Ingate Firewall & SIParator Product Training

SIP Trunking Focused

inGate

Common SIP Applications

SIP Trunking

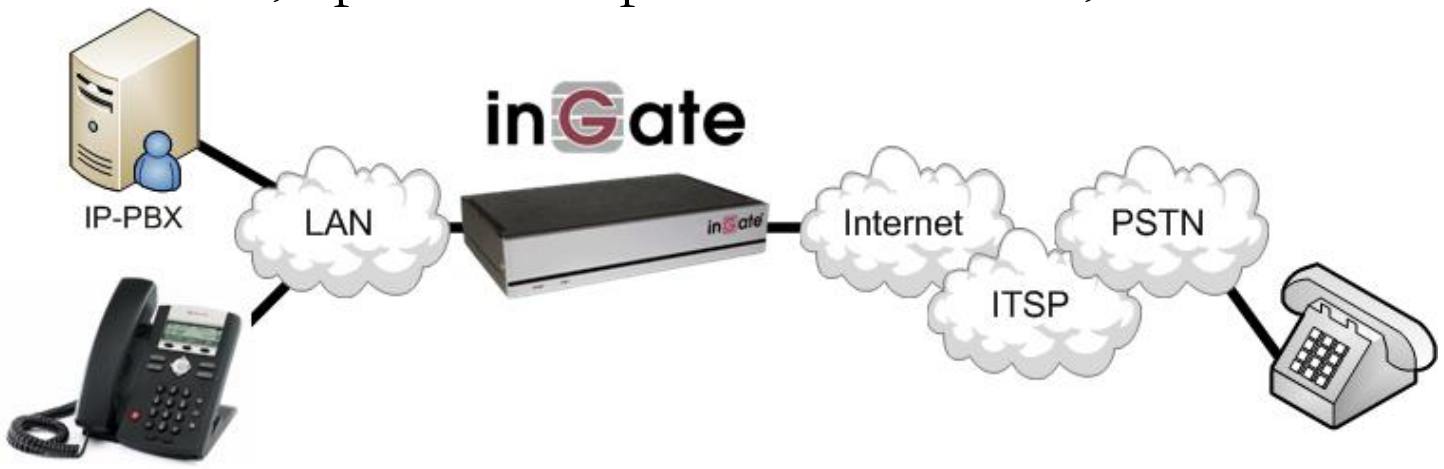
Remote Desktop

inGate

Ingate Product Training

Common SIP Applications

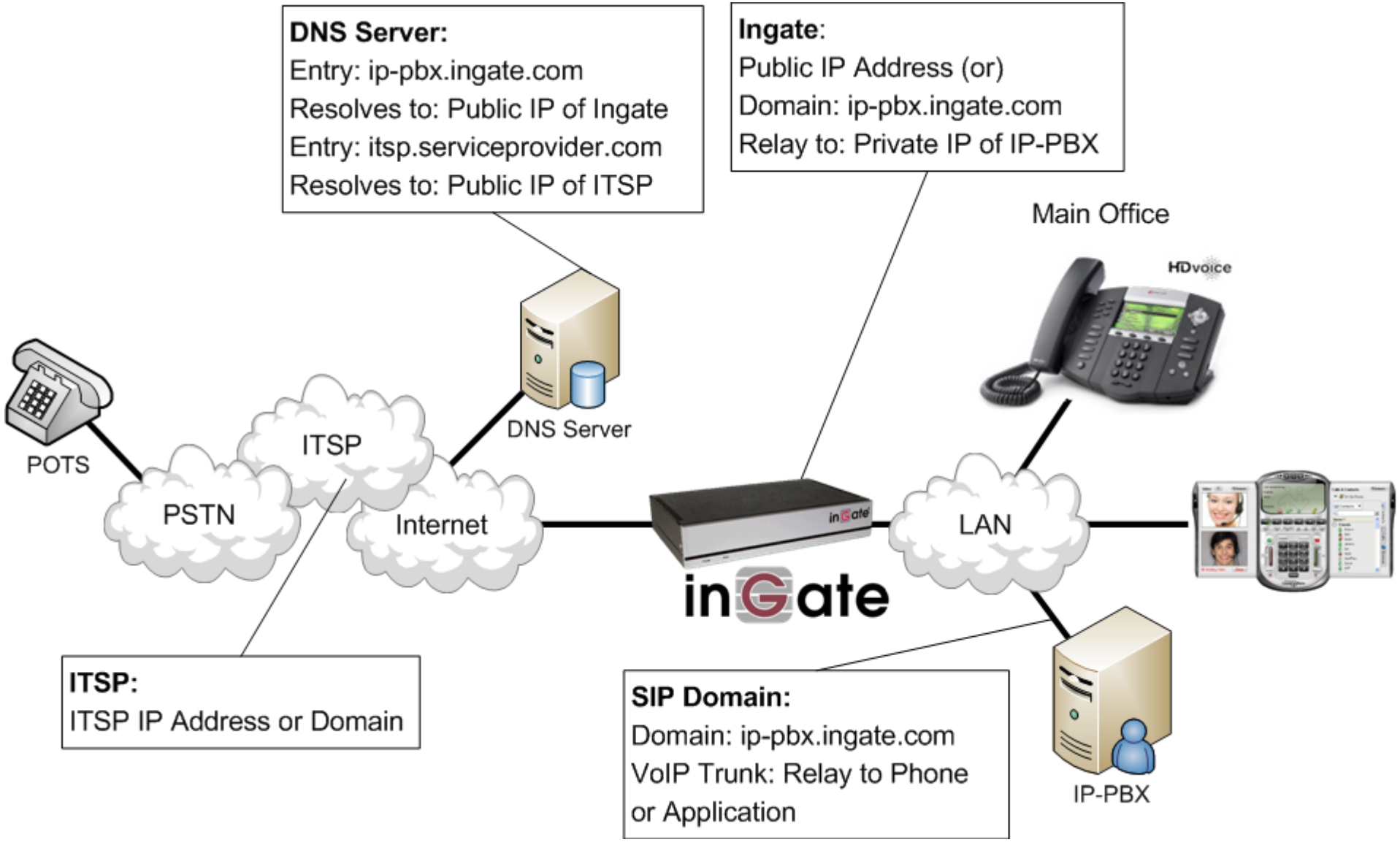
- SIP Trunking
  - A SIP Trunk is a concurrent call that is routed over the IP backbone of a carrier (ITSP) using VoIP technology.
  - SIP Trunks are used in conjunction with an IP-PBX and are thought of as replacements for traditional PRI or analog circuits.
  - The popularity of SIP Trunks is due primarily 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

Ingate Product Training

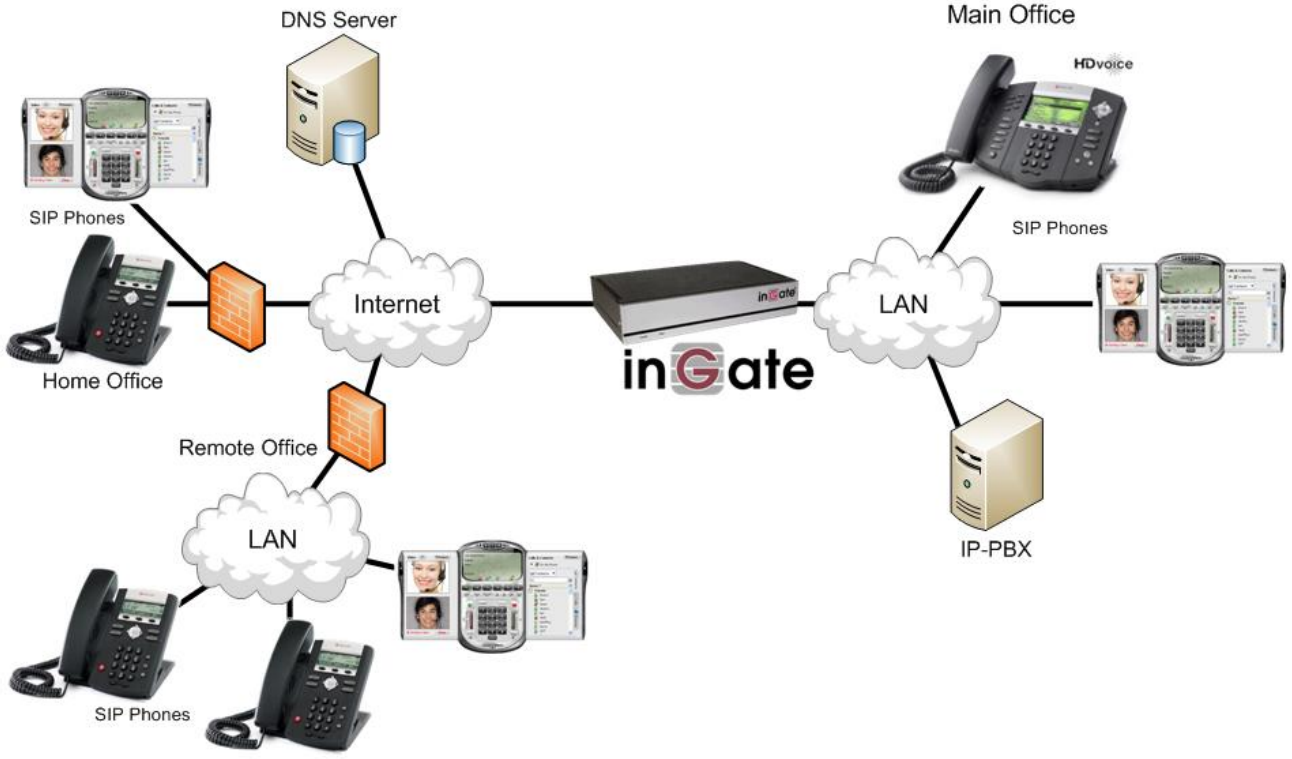
Common SIP Applications



Ingate Product Training

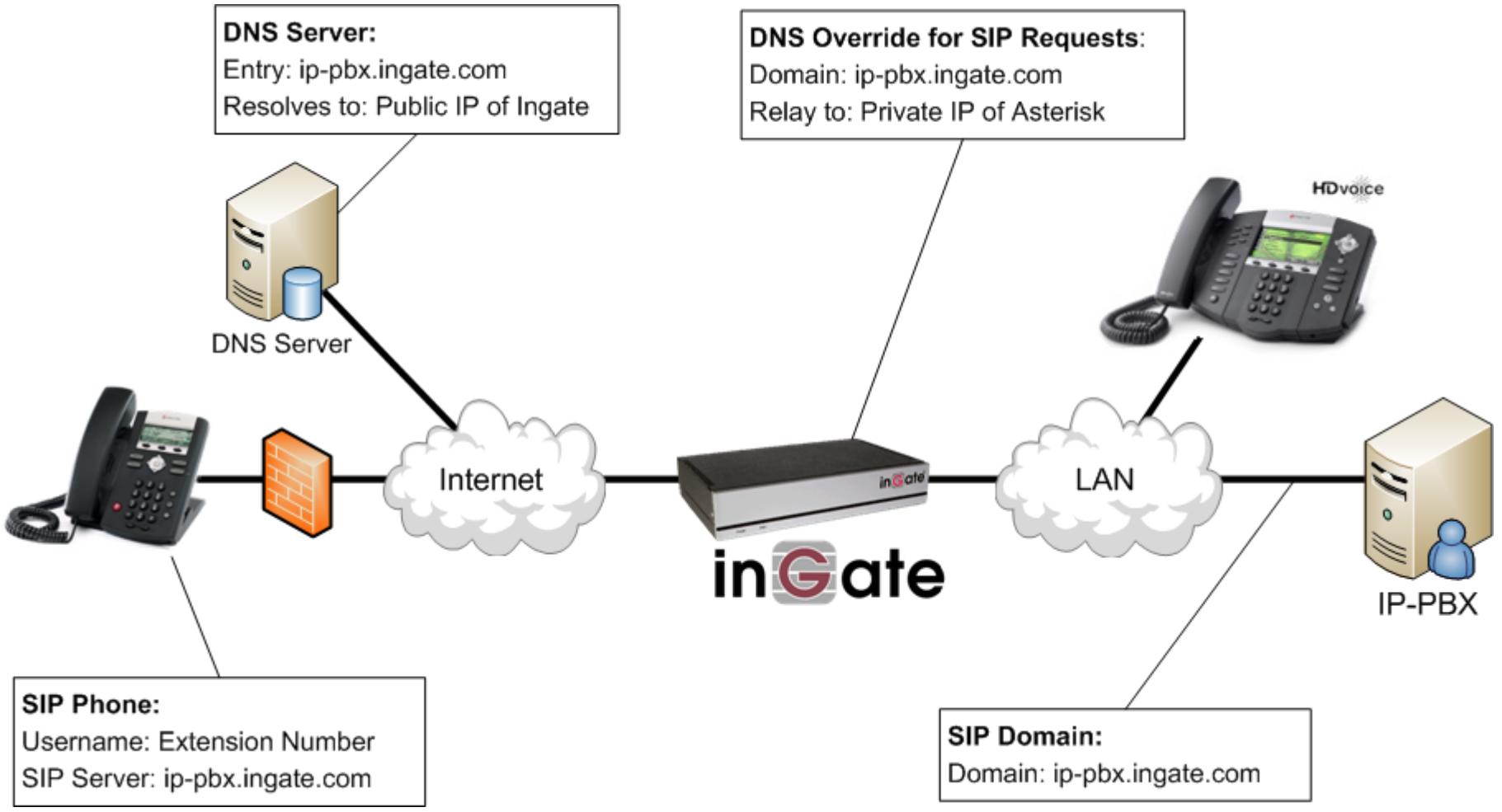
Common SIP Applications

- 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



inGate

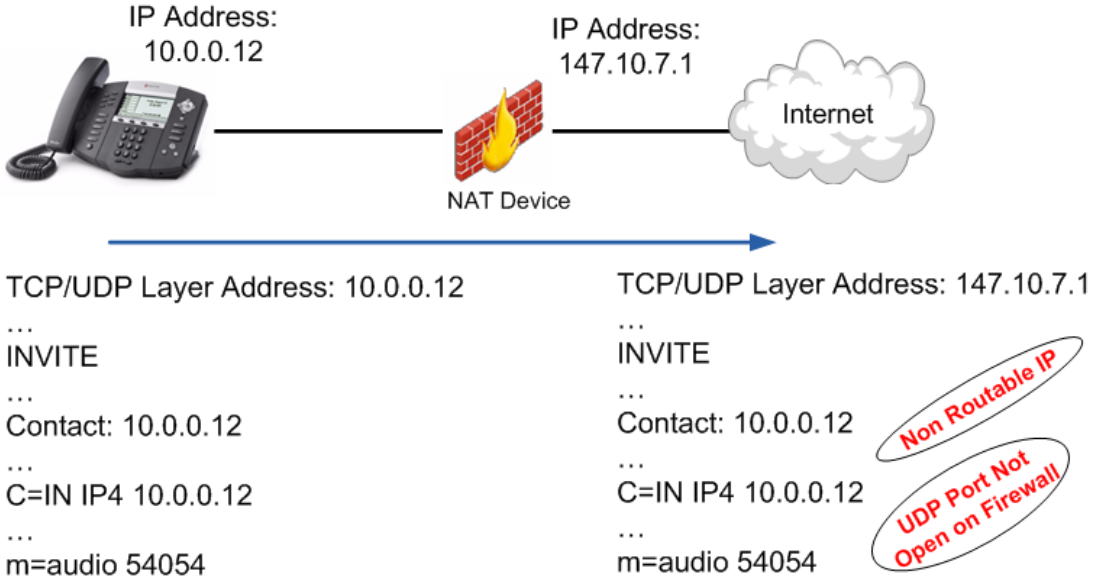
Common SIP Deployment Issues

inGate

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

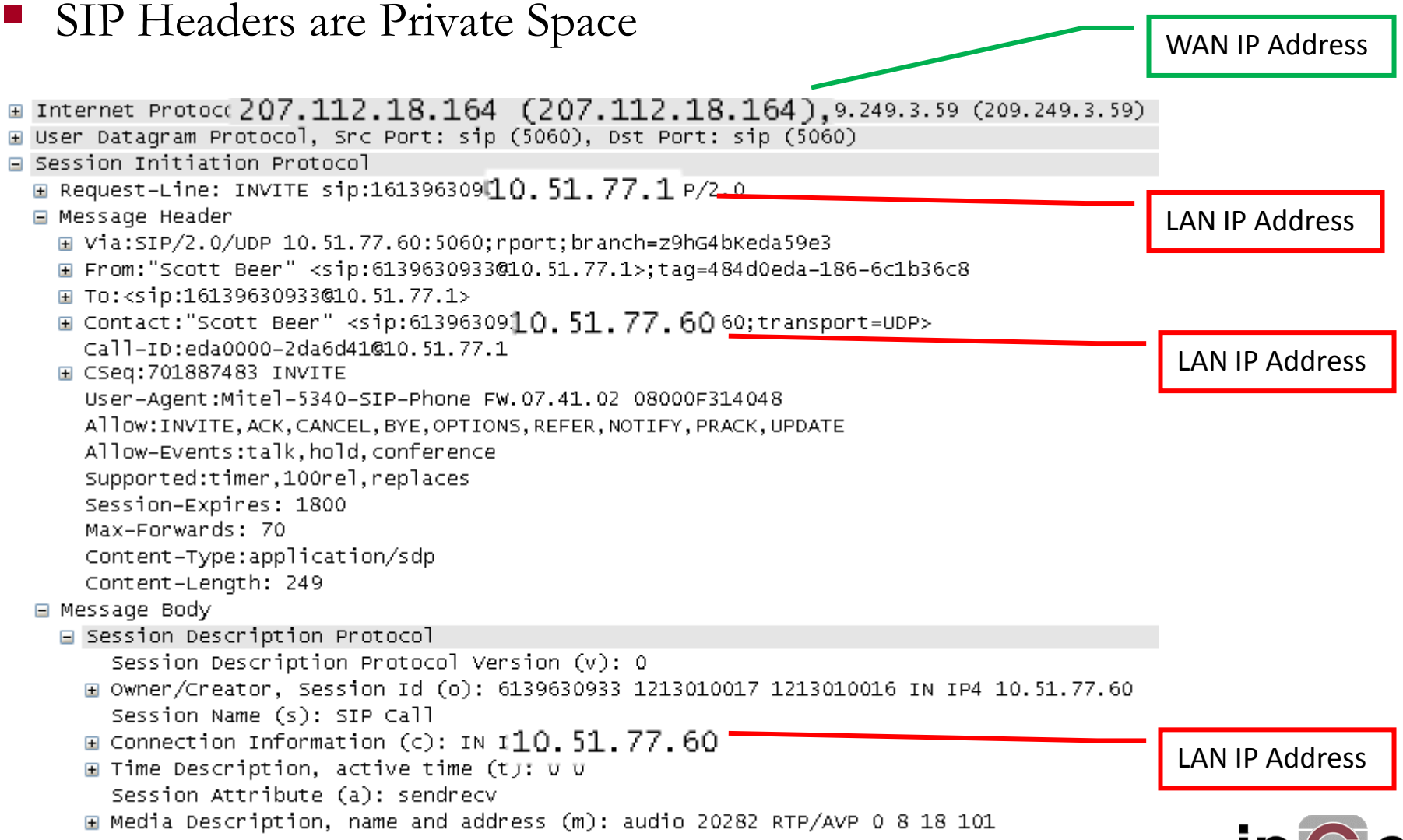
Common Deployment Issues

- **Before NAT**
  - TCP/IP Header is Private Space
  - SIP Headers are Private Space

Ingate Product Training

Common Deployment Issues

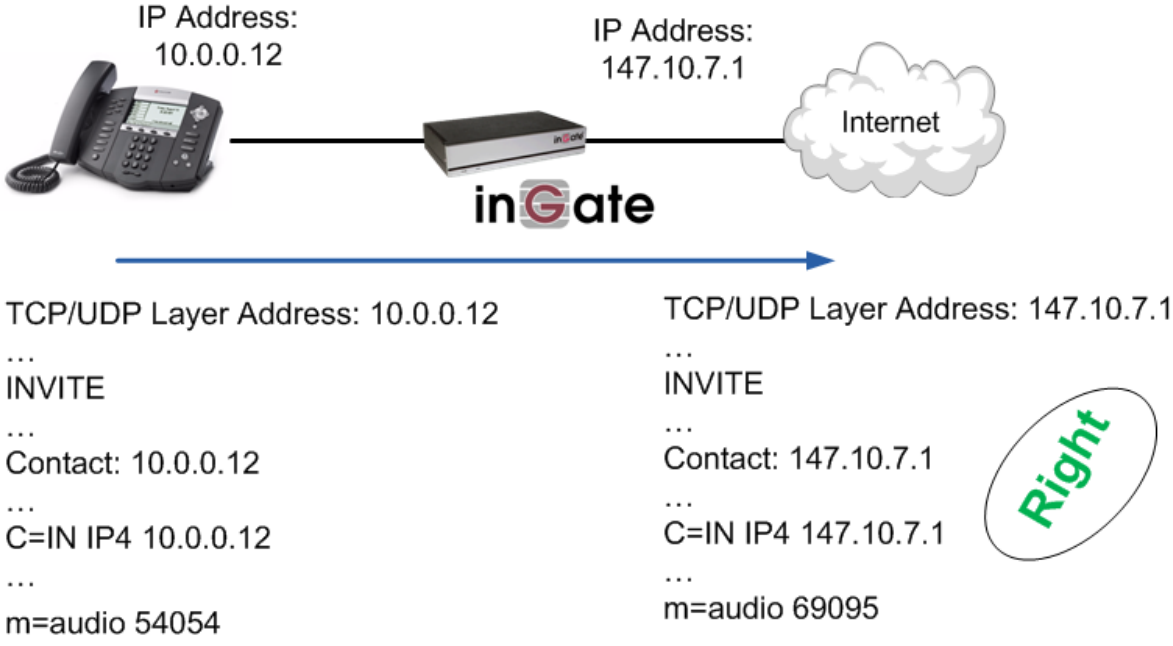
- **After NAT**
  - TCP/IP Header is Public Space
  - SIP Headers are Private Space



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

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

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 an 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

Ingate Product Training

Common Deployment Issues

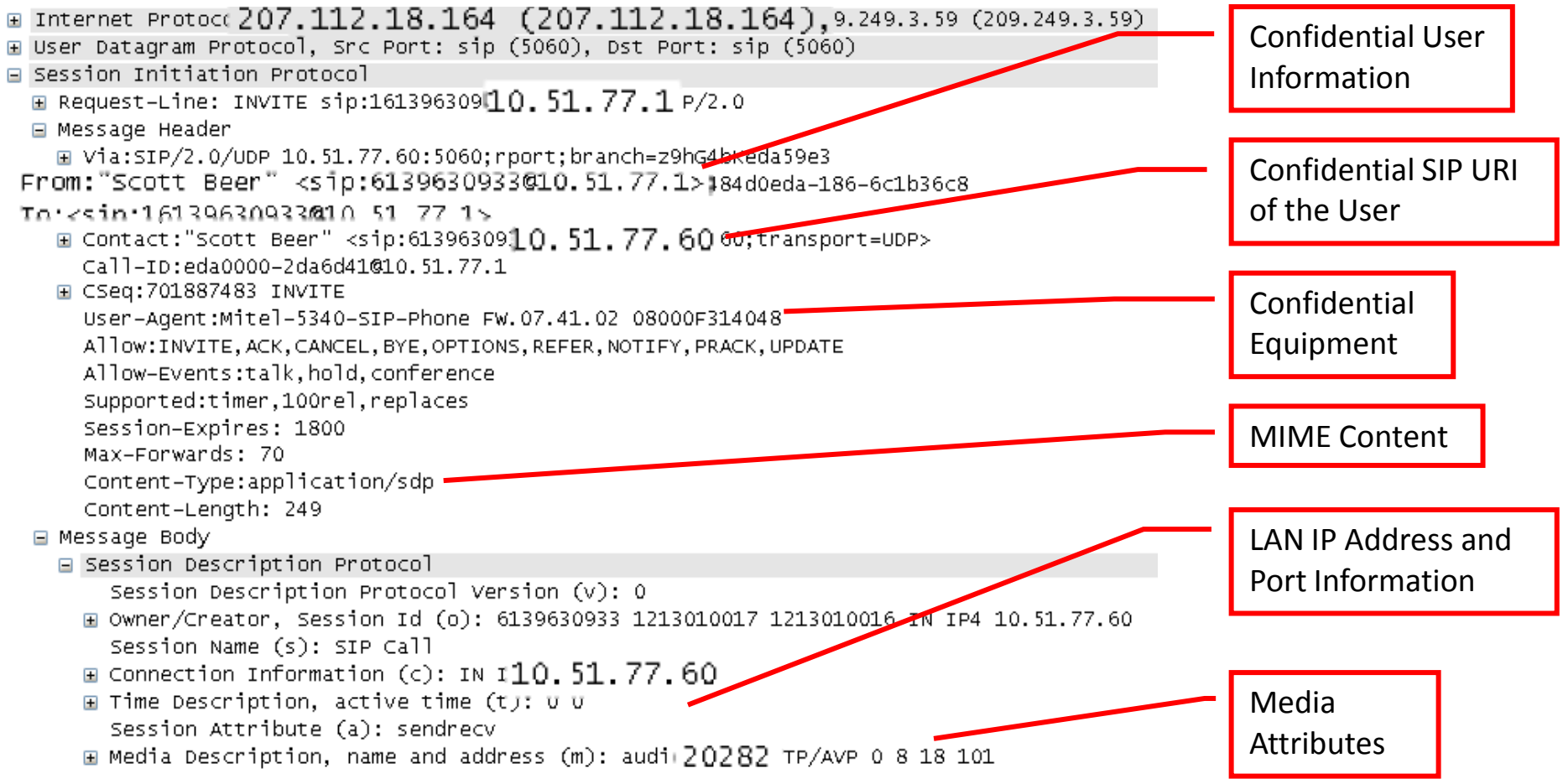
- **Problem #3 – SIP Security**
  - SIP is written in clear text within the datagram of a UDP or TCP Transport.
  - Confidential User/SIP URI Information
    - A SIP URI is like an Email Address, once someone has it, they who you are and where you are located.
    - The malicious person or software can send SIP Request after SIP Request to your SIP URI. Some malicious uses like DoS Attacks, SPIT Attacks, Intrusion of Services, Toll Fraud, Tele-markers 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

Ingate Product Training

Common Deployment Issues

- **Why is SIP Insecure?**
  - Written in clear text within the datagram of a UDP or TCP Transport.



