AlliedWare TM OS

How To | Configure the Firewall VoIP Support Service (SIP ALG)

Introduction

SIP (Session Initiation Protocol) is an increasingly popular protocol for managing VoIP call setup. The structure of the packets involved in a SIP exchange is relatively complex, and involves embedded IP addresses (i.e. IP addresses embedded into the payload of the packet, not just IP addresses in the packet header).

Protocols that involve embedding IP addresses into packet payloads are typically rather challenged by NAT. SIP is no exception to this rule. In order for SIP to operate successfully through a NATing firewall, it is necessary for the firewall to be able to reach right into the payload of outgoing packets, and translate any embedded private addresses into the correct public addresses (and vice versa for incoming packets).

The AlliedWare firewall does include the functionality required to perform this invasive updating of SIP packet payloads. The agent within the firewall that performs this activity is referred to as the SIP ALG (Application Level Gateway).

What information will you find in this document?

This document describes a typical SIP ALG application and takes you through a step-by-step configuration example. This is followed up with some helpful monitoring and diagnostic information. Then the document ends with information about configuring the VoIP PIC and another configuration example.

The document is divided into the following sections:

Which products does it apply to?

This Note applies to the following Allied Telesis routers and managed layer 3 switches:

- AR400 and AR700 series routers
- AT-8800, Rapier, and Rapier i series switches
- AT-9800 series switches

It requires AlliedWare software version 2.7.5 or later.

Related How To Notes

You may also find the following How To Notes useful:

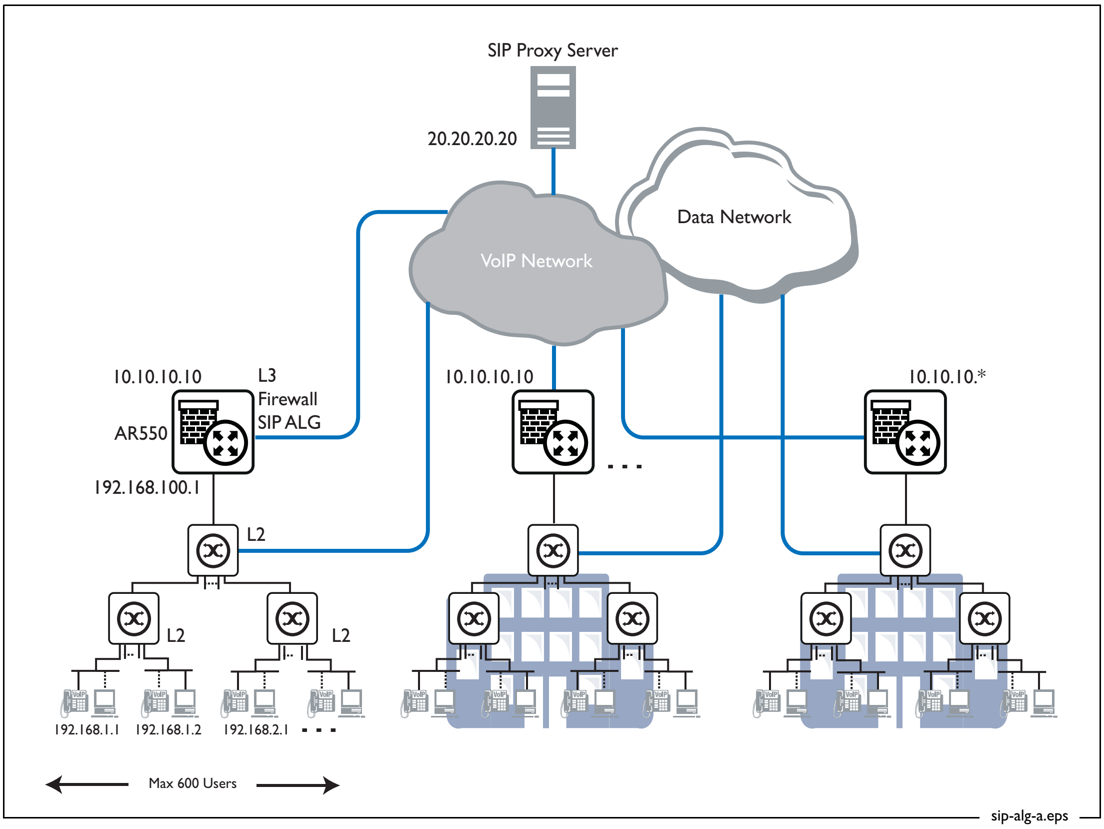
- *How To Configure Some Basic Firewall And VPN Scenarios*
- *How To Configure The Firewall Using The Graphical User Interface (GUI)*
- *How To Apply Firewall Policies And Rules*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

