: Transmit RTP/SAVP with sdescriptions offer
 Transmit RTP/SAVP with sdescriptions offer
 Transmit RTP/AVP with sdescriptions offer

Force Record-Route for All Requests (Help)
Recommended setting: No
Always force Record-Route: Yes No

Accept TCP Marked As TLS (Help)

Programming: SIP Services

Remote SIP Connectivity

- Allows SIP client behind NAT boxes to use SIP.

The screenshot shows a web-based configuration interface for SIP services. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services (highlighted in red), SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-navigation bar with buttons for Basic, Signaling Encryption, Media Encryption, Interoperability, Sessions and Media, Remote SIP Connectivity (highlighted in red), and VoIP Survival. The main content area is titled "Remote SIP Connectivity" and contains several sections:

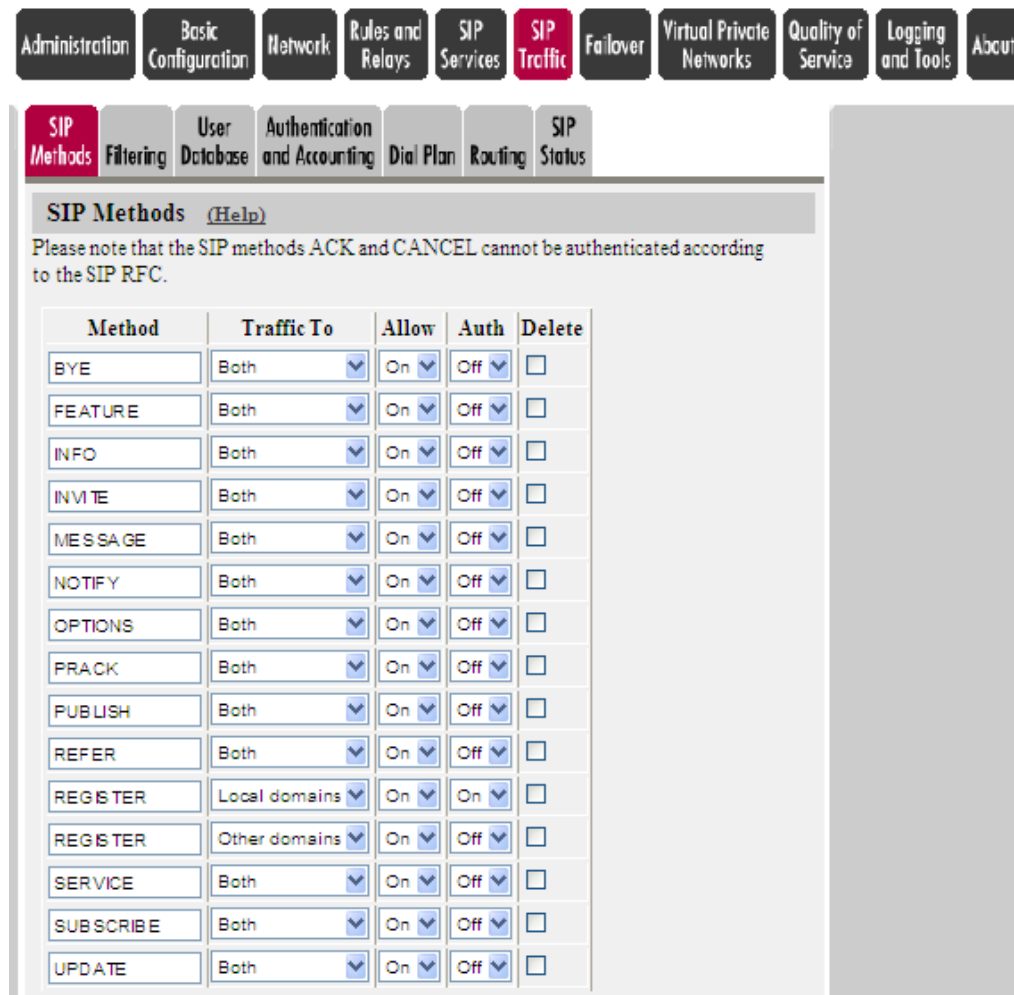
- STUN Server** (Help): STUN server: On Off
- Remote NAT Traversal** (Help): Remote NAT traversal: On Off
- NAT keepalive method:**
 - Use OPTIONS
 - Use short registration times
 - Use both OPTIONS and short registration times
- Media Route:**
 - Route media directly between clients behind the same NAT
 - Always route media through the firewall
- NAT timeout for UDP:** seconds
- NAT timeout for TCP:** seconds

Programming: SIP Traffic

Programming: SIP Traffic

SIP Methods

- Select which SIP methods the firewall should allow & authenticate



The screenshot shows a web-based configuration interface for SIP traffic. At the top, there is a navigation menu with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-menu includes SIP Methods (highlighted), Filtering, User Database, Authentication and Accounting, Dial Plan, Routing, and SIP Status. The main content area is titled 'SIP Methods (Help)' and contains a note: 'Please note that the SIP methods ACK and CANCEL cannot be authenticated according to the SIP RFC.' Below the note is a table with columns for Method, Traffic To, Allow, Auth, and Delete. The table lists various SIP methods with their respective configurations.

Method	Traffic To	Allow	Auth	Delete
BYE	Both	On	Off	<input type="checkbox"/>
FEATURE	Both	On	Off	<input type="checkbox"/>
INFO	Both	On	Off	<input type="checkbox"/>
INVITE	Both	On	Off	<input type="checkbox"/>
MESSAGE	Both	On	Off	<input type="checkbox"/>
NOTIFY	Both	On	Off	<input type="checkbox"/>
OPTIONS	Both	On	Off	<input type="checkbox"/>
PRACK	Both	On	Off	<input type="checkbox"/>
PUBLISH	Both	On	Off	<input type="checkbox"/>
REFER	Both	On	Off	<input type="checkbox"/>
REGISTER	Local domains	On	On	<input type="checkbox"/>
REGISTER	Other domains	On	Off	<input type="checkbox"/>
SERVICE	Both	On	Off	<input type="checkbox"/>
SUBSCRIBE	Both	On	Off	<input type="checkbox"/>
UPDATE	Both	On	Off	<input type="checkbox"/>

Programming: SIP Traffic

Filtering

- The **Proxy Rules** and **Default Policy For SIP Requests** settings control if sipfw should process requests, based on the sender IP address of the request

The screenshot displays the configuration interface for SIP Traffic. The top navigation bar includes tabs for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (selected), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar shows SIP Methods, Filtering (selected), User Database, Authentication and Accounting, Dial Plan, Routing, and SIP Status.

The main content area is divided into two sections:

- Proxy Rules** (Help): A table with columns for No., From Network, Action, and Delete. Below the table is an "Add new rows" button and a text input field containing "1".
- Default Policy For SIP Requests**: A section with three radio button options: "Process all" (selected), "Local only", and "Reject all".
- Content Types** (Help): A table with columns for Content Type, Allow, and Delete. The table lists several content types with their respective "Allow" settings (On or Off) and "Delete" checkboxes.