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

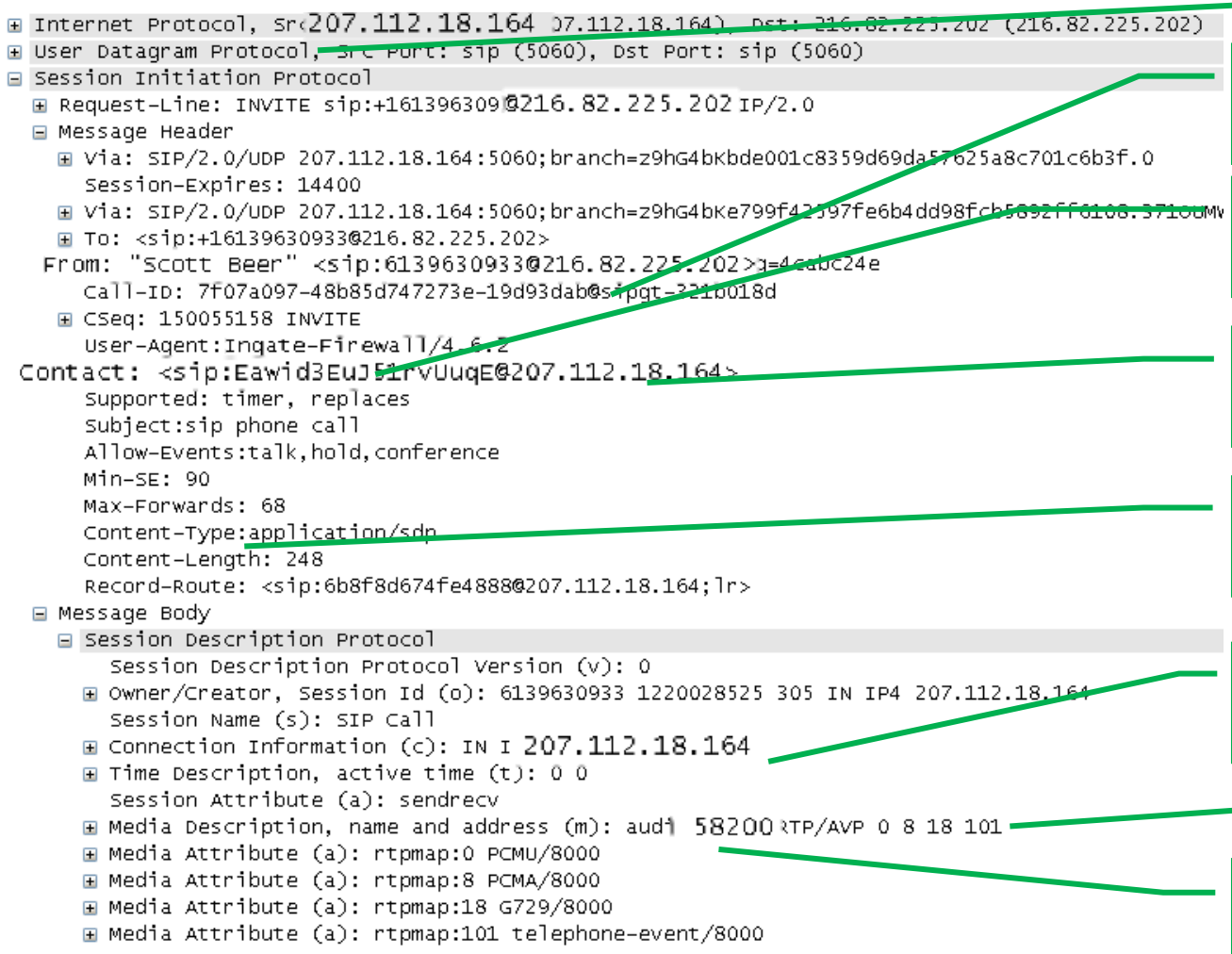
- **Resolution #3 – SIP Security**
  - Dynamic Encryption of SIP URI
    - Using the SIP Specification, enforce an Encrypted SIP URI where possible
  - Dynamic Port Allocation
    - Dynamically change ports on every call.
  - Hide LAN IP Address Scheme
    - Apply LAN to WAN Network Address Translation 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 statics 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

Ingate Product Training

Common Deployment Issues

- **How to make SIP Secure**



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

inGate

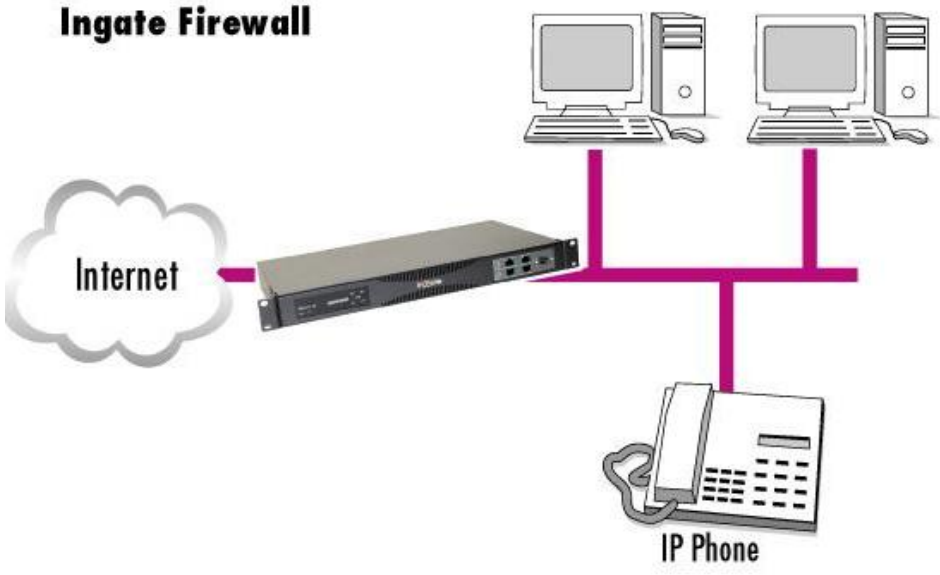
Introduction to Ingate Products

inGate

Ingate products

Firewalls

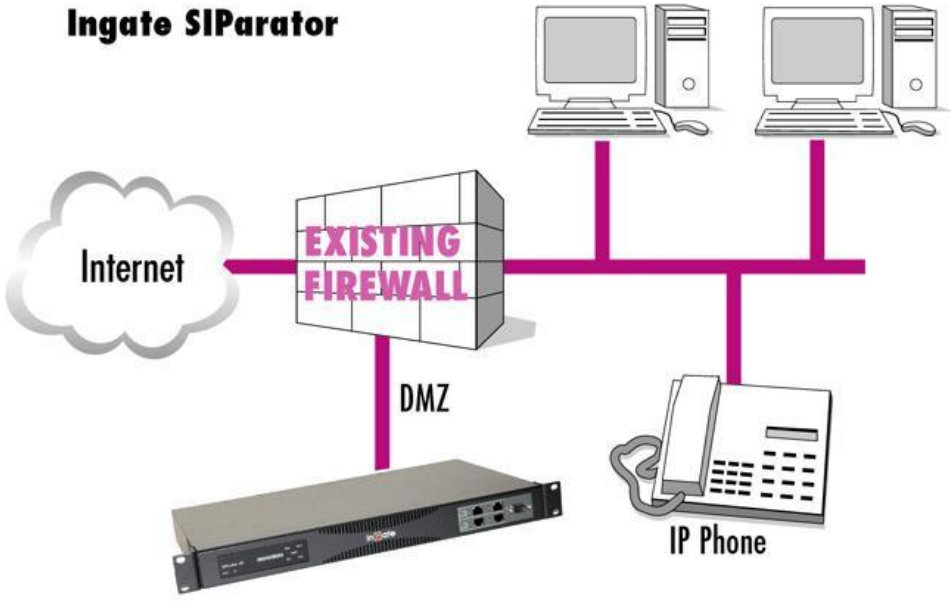
SIP-capable firewalls for computer security and communication



New and replacement installations

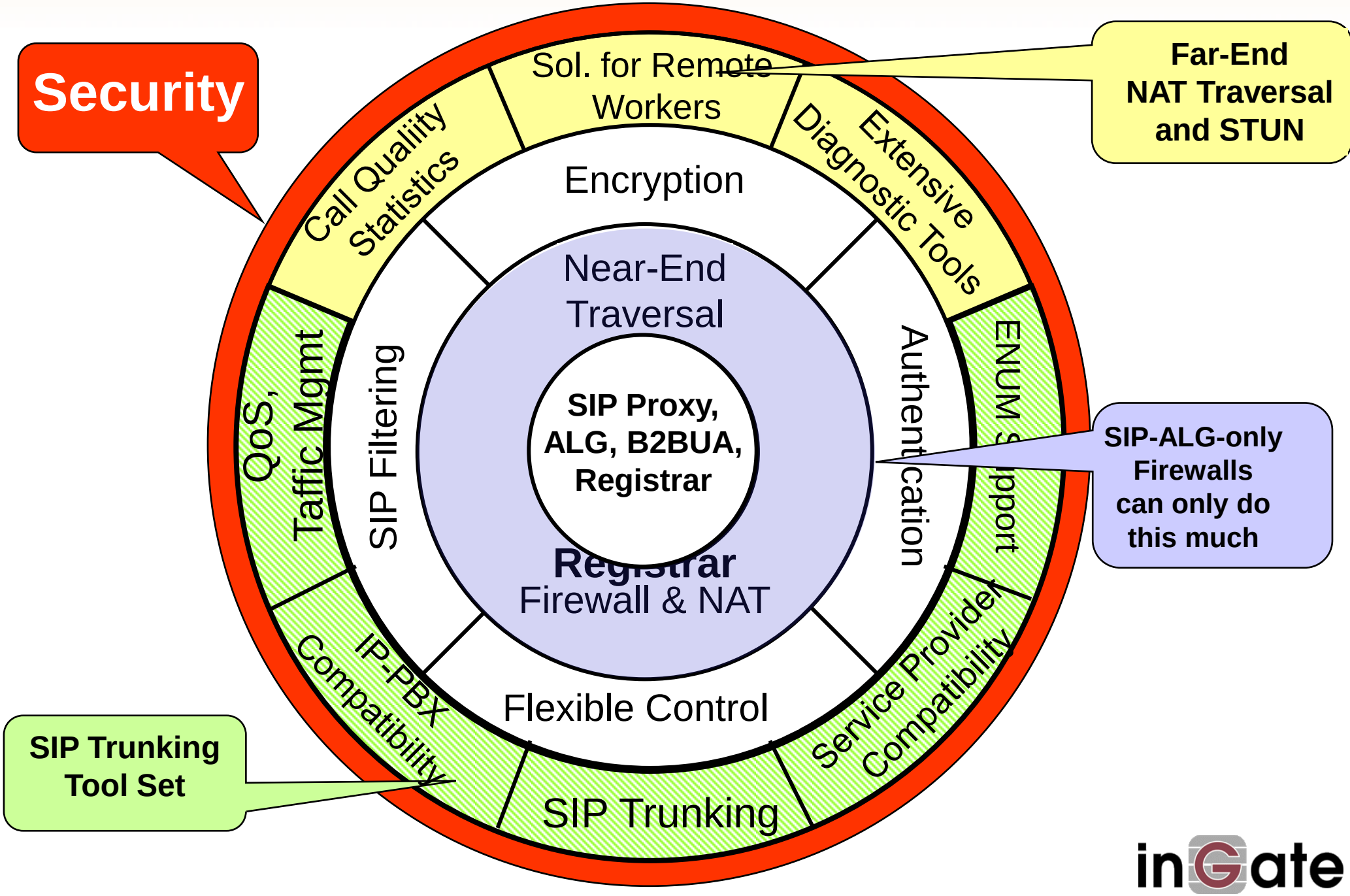
SIParator™

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



Preserve firewall investment and keep established security policies

Extensive SIP Feature Set



inGate

The Ingate Product Family

SW upgradable

SW upgradable

Firewall® 1190
or
SIParator® 19

50 Calls*

Firewall® 1500
or
SIParator®50

150 Calls*

Firewall® 1550
or
SIParator®55

350 Calls*

Firewall® 1650
or
SIParator® 65

650 Calls*

Firewall® 1950
or
SIParator® 95

1 800 Calls*

Licenses

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

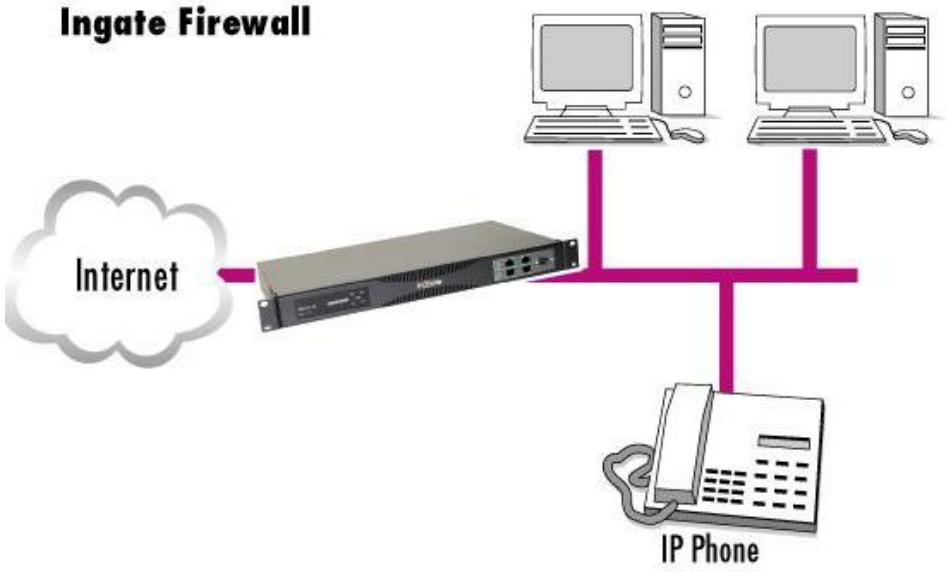
Capacity
- **Additional SIP Traversals**