Typical SIP ALG application

The SIP ALG can be a central element in the VoIP service for apartment complexes. In the example illustrated below, the L2 switches in the network separate VoIP traffic from other traffic. The VoIP calls **all** pass through a firewall dedicated to handling just the VoIP.

Figure 1: A network with a dedicated firewall for VoIP



Users in each apartment complex are assigned IP addresses from the private address range. The SIP packets arriving from these users to the firewall will have Private IP source addresses in their headers and embedded in their payloads. It is the responsibility of the firewall to ensure that the private addresses are all correctly translated to a public address (and vice versa for packets going in the other direction). In particular, the firewall needs to ensure that VoIP calls initiated from the public side are successfully directed to the correct user on the private side.

Now, the firewall has only a single public IP address, so all the users on the private side will appear to users on the public side to have the same IP address. So the different private users need to be differentiated by each using a different UDP port number for their VoIP traffic on the public side.

NAPT must be enabled

So, NAPT (Network Address and Port Translation) needs to be enabled on the VoIP firewall so that each user's SIP packets are translated to a unique source UDP port number.

It is the responsibility of the firewall to ensure that NAPT is correctly applied to all VoIP packets. It must ensure that the appropriate IP addresses and ports are used when the VoIP terminals communicate with the VoIP Proxy server. The public IP address and port combination used for each client must be constant so that connections to a known client can be initiated from the public side of the firewall.

Some more detail about SIP and SIP ALG

The Session Initiation Protocol (SIP), in conjunction with the Session Description Protocol (SDP), is an application layer protocol that is able to negotiate end-to-end sessions for users on the Internet. Such sessions can be used to carry various forms of multimedia data including voice traffic via RTP (VoIP). SIP utilises an infrastructure of SIP Proxy servers to allow Internet endpoints (SIP User Agents) to locate each other and negotiate session parameters. SIP supports four basic functions in order to establish, modify and terminate such multimedia sessions:

- Location of an Internet end point
- Signal of a desire to communicate
- Negotiation of session parameters to establish the session
- Tear down of an established session

A SIP Application Layer Gateway (ALG) provides functionality to allow VoIP traffic to pass both from the private to public and public to private side of the firewall when using Network Address & Port Translation (NAPT). The SIP-ALG inspects and modifies SIP traffic to allow SIP traffic to pass through the firewall so that person-to-person SIP sessions may be established. More exactly, NAPT mapping is provided from the users on the private side of the firewall to the SIP Proxy on the public side of the firewall by altering the IP addresses, UDP port numbers, and SIP/SDP messages in SIP packets.

The SIP Server is on the public side of the firewall and acts as a proxy for all SIP messages between SIP User Agents. The SIP traffic from the private routing domain to the SIP Proxy server will contain SIP and SDP information referencing that routing domain specifying network addresses that cannot be directly accessed from the public side of the firewall. Since this SIP and SDP information is used by SIP User Agents to determine the location of end points and the location of SIP Proxies between end points, key parts of it must be modified, along with SIP packet IP addresses and UDP port numbers. Translation of both request and reply packets is necessary in order for a SIP session to be fully negotiated.

Real-time Transport Protocol (RTP) and Real Time Control Protocol (RTCP) packets transport the actual voice data in a VoIP call. The SIP-ALG dynamically controls the opening and closing of logical ports in order to establish, maintain, and terminate the RTP sessions negotiated by the SIP protocol. The RTP/RTCP packets also have their IP addresses and port numbers modified in order to allow session traffic across the firewall once an end-to-end session is established.