Content Type	Allow	Delete
/*	On	<input type="checkbox"/>
application/SOAP	Off	<input type="checkbox"/>
application/adrl+x	Off	<input type="checkbox"/>
application/pdf+x	Off	<input type="checkbox"/>
application/vnd-mi	Off	<input type="checkbox"/>
application/vnd-mi	Off	<input type="checkbox"/>

- The **Content Type** table controls if sipfw should process requests, based on the content type of the request body
- */* - Allows All

Programming: SIP Traffic

Local Registrar

- Define SIP Users that register to the Ingate (server registrar)

The screenshot shows the InGate configuration interface. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-navigation bar with buttons for SIP Methods, Filtering, Local Registrar (highlighted), Authentication and Accounting, SIP Accounts, Dial Plan, Routing, and SIP Status.

The main content area is titled "Local SIP Domains (Help)" and contains a table with two columns: "Domain" and "Delete Row".

Domain	Delete Row
10.51.77.1	<input type="checkbox"/>
sip.office-on-the.n	<input type="checkbox"/>

Below the table is a button "Add new rows" followed by a text input field containing "1" and the text "rows".

The next section is titled "Registrar Limits" and contains three labels: "Timeout for registrations:", "Allowed number of users:", and "Allowed number of registrations per user:". Below these are three input fields: the first contains "3600" followed by "seconds", the second is empty with "(max 20)" next to it, and the third contains "5".

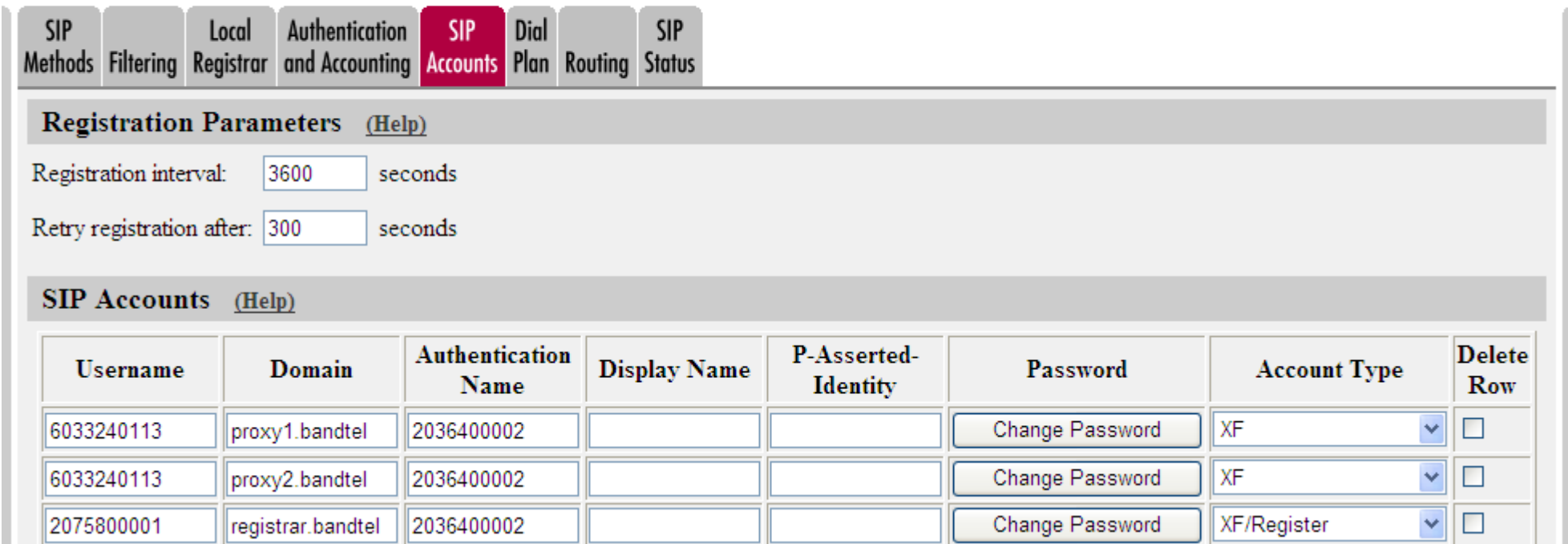
The final section is titled "Local SIP User Database (Help)" and contains a table with six columns: "Username", "Domain", "Authentication Name", "Password", "Register From", and "Delete Row".

Username	Domain	Authentication Name	Password	Register From	Delete Row
11200	10.51.77.1	11200	Change Password	LAN	<input type="checkbox"/>
5177	10.51.77.1	scott	Change Password	LAN	<input type="checkbox"/>
asterisk	10.51.77.1	asterisk	Change Password	LAN	<input type="checkbox"/>

Programming: SIP Traffic

SIP Accounts

- Define SIP Users for Service Providers
- Select behavior of these SIP Users (Ingate as client)



Registration Parameters [\(Help\)](#)

Registration interval: seconds

Retry registration after: seconds

SIP Accounts [\(Help\)](#)

Username	Domain	Authentication Name	Display Name	P-Asserted-Identity	Password	Account Type	Delete Row
<input type="text" value="6033240113"/>	<input type="text" value="proxy1.bandtel"/>	<input type="text" value="2036400002"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Change Password"/>	<input type="text" value="XF"/> <input type="button" value="v"/>	<input type="checkbox"/>
<input type="text" value="6033240113"/>	<input type="text" value="proxy2.bandtel"/>	<input type="text" value="2036400002"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Change Password"/>	<input type="text" value="XF"/> <input type="button" value="v"/>	<input type="checkbox"/>
<input type="text" value="2075800001"/>	<input type="text" value="registrar.bandtel"/>	<input type="text" value="2036400002"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Change Password"/>	<input type="text" value="XF/Register"/> <input type="button" value="v"/>	<input type="checkbox"/>

Programming: SIP Traffic

User Database: Account Type Selections

- **Register:** With this *Account* type, the firewall registers the username with the SIP server associated with the domain. You may enter the address to send the request to in the User Routing table. This is useful when you have a SIP client which cannot register properly.
- **XF:** With this *Account* type, the firewall 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 firewall replaces the From header as described above, then registers as described under Register above.