* Calls = Maximum Concurrent RTP Sessions = SIP Trunks

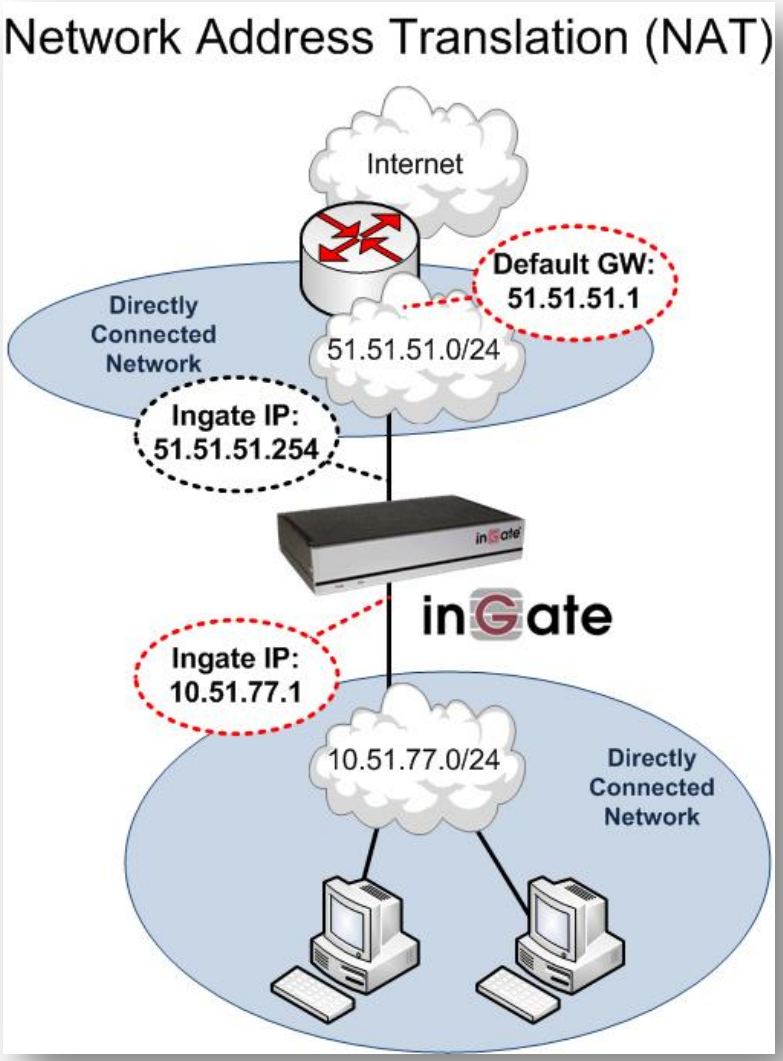
inGate

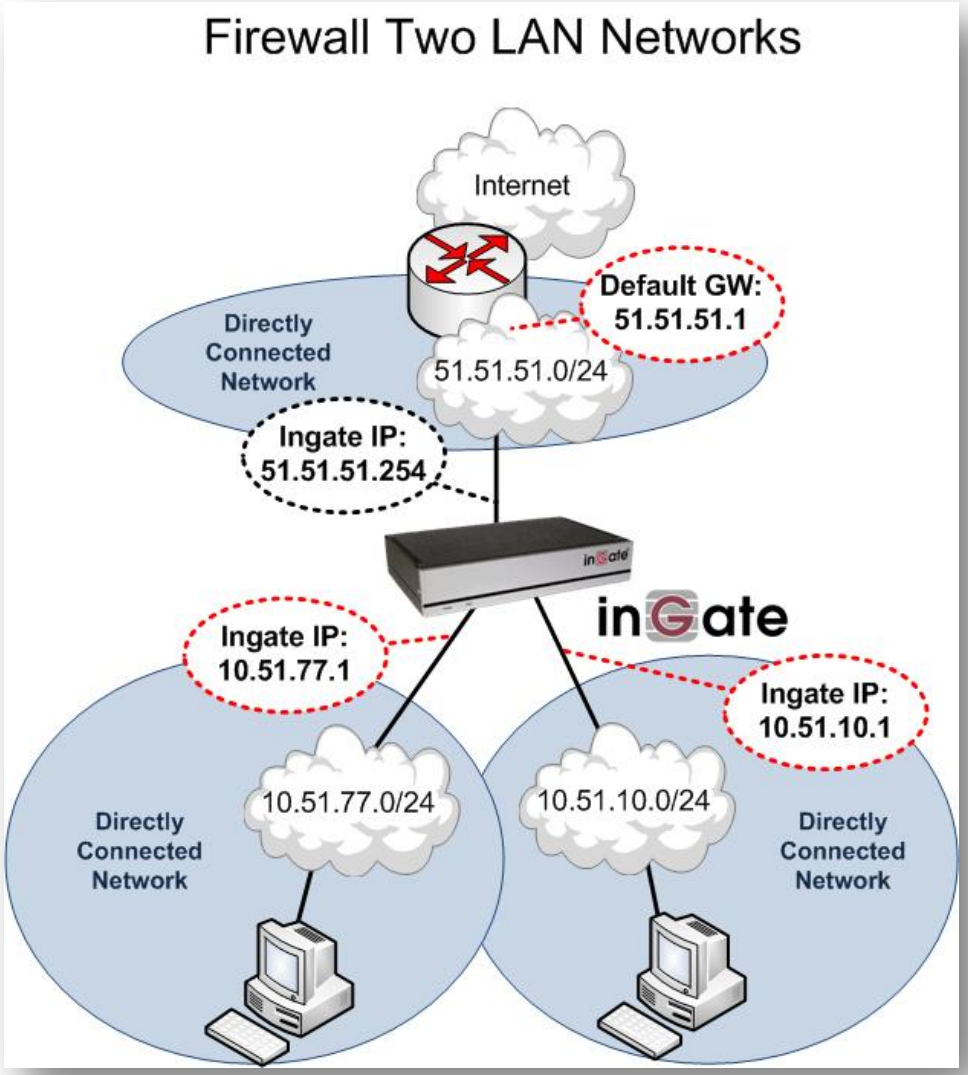
Connecting the Firewall

- 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



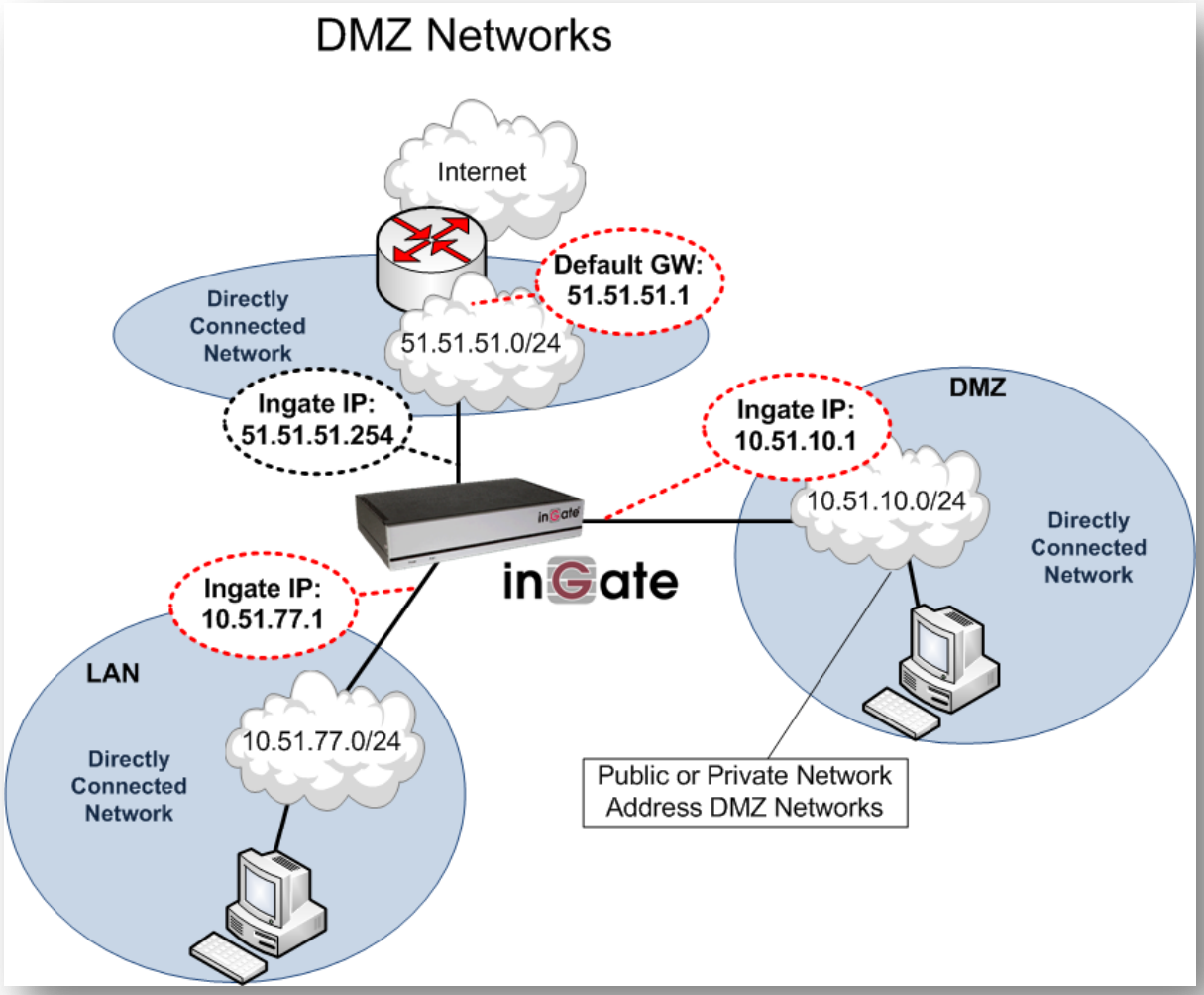
Connecting the Firewall

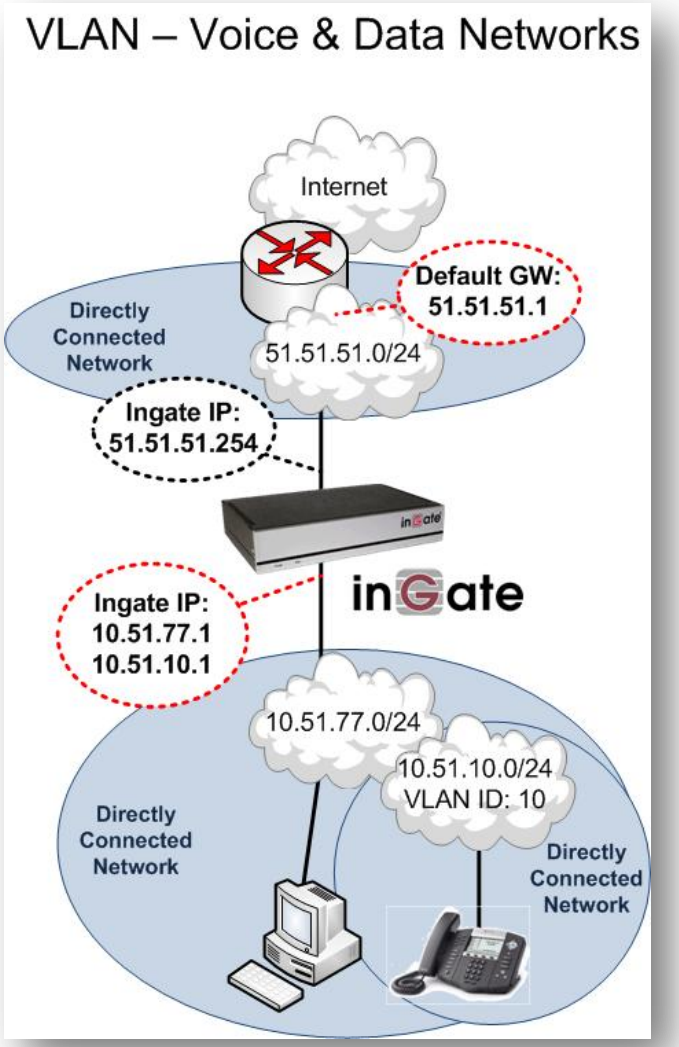




inGate

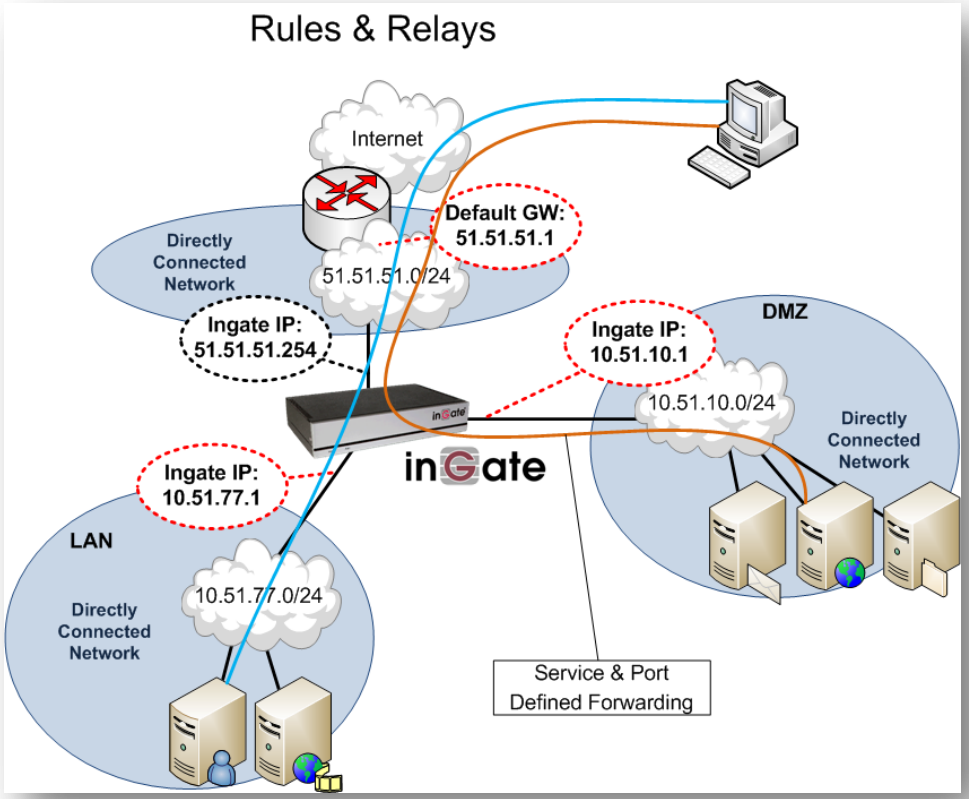
Connecting the Firewall

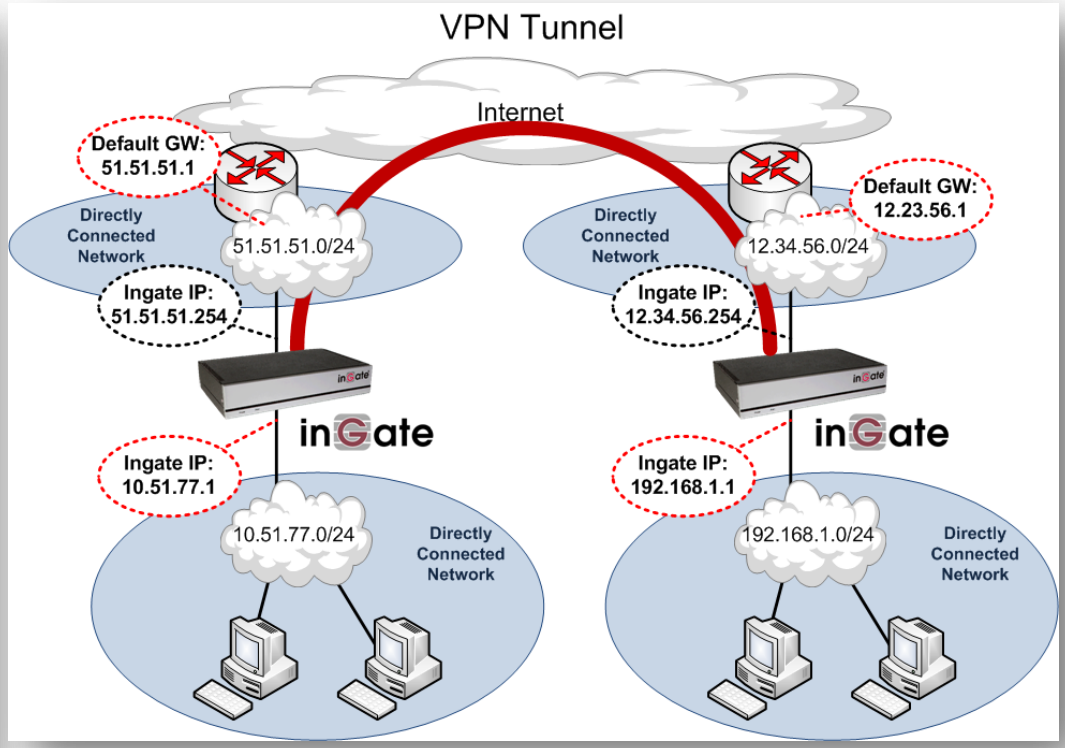




inGate

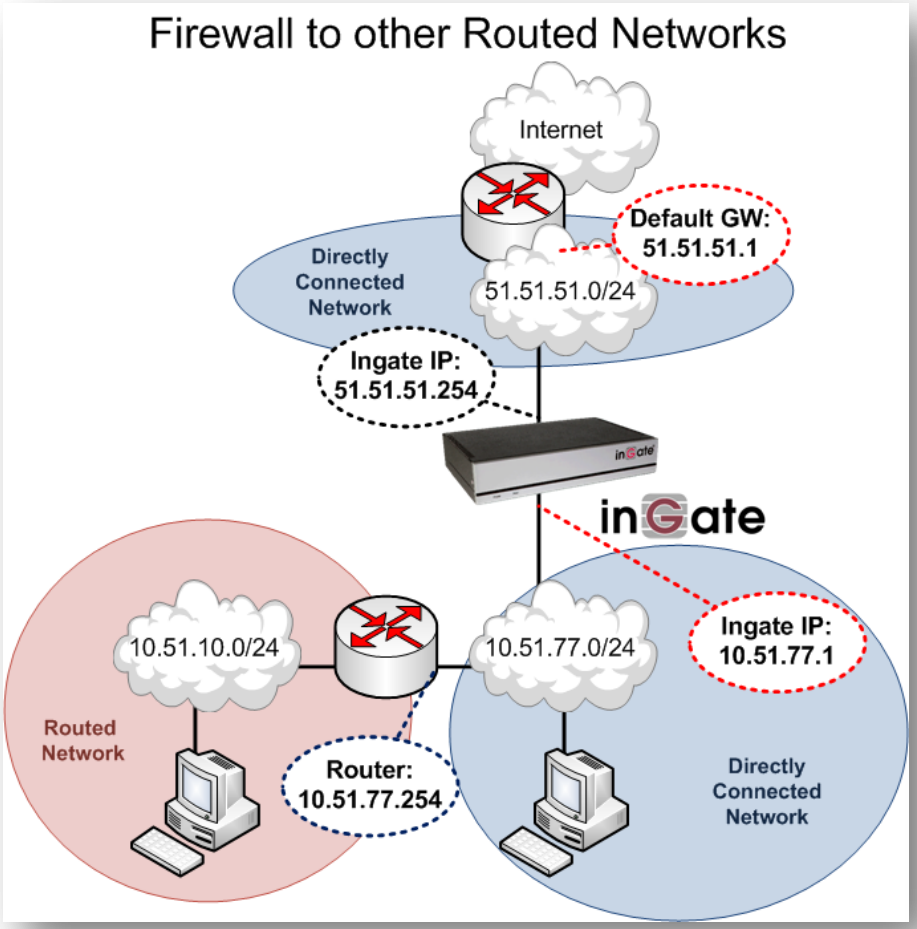
Connecting the Firewall

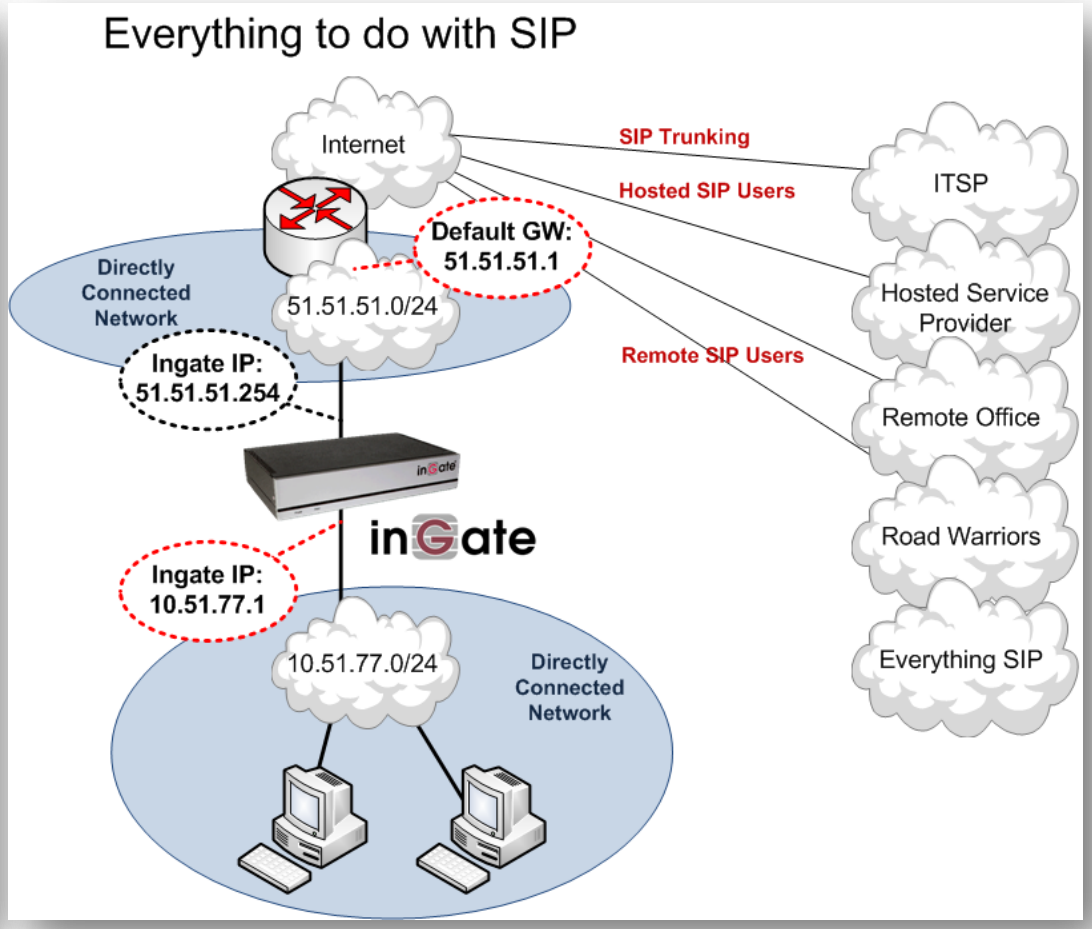




inGate

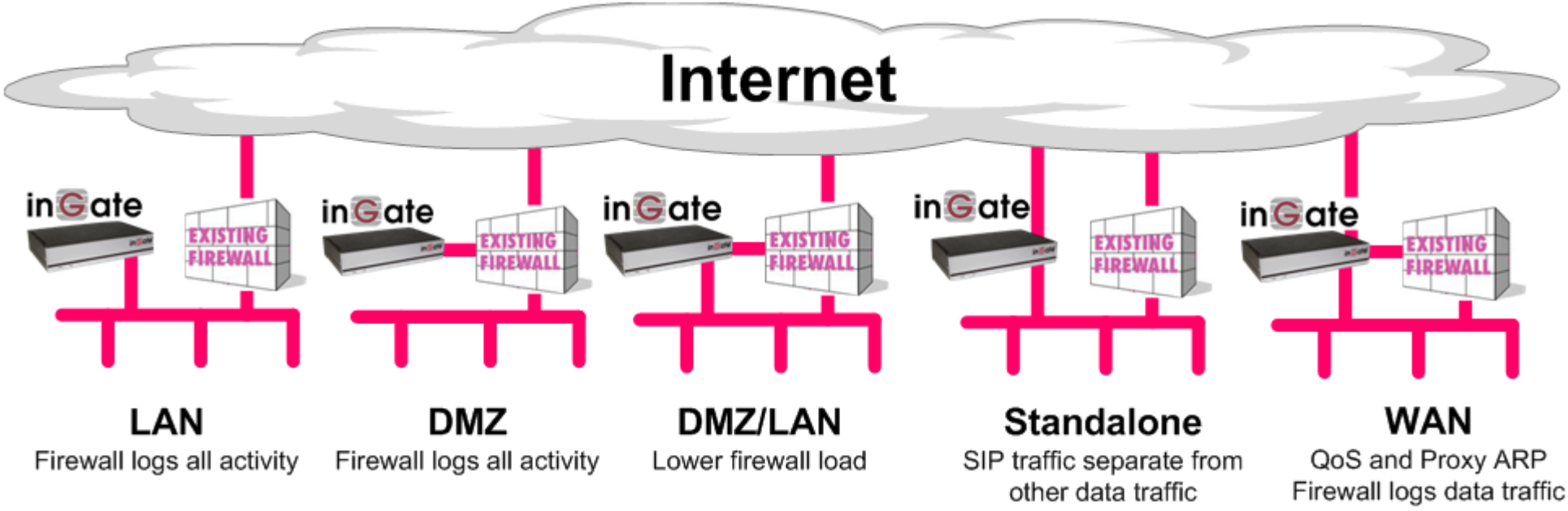
Connecting the Firewall





inGate

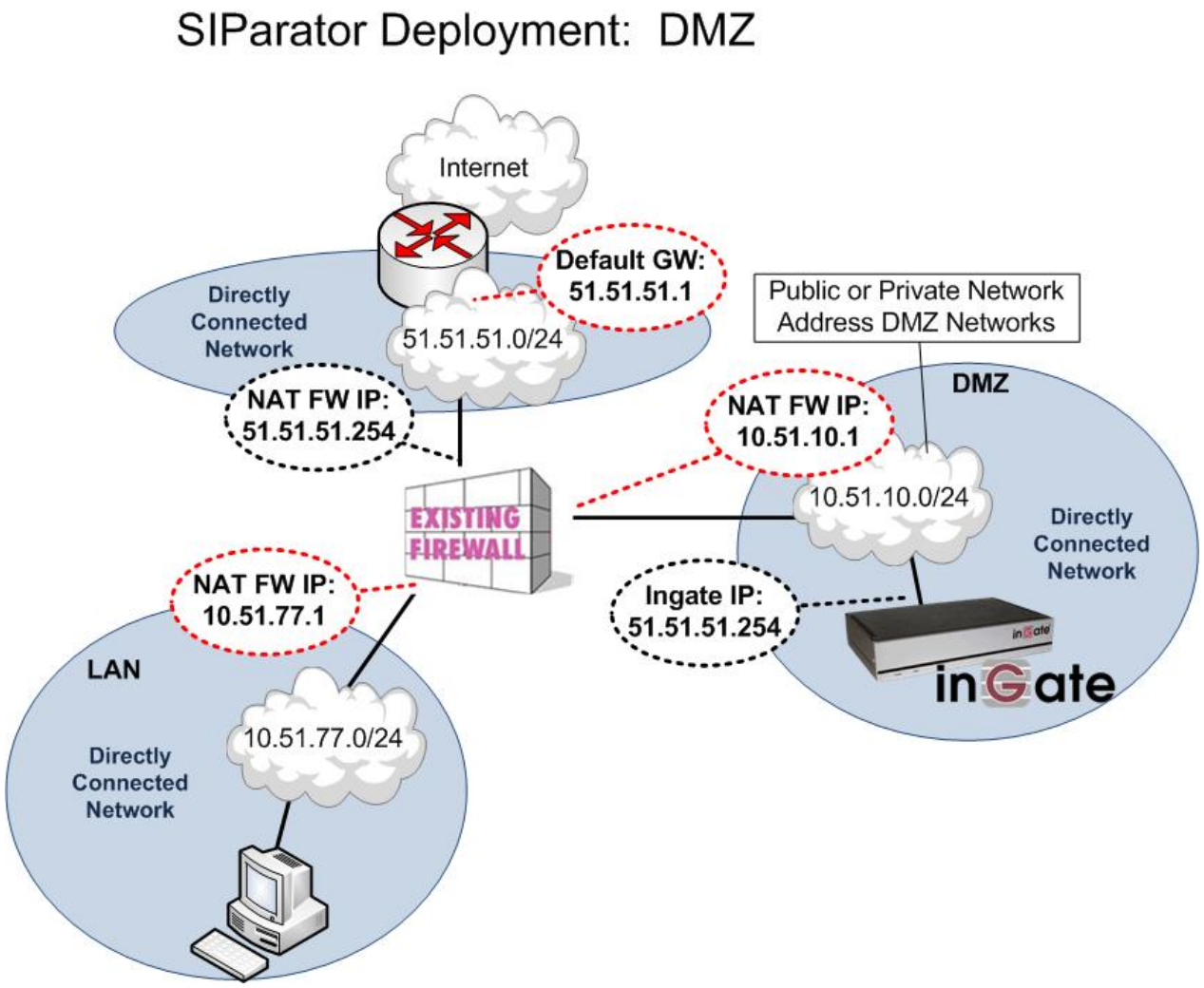
Connecting the SIParator®



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

Connecting the SIParator®

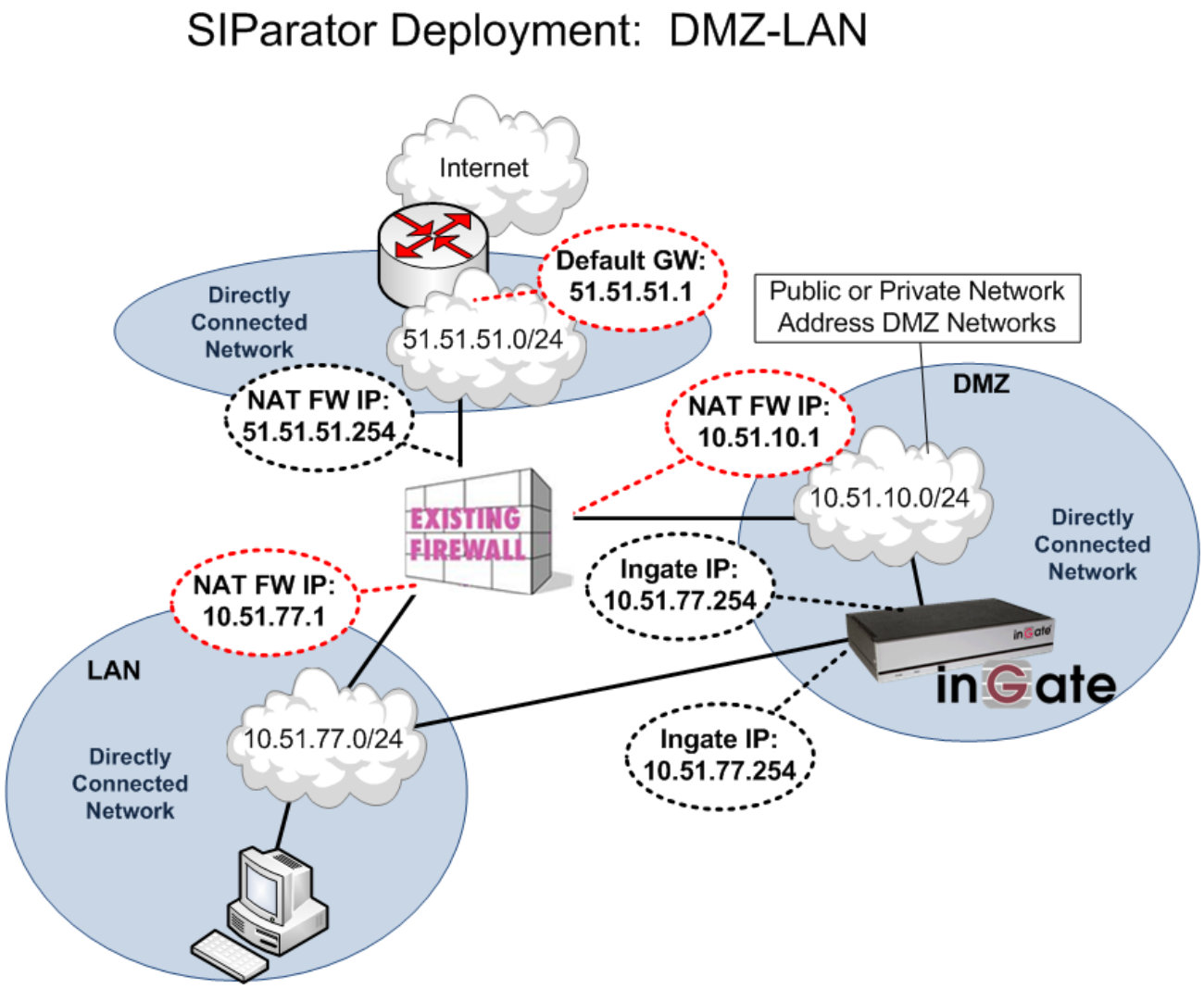
- NAT FW needs to Port FWD from Internet to DMZ and again from DMZ to LAN
- Increases number of Network hops
- Very Secure
- Ingate needs to know WAN IP address



inGate

Connecting the SIParator®

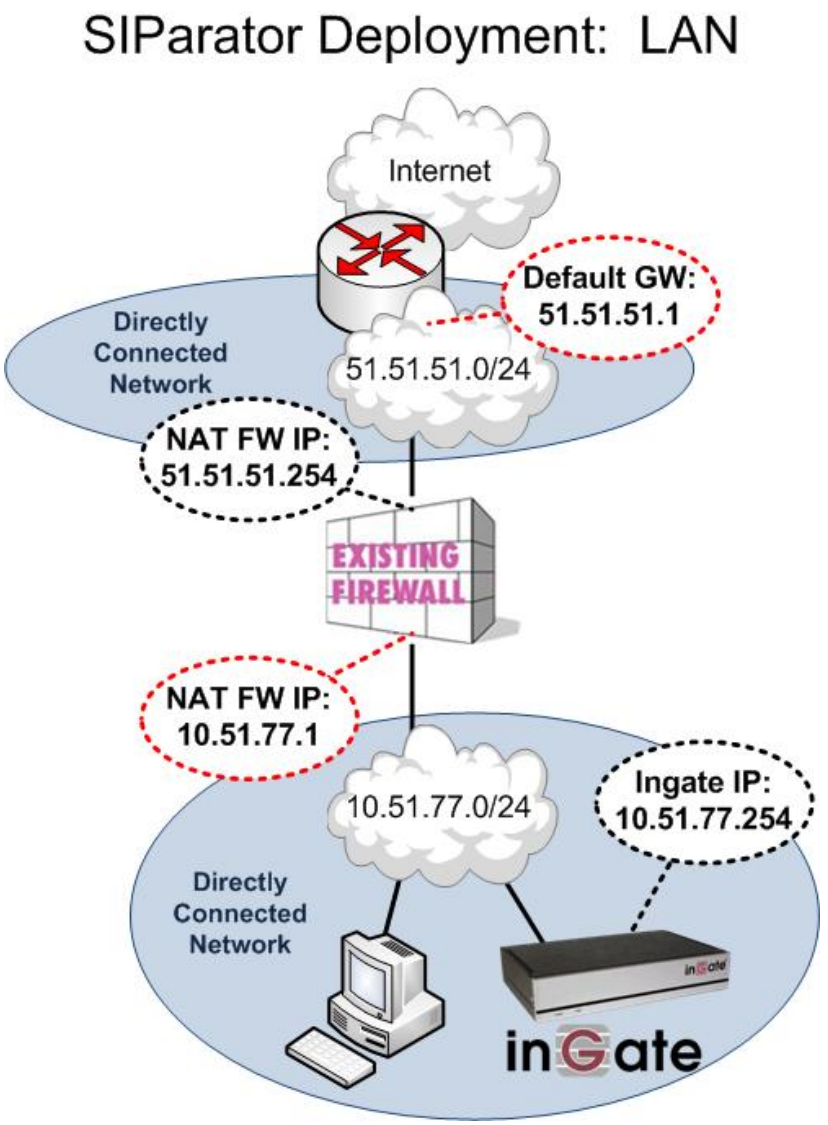
- NAT FW needs to Port FWD from Internet to DMZ
- Decreases Network hops
- Very Secure
- Ingate needs to know WAN IP address



inGate

Connecting the SIParator®

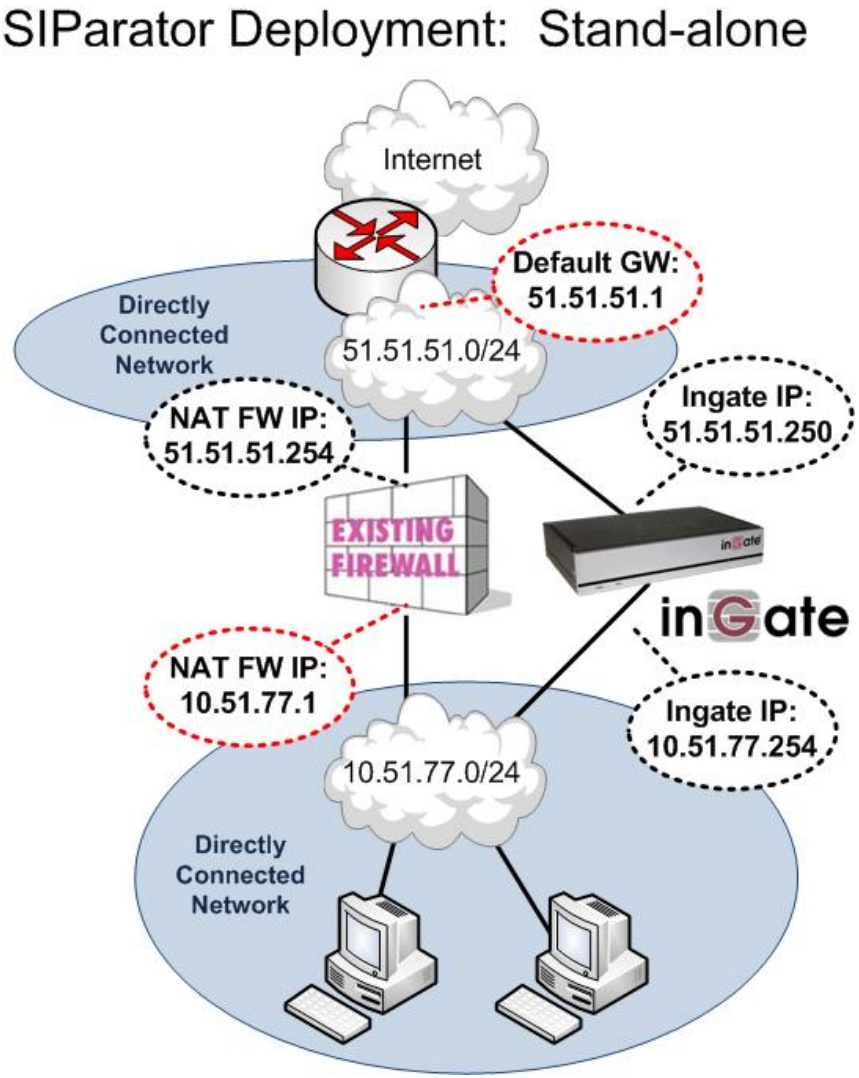
- NAT FW needs to Port FWD from Internet to LAN
- Decreases Network hops
- Least Secure
- Ingate needs to know WAN IP address



inGate

Connecting the SIParator®

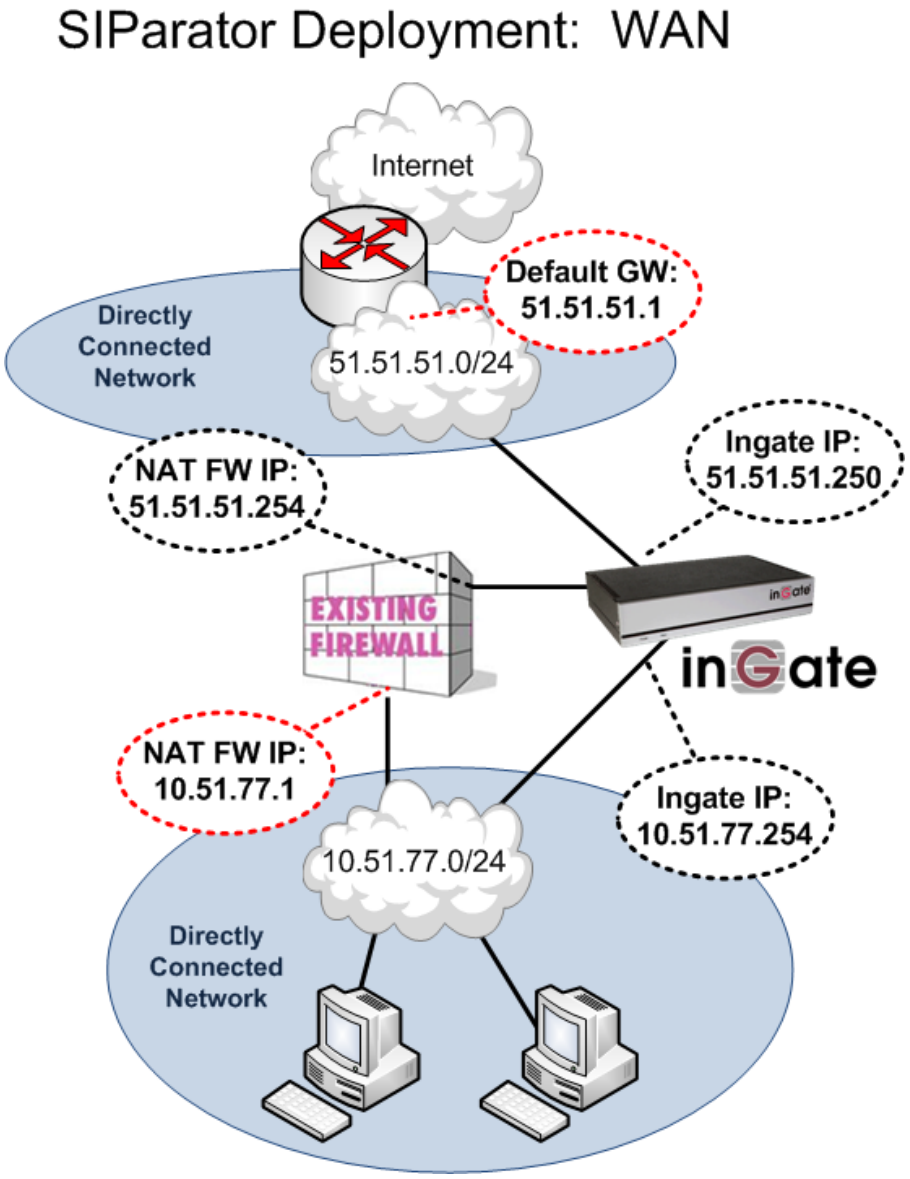
- Ingate has its own Public IP address
- One Network hop
- Very Secure
- Reduces impact to NAT FW
- No NAT FW setup required



inGate

Connecting the SIParator®

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

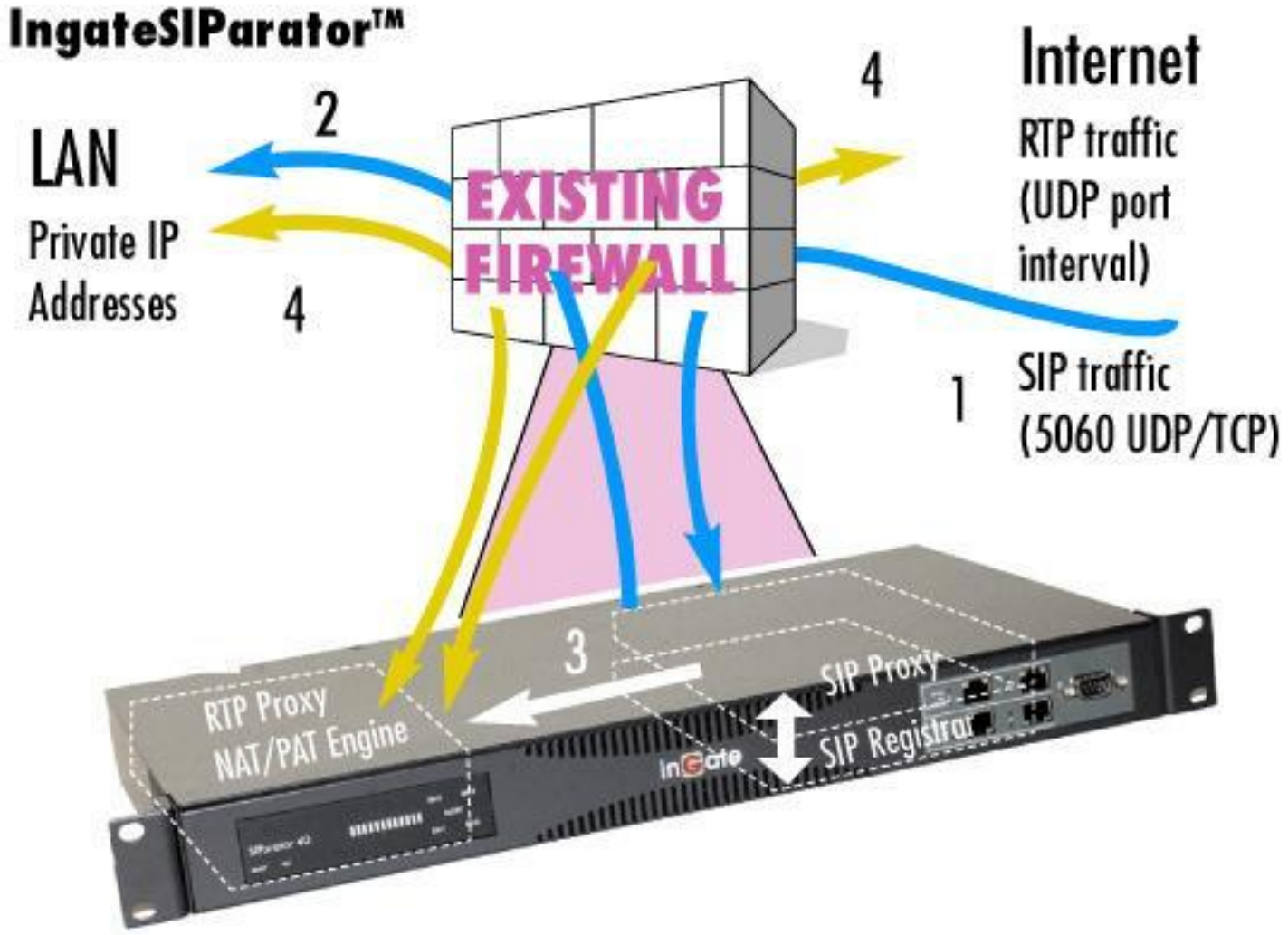


inGate

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 ISTP, 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®



inGate

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

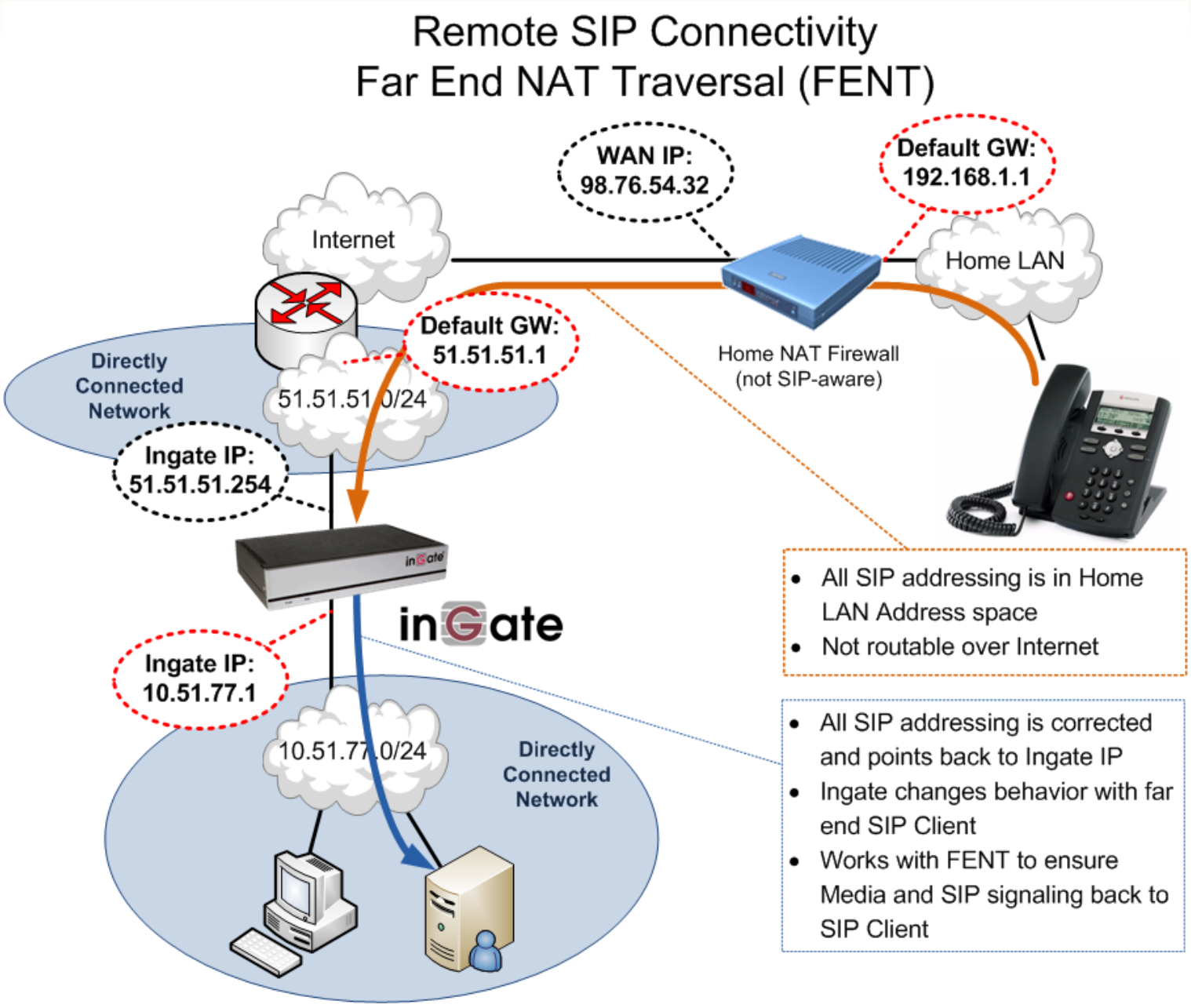
Optional Modules

Remote SIP Connectivity

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

inGate

Optional Modules



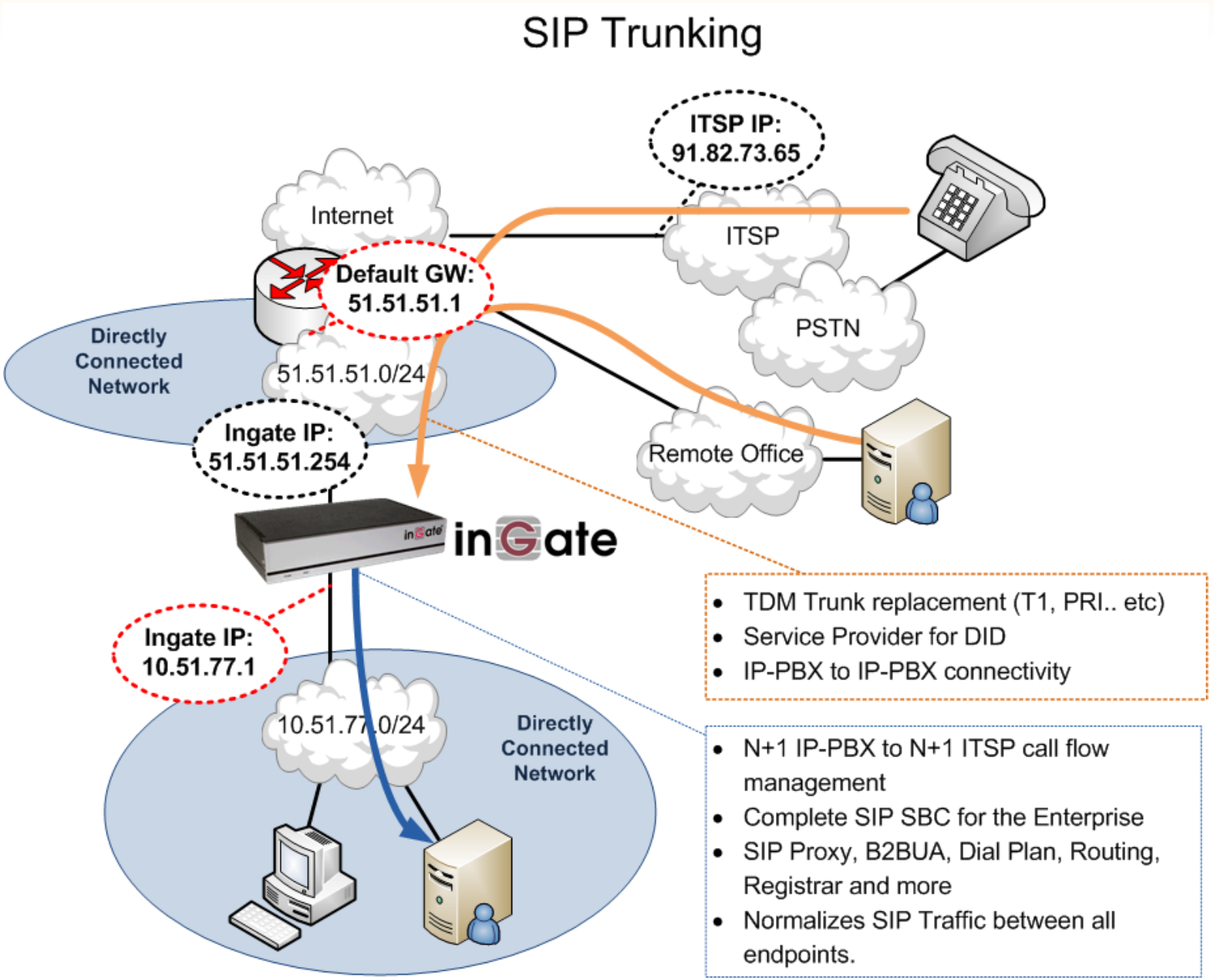
inGate

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



- TDM Trunk replacement (T1, PRI.. etc)
- Service Provider for DID
- IP-PBX to IP-PBX connectivity