Step-by-step configuration example

1. Configure general system and user settings

Set system name:

```
set system name=VoIPFirewall
```

Define a security officer:

```
add user=secoff pass=<your-secoff-password> priv=securityOfficer
  lo=yes telnet=yes
```

Do not forget your secoff password. You will have difficulty gaining access without your password when security mode is enabled on the router.

Enable system security:

```
enable system security
```

Now that security mode has been enabled, you need to be logged in as a security officer in order to enter most configuration-altering commands.

Login as the security officer:

```
login secoff
password: <your-secoff-password>
```

When security mode is enabled, any router configuration access will time out on inactivity to prevent unauthorised access. The default timeout is 60 seconds, but you may temporarily raise it to 600 seconds if desired. Set user time out:

```
set user securedelay=600
```

2. Configure IP

Add an IP interface - eth1. Interface eth1 provides the public connection interface, using a fixed address.

```
enable ip
add ip int=eth1 ip=192.102.1.1
```

Add the router interface to the LAN. The eth0 interface connects the router to the LAN.

```
add ip int=eth0 ip=192.168.1.1 mask=255.255.255.0
```

Specify the next hop. The default route next hop will be the gateway address.

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth1 next=192.102.1.100
```

3. Configure firewall basics

Enable the firewall and create a firewall policy:

```
enable firewall

create firewall policy=voip

enable firewall policy=voip icmp_f=all
```

Enable the SIP ALG agent within the firewall:

```
enable firewall sipalg
```

Add your firewall policy to the public side of the interface. The Internet-facing interface of the router is a public (not trusted) interface on the firewall.

```
add firewall policy=voip int=eth1 type=public
```

Add the firewall policy to the private side of the interface. The LAN-facing interface of the router is the private (trusted) interface on the firewall.

```
add firewall policy=voip int=eth0 type=private
```

Enable NAT for any general traffic that passes through the firewall.

```
add firewall policy=voip nat=enhanced interface=eth0 gblint=eth1
```

4. Configure firewall NAT rules

To ensure each user on the private LAN uses the same public IP address and UDP port every time they make a phone call, **static** NAPT must be used. A firewall NAT rule is applied to each private user. This rule specifies the source IP address and UDP port of the SIP packets from the user and the public IP address and UDP port to be used on the global network.

Apply a firewall NAT rule to each private user.

```
add firewall policy=voip ru=1 ac=nat int=eth0 prot=udp
  ip=192.168.1.2 po=5060 gblip=192.102.1.1 gblp=61001
  nattype=napt


add firewall policy=voip ru=2 ac=nat int=eth0 prot=udp
  ip=192.168.1.3 po=5060 gblip=192.102.1.1 gblp=61002
  nattype=napt


add firewall policy=voip ru=3 ac=nat int=eth0 prot=udp
  ip=192.168.1.4 po=5060 gblip=192.102.1.1 gblp=61003
  nattype=napt


add firewall policy=voip ru=4 ac=nat int=eth0 prot=udp
  ip=192.168.1.5 po=5060 gblip=192.102.1.1 gblp=61004
  nattype=napt


add firewall policy=voip ru=5 ac=nat int=eth0 prot=udp
  ip=192.168.1.6 po=5060 gblip=192.102.1.1 gblp=61005
  nattype=napt

  ...
```

When register messages are sent from the VoIP devices on the private LAN to the Proxy server (on the public side of the firewall), the source UDP ports on those register messages will be the port numbers specified in these firewall rules. Therefore, the SIP proxy server will register the users' phone numbers as all being at IP address 192.102.1.1, but with a different UDP port value for each user.

So, when calls are initiated from the public side of the firewall, the proxy will direct those calls to the UDP port number that has been registered for the phone number being called.

Then, the firewall must ensure that packets being sent to 192.102.1.1 on these particular UDP port numbers are delivered to the correct users on the private LAN.Thus achieved by NAT rules that map global IP addresses and ports to the corresponding private IP addresses. These rules specify the global destination IP address and UDP port of the SIP packets to the user and the private IP address and UDP port of the user.