Programming: SIP Traffic

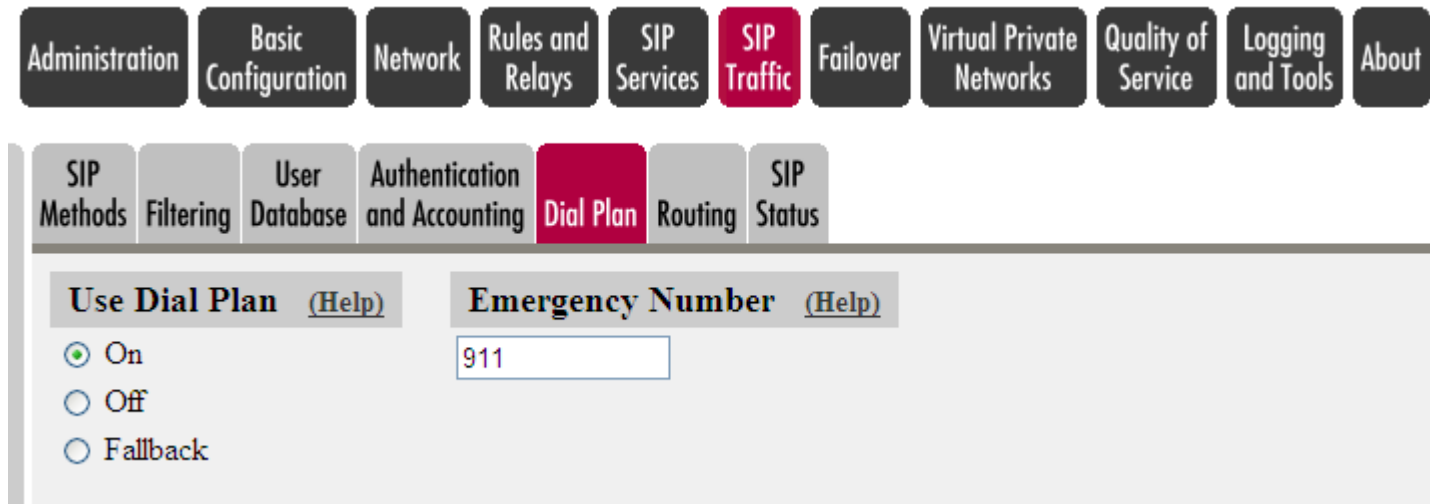
User Database: Account Type Selections

- **Domain:** This Account type can be used when sending requests to other domains where authentication is required. You must select this account in the Dial Plan when you forward requests to the domain in question. When that server requires authentication for its domain, the firewall sends the username and password configured here.
- **B2BUAWM:** With this Account type, the firewall replaces the From header as described under XF. It also changes the SDPs to the effect that media is always sent via the firewall.
- **B2BUAWM/Register:** With this Account type, the firewall acts as described under B2BUAWM above. It also registers the user as described under Register above.

Programming: SIP Traffic

Dial Plan

- On the **Dial Plan** page, you can perform advanced routing of SIP requests



The screenshot displays a web interface for configuring SIP traffic. At the top, a horizontal menu contains several tabs: Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted in red), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a secondary menu includes SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan (highlighted in red), Routing, and SIP Status. The main content area shows two sections: 'Use Dial Plan' with radio buttons for 'On' (selected), 'Off', and 'Fallback', and 'Emergency Number' with a text input field containing '911'.

Administration	Basic Configuration	Network	Rules and Relays	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
SIP Methods	Filtering	User Database	Authentication and Accounting	Dial Plan	Routing	SIP Status				
Use Dial Plan (Help)		Emergency Number (Help)								
<input checked="" type="radio"/> On		<input type="text" value="911"/>								
<input type="radio"/> Off										
<input type="radio"/> Fallback										

Programming: SIP Traffic

Dial Plan “Matching FROM Header”

- Requests can be matched on From header, sender IP address, transport method and network.

The screenshot shows a web-based configuration interface for SIP Traffic. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-navigation bar with buttons for SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan (highlighted), Routing, and SIP Status.

The main configuration area is divided into two sections:

- Use Dial Plan (Help)**: A section with three radio buttons: On, Off, and Fallback.
- Emergency Number (Help)**: A text input field containing the value "911".

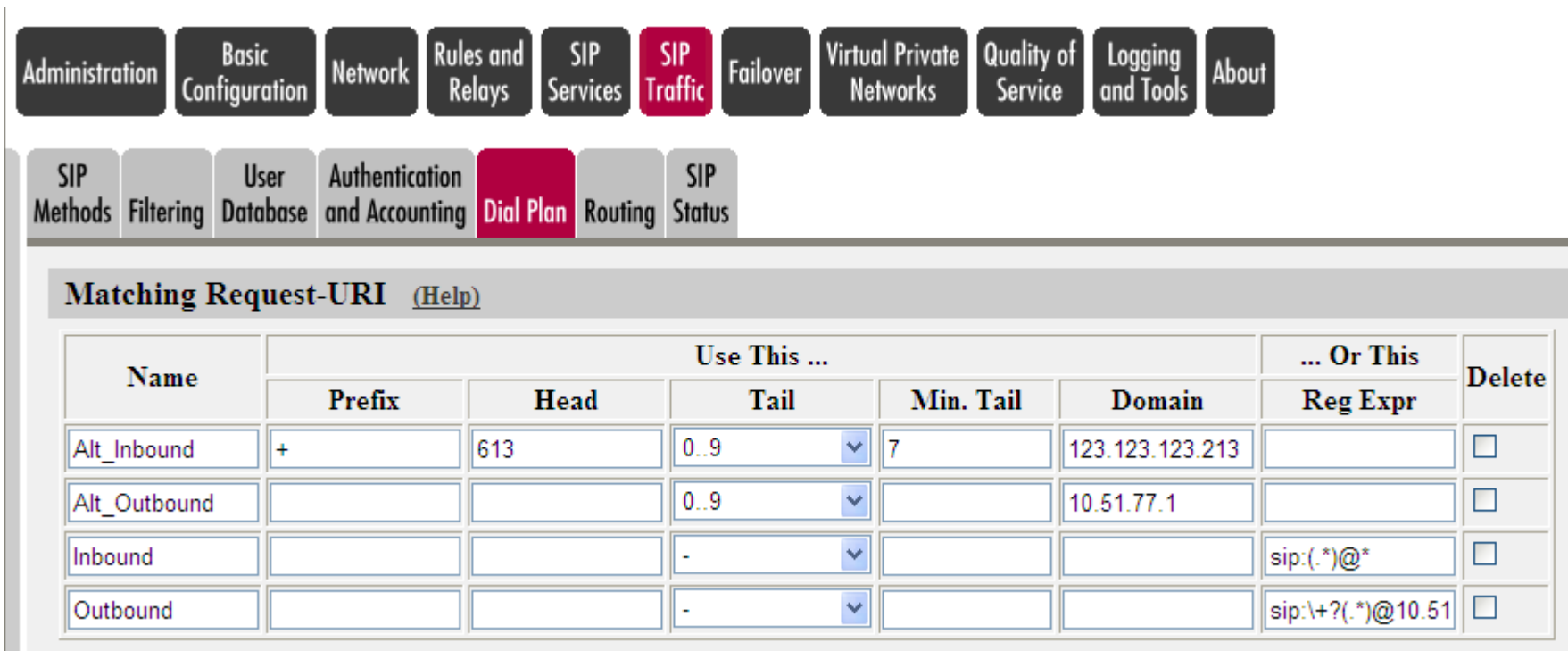
Below these sections is the **Matching From Header (Help)** section, which contains a table with the following columns: Name, Use This ... (Username, Domain), ... Or This (Reg Expr), Transport, Network, and Delete.

Name	Use This Or This	Transport	Network	Delete
	Username	Domain	Reg Expr			
Bandwidth.com	*	*		UDP	ITSP_IP	<input type="checkbox"/>
LAN	*	*		UDP	LAN	<input type="checkbox"/>
WAN	*	*		Any	WAN	<input type="checkbox"/>

Programming: SIP Traffic

Dial Plan “Matching Request URI”

- Requests can be matched on the Request-URI, which states where the request is bound.



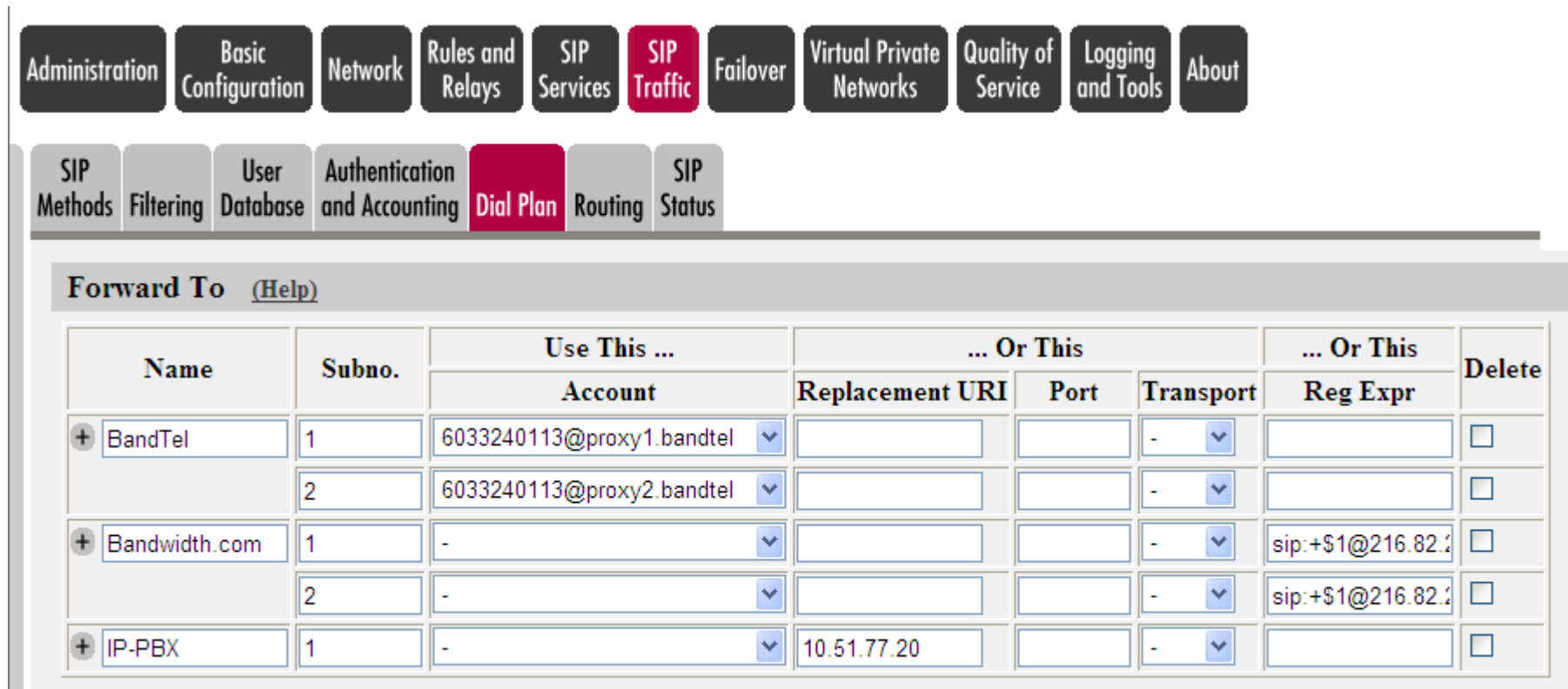
The screenshot shows the Asterisk SIP Traffic configuration interface. The top navigation bar includes buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar includes SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan (highlighted), Routing, and SIP Status. The main content area is titled "Matching Request-URI (Help)" and contains a table with the following data:

Name	Use This Or This	Delete
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
Alt_Inbound	+	613	0..9	7	123.123.123.213		<input type="checkbox"/>
Alt_Outbound			0..9		10.51.77.1		<input type="checkbox"/>
Inbound			-			sip:(.*)@*	<input type="checkbox"/>
Outbound			-			sip:\+?(.*)@10.51	<input type="checkbox"/>

Programming: SIP Traffic

Dial Plan “Forward To”

- Define destinations for the SIP requests



The screenshot shows a web-based configuration interface for SIP Traffic. The top navigation bar includes tabs for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a secondary navigation bar includes SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan (highlighted), Routing, and SIP Status. The main content area is titled "Forward To" with a "(Help)" link. It contains a table with the following columns: Name, Subno., Use This ... Account, ... Or This Replacement URI, Port, Transport, ... Or This Reg Expr, and Delete. The table lists three entries: BandTel, Bandwidth.com, and IP-PBX, each with multiple subnumbers and associated configuration values.

Name	Subno.	Use This Or This			... Or This	Delete
		Account	Replacement URI	Port	Transport	Reg Expr	
+ BandTel	1	6033240113@proxy1.bandtel			-		<input type="checkbox"/>
	2	6033240113@proxy2.bandtel			-		<input type="checkbox"/>
+ Bandwidth.com	1	-			-	sip:+\$1@216.82.2	<input type="checkbox"/>
	2	-			-	sip:+\$1@216.82.2	<input type="checkbox"/>
+ IP-PBX	1	-	10.51.77.20		-		<input type="checkbox"/>

Programming: SIP Traffic

Dial Plan “Dial Plan”

- Combine the **From Header**, **Request-URI** and **Forward To** tables in the **Dial Plan** table.

Administration Basic Configuration Network Rules and Relays SIP Services **SIP Traffic** Failover Virtual Private Networks Quality of Service Logging and Tools About

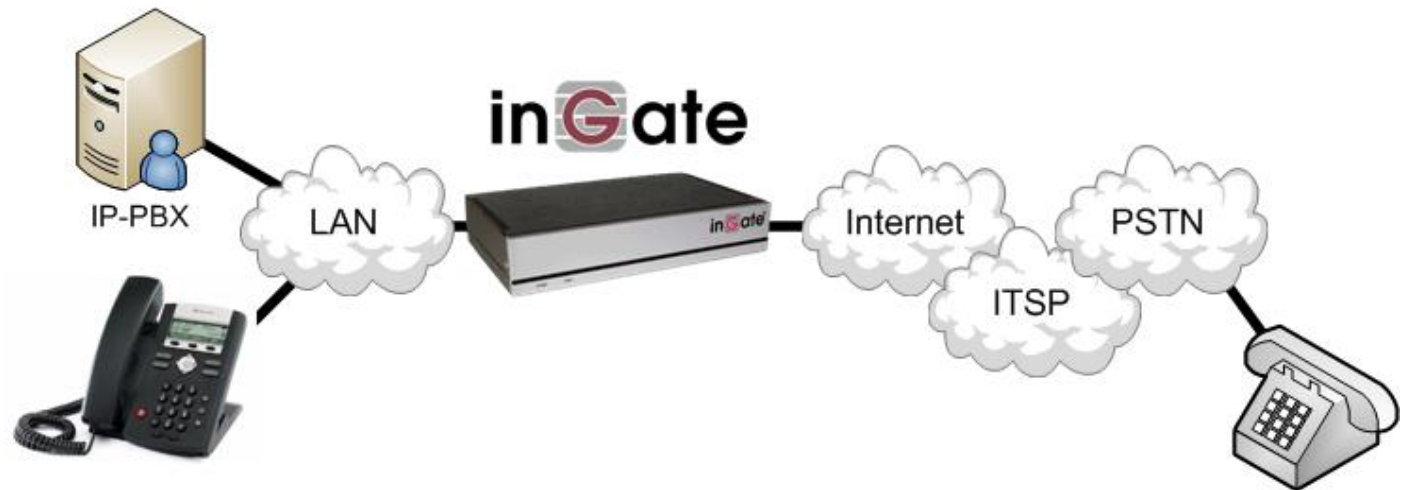
SIP Methods Filtering User Database Authentication and Accounting **Dial Plan** Routing SIP Status

Dial Plan [\(Help\)](#)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete
					Forward	ENUM				
1	Bandwidth.com	Inbound	Forward	IP-PBX			-	-		<input type="checkbox"/>
2	LAN	Outbound	Forward	BandTel			-	-		<input type="checkbox"/>
3	LAN	Outbound	Forward	Bandwidth.com			-	-		<input type="checkbox"/>
4	WAN	-	Reject	-			-	-		<input type="checkbox"/>
5	WAN	Inbound	Forward	IP-PBX			-	-		<input type="checkbox"/>

Programming: SIP Traffic

How Does It Work?



- Outgoing Call
 - SIP Phone sends INVITE to 6135552000@IP_IP-PBX
 - IP-PBX sends INVITE to 6135552000@IP_Ingate
 - Ingate sends INVITE to 6135552000@IP_ITSP
- Incoming Call
 - ITSP sends INVITE to 6135554455@IP_Ingate
 - Ingate sends INVITE to 6135554455@IP_IP-PBX
 - IP-PBX sends INVITE to ExtNumber@IP_Phone

Programming: SIP Traffic

Dial Plan “Method in the Dial Plan”

- Select which methods should be processed by the **Dial Plan**.

The screenshot shows a web-based configuration interface for SIP Traffic. The top navigation bar includes: Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar includes: SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan (highlighted), Routing, and SIP Status. The main content area is titled 'Methods in Dial Plan (Help)' and contains a warning: 'The ACK, PRACK, CANCEL, BYE, NOTIFY, UPDATE and INFO methods cannot be handled by the Dial Plan.' Below the warning is a table with columns 'Method' and 'Delete'. The table lists the following methods: INVITE, OPTIONS, SUBSCRIBE, MESSAGE, and REFER, each with an unchecked checkbox in the 'Delete' column. To the right of the table is a section titled 'REGISTER in Dial Plan (Help)' with two radio button options: 'Keep To headers for REGISTER requests passed through the Dial Plan' (which is selected) and 'Rewrite To headers for REGISTER requests passed through the Dial Plan'.

Method	Delete
INVITE	<input type="checkbox"/>
OPTIONS	<input type="checkbox"/>
SUBSCRIBE	<input type="checkbox"/>
MESSAGE	<input type="checkbox"/>
REFER	<input type="checkbox"/>

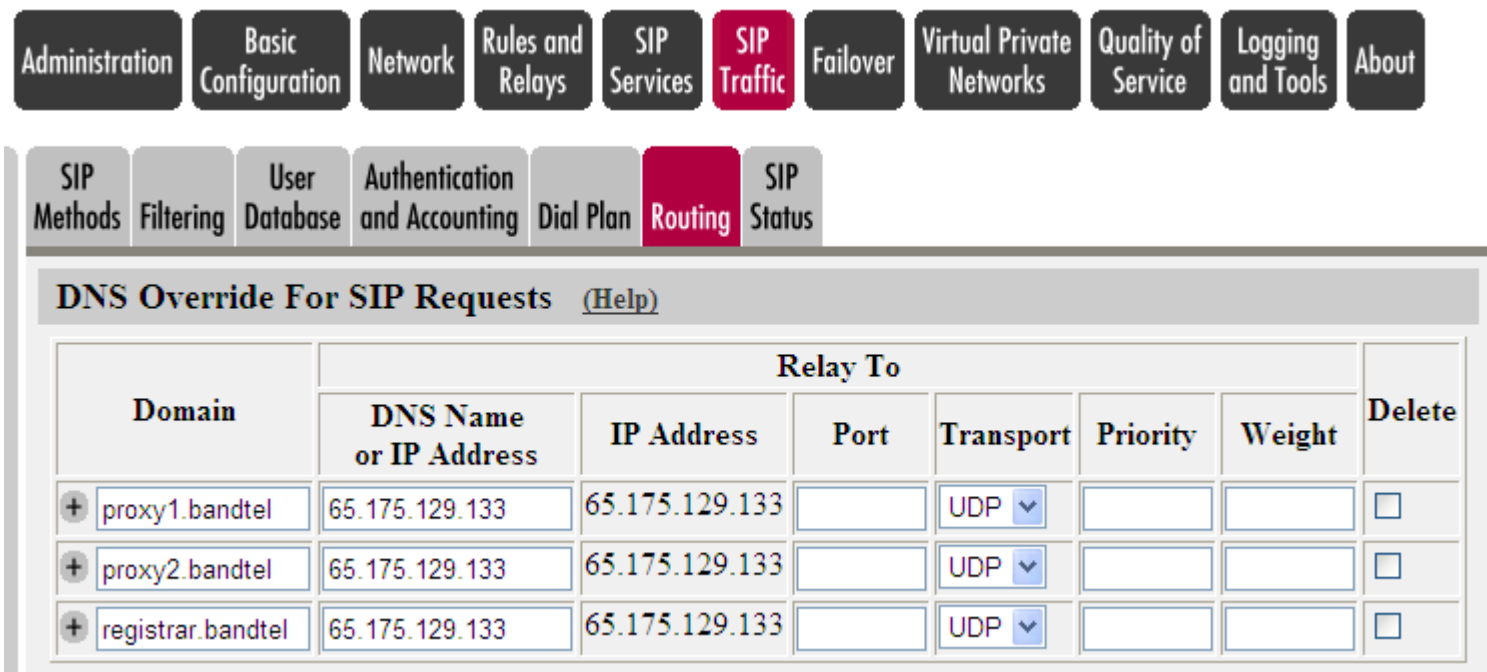
REGISTER in Dial Plan (Help)

- Keep To headers for REGISTER requests passed through the Dial Plan
- Rewrite To headers for REGISTER requests passed through the Dial Plan

Programming: SIP Traffic

Routing “DNS Override for SIP Requests”

- Enter SIP domains to which traffic should be sent, but which for some reason cannot be looked up using DNS



The screenshot displays a web-based configuration interface for SIP Traffic. The top navigation bar includes tabs for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar shows SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan, Routing (highlighted), and SIP Status. The main content area is titled "DNS Override For SIP Requests" with a "(Help)" link. It contains a table with the following structure:

Domain	Relay To						Delete
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	
+ proxy1.bandtel	65.175.129.133	65.175.129.133		UDP			<input type="checkbox"/>
+ proxy2.bandtel	65.175.129.133	65.175.129.133		UDP			<input type="checkbox"/>
+ registrar.bandtel	65.175.129.133	65.175.129.133		UDP			<input type="checkbox"/>

Programming: SIP Traffic

Routing “Class 3XX Processing & SIP Routing Order”

- Class 3xx Messages Processing concerns how to process redirect requests
- SIP Routing Order priorities which function to process first

The screenshot displays a web-based configuration interface for SIP services. At the top, a horizontal menu contains the following items: Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted in red), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a secondary menu includes SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan, Routing (highlighted in red), and SIP Status. The main content area is divided into two sections: 'SIP Routing Order' and 'Class 3xx Message Processing'. The 'SIP Routing Order' section contains a table with three rows, each with a 'No.' field and a 'Routing Function' field. The 'Class 3xx Message Processing' section contains two radio button options: 'Forward all' (selected) and 'Follow redirects'.

No.	Routing Function
1	DNS Override
2	Local Registrar
3	Dial Plan

Forward all
 Follow redirects

Programming: SIP Traffic

Routing “Static Registrations”

- Statically forward the requests from one SIP URI to another.

The screenshot displays the inGate web interface. At the top, a navigation bar contains buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-menu for SIP Services is visible, with 'Routing' highlighted. The main content area is titled 'Static Registrations' with a '(Help)' link. It contains a table with the following structure:

Requests To User	Also Forward To			Delete
	User	sip/sips	Transport	
+ 030060332401136	scott@ingate.com	sip	-	<input type="checkbox"/>

Programming: SIP Traffic

Routing “Local REFER Handling”

- SIP Trunking Service Providers can not handle a REFER Method. Many IP-PBX require to send REFERs for Transferring calls. This ensure the Ingate handles the REFER locally.

The screenshot displays the InGate configuration interface. At the top, a navigation bar contains buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-menu for SIP Services is visible, with Routing highlighted. The main content area is titled 'Local REFER Handling (Help)' and contains the following settings:

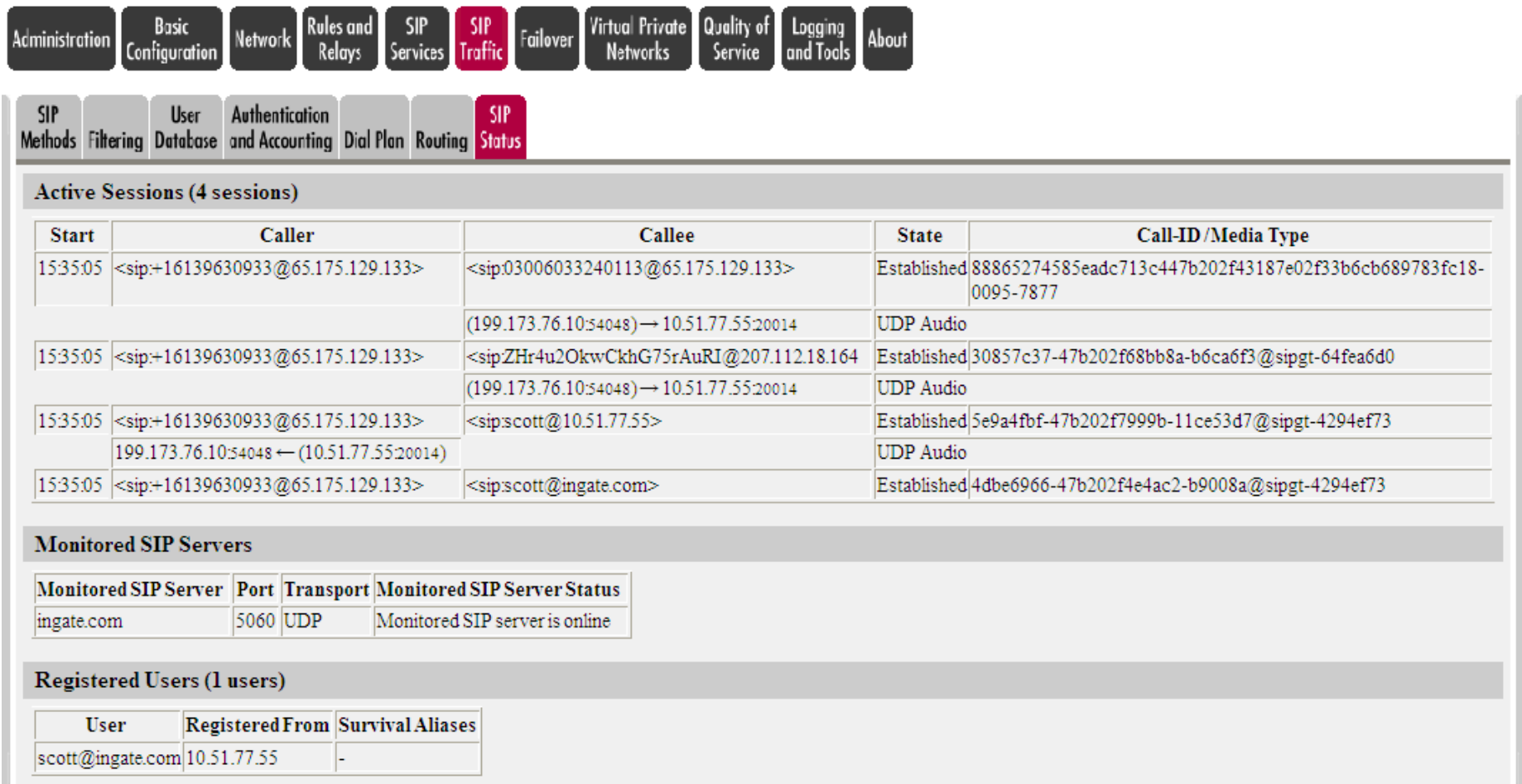
- Always handle REFER locally
- For clients not supporting REFER
- For clients not supporting replaces
- For dialogs with specified From URI

Below these settings, there is a section titled 'From URIs For Which REFER is Handled Locally' with a text input field containing 'URI' and a 'Delete' button.

Programming: SIP Traffic

SIP Status

- Shows current SIP activity



The screenshot shows the Asterisk SIP Status page. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic (highlighted), Failover, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this is a sub-navigation bar with buttons for SIP Methods, Filtering, User Database, Authentication and Accounting, Dial Plan, Routing, and SIP Status (highlighted). The main content area is divided into three sections: Active Sessions (4 sessions), Monitored SIP Servers, and Registered Users (1 users).

Active Sessions (4 sessions)

Start	Caller	Callee	State	Call-ID/Media Type	
15:35:05	<sip:+16139630933@65.175.129.133>	<sip:03006033240113@65.175.129.133>	Established	88865274585eadc713c447b202f43187e02f33b6cb689783fc18-0095-7877	
		(199.173.76.10:54048) → 10.51.77.55:20014	UDP Audio		
15:35:05	<sip:+16139630933@65.175.129.133>	<sip:ZHR4u2OkwCkhG75rAuRI@207.112.18.164	Established	30857c37-47b202f68bb8a-b6ca6f3@sigpt-64fea6d0	
		(199.173.76.10:54048) → 10.51.77.55:20014	UDP Audio		
15:35:05	<sip:+16139630933@65.175.129.133>	<sip:scott@10.51.77.55>	Established	5e9a4fbf-47b202f7999b-11ce53d7@sigpt-4294ef73	
	199.173.76.10:54048 ← (10.51.77.55:20014)		UDP Audio		
15:35:05	<sip:+16139630933@65.175.129.133>	<sip:scott@ingate.com>	Established	4dbe6966-47b202f4e4ac2-b9008a@sigpt-4294ef73	

Monitored SIP Servers

Monitored SIP Server	Port	Transport	Monitored SIP Server Status
ingate.com	5060	UDP	Monitored SIP server is online

Registered Users (1 users)

User	Registered From	Survival Aliases
scott@ingate.com	10.51.77.55	-

Exercise #2

Dial Plan

Overall Training Setup

Training Station #2



Softphone
DID #: 6135552222
IP Address: 10.20.20.20

Laptop
IP Address: 10.20.20.20
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A9-7F-15
Eth0 (Inside) IP Address: 10.20.20.22
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.22
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #3



Softphone
DID #: 6135553333
IP Address: 10.30.30.30

Laptop
IP Address: 10.30.30.30
Mask: 255.255.255.0
Default GW: 10.30.30.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-63
Eth0 (Inside) IP Address: 10.30.30.33
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.33
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #1



Softphone
DID #: 6135551111
IP Address: 10.10.10.10

Laptop
IP Address: 10.10.10.10
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-39
Eth0 (Inside) IP Address: 10.10.10.11
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.11
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

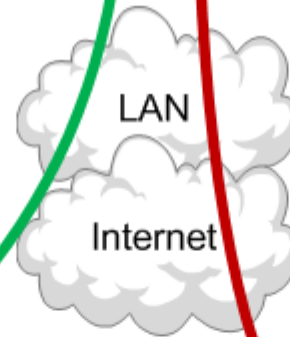
Training Station #4



Softphone
DID #: 6135554444
IP Address: 10.40.40.40

Laptop
IP Address: 10.40.40.40
Mask: 255.255.255.0
Default GW: 10.40.40.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-AD-B5-02
Eth0 (Inside) IP Address: 10.40.40.44
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.44
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Exercise #3

SIP Security – Lock to Source IP

Overall Training Setup

Training Station #2



Softphone
DID #: 6135552222
IP Address: 10.20.20.20

Laptop
IP Address: 10.20.20.20
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A9-7F-15
Eth0 (Inside) IP Address: 10.20.20.22
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.22
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #3



Softphone
DID #: 6135553333
IP Address: 10.30.30.30

Laptop
IP Address: 10.30.30.30
Mask: 255.255.255.0
Default GW: 10.30.30.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-63
Eth0 (Inside) IP Address: 10.30.30.33
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.33
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #1



Softphone
DID #: 6135551111
IP Address: 10.10.10.10

Laptop
IP Address: 10.10.10.10
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-39
Eth0 (Inside) IP Address: 10.10.10.11
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.11
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

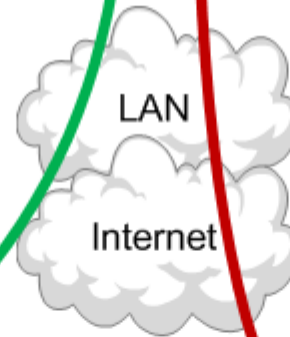
Training Station #4



Softphone
DID #: 6135554444
IP Address: 10.40.40.40

Laptop
IP Address: 10.40.40.40
Mask: 255.255.255.0
Default GW: 10.40.40.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-AD-B5-02
Eth0 (Inside) IP Address: 10.40.40.44
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.44
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Troubleshooting

Troubleshooting

Logging Configuration

- SIP Events will ensure SIP calls are logged.

The screenshot shows a web-based configuration interface. At the top, there is a navigation bar with buttons for Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools (highlighted in red), and About. Below this is a sub-navigation bar with buttons for Display Log, Packet Capture, Check Network, Logging Configuration (highlighted in red), Log Classes, and Log Sending. The main content area is titled "Logging Configuration" and contains two columns of settings. The left column is for "VPN Events" and the right column is for "SIP Events". Each setting consists of a label and a dropdown menu, all of which are currently set to "Local".

VPN Events (Help)	SIP Events (Help)
Log class for IPsec key negotiations: Local	Log class for SIP signaling: Local
Log class for IPsec key negotiation debug messages: -	Log class for SIP packets: Local
Log class for IKE and NAT-T packets: Local	Log class for SIP license messages: Local
Log class for ESP packets: -	Log class for SIP errors: Local
Log class for IPsec user authentications: Local	Log class for SIP media messages: Local
Log class for packets to and from blacklisted IP addresses: Local	Log class for SIP debug messages: Local

Troubleshooting

Logging & Tools

- Display # Rows/Page
- Show Newest on Top
- Select SIP Log Attributes
- Select “Show internal SIP Signaling”

Display Log Packet Capture Check Network Display Load Logging Configuration Log Classes Log Sending

Search the Log (Help)
Display log: 800 rows/page (timeout: seconds)
 Periodical search: 30 seconds until next search

Support Report (Help)
Include configuration database:
 Yes No
Make sure the Log class for SIP debug messages is set to Local if you have a SIP-related problem.
Export support report

Packet selection: only those packets that meet the search criteria in the three sections below will be selected. This selection will only have effect on the IP packets as selected choice.

Packet Type Selection
All packets

IP Address Selection (Help)
A: not this address
B: not this address
 A src A dst A any
 A to B B to A Between A&B not this combination

Protocol/Port Selection
 All IP protocols
 TCP
 UDP
 ICMP
 ESP
 Protocol number: (Help) not

SIP Packet Selection (Help)
Call-ID: Show internal SIP signaling
SIP Methods:
IP addresses:
From Header:
To Header:

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 This
 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

Troubleshooting

Packet Capture

- Creates a Wireshark PCAP network trace.
- Network Interface Selection – All Interfaces
- Start – Stop - Download

The screenshot shows the InGate Firewall web interface for Packet Capture configuration. The top navigation bar includes: Administration, Basic Configuration, Network, Rules and Relays, SIP Services, SIP Traffic, Failover, Virtual Private Networks, Quality of Service, Logging and Tools (highlighted), and About. The main content area has a sub-navigation bar with: Display Log, Packet Capture (highlighted), Check Network, Logging Configuration, Log Classes, and Log Sending. The page displays the following information:

- Capture status: Inactive Captured data size: 17 kB
- Text: Ingate Firewall has a built-in packet capture function which produces pcap trace files. You can select to capture traffic on one specific interface or on all interfaces.
- Text: For contacts with the Ingate Support Team, a packet capture is not what is usually expected (sometimes it is even not useful). For these purposes, please always send a Support Report .
- Section: Network Interface Selection
 - Dropdown menu: All Interfaces
 - Text: You can also select the type of IP packets to capture, based on IP address, protocol and port.
- Section: IP Address Selection (Help)
 - A: not this address
 - B: not this address
 - Radio buttons: A src A dst A any
 - Radio buttons: A to B B to A Between A&B not this combination
- Section: Protocol/Port Selection
 - All IP protocols
 - TCP
 - UDP
 - ICMP
 - ESP
 - Protocol number: (Help) not
- Buttons: Start capture, Stop capture, Download captured data, Delete captured data

Exercise #4

Packet Capture

THE END

inGgate

Overall Training Setup

Training Station #2



Softphone
DID #: 6135552222
IP Address: 10.20.20.20

Laptop
IP Address: 10.20.20.20
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A9-7F-15
Eth0 (Inside) IP Address: 10.20.20.22
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.22
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #3



Softphone
DID #: 6135553333
IP Address: 10.30.30.30

Laptop
IP Address: 10.30.30.30
Mask: 255.255.255.0
Default GW: 10.30.30.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-63
Eth0 (Inside) IP Address: 10.30.30.33
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.33
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Training Station #1



Softphone
DID #: 6135551111
IP Address: 10.10.10.10

Laptop
IP Address: 10.10.10.10
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-39
Eth0 (Inside) IP Address: 10.10.10.11
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.11
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

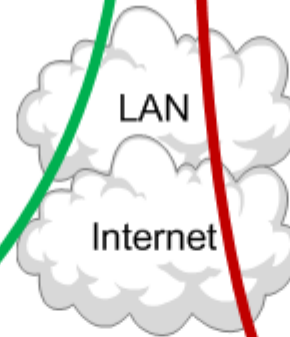
Training Station #4



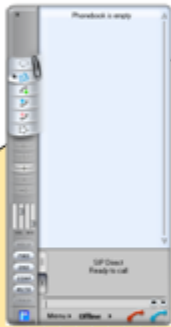
Softphone
DID #: 6135554444
IP Address: 10.40.40.40

Laptop
IP Address: 10.40.40.40
Mask: 255.255.255.0
Default GW: 10.40.40.1
DNS: 65.175.129.149

Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-AD-B5-02
Eth0 (Inside) IP Address: 10.40.40.44
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.44
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Training Station #1



Softphone

DID #: 6135551111
IP Address: 10.10.10.10



Laptop

IP Address: 10.10.10.10
Mask: 255.255.255.0
Default GW: 10.10.10.1
DNS: 65.175.129.149



Ingate SIParator 19

Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-39
Eth0 (Inside) IP Address: 10.10.10.11
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.11
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Softphone

Call Training Station #2:
6135552222@10.10.10.11

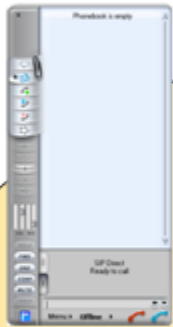
MAKE A CALL



Training Station #2

IP Address: 123.123.123.22
Softphone DID: 6135552222

Training Station #2



Softphone

DID #: 6135552222
IP Address: 10.20.20.20



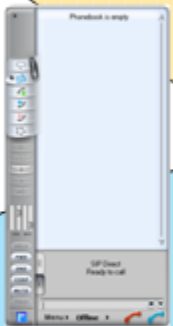
Laptop

IP Address: 10.20.20.20
Mask: 255.255.255.0
Default GW: 10.20.20.1
DNS: 65.175.129.149



Ingate SIParator 19

Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-7F-15
Eth0 (Inside) IP Address: 10.20.20.22
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.22
Mask: 255.255.255.0
Default GW: 123.123.123.1
DNS: 65.175.129.149



Softphone

Call Training Station #1:
6135551111@10.20.20.22

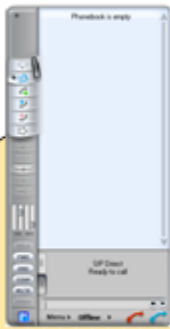
MAKE A CALL



Training Station #1

IP Address: 12.34.56.11
Softphone DID: 6135551111

Training Station #3



Softphone

DID #: 6135553333
IP Address: 10.30.30.30



Laptop

IP Address: 10.30.30.30
Mask: 255.255.255.0
Default GW: 10.30.30.1
DNS: 65.175.129.149



Ingate SIParator 18

Username: admin
Password: admin
MAC Address: 00-D0-C9-A5-81-63
Eth0 (Inside) IP Address: 10.30.30.33
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.33
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Softphone

Call Training Station #4:
6135554444@10.30.30.33

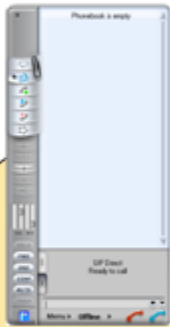
MAKE A CALL



Training Station #4

IP Address: 12.34.56.44
Softphone DID: 6135554444

Training Station #4



Softphone

DID #: 6135554444
IP Address: 10.40.40.40



Laptop

IP Address: 10.40.40.40
Mask: 255.255.255.0
Default GW: 10.40.40.1
DNS: 65.175.129.149



Ingate SIParator 19

Username: admin
Password: admin
MAC Address: 00-D0-C9-AD-B5-02
Eth0 (Inside) IP Address: 10.40.40.44
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.44
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149



Softphone

Call Training Station #3:
6135553333@10.40.40.44

MAKE A CALL



Training Station #3

IP Address: 123.123.123.33
Softphone DID: 6135553333