- N+1 IP-PBX to N+1 ITSP call flow management
- Complete SIP SBC for the Enterprise
- SIP Proxy, B2BUA, Dial Plan, Routing, Registrar and more
- Normalizes SIP Traffic between all endpoints.

inGate

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

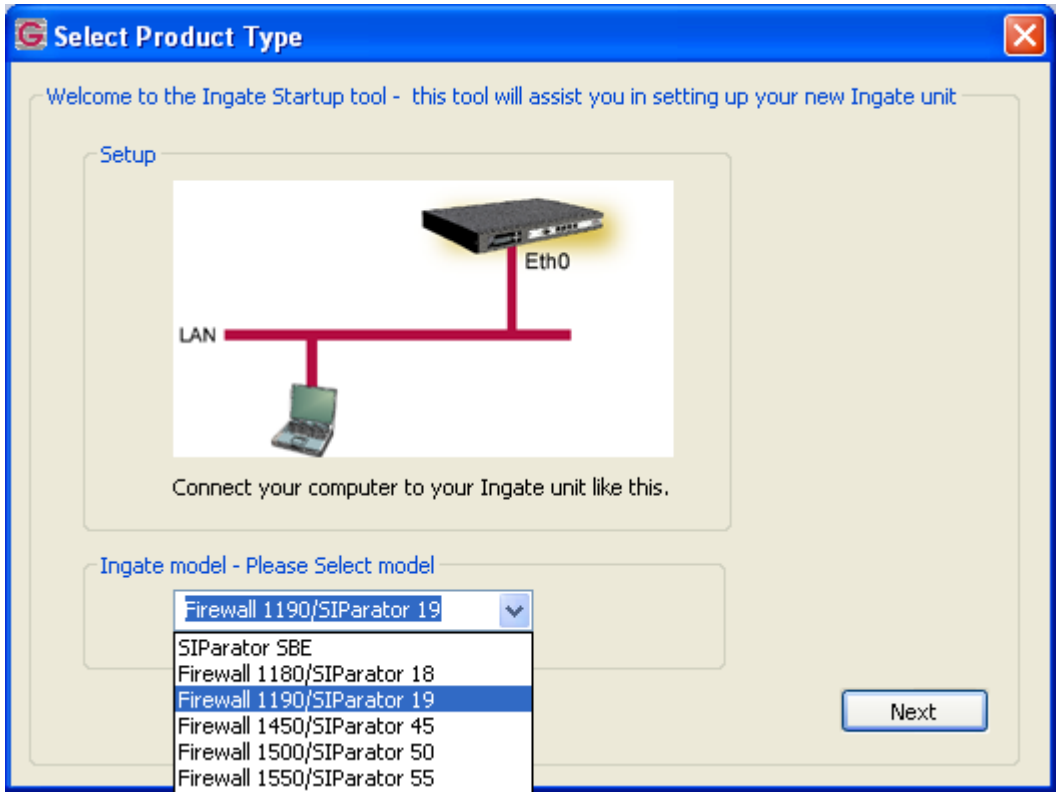
Startup Tool

- "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

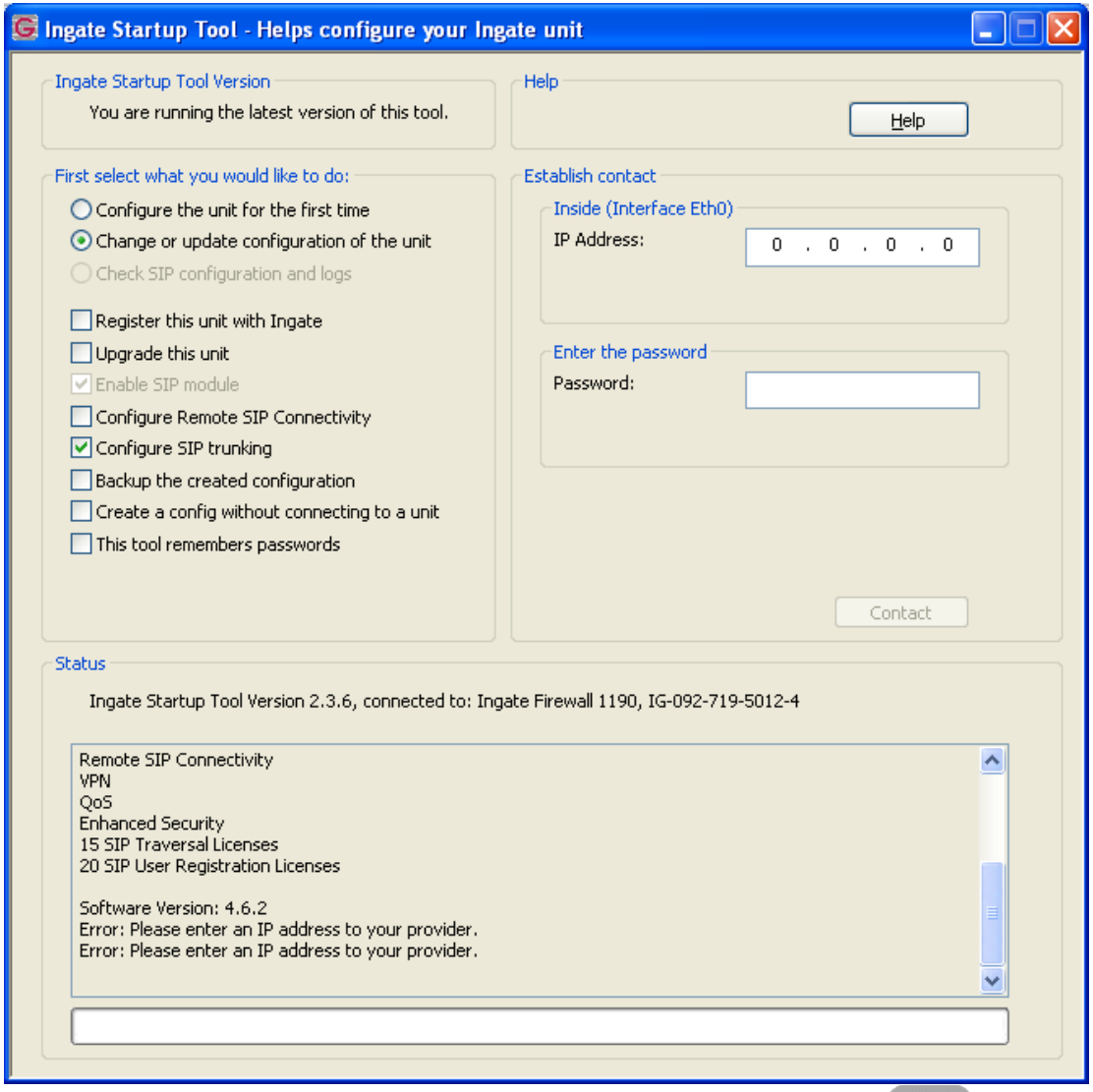


Ingate Startup Tool

Startup Tool Title Reference

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

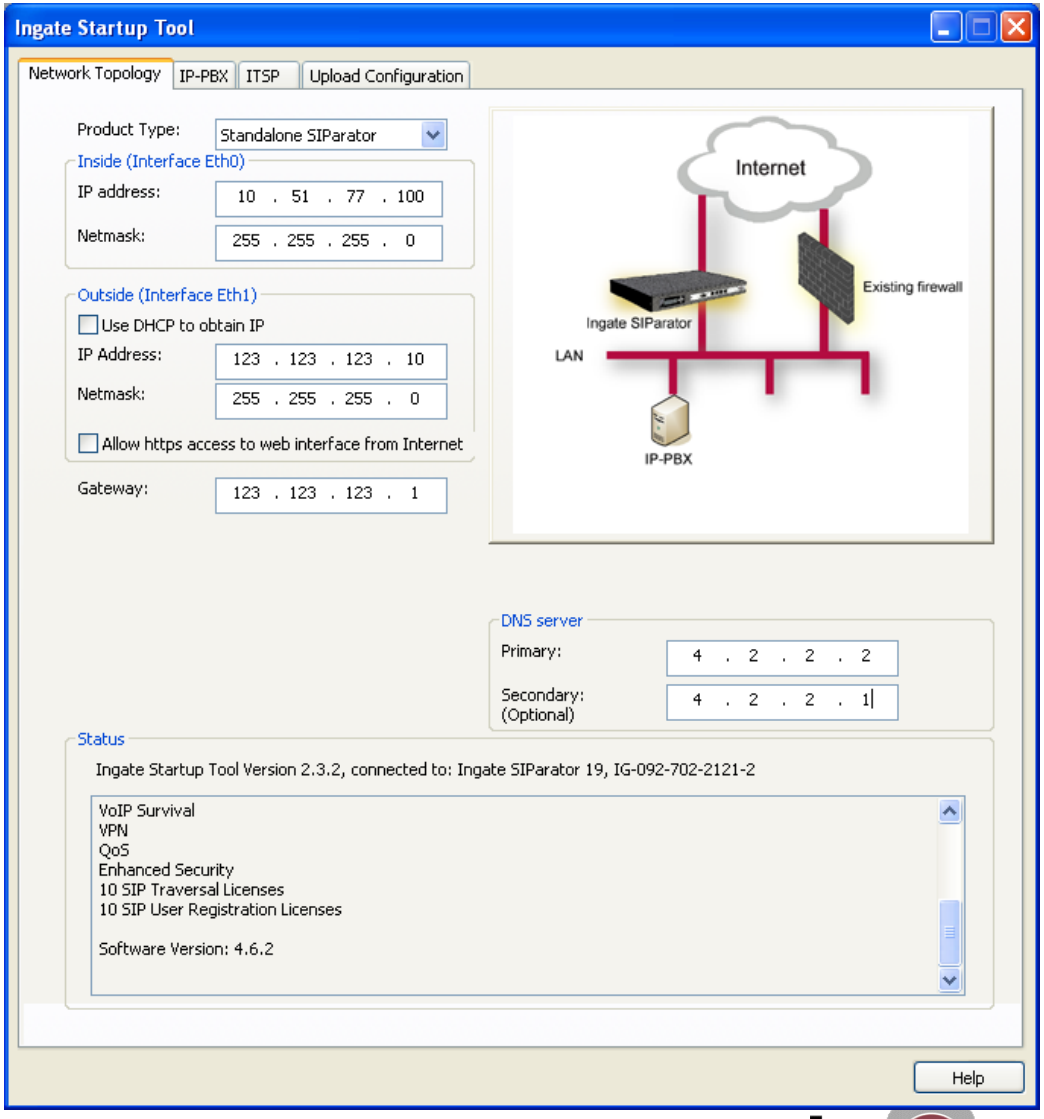
- IP/MAC Address
- Password



Ingate Startup Tool

Startup Tool - Network Topology

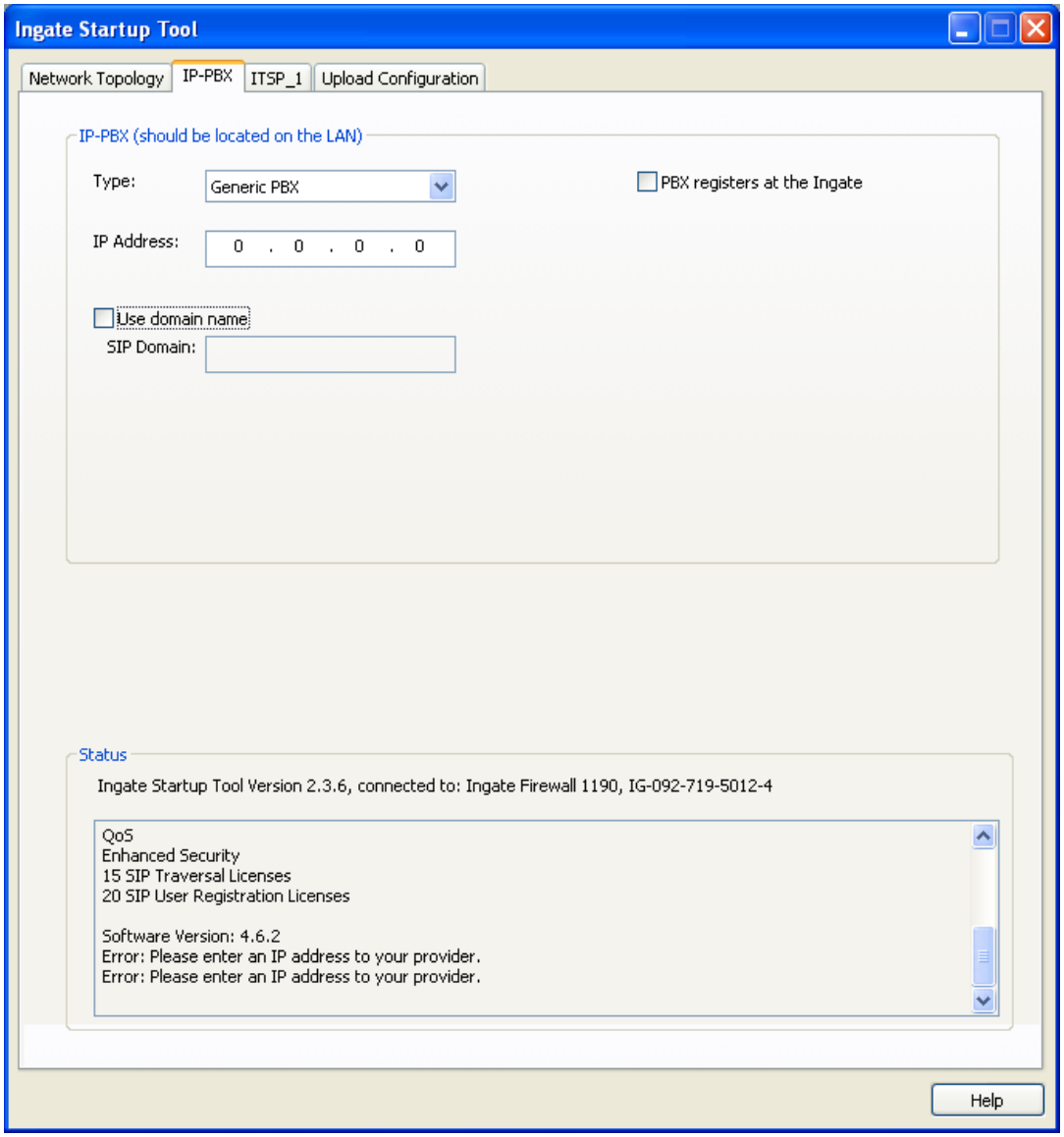
- Firewall or SIParator deployment type
- Inside (Eth0) - Private
- Outside (Eth1) - Public
- Default Gateway
- DNS Server



Ingate Startup Tool

Startup Tool – IP-PBX

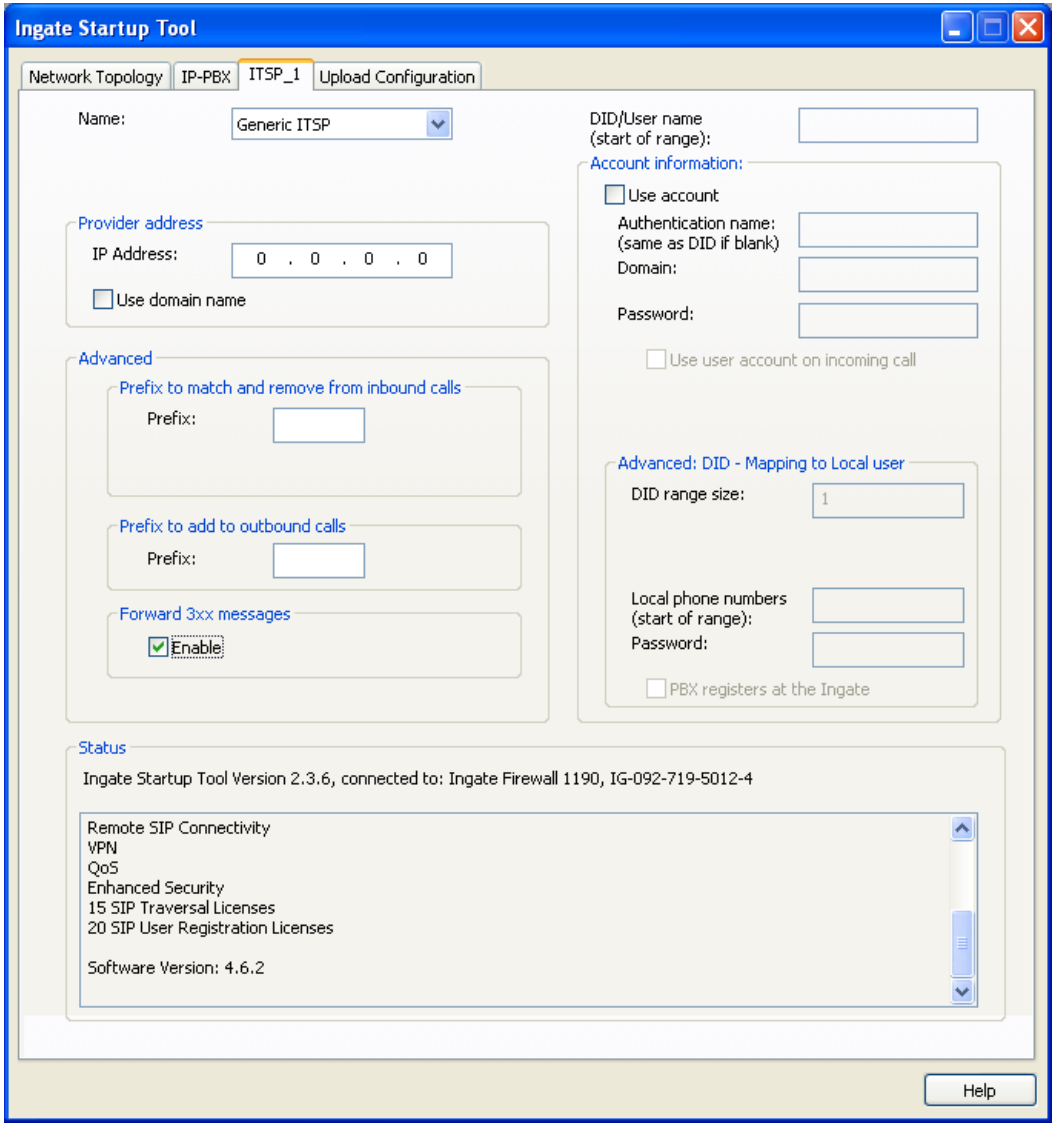
- Select IP-PBX
  - Provide IP Address



Ingate Startup Tool

Startup Tool – ITSP_1

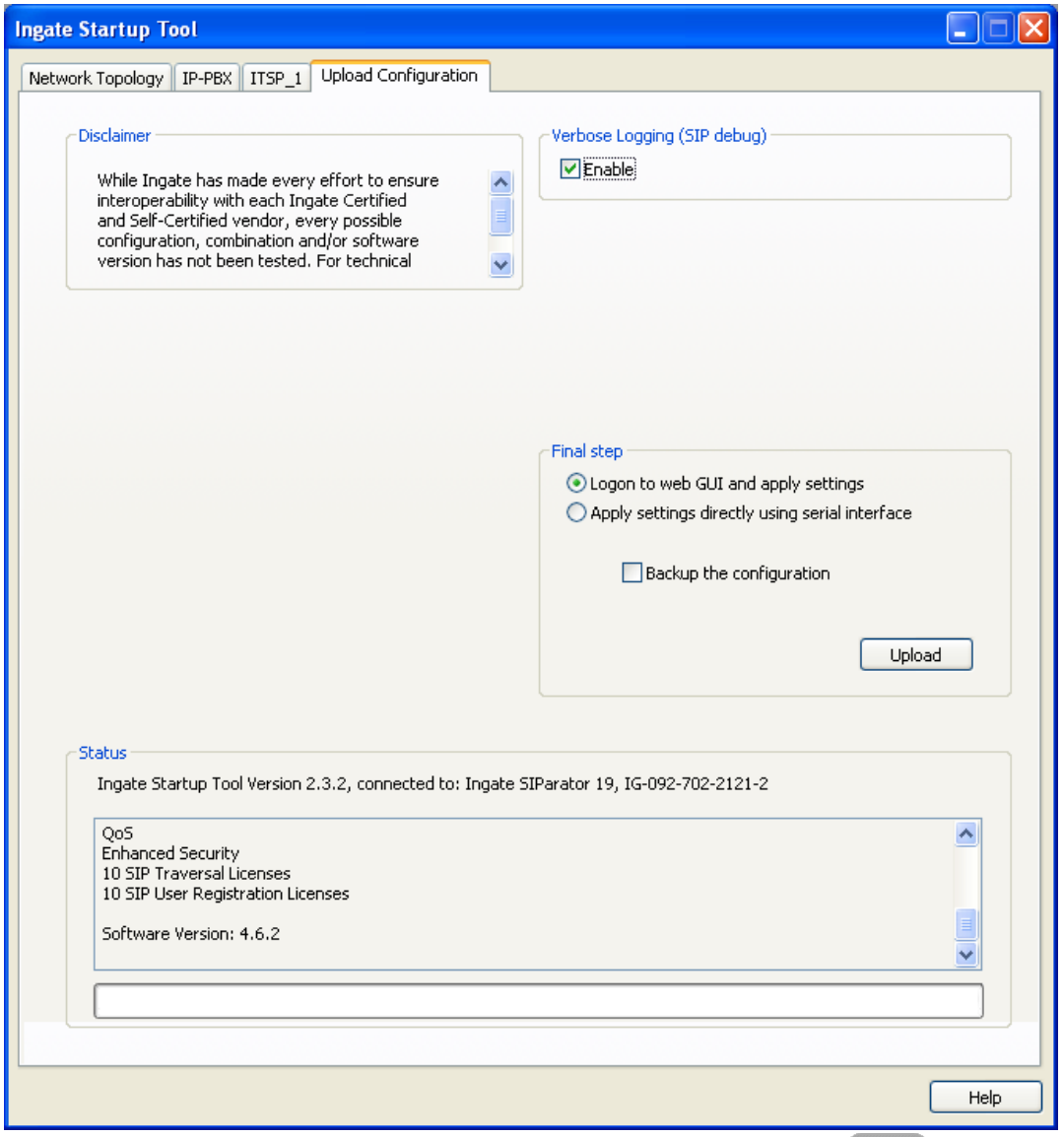
- Select Trunking Provider
  - Account Information



Ingate Startup Tool

Startup Tool – Upload Config

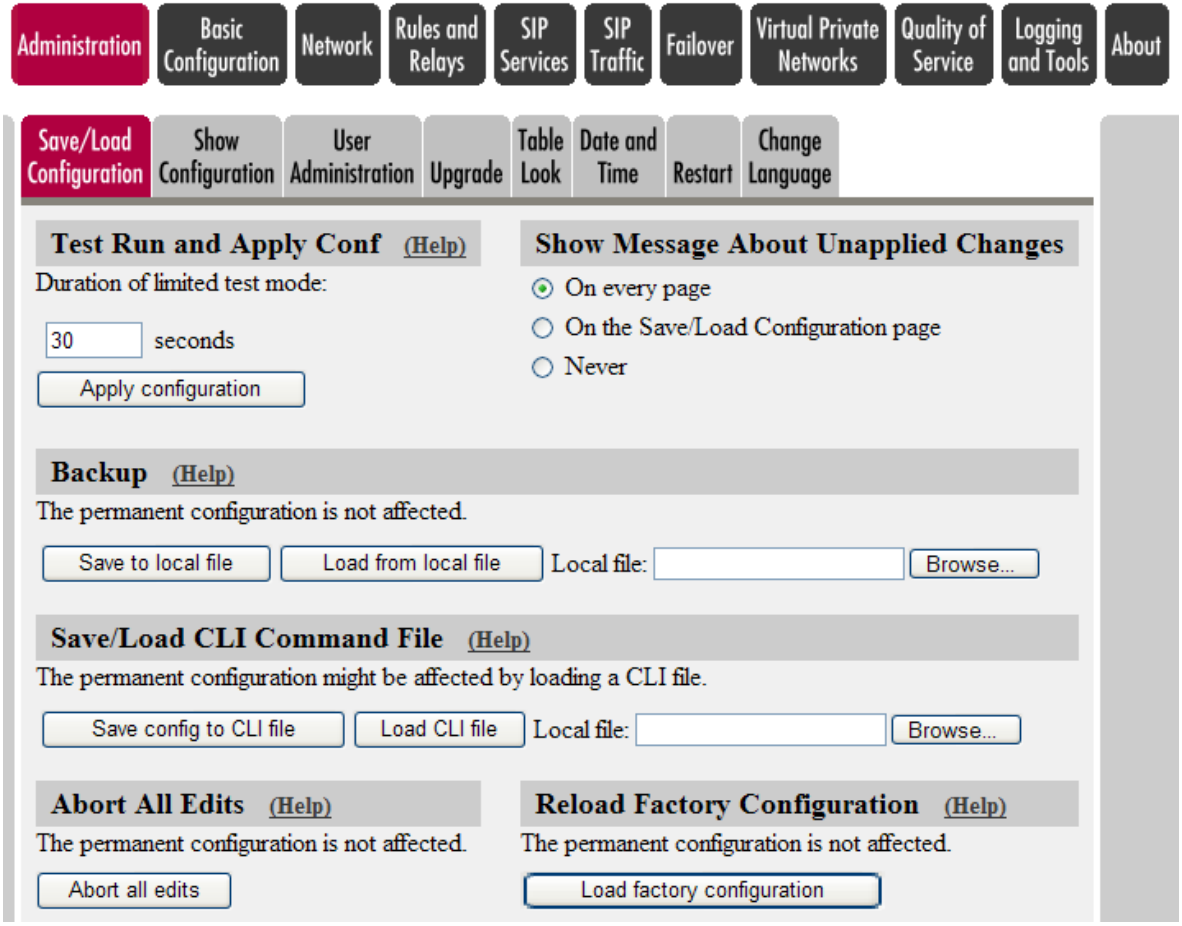
- Login to web GUI and apply settings
- Upload



Ingate Startup Tool

Startup Tool – Apply the Config

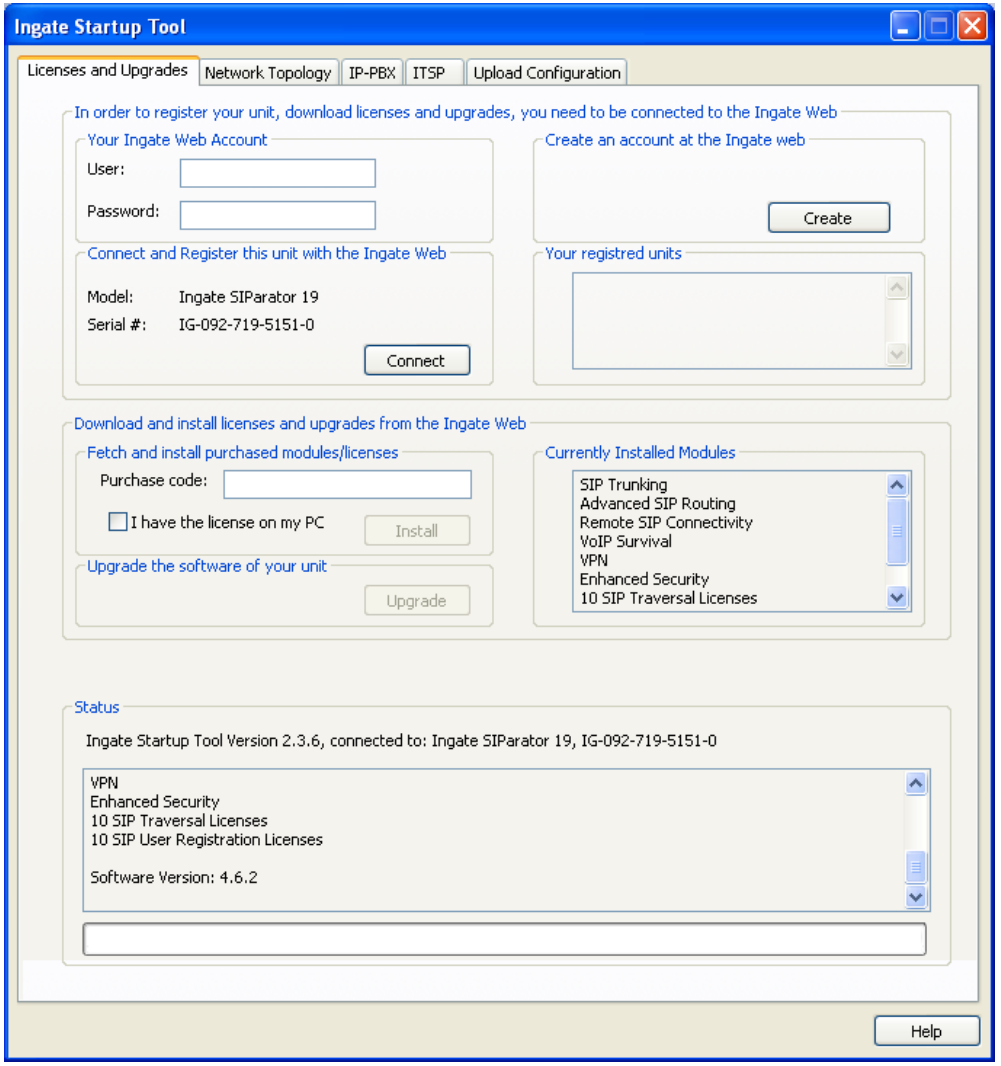
- The Startup Tool will launch a browser to have the installer Apply the Configuration.