```
add firewall policy=voip ru=11 ac=nat int=eth1 prot=udp
  gblip=192.102.1.1 gblp=61001 po=5060 ip=192.168.1.2
  nattype=napt


add firewall policy=voip ru=12 ac=nat int=eth1 prot=udp
  gblip=192.102.1.1 gblp=61002 po=5060 ip=192.168.1.3
  nattype=napt


add firewall policy=voip ru=13 ac=nat int=eth1 prot=udp
  gblip=192.102.1.1 gblp=61003 po=5060 ip=192.168.1.4
  nattype=napt


add firewall policy=voip ru=14 ac=nat int=eth1 prot=udp
  gblip=192.102.1.1 gblp=61004 po=5060 ip=192.168.1.5
  nattype=napt


add firewall policy=voip ru=15 ac=nat int=eth1 prot=udp
  gblip=192.102.1.1 gblp=61005 po=5060 ip=192.168.1.6
  nattype=napt

...
```

These rules are effectively the mirror image of the rules applied further above to the eth0 interface.

Note: If phone calls are **never** to be initiated from the public side of the firewall, i.e. will **always** be initiated from the users of the private side of the firewall, then the NAT rules are completely unnecessary. The SIP ALG is capable of doing all the address translation required to correctly manage multiple simultaneous calls initiated from the private side.

Monitoring and diagnostics

Once the network is setup it is important to be able to monitor the current state and debug problems. The firewall has comprehensive debugging and counters for this purpose.

```
    show firewall session

    enable firewall policy=voip debug=sipalg
```

The **debug=sipalg** option provides very detailed tracing of the SIP packet parsing and content altering that the SIP ALG agent is performing. The debug outputs the pre-processed form of each SIP packet passing through, then lists the activities being performed on the packet, and finally displays the port-processing form of the packet. Typical output looks like:

```
SIPALG DEBUG - Incoming unprocessed message:
SIP/2.0 180 Ringing
    Via: SIP/2.0/UDP 172.28.34.20:61001;branch=z9hG4bK5b93297f
    From: <sip:2002@172.28.254.4>;tag=1509138271
    To: <sip:1001@172.28.254.4>;tag=1509138271
    Call-ID: 444742994@172.28.34.20
    CSeq: 1724088549 INVITE
    user-agent: ATI-AR027 Rel 1-0-0
    Content-Length: 0

SIPALG DEBUG: Looking for 'CSeq' field

SIPALG DEBUG: Processing a "180 or 183" message - Incoming

SIPALG DEBUG: Looking for 'Call-ID' field

SIPALG DEBUG: Updating 'Call-ID' field

SIPALG DEBUG: Searching for IP address:172.28.34.20

SIPALG DEBUG: IP- Pre:Call-ID: 444742994@172.28.34.20

SIPALG DEBUG: Replacing string:172.28.34.20 in field with:192.168.2.2

SIPALG DEBUG: IP- Post:Call-ID: 444742994@192.168.2.2

SIPALG DEBUG: Operation succeeded

SIPALG DEBUG: Looking for 'Via' field

SIPALG DEBUG: Updating 'Via' field

SIPALG DEBUG: Searching for IP address:172.28.34.20

SIPALG DEBUG: IP- Pre:Via: SIP/2.0/UDP
172.28.34.20:61001;branch=z9hG4bK5b93297f

SIPALG DEBUG: Replacing string:172.28.34.20:61001 in field
with:192.168.2.2:5060

SIPALG DEBUG: IP- Post:Via: SIP/2.0/UDP
192.168.2.2:5060;branch=z9hG4bK5b93297f

SIPALG DEBUG: Operation succeeded

SIPALG DEBUG - Incoming processed message:

SIP/2.0 180 Ringing
    Via: SIP/2.0/UDP 192.168.2.2:5060;branch=z9hG4bK5b93297f
    From: <sip:2002@172.28.254.4>;tag=1509138271
    To: <sip:1001@172.28.254.4>;tag=1509138271
    Call-ID: 444742994@192.168.2.2
    CSeq: 1724088549 INVITE
    user-agent: ATI-AR027 Rel 1-0-0
    Content-Length: 0
```

Appendix A: Configuring the VoIP PIC

The AR027 2-port FXS PIC card is fully interoperable with the SIP ALG.

In a multi-tenanted unit scenario, small businesses tenants can use an Allied Telesis router as their network gateway. By installing the AR027 PIC into the router, they can integrate the VoIP endpoint into the gateway router.

The business may perform yet another layer of NAT in order to host their own network behind the one private address allocated to them by the MTU network service provider. But, the integrated VoIP PIC will use the provider-allocated address for its calls, and so no extra level of SIP translation would need to be performed by this gateway router.

A typical configuration would be:

```
enable ip
add ip int=eth0 ip=192.168.1.129
add ip int=vlan1 ip=10.1.1.1
add ip route=0.0.0.0 int=eth0 next=192.168.1.1

set voip boot=c-1-0-0.bin server=flash
set voip pub int=eth0
set voip fi=ss-1-0-0.bin prot=sip ty=fxs
ena voip prot=sip engine=bay0.fxs0
cre sip int=bay0.fxs0.0 phone=1001 domain=20.20.20.20
  proxy=20.20.20.20
set sip int=bay0.fxs0.0 location=20.20.20.20