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



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

LAN

Internet

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

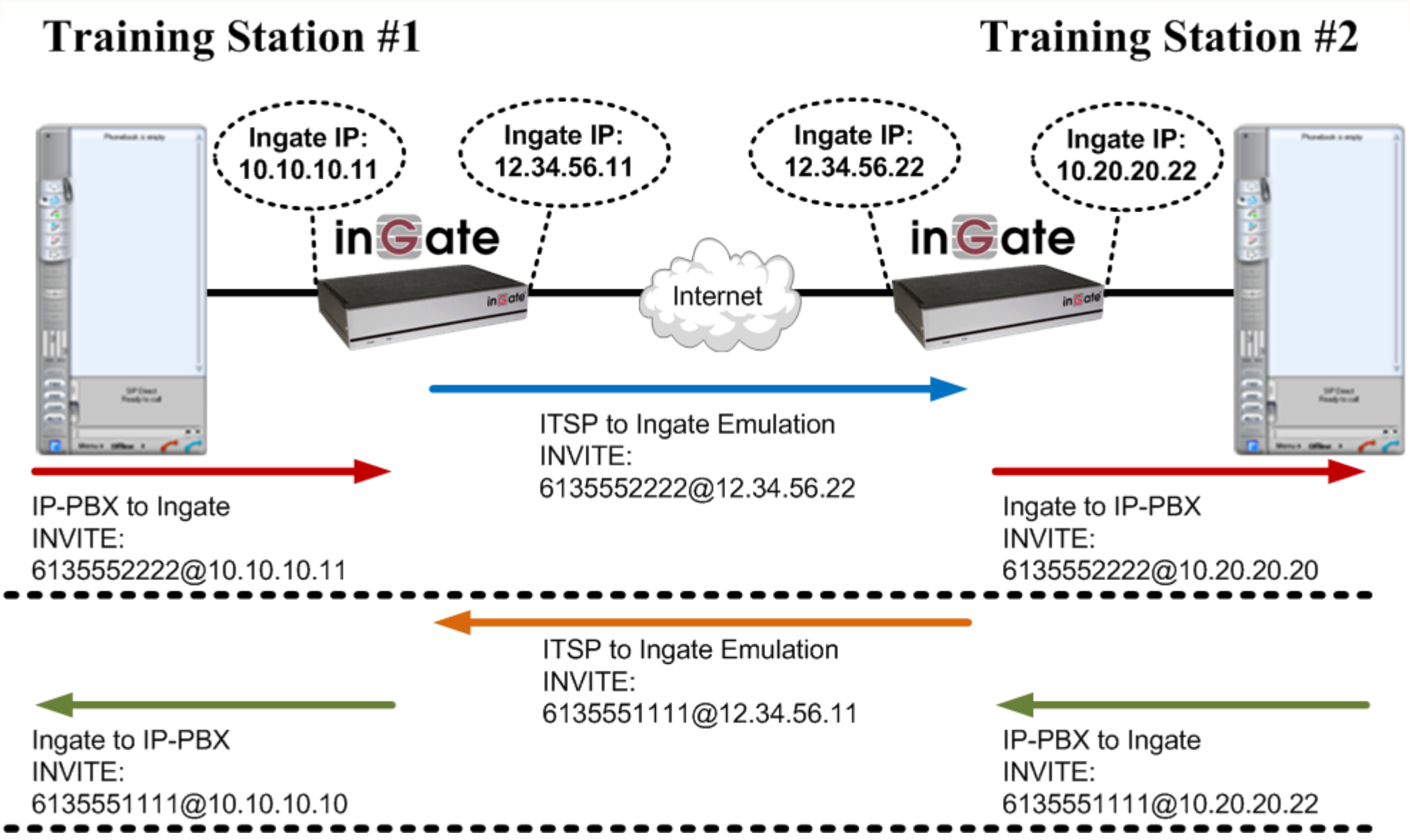


Softphone
DID #: 6135554444
IP Address: 10.40.40.40

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
Ingate IP:
10.10.10.11
Ingate IP:
12.34.56.11
Ingate IP:
12.34.56.22
Ingate IP:
10.20.20.22
inGate
inGate
Internet
ITSP to Ingate Emulation
INVITE:
6135552222@12.34.56.22
IP-PBX to Ingate
INVITE:
6135552222@10.10.10.11
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 | Default Gateways | All Interfaces | NAT | VLAN | Eth0 | Eth1 | Eth2 | Interface Status | PPPoE

Networks and Computers

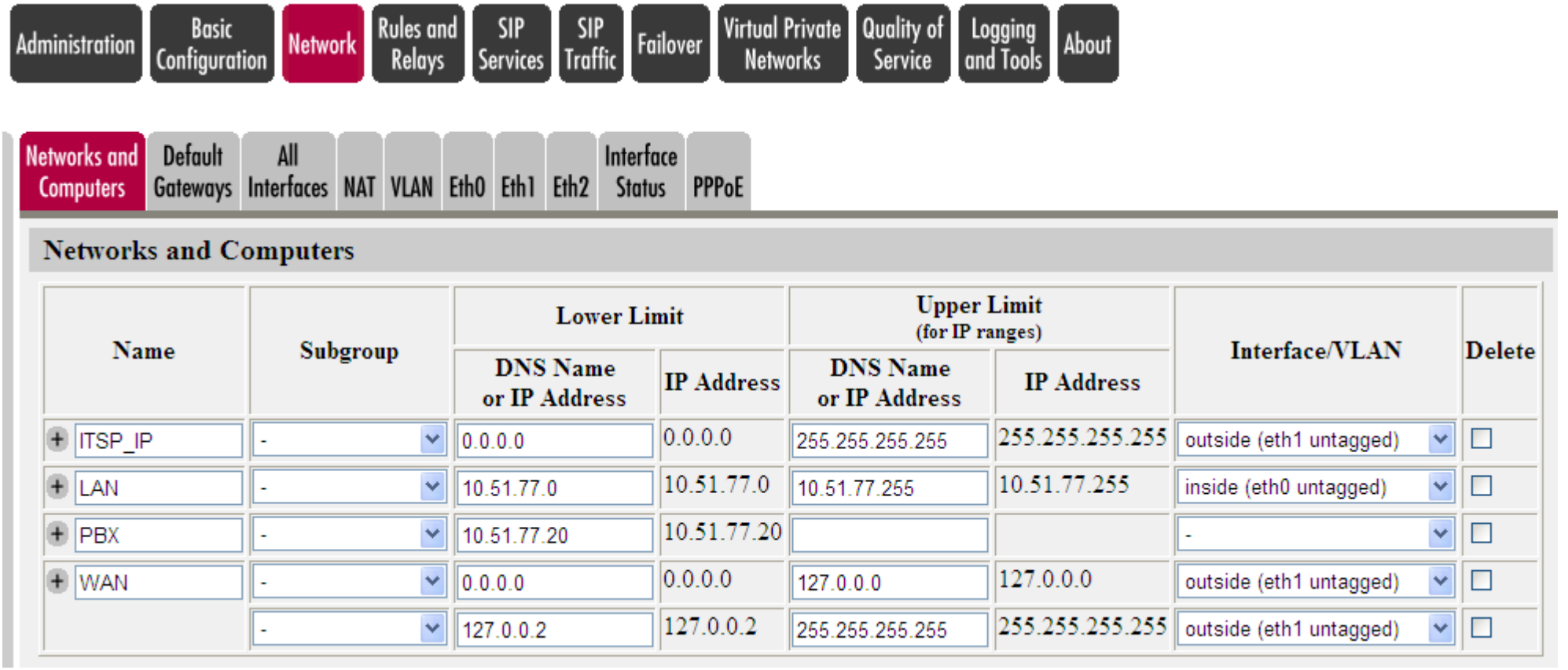
Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
ITSP_IP	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	☐
LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	inside (eth0 untagged)	☐
PBX	-	10.51.77.20	10.51.77.20			-	☐
WAN	-	0.0.0.0	0.0.0.0	127.0.0.0	127.0.0.0	outside (eth1 untagged)	☐
	-	127.0.0.2	127.0.0.2	255.255.255.255	255.255.255.255	outside (eth1 untagged)	☐

Programming: Network

Programming: Network

Networks & Computers

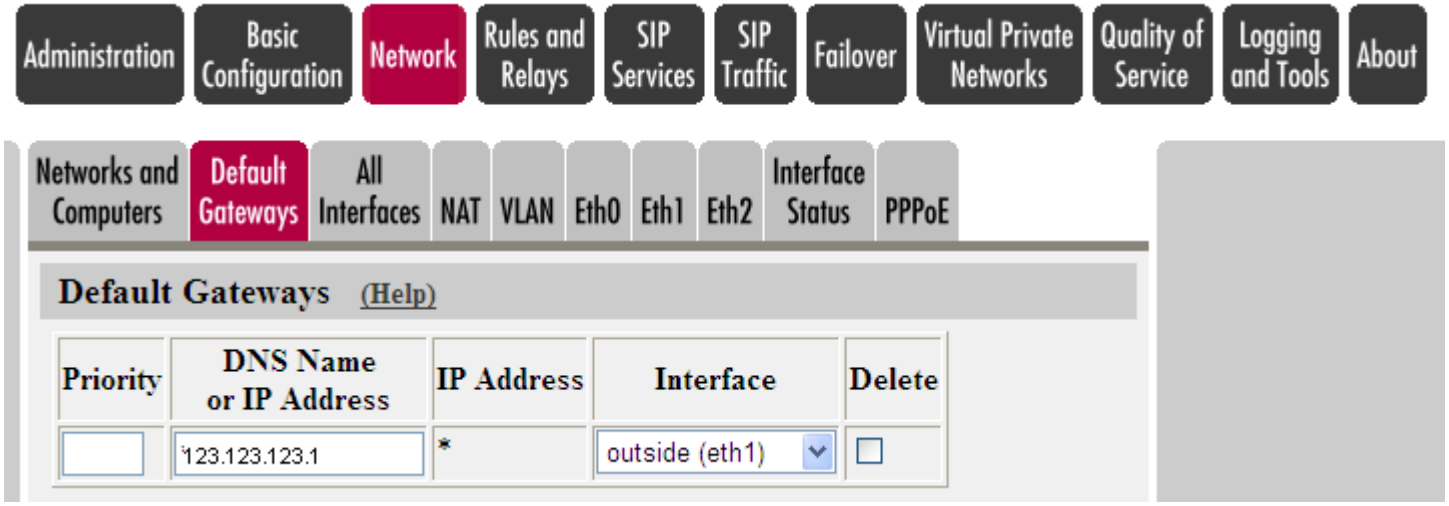
- Provides a view of the Network connected on each interface as a Routing Table.



Programming: Network

Default Gateway

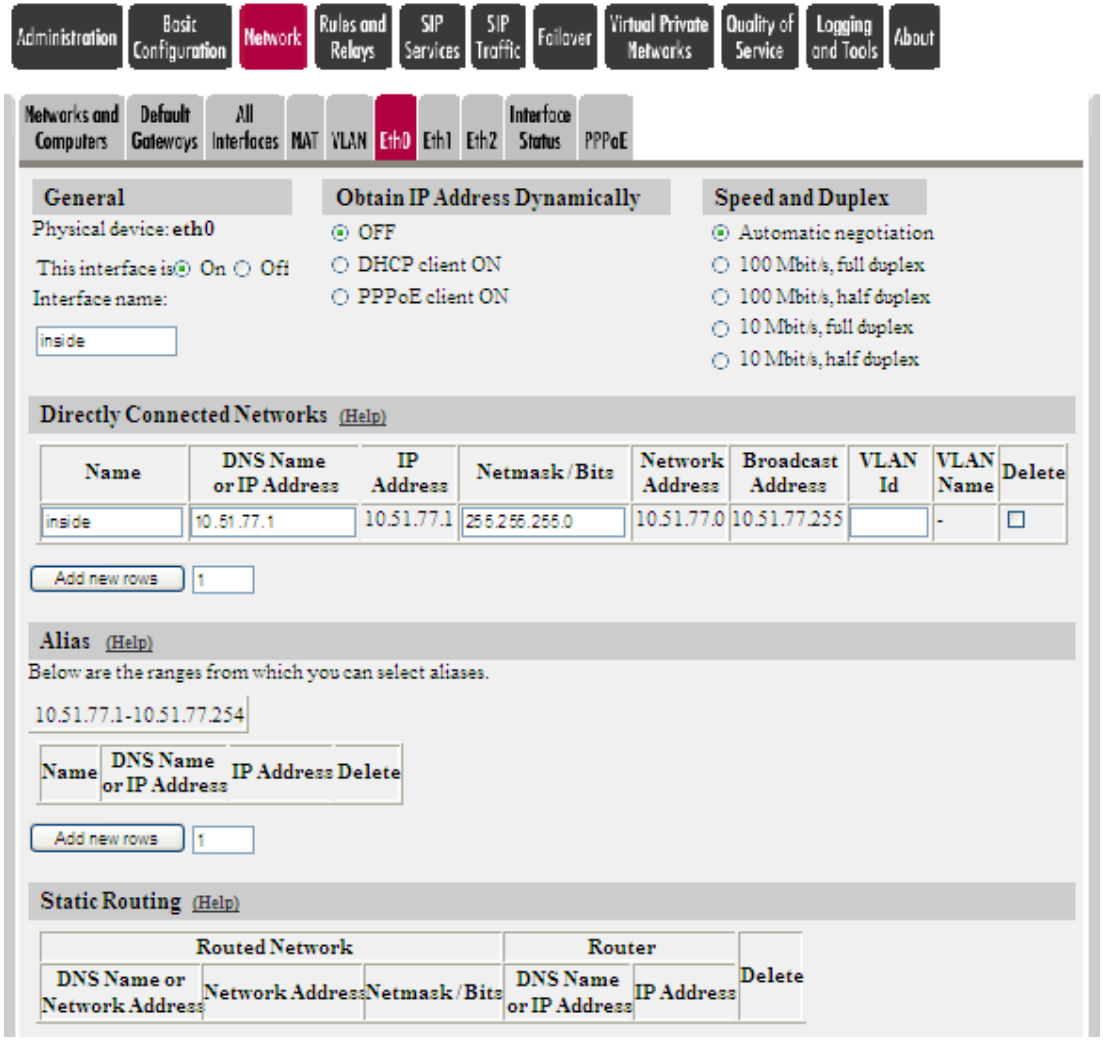
- The Default Gateway to the Internet, provided by the ISP.



Programming: Network

Eth0 Network Interface

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

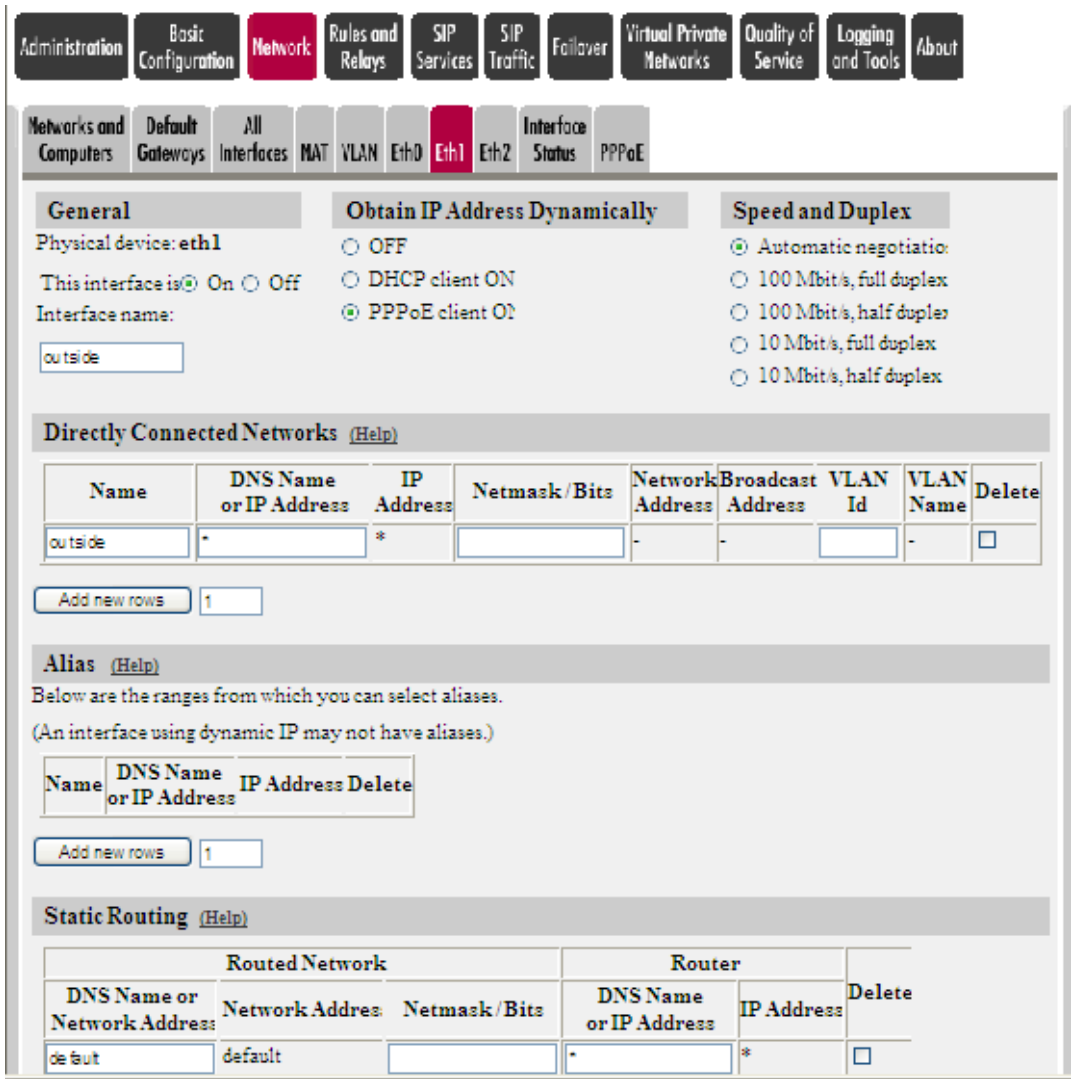


- Static Routing – defines Router address for other network address on the LAN.

Programming: Network

Eth1 Network Interface

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



- PPPoE or DHCP IP address assignment are possible.

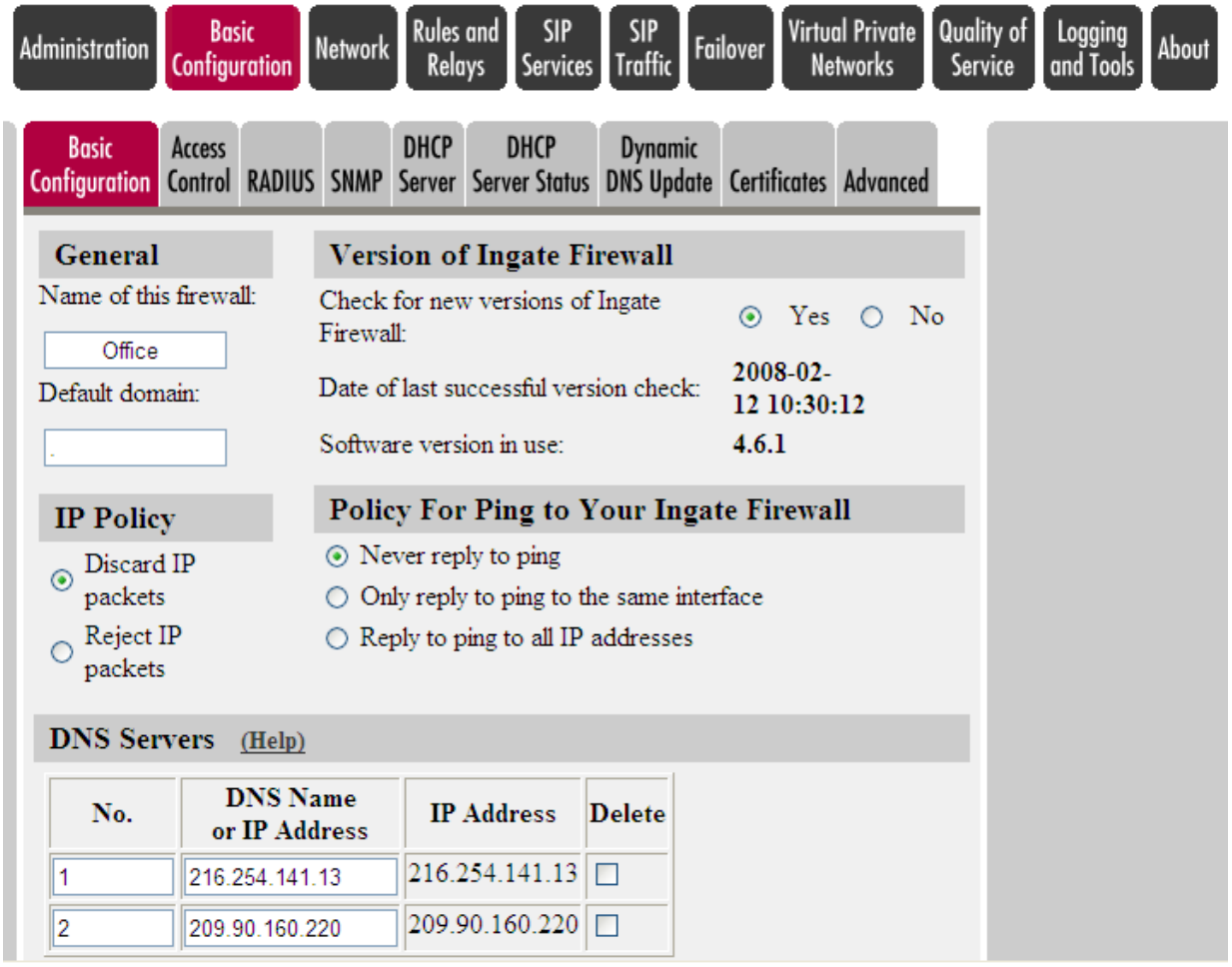
Programming: Basic Configuration

inGate

Programming: Basic Configuration

Basic Configuration

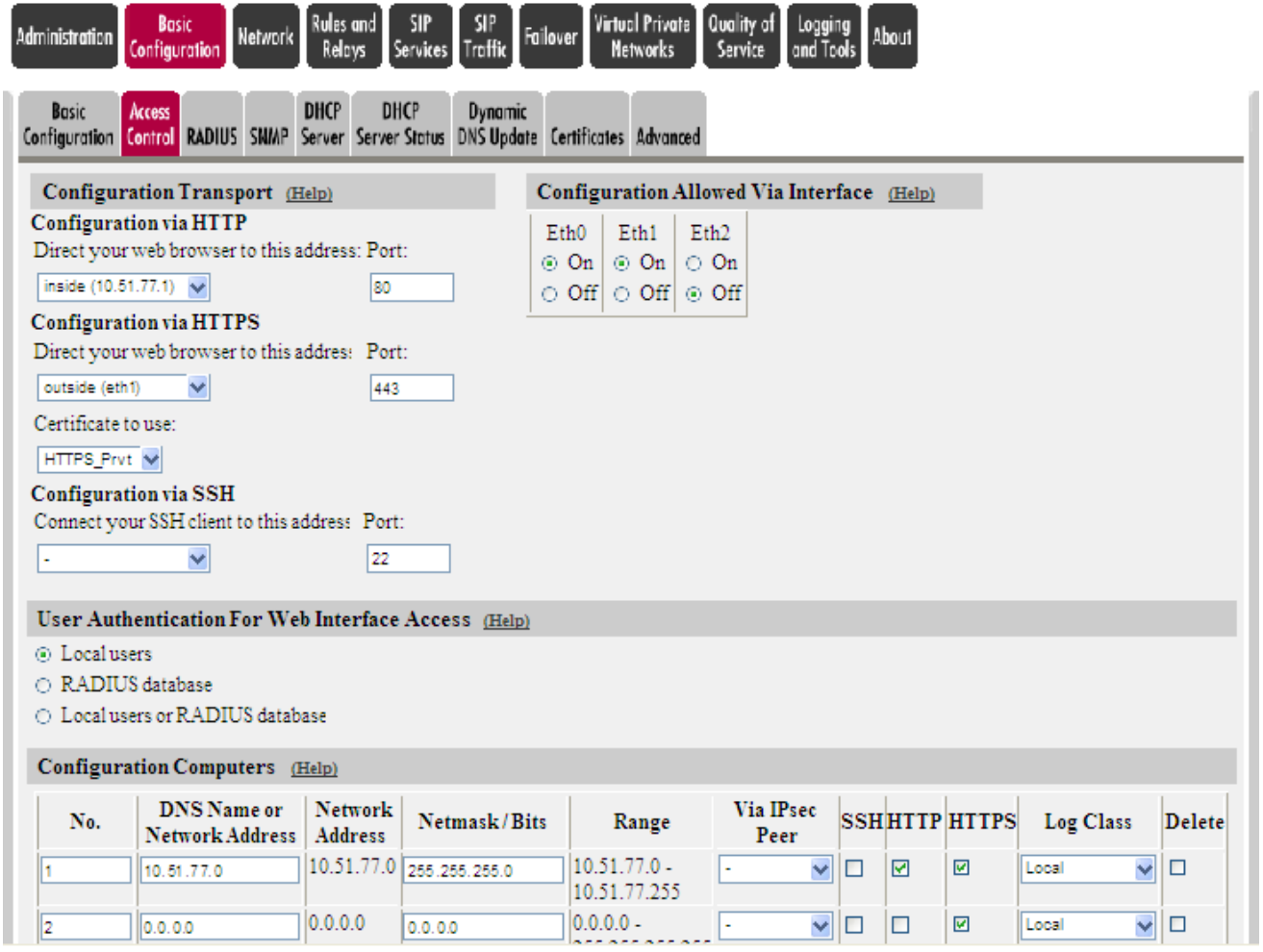
- Provides DNS Server addresses.



Programming: Basic Configuration

Access Control

- Provides configuration for HTTP and HTTPS access.



inGate

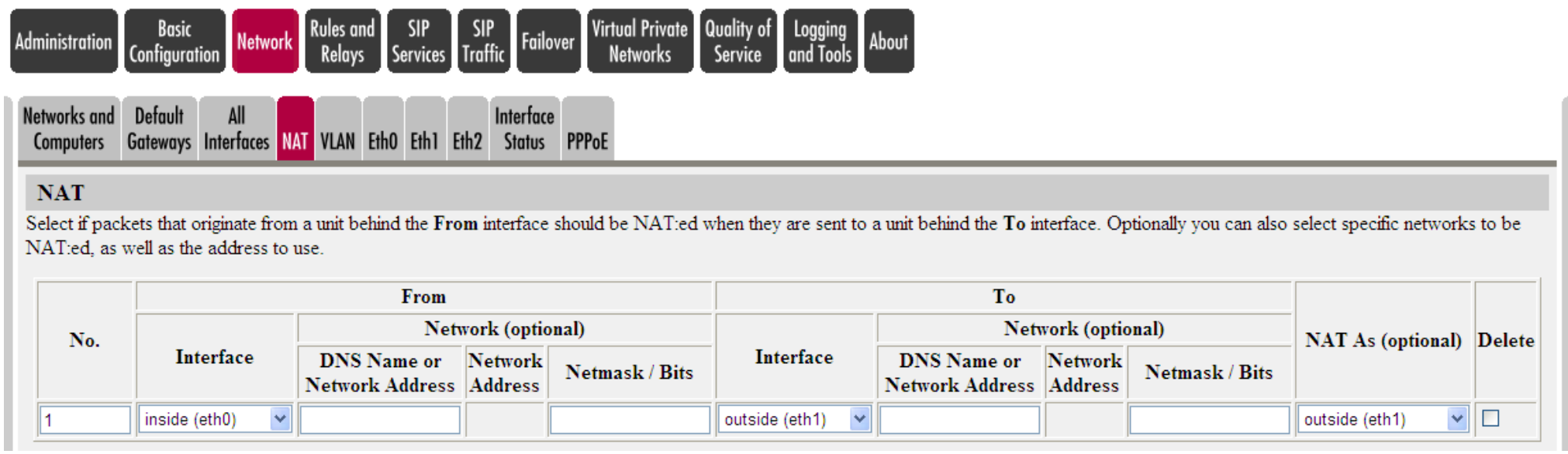
Programming: NAT & Rules and Relays

Firewall Only

Programming: NAT

NAT

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

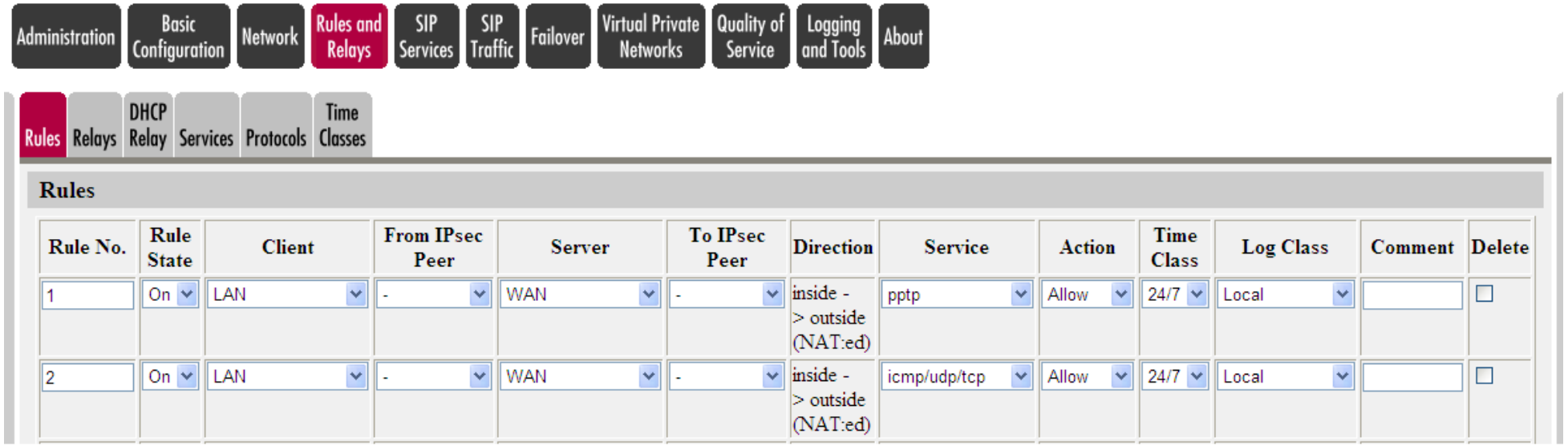


inGate

Programming: Rules & Relays

Rules

- Define specific Service from Client to Server networks.

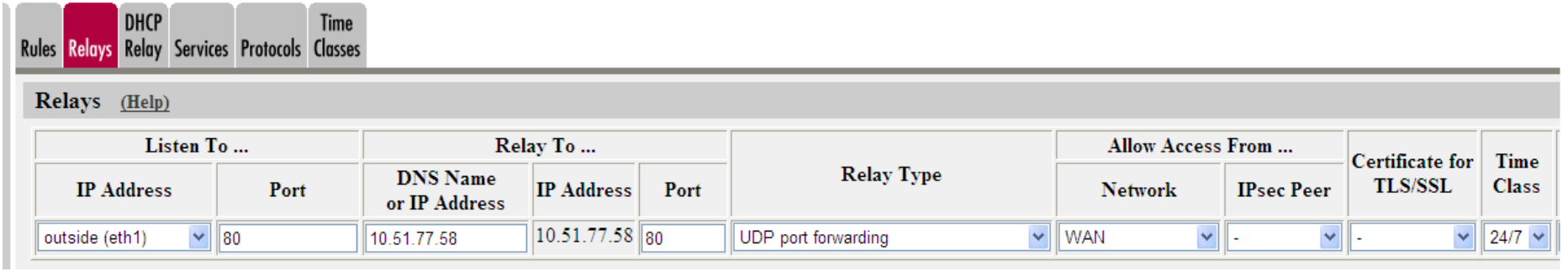


inGate

Programming: Rules & Relays

Relays

- Direct specific Traffic to specific locations



inGate

Programming:
Quality of Service

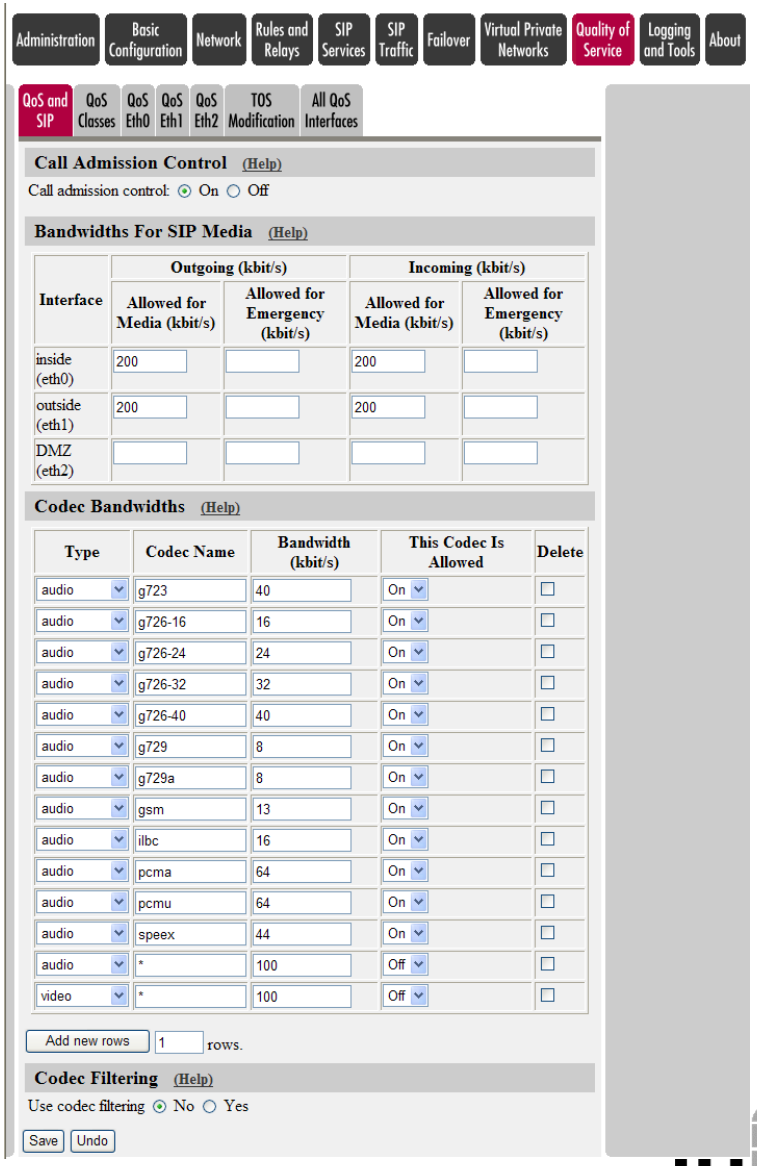
Firewall Only

inGate

Programming: QoS

Quality of Service – Call Admission Control

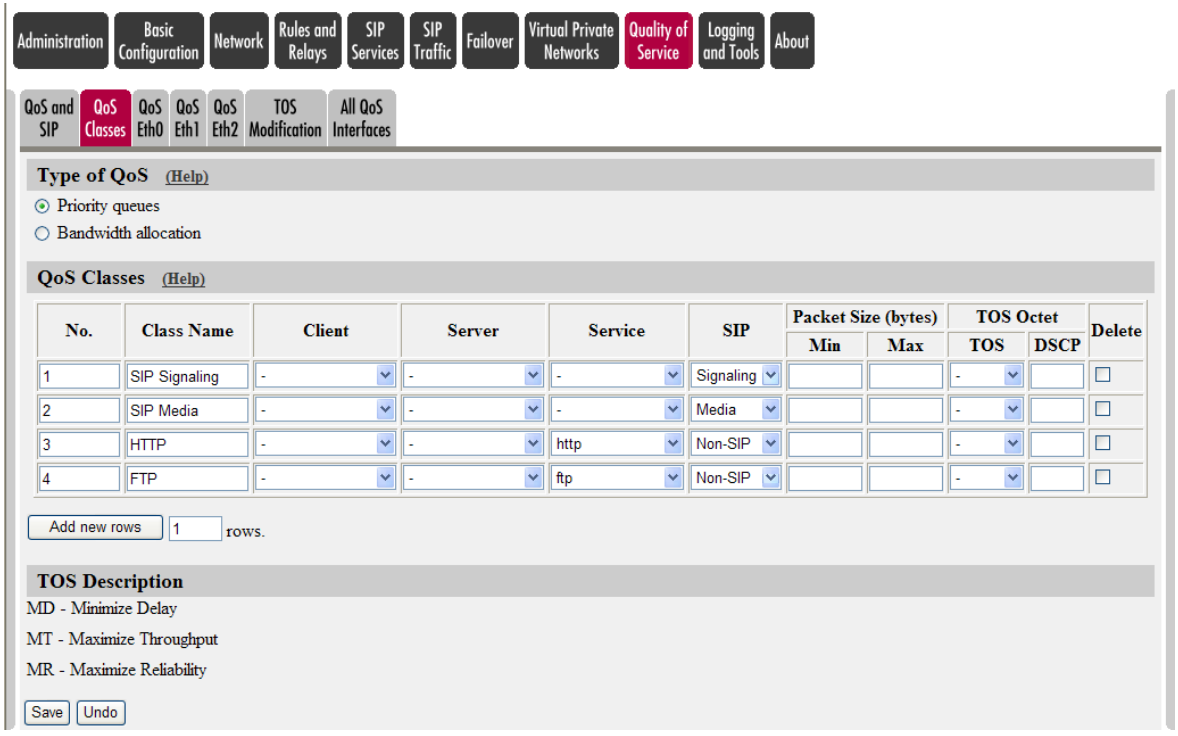
- You can make the firewall reject SIP calls when there is not bandwidth enough left to get media streams through satisfactorily.
- Bandwidth for SIP Media - define BW Reservations
- Codec Bandwidth – define Codec BW



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.



Programming: QoS

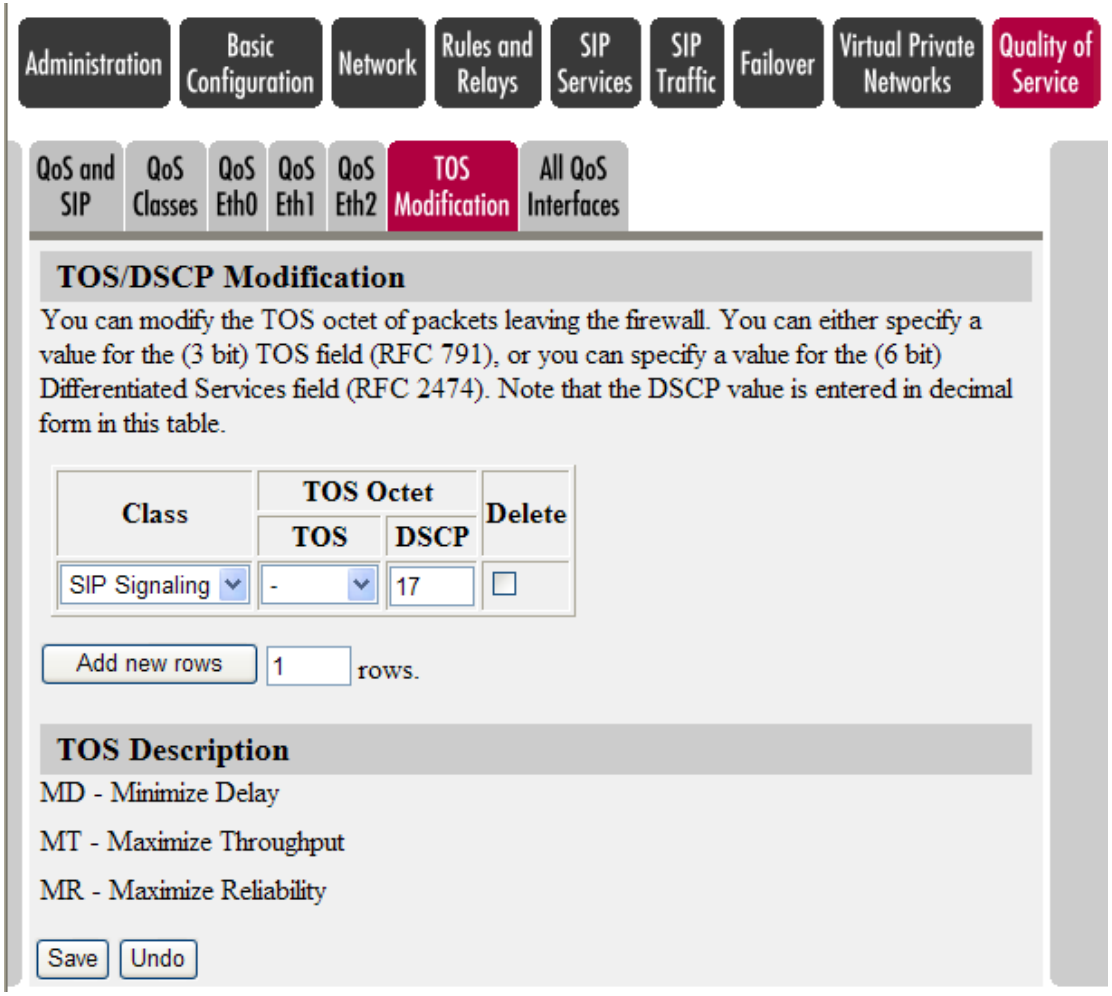
Quality of Service – Most Restricted Interface

- 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).

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).



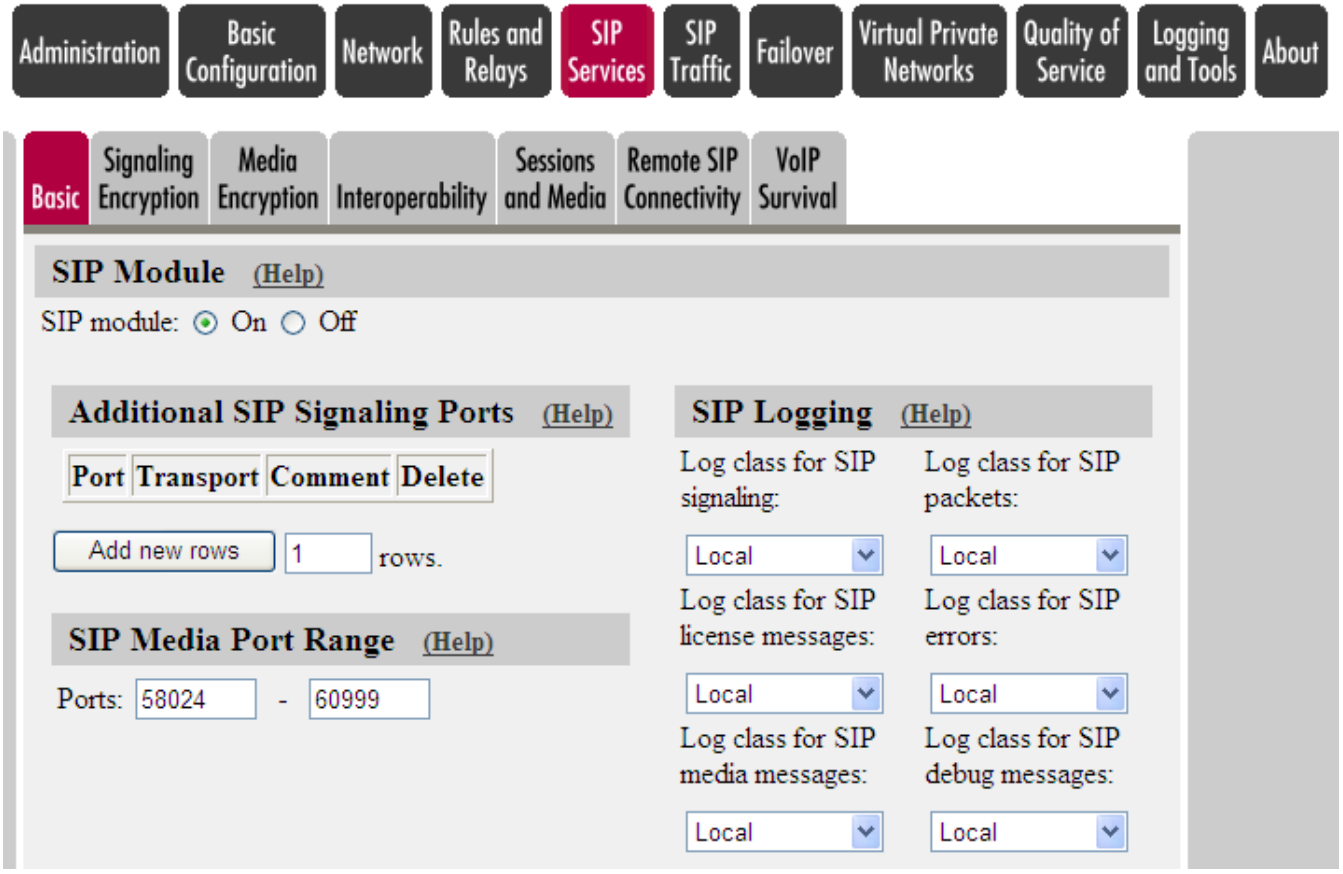
Programming: SIP Services

inGate

Programming: SIP Services

Basic

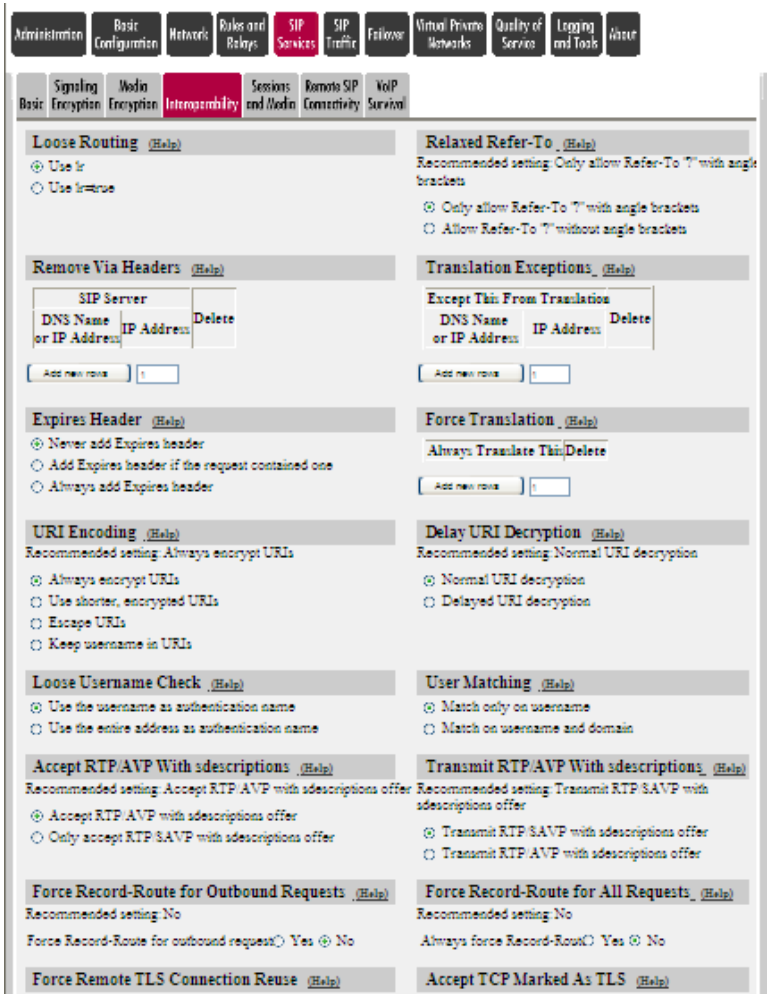
- Turn On SIP Module.
- Define Media Port Range.



Programming: SIP Services

Interoperability

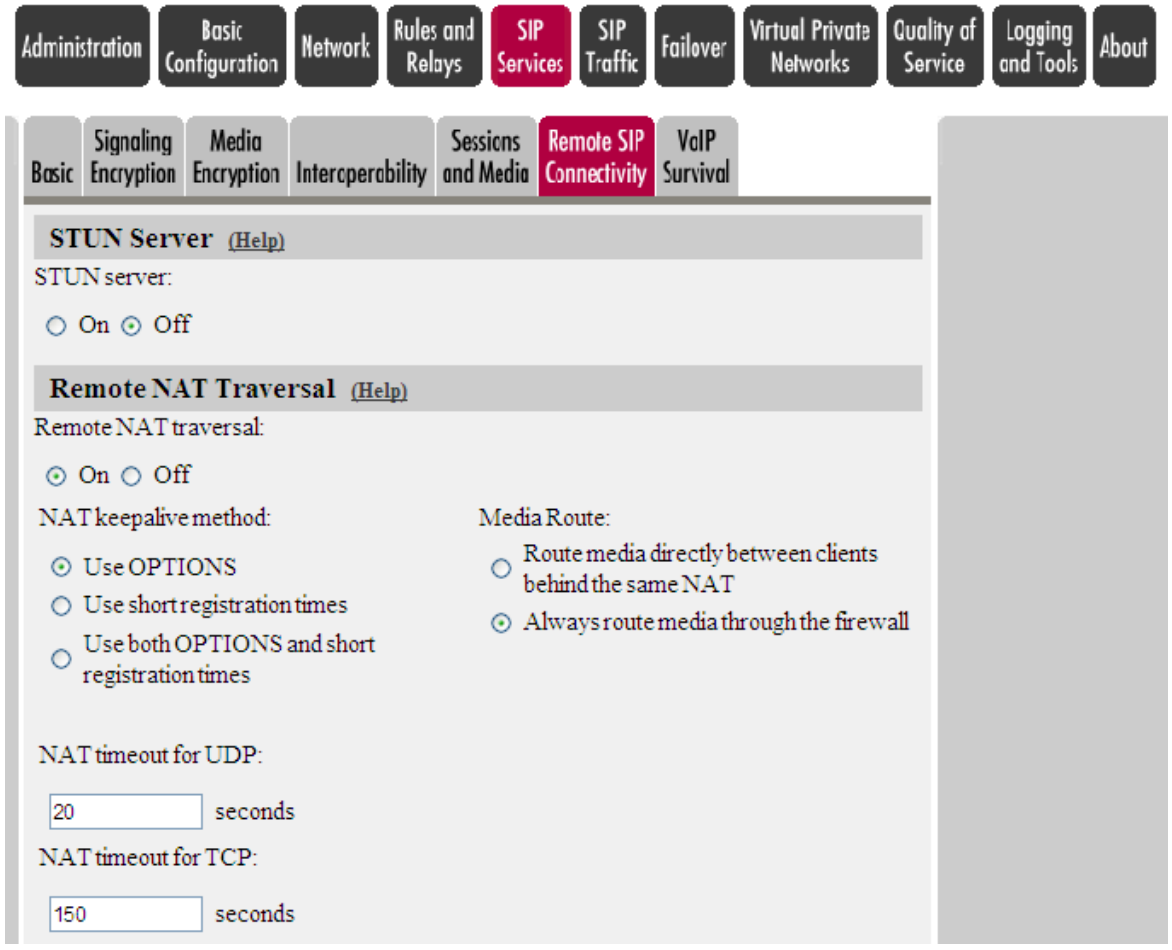
- Common deviations from the standard



Programming: SIP Services

Remote SIP Connectivity

- Allows SIP client behind NAT boxes to use SIP.



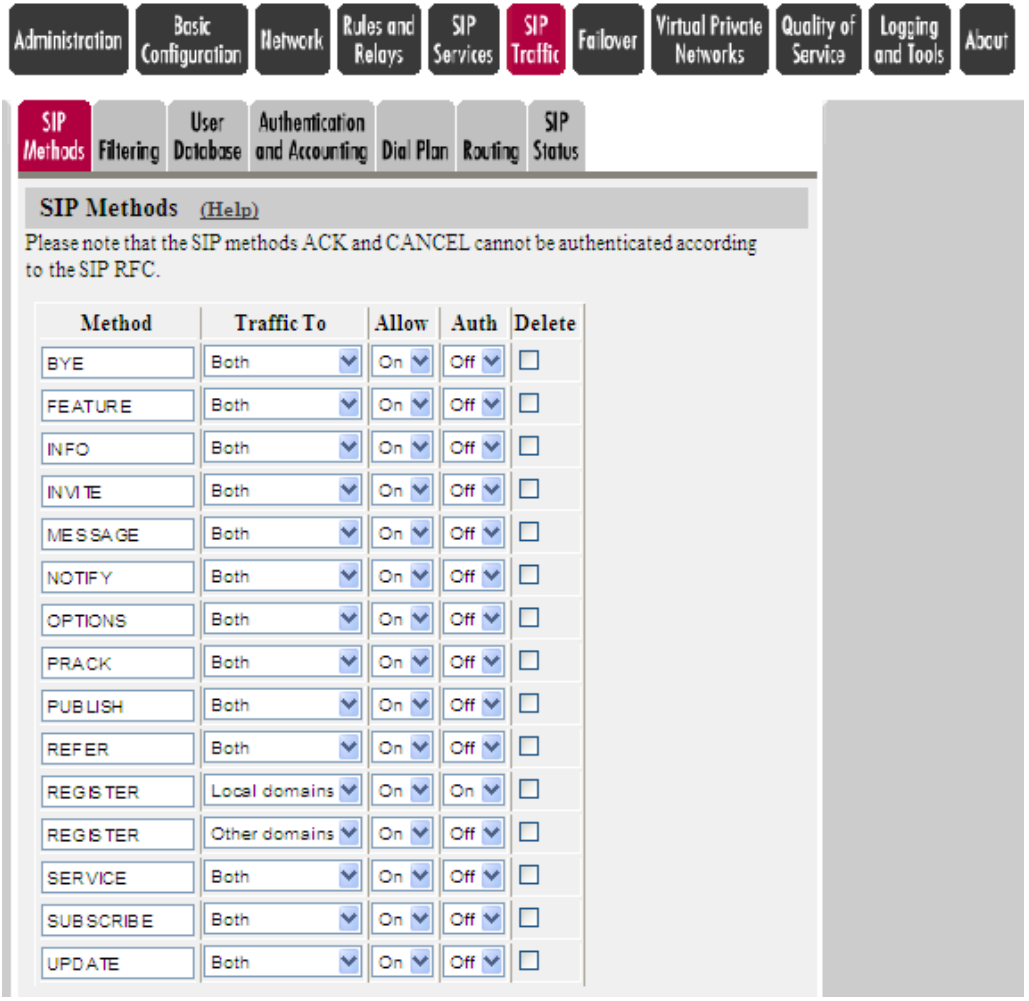
Programming: SIP Traffic

inGate

Programming: SIP Traffic

SIP Methods

- Select which SIP methods the firewall should allow & authenticate

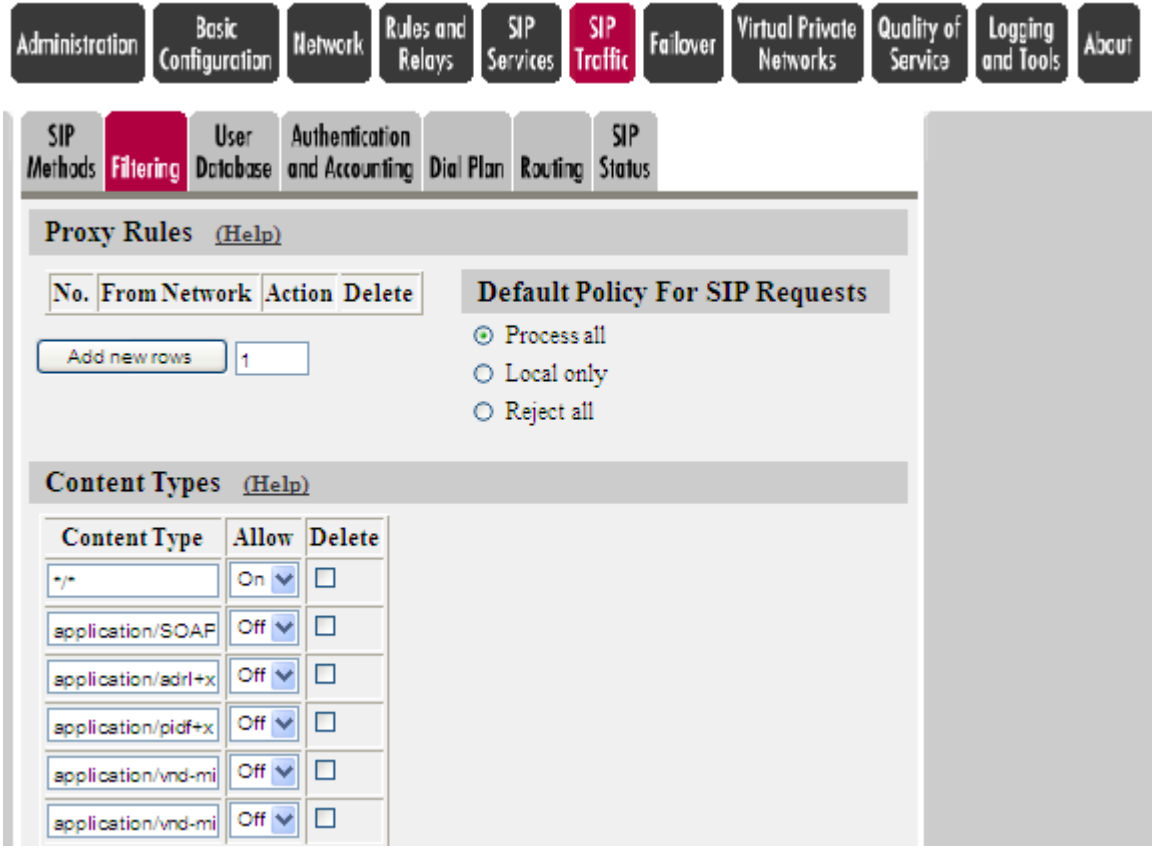


inGate

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



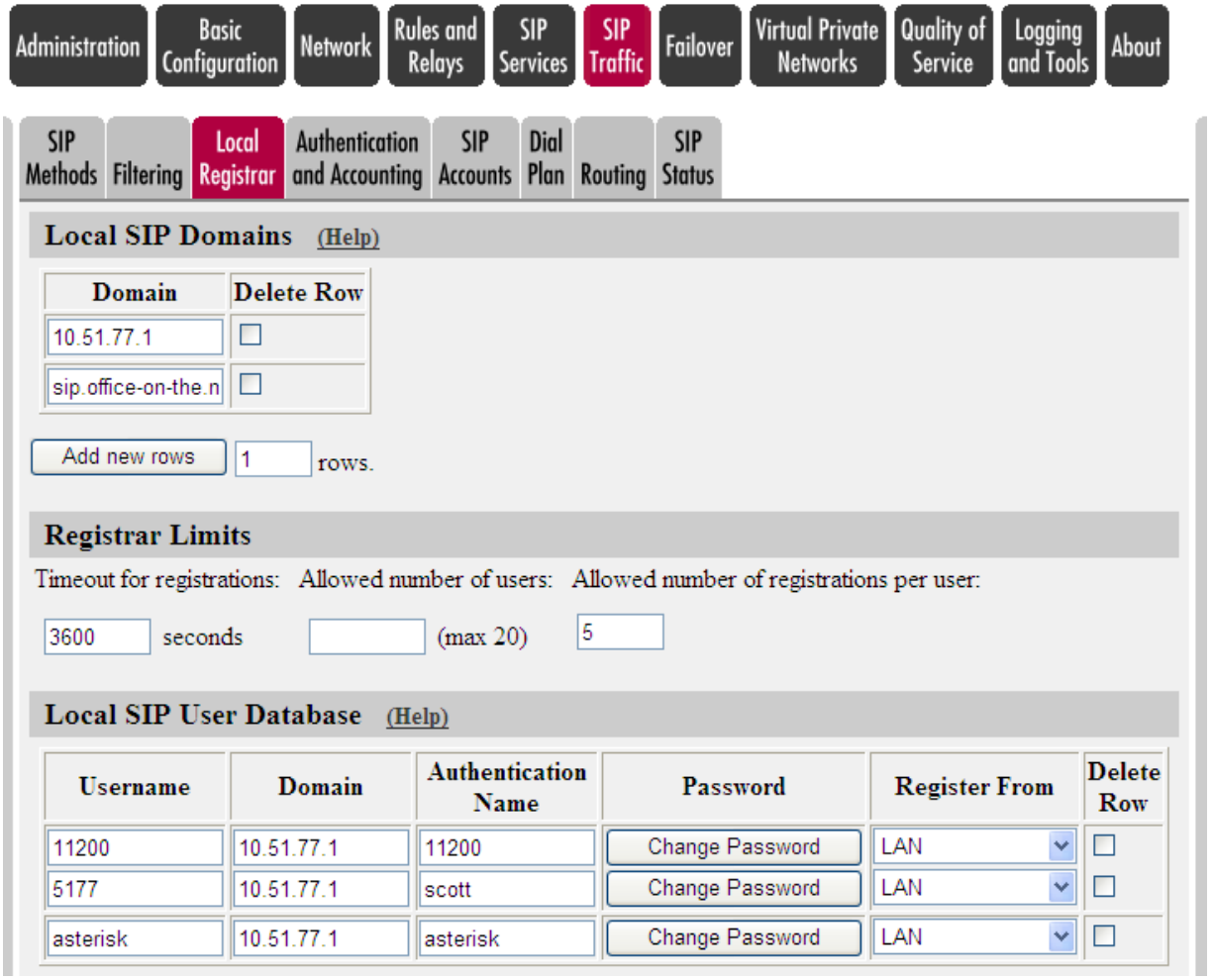
- The **Content Type** table controls if sipfw should process requests, based on the content type of the request body
- */* - Allows All

inGate

Programming: SIP Traffic

Local Registrar

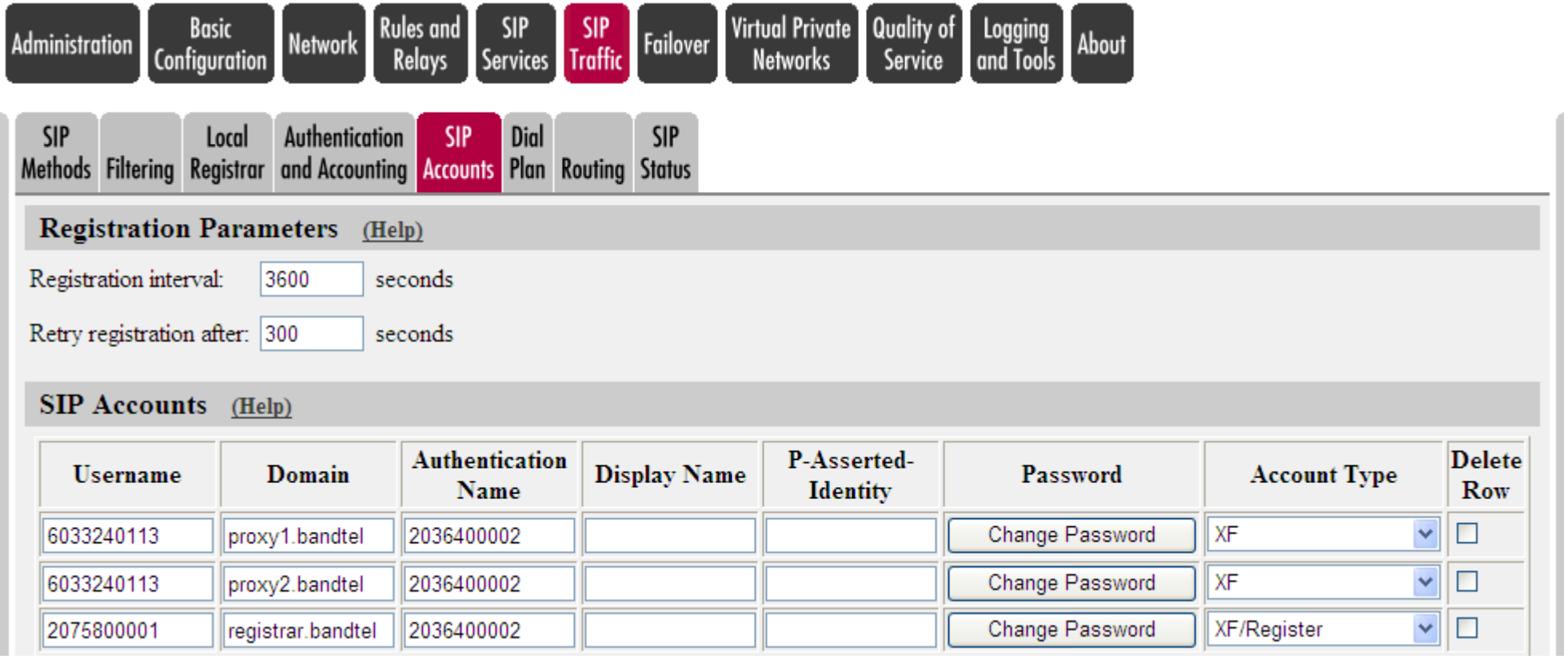
- Define SIP Users that register to the Ingate (server registrar)



Programming: SIP Traffic

SIP Accounts

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



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

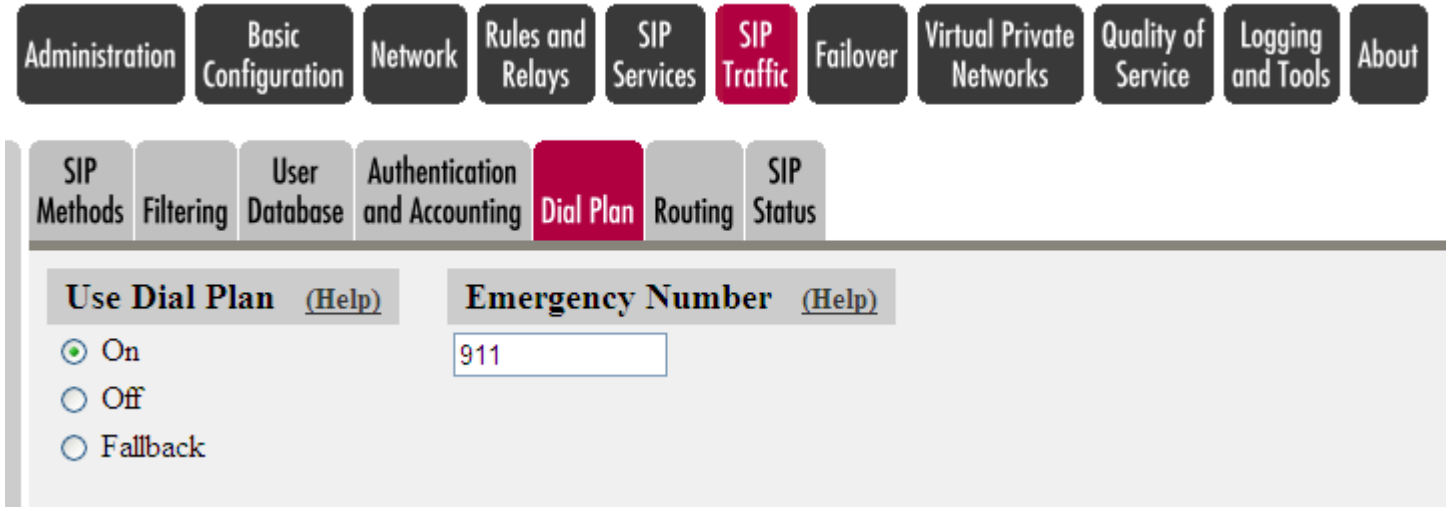
User Database: Account Type Selections

- **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

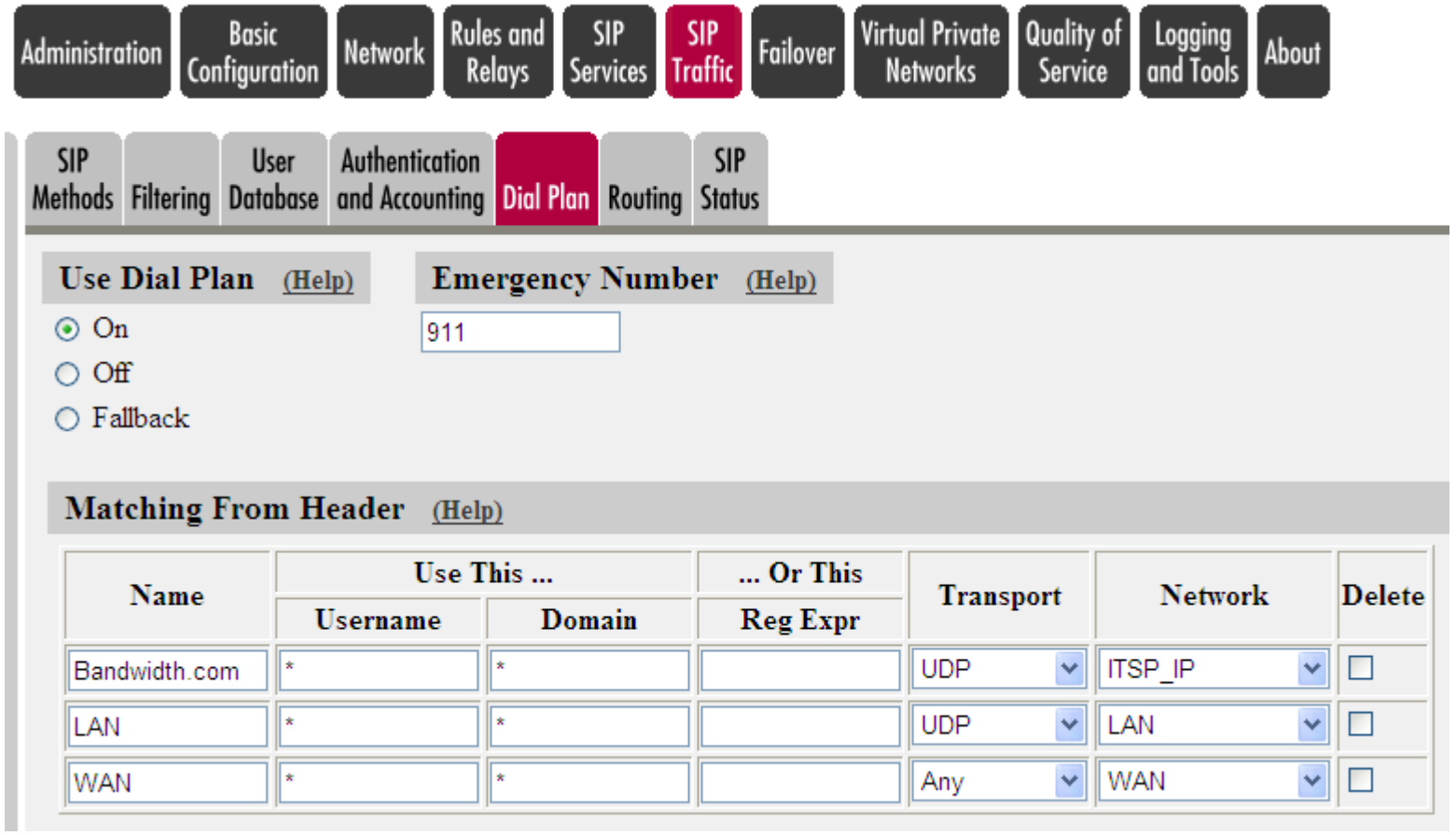


inGate

Programming: SIP Traffic

Dial Plan "Matching FROM Header"

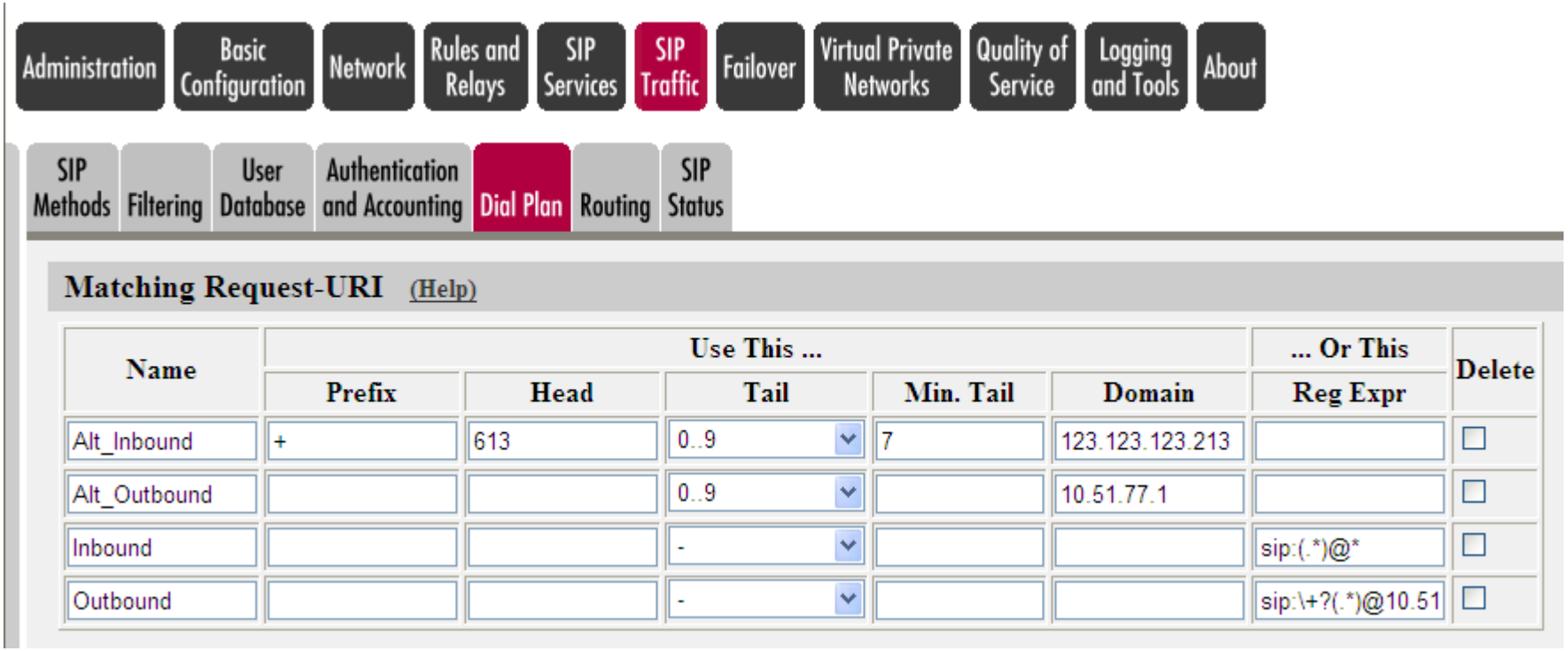
- Requests can be matched on From header, sender IP address, transport method and network.



Programming: SIP Traffic

Dial Plan "Matching Request URI"

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

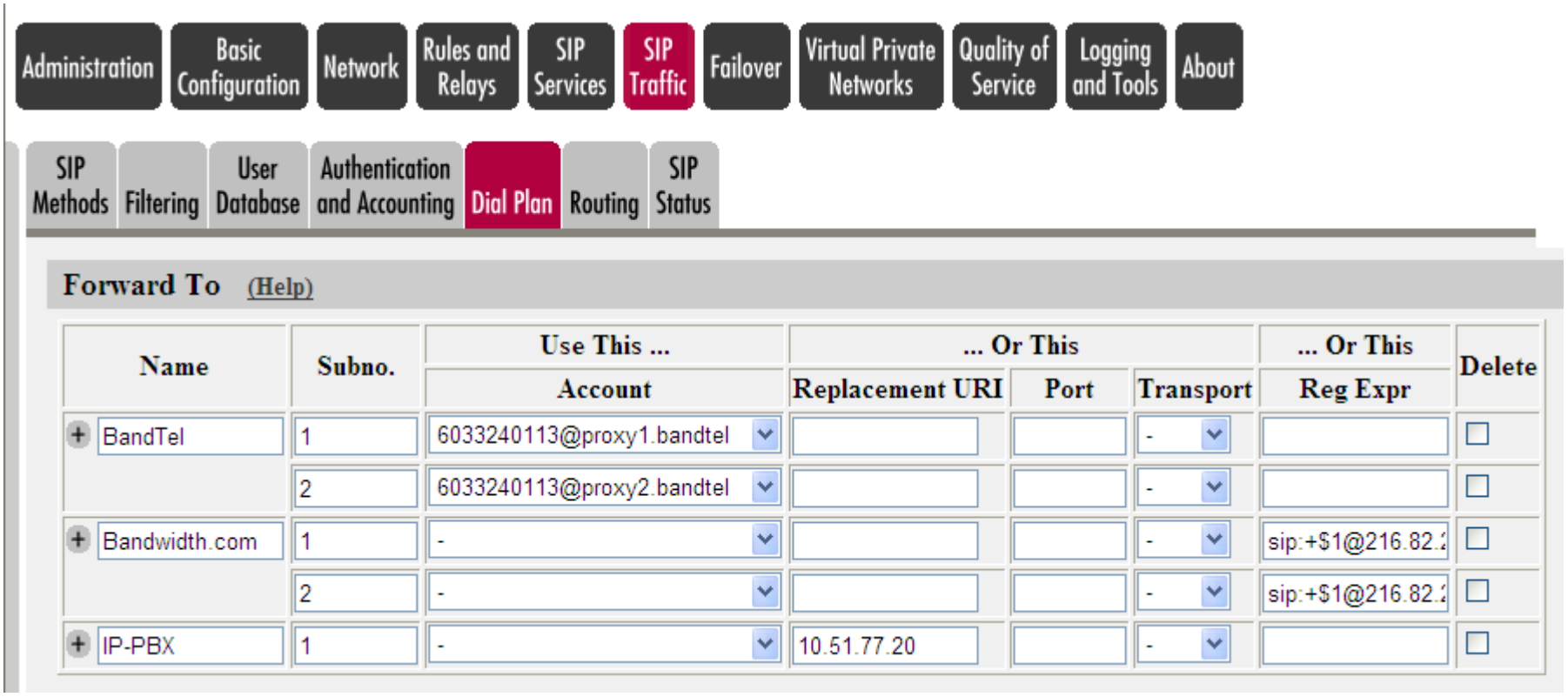


inGate

Programming: SIP Traffic

Dial Plan "Forward To"

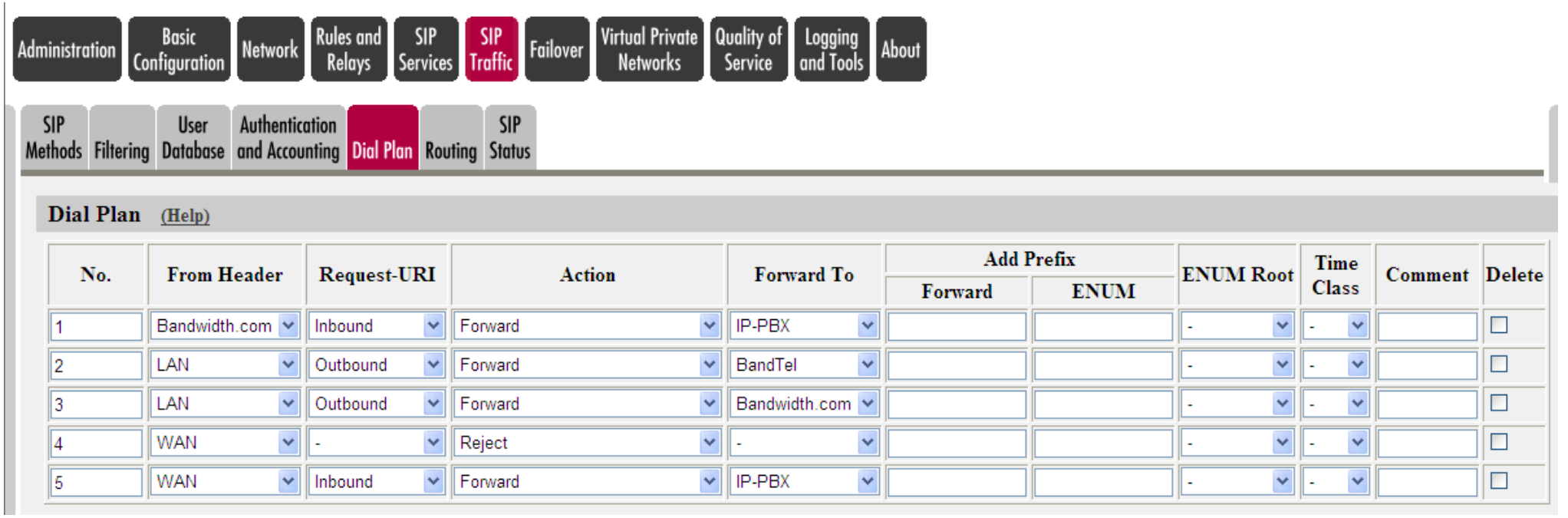
- Define destinations for the SIP requests



Programming: SIP Traffic

Dial Plan "Dial Plan"

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



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			-	-		☐
2	LAN	Outbound	Forward	BandTel			-	-		☐
3	LAN	Outbound	Forward	Bandwidth.com			-	-		☐
4	WAN	-	Reject	-			-	-		☐
5	WAN	Inbound	Forward	IP-PBX			-	-		☐

inGate

Programming: SIP Traffic

How Does It Work?

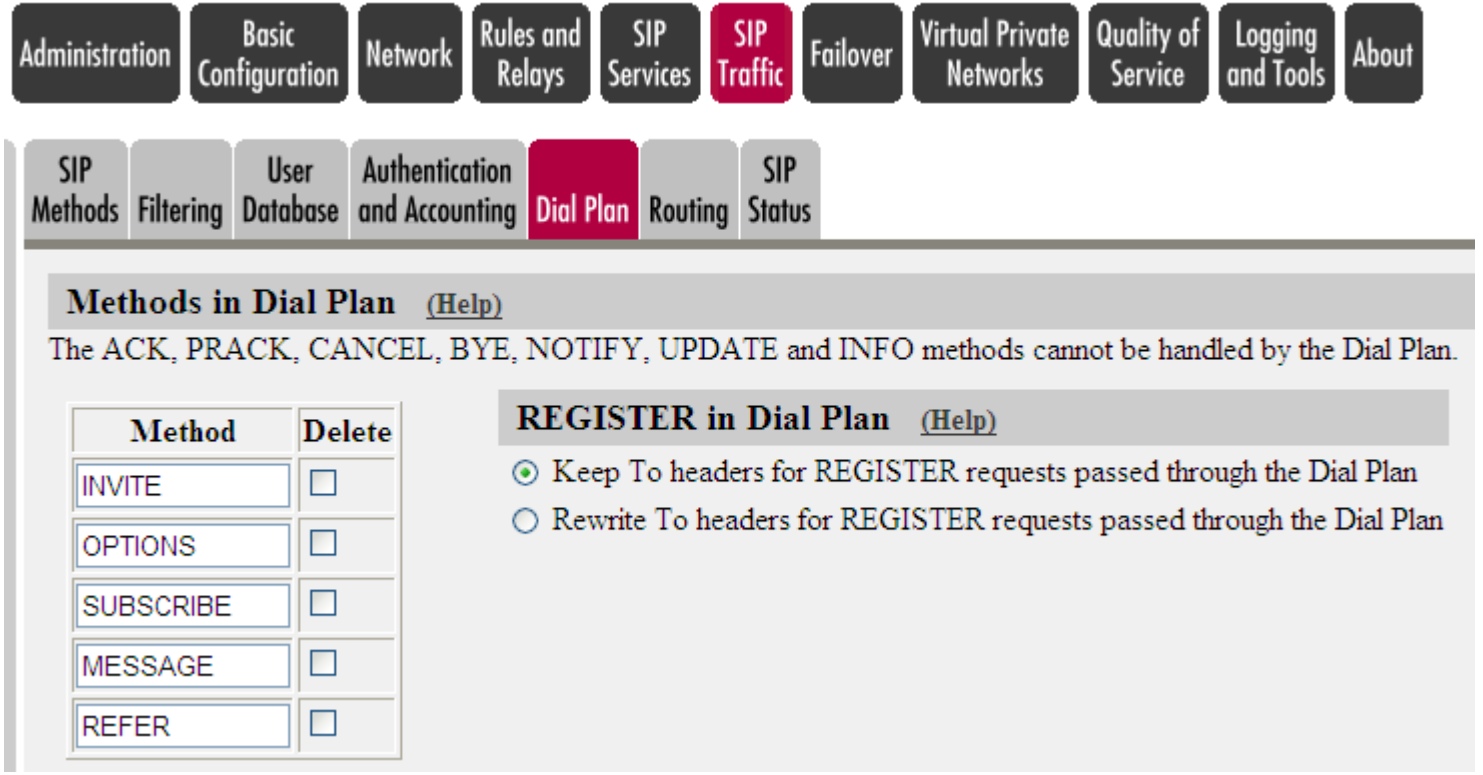
- Outgoing Call
  - SIP Phone sends INVITE to 6135552000@IP_IP-PBX
  - IP-PBX sends INVITE to 6135552000@IP_Ingate
  - Ingate sends INVITE to 6135552000@IP_ITSP
- Incoming Call
  - ITSP sends INVITE to 6135554455@IP_Ingate
  - Ingate sends INVITE to 6135554455@IP_IP-PBX
  - IP-PBX sends INVITE to ExtNumber@IP_Phone

inGate

Programming: SIP Traffic

Dial Plan "Method in the Dial Plan"

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

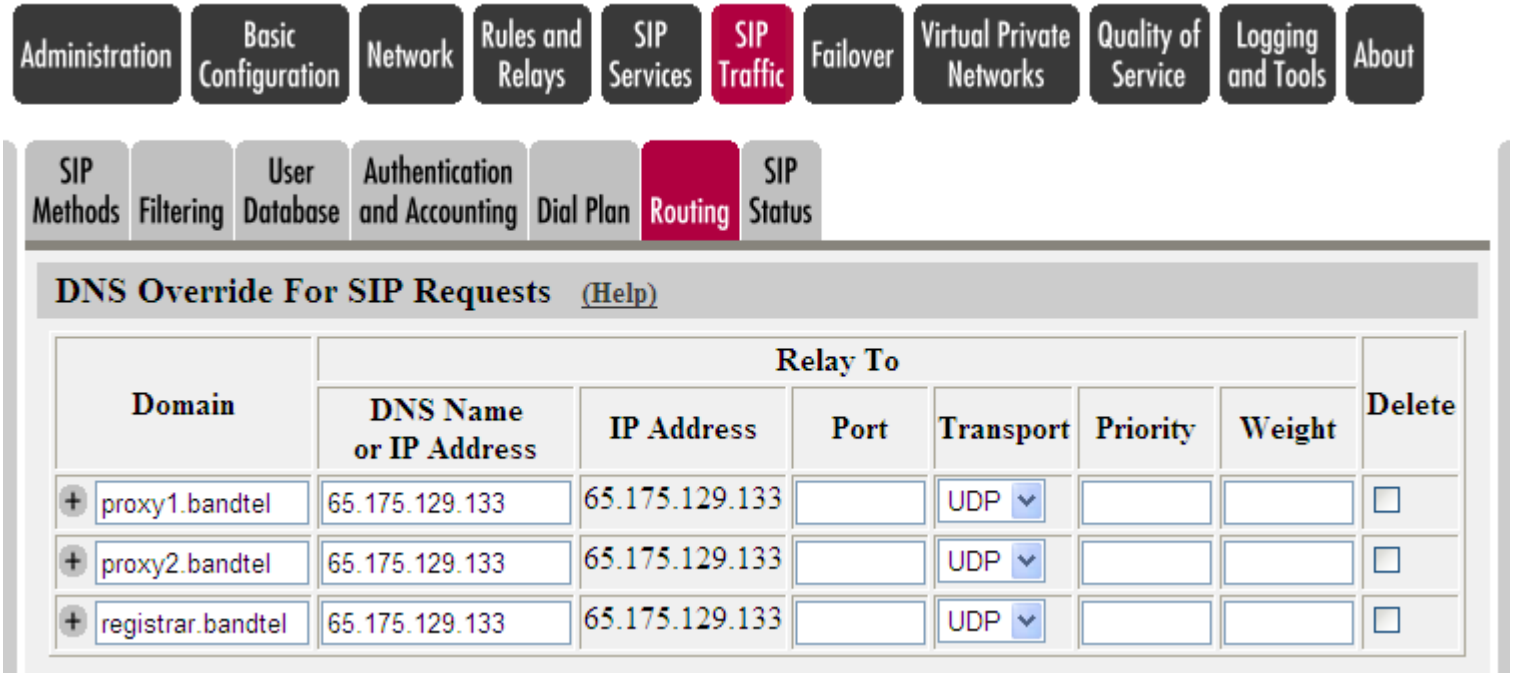


inGate

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

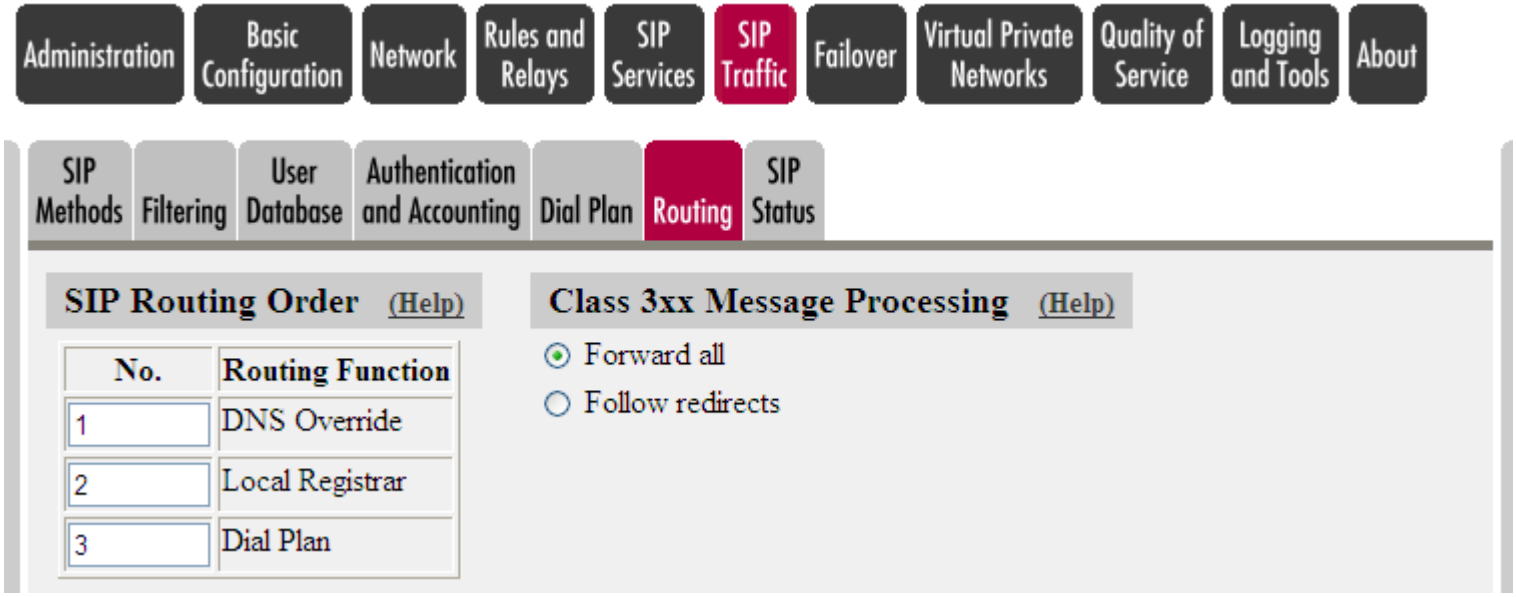


inGate

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

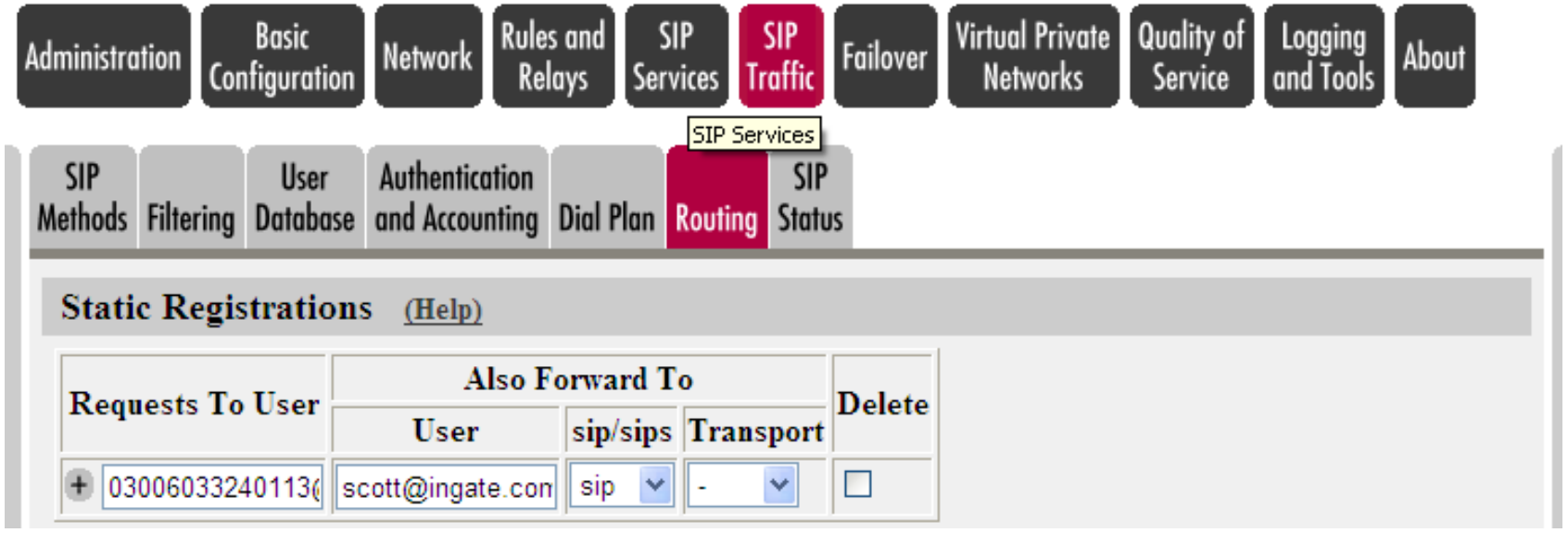


inGate

Programming: SIP Traffic

Routing "Static Registrations"

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

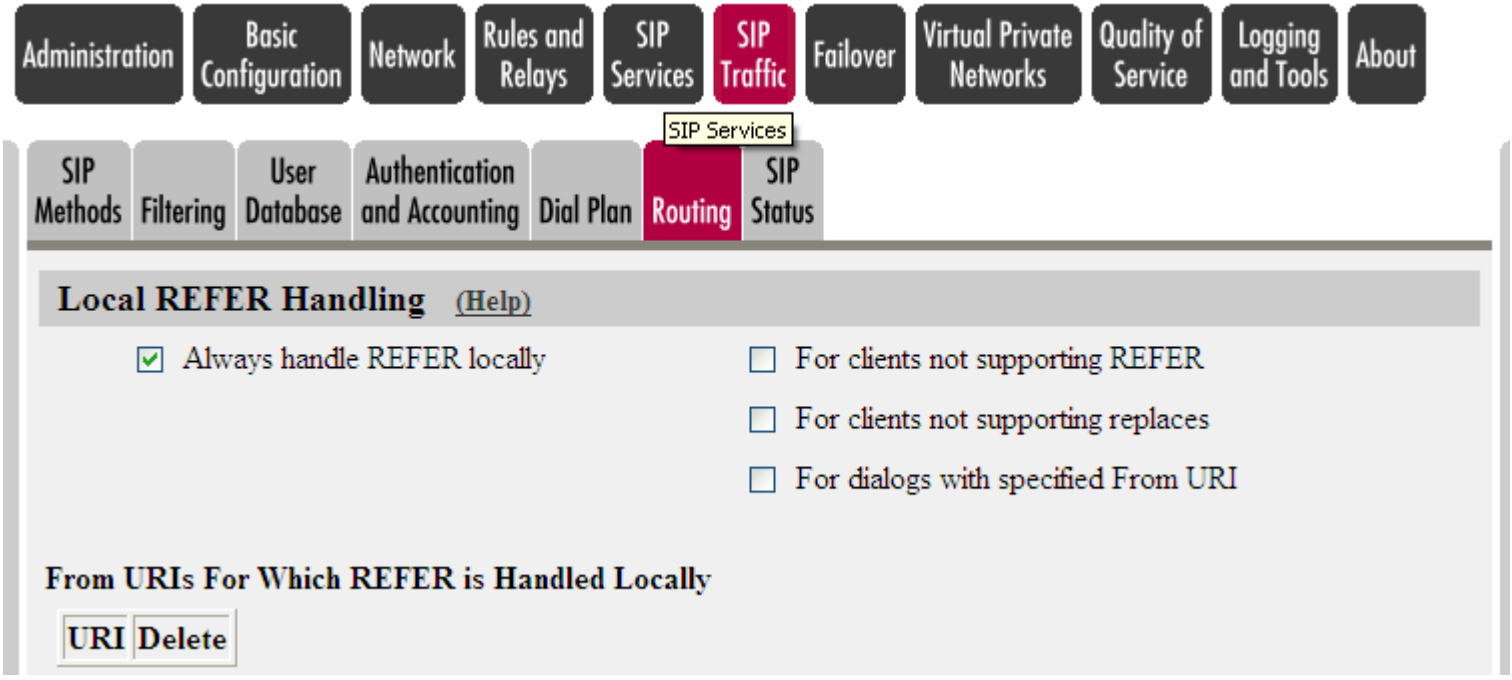


inGate

Programming: SIP Traffic

Routing "Local REFER Handling"

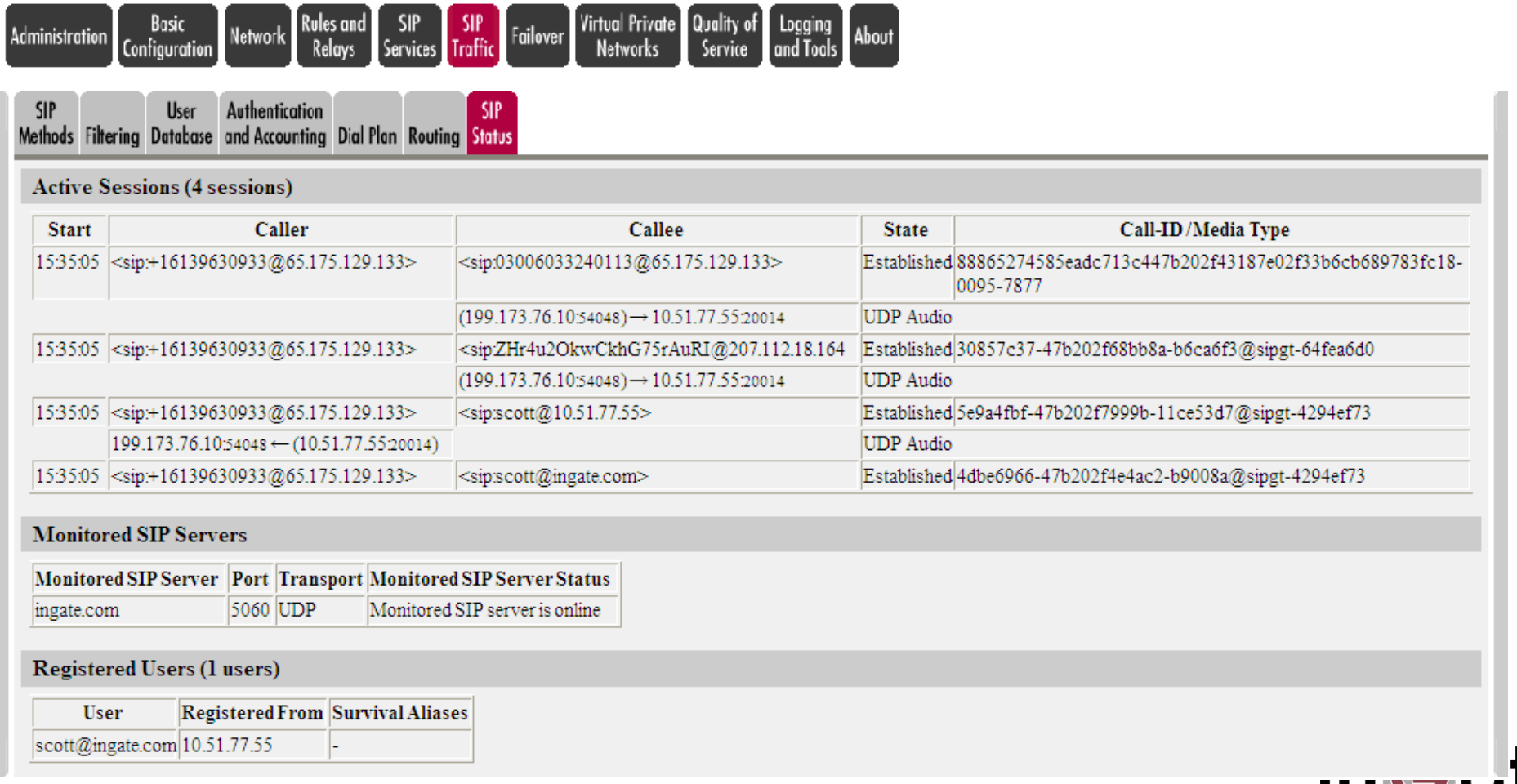
- SIP Trunking Service Providers can not handle a REFER Method. Many IP-PBX require to send REFERs for Transferring calls. This ensure the Ingate handles the REFER locally.



Programming: SIP Traffic

SIP Status

- Shows current SIP activity



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

LAN

Internet

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

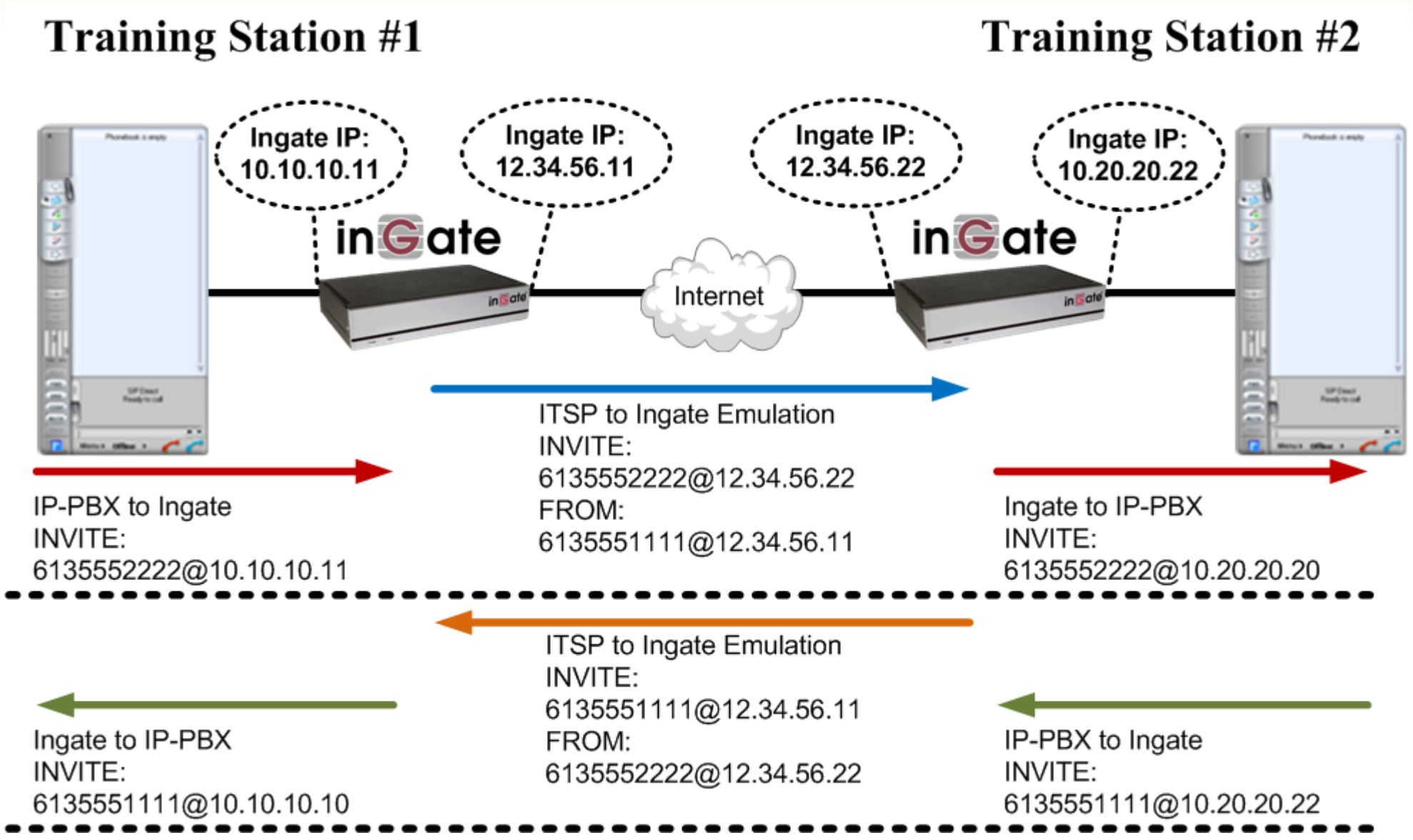


Softphone
DID #: 6135554444
IP Address: 10.40.40.40

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 #2



inGate

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

LAN

Internet

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

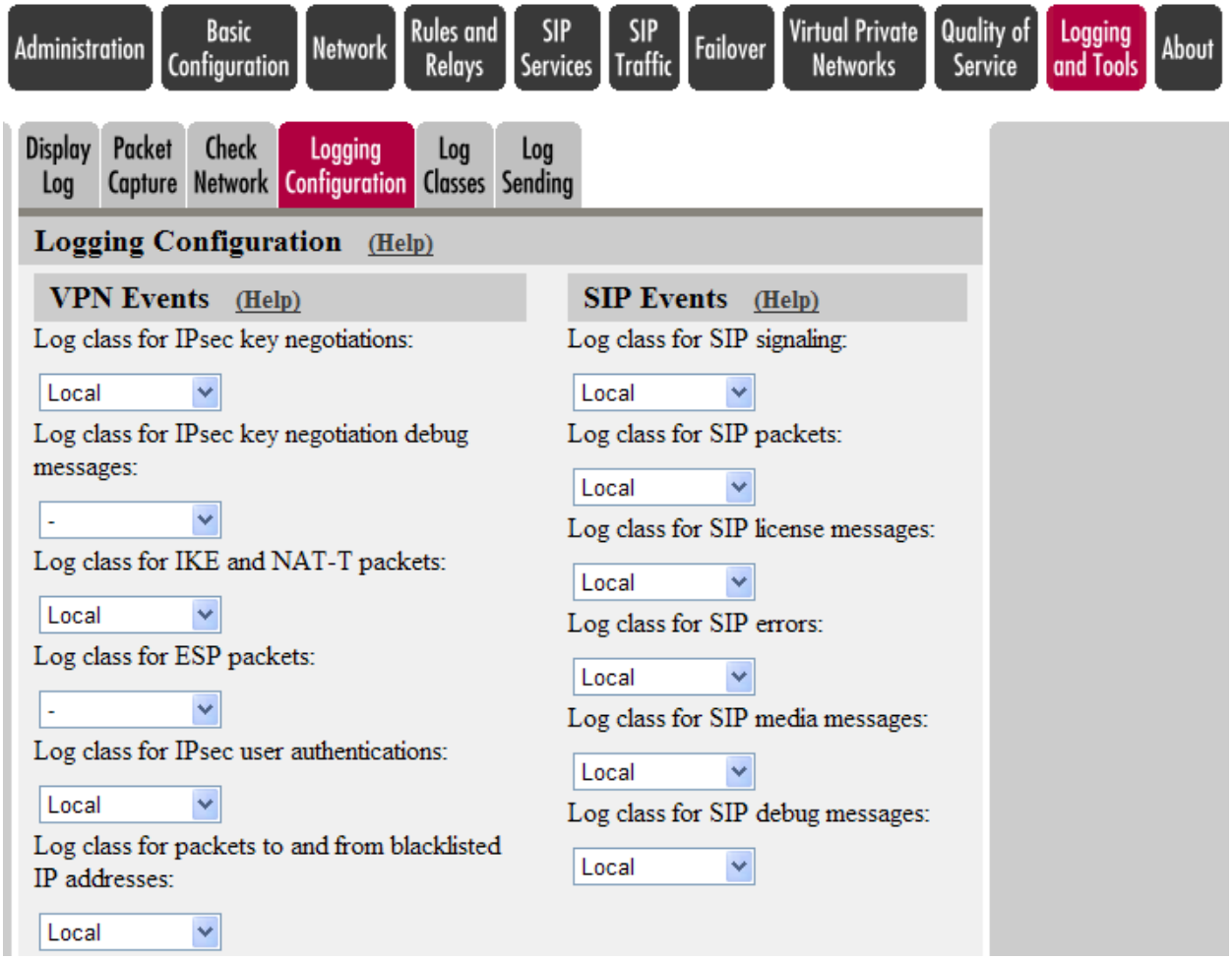
Ingate SIParator 19
Username: admin
Password: admin
MAC Address: 00-D0-C9-AD-B5-02
Eth0 (Inside) IP Address: 10.40.40.44
Mask: 255.255.255.0
Eth1 (Outside) IP Address: 12.34.56.44
Mask: 255.255.255.0
Default GW: 12.34.56.1
DNS: 65.175.129.149

Troubleshooting

Troubleshooting

Logging Configuration

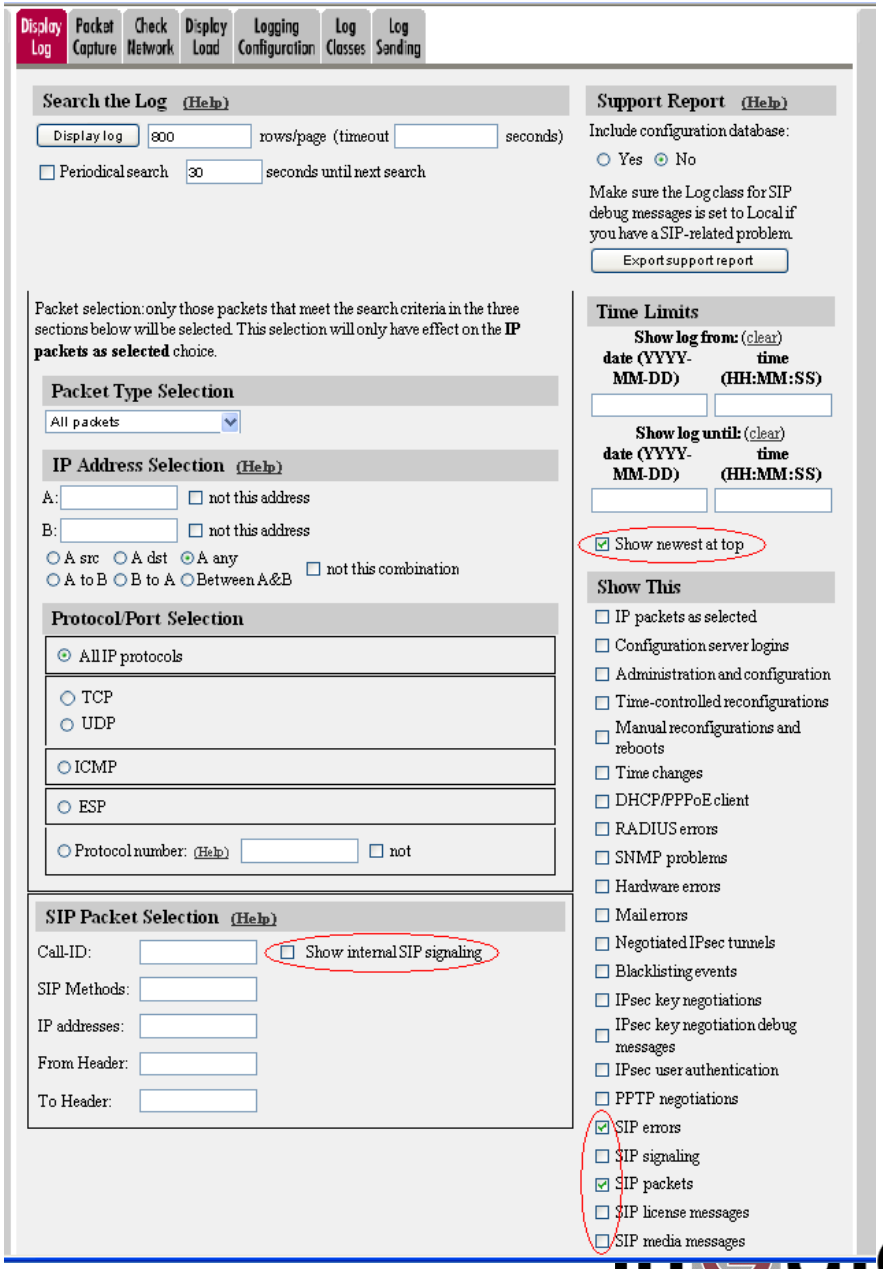
- SIP Events will ensure SIP calls are logged.



Troubleshooting

Logging & Tools

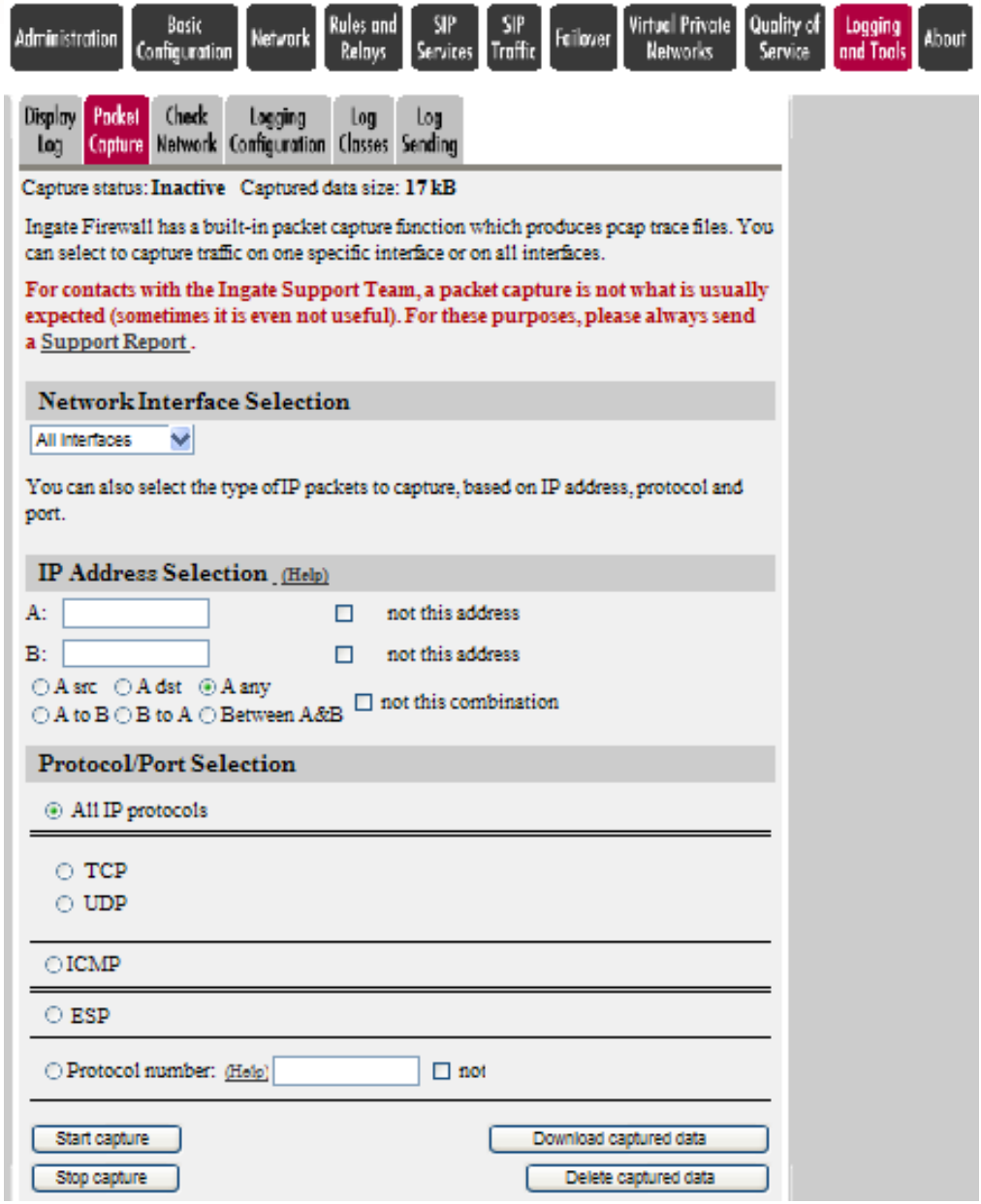
- Display # Rows/Page
- Show Newest on Top
- Select SIP Log Attributes
- Select "Show internal SIP Signaling"



Troubleshooting

Packet Capture

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



Exercise #4
Packet Capture

THE END

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

LAN

Internet

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

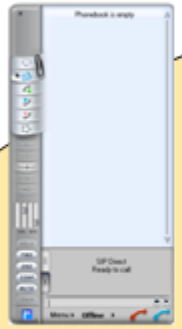


Softphone
DID #: 6135554444
IP Address: 10.40.40.40

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

MAKE A CALL

Softphone
Call Training Station #2:
6135552222@10.10.10.11

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

MAKE A CALL

Training Station #1
IP Address: 12.34.56.11
Softphone DID: 6135551111

Softphone
Call Training Station #1:
6135551111@10.20.20.22

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

MAKE A CALL

Softphone
Call Training Station #4:
6135554444@10.30.30.33

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

MAKE A CALL

Training Station #3
IP Address: 123.123.123.33
Softphone DID: 6135553333

Softphone
Call Training Station #3:
6135553333@10.40.40.44