enable firewall
create firewall policy=soho
enable firewall policy=soho icmp_f=all
add firewall policy=soho int=vlan1 type=private
add firewall policy=soho int=eth0 type=public
add firewall policy=soho nat=enhanced int=vlan1 gblint=eth0
```

Note: You can download required files for the PIC from its Product Support section. Access this from www.alliedtelesis.com/products/detail.aspx?pid=139&lid=38

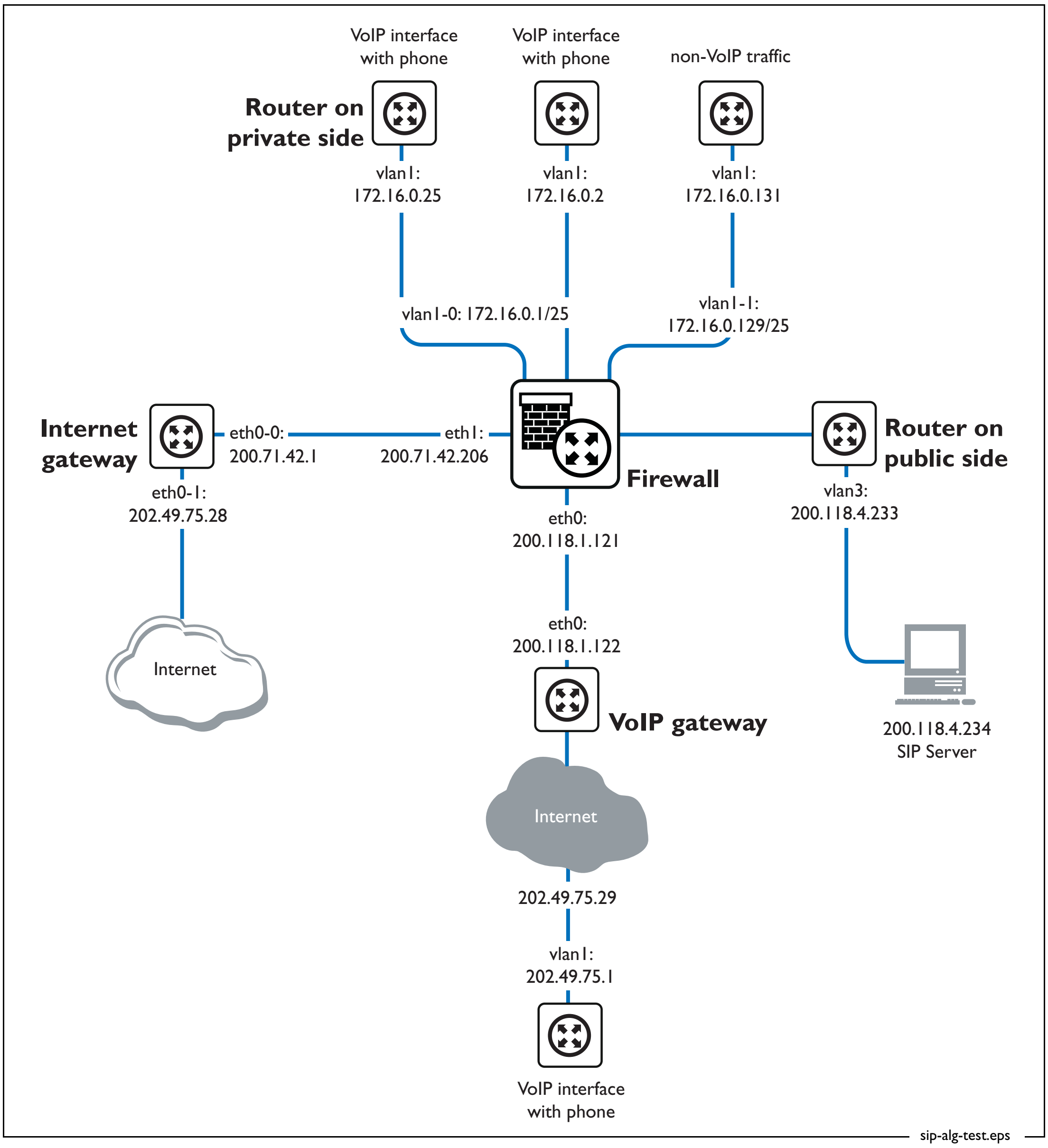
Appendix B: Configuring SIP on a different public interface to one already assigned for VoIP traffic

In this example, a customer wants to:

- send voice traffic out one public interface
- send non-voice traffic out another public interface, and
- put the SIP server on a third public interface

To achieve this, we multi-home vlan1 so that the VoIP traffic is in its own subnet. This lets us direct VoIP out one public interface and direct all other traffic out the other public interface.

The following figure shows our test network for this solution. The firewall's interface to the private LAN is vlan1, which is multi-homed. The firewall configuration uses policy routing to direct internet traffic out eth1, and uses firewall rules to direct VoIP traffic out eth0. We cannot use policy routing to control VoIP traffic because the SIP server would not register the private VoIP phones.



Multi-homing the private interface

Add new firewall rules

Firewall rules need to be added for each user VoIP phone. The rules are similar to those detailed in the configuration section of this How To Note (see page 5), but this particular solution requires an extra rule. So this means **three** rules for each new VoIP phone. Remember the following comment from step 4 on page 6:

To ensure each user on the private LAN uses the same public IP address and UDP port every time they make a phone call, ***static*** *NAPT must be used. A firewall NAT rule is applied to each private user. This rule specifies the source IP address and UDP port of the SIP packets from the user and the public IP address and UDP port to be used on the global network.*

Configuring the test network

We configured two VoIP IP phones; one is 172.16.0.2 and the other is 172.16.0.25. As the configuration script on page 12 shows, these IP addresses are in three firewall rules (underlined in the script). So for each additional VoIP phone in your network, you need to make three equivalent rules. We numbered the firewall rules in a way that makes addition of new ones easier.

Our testing checked that the firewall only sends VoIP traffic out via eth0 and sends all other traffic that originates from the private side out via eth1. This was tested by telneting to the internet address. For ease of testing, we set up 2 “internets” and tested that private users could not telnet to the internet address accessible via eth0, but were able to reach the internet via eth1. This simulated web browsing.

The following pages have the configuration scripts for each of the named devices in the figure on page 10:

- Firewall (page 12)
- Router on private side of firewall (page 13)
- Router on public side of firewall (page 13)
- VoIP gateway (page 13)
- Internet gateway (page 13)

Firewall

```
# VLAN general configuration
create vlan="dmz" vid=3

# VLAN port configuration
add vlan="3" port=3

# IP configuration
enable ip
add ip int=vlan1-0 ip=172.16.0.1 mask=255.255.255.128
# Use a policy filter to select non-VoIP traffic
# Note that 172.16.0.128 is the subnet address for vlan1-1
add ip fil=102 ty=policy so=172.16.0.128 ent=1 sm=255.255.255.128 poli=1
add ip int=vlan1-1 ip=172.16.0.129 mask=255.255.255.128 pol=102
add ip int=eth0-0 ip=200.118.1.121 mask=255.255.255.252
add ip int=eth1-0 ip=200.71.42.206
add ip int=vlan3-0 ip=200.118.4.233 mask=255.255.255.248
set ip loc ip=172.16.0.129 pol=102
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0-0 next=200.118.1.122
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth1-0 next=200.71.42.1 poli=1

# Firewall configuration
enable firewall
create firewall policy="main"
enable firewall policy="main" icmp_f=all
add firewall policy="main" int=vlan1-1 type=private
add firewall policy="main" int=vlan1-0 type=private
add firewall policy="main" int=vlan3-0 type=public
add firewall policy="main" int=eth1-0 type=public
add firewall policy="main" int=eth0-0 type=public
add firewall poli="main" nat=enhanced int=vlan1-1 gblin=eth1-0 gblip=200.71.42.206
add firewall poli="main" nat=enhanced int=vlan1-0 gblin=eth1-0 gblip=200.71.42.206

add firewall poli="main" ru=1 ac=nat int=vlan3-0 prot=udp po=5060 ip=172.16.0.2
gblip=200.118.4.233 natt=na gblp=61001
add firewall poli="main" ru=2 ac=nat int=vlan3-0 prot=udp po=5060 ip=172.16.0.25
gblip=200.118.4.233 natt=na gblp=61025
#Add SIP firewall rules here for any extra phones you have

add firewall poli="main" ru=20 ac=nat int=eth0-0 prot=udp po=5060 ip=172.16.0.2
gblip=200.118.4.233 natt=na gblp=61001
add firewall poli="main" ru=21 ac=nat int=eth0-0 prot=udp po=5060 ip=172.16.0.25
gblip=200.118.4.233 natt=na gblp=61025
#And also add SIP firewall rules here for extra phones


add firewall poli="main" ru=40 ac=nat int=eth0-0 prot=tcp po=23 ip=200.118.1.121
gblip=200.118.1.121 gblp=23

add firewall poli="main" ru=60 ac=nat int=vlan1-0 prot=udp po=5060 ip=172.16.0.2
gblip=200.118.4.233 natt=na gblp=61001
add firewall poli="main" ru=61 ac=nat int=vlan1-0 prot=udp po=5060 ip=172.16.0.25
gblip=200.118.4.233 natt=na gblp=61025
#And also add SIP firewall rules here for extra phones

enable firewall sipalg
```

Router on private side of firewall

```
# IP configuration
enable ip
add ip int=vlan1 ip=172.16.0.25 mask=255.255.255.128
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan1 next=172.16.0.1

# VoIP configuration
set voip boot=c-1-0-0.bin server=flash
set voip pub int=vlan1
set voip fi=ss-1-0-0.bin prot=sip ty=fxs
ena voip prot=sip engine=bay0.fxs0
cre sip int=bay0.fxs0.0 ph=1025 do=200.118.4.234 proxy=200.118.4.234
set sip int=bay0.fxs0.0 locati=200.118.4.234
```

Router on public side of firewall

```
# IP configuration
enable ip
add ip int=vlan1 ip=202.49.75.1
add ip rou=0.0.0.0 mask=0.0.0.0 int=vlan1 next=202.49.75.29

# VoIP configuration
set voip boot=c-1-0-0.bin server=flash
set voip pub int=vlan1
set voip fi=ss-1-0-0.bin prot=sip ty=fxs
ena voip prot=sip engine=bay0.fxs0
cre sip int=bay0.fxs0.0 ph=1001 do=200.118.4.234 proxy=200.118.4.234
set sip int=bay0.fxs0.0 locati=200.118.4.234
```

VoIP gateway

```
# IP configuration
enable ip
add ip int=eth0 ip=200.118.1.122 mask=255.255.255.252
add ip int=eth1 ip=202.49.75.30
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.118.1.121
```

Internet gateway

```
# IP configuration
enable ip
add ip int=eth0-0 ip=200.71.42.1
add ip int=eth0-1 ip=202.49.75.28
set ip loc ip=202.49.75.28
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0-0 next=200.71.42.206
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis™