



**Concepts & Examples
ScreenOS Reference Guide**

**Volume 6:
Voice-over-Internet Protocol**

Release 5.4.0, Rev. A

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-015773-01, Revision A

Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: ScreenOS Team

Editor: Lisa Eldridge

Table of Contents

	About This Volume	v
	Document Conventions.....	vi
	CLI Conventions	vi
	Illustration Conventions.....	vii
	Naming Conventions and Character Types.....	viii
	WebUI Conventions.....	viii
	Juniper Networks Documentation	ix
Chapter 1	H.323 Application Layer Gateway	1
	Overview	1
	Examples	2
	Example: Gatekeeper in the Trust Zone	2
	Example: Gatekeeper in the Untrust Zone	3
	Example: Outgoing Calls with NAT	4
	Example: Incoming Calls with NAT.....	7
	Example: Gatekeeper in the Untrust Zone with NAT.....	10
Chapter 2	Session Initiation Protocol Application Layer Gateway	13
	Overview	13
	SIP Request Methods	14
	Classes of SIP Responses	16
	ALG—Application-Layer Gateway	17
	SDP	18
	Pinhole Creation.....	19
	Session Inactivity Timeout.....	20
	SIP Attack Protection	21
	Example: SIP Protect Deny	21
	Example: Signaling-Inactivity and Media-Inactivity Timeouts	22
	Example: UDP Flooding Protection	22
	Example: SIP Connection Maximum	23
	SIP with Network Address Translation	23
	Outgoing Calls	24
	Incoming Calls.....	24
	Forwarded Calls.....	25
	Call Termination.....	25
	Call Re-INVITE Messages	25
	Call Session Timers.....	25
	Call Cancellation.....	26
	Forking.....	26
	SIP Messages	26
	SIP Headers.....	26
	SIP Body.....	28
	SIP NAT Scenario.....	28

Chapter 2 Continued	Examples	30
	Incoming SIP Call Support Using the SIP Registrar.....	31
	Example: Incoming Call (Interface DIP).....	32
	Example: Incoming Call (DIP Pool).....	35
	Example: Incoming Call with MIP	37
	Example: Proxy in the Private Zone	39
	Example: Proxy in the Public Zone	41
	Example: Three-Zone, Proxy in the DMZ	44
	Example: Untrust Intrazone	47
	Example: Trust Intrazone.....	51
	Example: Full-Mesh VPN for SIP.....	53
	Bandwidth Management for VoIP Services	62
Chapter 3	Media Gateway Control Protocol Application Layer Gateway	65
	Overview	65
	MGCP Security	66
	About MGCP.....	66
	Entities in MGCP.....	66
	Endpoint	67
	Connection	67
	Call.....	67
	Call Agent	67
	Commands.....	68
	Response Codes	70
	Examples	71
	Media Gateway in Subscribers' Homes—Call Agent at the ISP.....	71
	ISP-Hosted Service.....	74
Chapter 4	Skinny Client Control Protocol Application Layer Gateway	79
	Overview	79
	SCCP Security	80
	About SCCP.....	81
	SCCP Components.....	81
	SCCP Client.....	81
	Call Manager	81
	Cluster	81
	SCCP Transactions.....	82
	Client Initialization	82
	Client Registration.....	82
	Call Setup.....	83
	Media Setup	83
	SCCP Control Messages and RTP Flow.....	84
	SCCP Messages.....	85
	Examples	85
	Example: Call Manager/TFTP Server in the Trust Zone.....	86
	Example: Call Manager/TFTP Server in the Untrust Zone	88
	Example: Three-Zone, Call Manager/TFTP Server in the DMZ	90
	Example: Intrazone, Call Manager/TFTP Server in Trust Zone	93
	Example: Intrazone, Call Manager/TFTP Server in Untrust Zone	97
	Example: Full-Mesh VPN for SCCP	99
	Index.....	IX-I

About This Volume

Volume 6: Voice-over-Internet Protocol describes the supported VoIP Application Layer Gateways (ALGs) and contains the following chapters:

- Chapter 1, “H.323 Application Layer Gateway,” describes the H.323 protocol and provides examples of typical scenarios.
- Chapter 2, “Session Initiation Protocol Application Layer Gateway,” describes the Session Initiation Protocol (SIP) and shows how the SIP ALG processes calls in Route and Network Address Translation (NAT) modes. Examples of typical scenarios follow a summary of the SIP architecture.
- Chapter 3, “Media Gateway Control Protocol Application Layer Gateway,” presents an overview of the Media Gateway Control Protocol (MGCP) ALG and lists the firewall security features of the implementation. Examples of typical scenarios follow a summary of the MGCP architecture.
- Chapter 4, “Skinny Client Control Protocol Application Layer Gateway,” presents an overview of the Skinny Client Control Protocol (SCCP) ALG and lists the firewall security features of the implementation. Examples of typical scenarios follow a summary of the SCCP architecture.

Document Conventions

This document uses several types of conventions, which are introduced in the following sections:

- “CLI Conventions” on this page
- “Illustration Conventions” on page vii
- “Naming Conventions and Character Types” on page viii
- “WebUI Conventions” on page viii

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- Anything inside square brackets [] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example:

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

means “set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface.”

- Variables are in *italic* type:

```
set admin user name1 password xyz
```

In text:




- Commands are in **boldface** type.
- Variables are in *italic* type.

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u kath j12fmt54** is enough to enter the command **set admin user kathleen j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Illustration Conventions

The following figure shows the basic set of images used in illustrations throughout this manual.

Figure 1: Images in Manual Illustrations

	Autonomous System		Local Area Network (LAN) with a Single Subnet (example: 10.1.1.0/24)
	Generic Security Device		Internet
	Virtual Routing Domain		Dynamic IP (DIP) Pool
	Security Zone		Desktop Computer
	Security Zone Interface White = Protected Zone Interface (example = Trust Zone) Black = Outside Zone Interface (example = Untrust Zone)		Laptop Computer
	Tunnel Interface		Generic Network Device (examples: NAT Server, Access Concentrator)
	VPN Tunnel		Server
	Router		Hub
	Switch		Policy Engine
			IP Telephone

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations:

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes; for example:
set address trust “local LAN” 10.1.1.0/24
- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, “ local LAN ” becomes “local LAN”.
- Multiple consecutive spaces are treated as a single space.
- Name strings are case-sensitive, although many CLI keywords are case-insensitive. For example, “local LAN” is different from “local lan”.

ScreenOS supports the following character types:

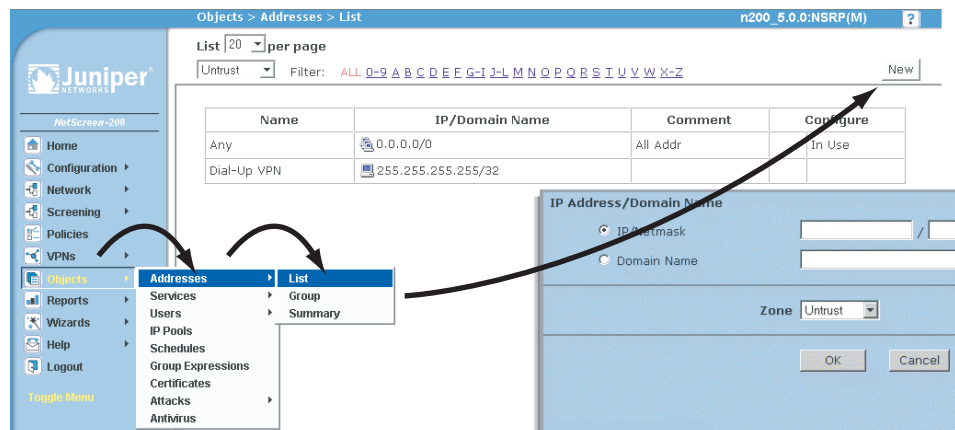
- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.
- ASCII characters from 32 (0x20 in hexadecimal) to 255 (0xff), except double quotes (“ ”), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NOTE: A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your browser supports.

WebUI Conventions

A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

Figure 2: WebUI Navigation



To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: addr_1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.2.2.5/32
 Zone: Untrust

Figure 3: Navigational Path and Configuration Settings

The screenshot shows the Juniper Networks WebUI configuration page for an address object. The breadcrumb navigation at the top reads "Objects > Addresses > Configuration". The page title is "n200_5.0.0:NSRP(M)". On the left is a navigation menu with options: Home, Configuration, Network, Screening, Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main configuration area contains the following fields:

- Address Name:** addr_1
- Comment:** (empty text box)
- IP Address/Domain Name:**
 - IP/Netmask: 10.2.2.5 / 32
 - Domain Name: (empty text box)
- Zone:** Untrust (dropdown menu)
- Buttons:** OK and Cancel

Juniper Networks Documentation

To obtain technical documentation for any Juniper Networks product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

techpubs-comments@juniper.net

Chapter 1

H.323 Application Layer Gateway

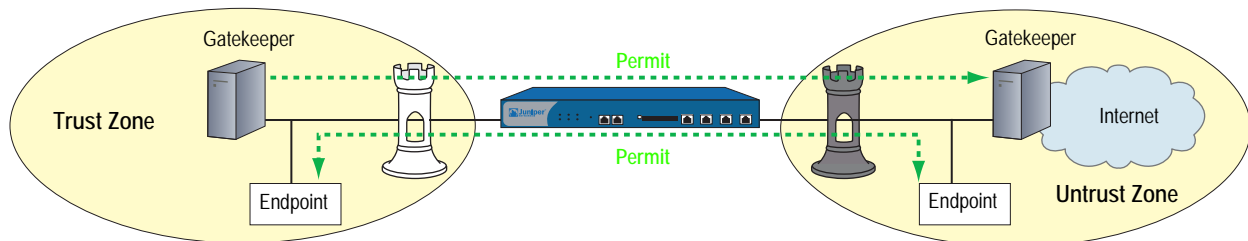
This chapter describes the H.323 protocol and provides examples for configuring the H.323 Application Layer Gateway (ALG) on a Juniper Networks security device. This chapter contains the following sections:

- “Overview” on this page
- “Examples” on page 2

Overview

The H.323 Application Layer Gateway (ALG) lets you secure Voice-over-IP (VoIP) communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, gatekeeper devices manage call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones or in the same zone.

Figure 1: H.323 Protocol



NOTE: The illustrations in this chapter use IP phones for illustrative purposes, although it is possible to make configurations for other hosts that use VoIP, such as NetMeeting multimedia devices.

Examples

This section contains the following configuration scenarios:

- “Example: Gatekeeper in the Trust Zone” on this page
- “Example: Gatekeeper in the Untrust Zone” on page 3
- “Example: Outgoing Calls with NAT” on page 4
- “Example: Incoming Calls with NAT” on page 7
- “Example: Gatekeeper in the Untrust Zone with NAT” on page 10

Example: Gatekeeper in the Trust Zone

In the following example, you set up two policies that allow H.323 traffic to pass between IP phone hosts and a gatekeeper in the Trust zone, and an IP phone host (2.2.2.5) in the Untrust zone. In this example, the security device can be in either Transparent mode or Route mode. Both the Trust and Untrust security zones are in the trust-vr routing domain.

Figure 2: H.323 Gatekeeper in the Trust Zone



WebUI

1. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: IP_Phone
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.5/32
 Zone: Untrust

2. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), Any
 Destination Address:
 Address Book Entry: (select), IP_Phone
 Service: H.323
 Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone
 Destination Address:
 Address Book Entry: (select), Any
 Service: H.323
 Action: Permit

CLI

1. **Address**
 set address untrust IP_Phone 2.2.2.5/32
2. **Policies**
 set policy from trust to untrust any IP_Phone h.323 permit
 set policy from untrust to trust IP_Phone any h.323 permit
 save

Example: Gatekeeper in the Untrust Zone

Because Transparent mode and Route mode do not require address mapping of any kind, security device configuration for a gatekeeper in the Untrust zone is usually identical to the configuration for a gatekeeper in the Trust zone.

In the following example, you set up two policies to allow H.323 traffic to pass between IP phone hosts in the Trust zone, and the IP phone at IP address 2.2.2.5 (and the gatekeeper) in the Untrust zone. The device can be in Transparent or Route mode. Both the Trust and Untrust security zones are in the trust-vr routing domain.

Figure 3: H.323 Gatekeeper in the Untrust Zone



WebUI

1. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: IP_Phone
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.5/32
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: Gatekeeper
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.10/32
 Zone: Untrust

2. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), Any
 Destination Address:
 Address Book Entry: (select), IP_Phone
 Service: H.323
 Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone
 Destination Address:
 Address Book Entry: (select), Any
 Service: H.323
 Action: Permit

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), Any
 Destination Address:
 Address Book Entry: (select), Gatekeeper
 Service: H.323
 Action: Permit

CLI

1. Addresses

```
set address untrust IP_Phone 2.2.2.5/32
set address untrust gatekeeper 2.2.2.10/32
```

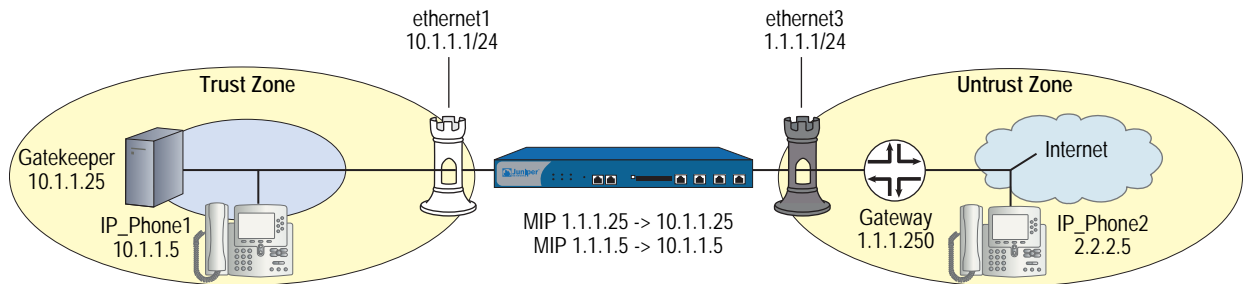
2. Policies

```
set policy from trust to untrust any IP_Phone h.323 permit
set policy from trust to untrust any gatekeeper h.323 permit
set policy from untrust to trust IP_Phone any h.323 permit
set policy from untrust to trust gatekeeper any h.323 permit
save
```

Example: Outgoing Calls with NAT

When the security device uses NAT (Network Address Translation), a gatekeeper or endpoint device in the Trust zone has a private address, and when it is in the Untrust zone it has a public address. When you set a security device in NAT mode, you must map a public IP address to each device that needs to receive incoming traffic with a private address.

In this example, the devices in the Trust zone include the endpoint host (10.1.1.5) and the gatekeeper device (10.1.1.25). IP_Phone2 (2.2.2.5) is in the Untrust zone. You configure the security device to allow traffic between the endpoint host IP_Phone1 and the gatekeeper in the Trust zone and the endpoint host IP_Phone2 in the Untrust zone. Both the Trust and Untrust security zones are in the trust-vr routing domain.

Figure 4: Network Address Translation—Outgoing Calls**WebUI****1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Select the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 1.1.1.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: IP_Phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.5/32
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: Gatekeeper
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.25/32
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: IP_Phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.5/32
 Zone: Untrust

3. Mapped IP Addresses

Network > Interfaces > Edit (for ethernet3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.5
Netmask: 255.255.255.255
Host IP Address: 10.1.1.5
Host Virtual Router Name: trust-vr

Network > Interfaces > Edit (for ethernet3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.25
Netmask: 255.255.255.255
Host IP Address: 10.1.1.25
Host Virtual Router Name: trust-vr

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0
Gateway: (select)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), IP_Phone1
Destination Address:
Address Book Entry: (select), IP_Phone2
Service: H.323
Action: Permit

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Gatekeeper
Destination Address:
Address Book Entry: (select), IP_Phone2
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), IP_Phone2
Destination Address:
Address Book Entry: (select), MIP(1.1.1.5)
Service: H.323
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone2
 Destination Address:
 Address Book Entry: (select), MIP(1.1.1.25)
 Service: H.323
 Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address trust IP_Phone1 10.1.1.5/32
set address trust gatekeeper 10.1.1.25/32
set address untrust IP_Phone2 2.2.2.5/32
```

3. Mapped IP Addresses

```
set interface ethernet3 mip 1.1.1.5 host 10.1.1.5
set interface ethernet3 mip 1.1.1.25 host 10.1.1.25
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

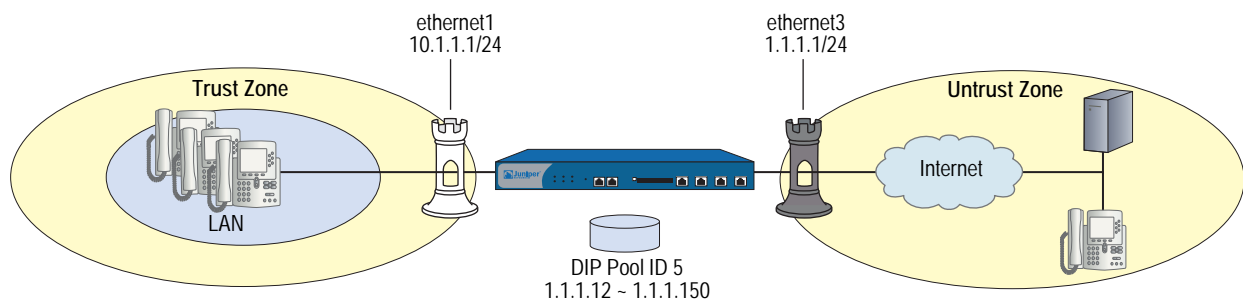
5. Policies

```
set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
set policy from trust to untrust gatekeeper IP_Phone2 h.323 permit
set policy from untrust to trust IP_Phone2 mip(1.1.1.5) h.323 permit
set policy from untrust to trust IP_Phone2 mip (1.1.1.25) h.323 permit
save
```

Example: Incoming Calls with NAT

In this example, you configure the security device to accept incoming calls over a NAT boundary. To do this, you can create a DIP address pool for dynamically allocating destination addresses. This differs from most configurations, where a DIP pool provides source addresses only.

Figure 5: Network Address Translation—Incoming Calls



The name of the DIP pool can be `DIP(id_num)` for a user-defined DIP, or `DIP(interface)` when the DIP pool uses the same address as an interface IP address. You can use such address entries as destination addresses in policies, together with the services H.323, SIP, or other VoIP (Voice-over-IP) protocols, to support incoming calls.

The following example uses DIP in an H.323 VoIP configuration. The keyword “incoming” instructs the device to add the DIP and interface addresses to the global zone.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 1.1.1.1/24

2. DIP with Incoming NAT

Network > Interface > Edit (for ethernet3) > DIP > New: Enter the following, then click **OK**:

ID: 5
 IP Address Range: (select), 1.1.1.12 ~ 1.1.1.150
 Port Translation: (select)
 In the same subnet as the interface IP or its secondary IPs: (select)
 Incoming NAT: (select)

3. Addresses

Objects > Addresses > List > New (for Trust): Enter the following, then click **OK**:

Address Name: IP_Phones1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.5/24
 Zone: Trust

Objects > Addresses > List > New (for Untrust): Enter the following, then click **OK**:

Address Name: IP_Phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.5/32
 Zone: Untrust

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phones1
 Destination Address:
 Address Book Entry: (select), Any
 Service: H.323
 Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone2
 Destination Address:
 Address Book Entry: (select), DIP(5)
 Service: H.323
 Action: Permit

CLI**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP with Incoming NAT

```
set interface ethernet3 dip 5 1.1.1.12 1.1.1.150 incoming
```

3. Addresses

```
set address trust IP_Phones1 10.1.1.5/24
set address untrust IP_Phone2 2.2.2.5/32
```

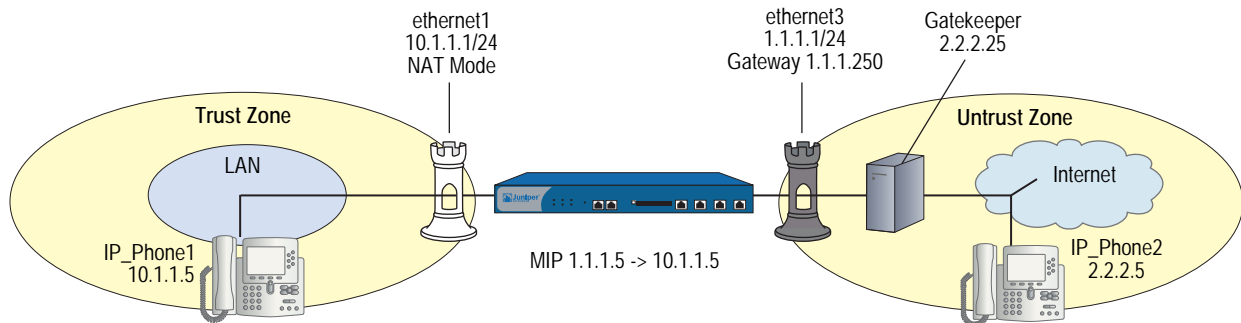
4. Policies

```
set policy from trust to untrust IP_Phones1 any h.323 nat src dip 5 permit
set policy from untrust to trust IP_Phone2 dip(5) h.323 permit
save
```

Example: Gatekeeper in the Untrust Zone with NAT

In this example, the gatekeeper device (2.2.2.25) and host IP_Phone2 (2.2.2.5) are in the Untrust zone and host IP_Phone1 (10.1.1.5) is in the Trust zone. You configure the security device to allow traffic between host IP_Phone1 in the Trust zone and host IP_Phone2 (and the gatekeeper) in the Untrust zone. Both the Trust and Untrust security zones are in the trust-vr routing domain.

Figure 6: Gatekeeper in the Untrust Zone



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 1.1.1.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: IP_Phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.5/32
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: Gatekeeper
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.25/32
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: IP_Phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.5/32
 Zone: Untrust

3. Mapped IP Address

Network > Interfaces > Edit (for ethernet3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.5
 Netmask: 255.255.255.255
 Host IP Address: 10.1.1.5

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0
 Gateway: (select)
 Interface: ethernet3
 Gateway IP Address: 1.1.1.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone1
 Destination Address:
 Address Book Entry: (select), IP_Phone2
 Service: H.323
 Action: Permit

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone1
 Destination Address:
 Address Book Entry: (select), Gatekeeper
 Service: H.323
 Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), IP_Phone2
 Destination Address:
 Address Book Entry: (select), MIP(1.1.1.5)
 Service: H.323
 Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Gatekeeper
Destination Address:
Address Book Entry: (select), MIP(1.1.1.5)
Service: H.323
Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address trust IP_Phone1 10.1.1.5/32
set address untrust gatekeeper 2.2.2.25/32
set address untrust IP_Phone2 2.2.2.5/32
```

3. Mapped IP Addresses

```
set interface ethernet3 mip 1.1.1.5 host 10.1.1.5
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. Policies

```
set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
set policy from trust to untrust IP_Phone1 gatekeeper h.323 permit
set policy from untrust to trust IP_Phone2 mip(1.1.1.5) h.323 permit
set policy from untrust to trust gatekeeper mip(1.1.1.5) h.323 permit
save
```

Chapter 2

Session Initiation Protocol Application Layer Gateway

This chapter describes the Session Initiation Protocol (SIP) Application Layer Gateway (ALG) and contains the following sections:

- “Overview” on this page
- “SIP with Network Address Translation” on page 23
- “Examples” on page 30

Overview

Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet. Such sessions might include conferencing, telephony, or multimedia, with features such as instant messaging and application-level mobility in network environments.

Juniper Networks security devices support SIP as a service and can screen SIP traffic, allowing and denying it based on a policy that you configure. SIP is a predefined service in ScreenOS and uses port 5060 as the destination port.

SIP’s primary function is to distribute session-description information and, during the session, to negotiate and modify the parameters of the session. SIP is also used to terminate a multimedia session.

Session-description information is included in INVITE and ACK messages and indicates the multimedia type of the session, for example, voice or video. Although SIP can use different description protocols to describe the session, the Juniper Networks SIP ALG supports only Session Description Protocol (SDP).

SDP provides information that a system can use to join a multimedia session. SDP might include information such as IP addresses, port numbers, times, and dates. Note that the IP address and port number in the SDP header (the “c = ” and “m = ” fields, respectively) are the address and port where the client wants to receive the media streams and not the IP address and port number from which the SIP request originates (although they can be the same). See “SDP” on page 18 for more information.

SIP messages consist of requests from a client to a server and responses to the requests from a server to a client with the purpose of establishing a session (or a call). A User Agent (UA) is an application that runs at the endpoints of the call and consists of two parts: the User Agent Client (UAC), which sends SIP requests on behalf of the user; and a User Agent Server (UAS), which listens to the responses and notifies the user when they arrive. Examples of UAs are SIP proxy servers and phones.

SIP Request Methods

The SIP transaction model includes a number of request and response messages, each of which contains a *method* field that denotes the purpose of the message. ScreenOS supports the following method types and response codes:

- INVITE—A user sends an INVITE request to invite another user to participate in a session. The body of an INVITE request may contain the description of the session. In NAT mode, the IP addresses in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.
- ACK—The user from whom the INVITE originated sends an ACK request to confirm reception of the final response to the INVITE request. If the original INVITE request did not contain the session description, the ACK request must include it. In NAT mode, the IP addresses in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.
- OPTIONS—Used by the User Agent (UA) to obtain information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports. In NAT mode, when the OPTIONS request is sent from a UA outside NAT to a proxy inside NAT, the SIP ALG translates the address in the Request-URI and the IP address in the To: field to the appropriate IP address of the internal client. When the UA is inside NAT and the proxy is outside NAT, the SIP ALG translates the From:, Via:, and Call-ID: fields as shown in Table 2 on page 27.
- BYE—A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session. In NAT mode, the IP addresses in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.
- CANCEL—A user can send a CANCEL request to cancel a pending INVITE request. A CANCEL request has no effect if the SIP server processing the INVITE had sent a final response for the INVITE before it received the CANCEL. In NAT mode, the IP addresses in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.

- REGISTER—A user sends a REGISTER request to a SIP *registrar* server to inform it of the current location of the user. A SIP registrar server records all the information it receives in REGISTER requests and makes this information available to any SIP server attempting to locate a user. In NAT mode, REGISTER requests are handled as follows:
 - REGISTER requests from an external client to an internal registrar—When the SIP ALG receives the incoming REGISTER request it translates the IP address, if any, in the Request-URI. Incoming REGISTER messages are allowed only to a MIP or VIP address. No translation is needed for the outgoing response.
 - REGISTER requests from an internal client to an external registrar—When the SIP ALG receives the outgoing REGISTER request it translates the IP addresses in the To:, From:, Via:, Call-ID:, and Contact: header fields. A backward translation is performed for the incoming response.
- Info—Used to communicate mid-session signaling information along the signaling path for the call. In NAT mode, the IP addresses in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.
- Subscribe—Used to request current state and state updates from a remote node. In NAT mode, the address in the Request-URI is changed to a private IP address if the message is coming from the external network into the internal network. The IP addresses in Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in the table in Table 2 on page 27.
- Notify—Sent to inform subscribers of changes in state to which the subscriber has a subscription. In NAT mode, the IP address in the Request-URI: header field is changed to a private IP address if the message is coming from the external network into the internal network. The IP address in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.
- Refer—Used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request. In NAT mode, the IP address in the Request-URI is changed to a private IP address if the message is coming from the external network into the internal network. The IP addresses in the Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.

For example, if user A in a private network refers user B, in a public network, to user C, who is also in the private network, the SIP ALG allocates a new IP address and port number for user C so that user C can be contacted by user B. If user C is registered with a registrar, however, its port mapping is stored in the ALG NAT table and is reused to perform the translation.

- Update—Used to open pinhole for new or updated SDP information. The Via:, From:, To:, Call-ID:, Contact:, Route:, and Record-Route: header fields are modified as shown in Table 2 on page 27.
- 1xx, 202, 2xx, 3xx, 4xx, 5xx, 6xx Response Codes—Used to indicate the status of a transaction. Header fields are modified as shown in Table 2 on page 27.

Classes of SIP Responses

SIP responses provide status information about SIP transactions and include a response code and a reason phrase. SIP responses are grouped into the following classes:

- Informational (100 to 199)—Request received, continuing to process the request.
- Success (200 to 299)—Action successfully received, understood, and accepted.
- Redirection (300 to 399)—Further action required to complete the request.
- Client Error (400 to 499)—Request contains bad syntax or cannot be fulfilled at this server.
- Server Error (500 to 599)—Server failed to fulfill an apparently valid request.
- Global Failure (600 to 699)—Request cannot be fulfilled at any server.

Table 1 provides a complete list of current SIP responses, all of which are supported on Juniper Networks security devices.

Table 1: SIP Responses

Class	Response Code-Reason Phrase	Response Code-Reason Phrase	Response Code-Reason Phrase
Informational	100 Trying	180 Ringing	181 Call is being forwarded
	182 Queued	183 Session progress	
Success	200 OK	202 Accepted	
Redirection	300 Multiple choices	301 Moved permanently	302 Moved temporarily
	305 Use proxy	380 Alternative service	
Client Error	400 Bad request	401 Unauthorized	402 Payment required
	403 Forbidden	404 Not found	405 Method not allowed
	406 Not acceptable	407 Proxy authentication required	408 Request time-out
	409 Conflict	410 Gone	411 Length required
	413 Request entity too large	414 Request-URL too large	415 Unsupported media type
	420 Bad extension	480 Temporarily not available	481 Call leg/transaction does not exist
	482 Loop detected	483 Too many hops	484 Address incomplete
	485 Ambiguous	486 Busy here	487 Request canceled
	488 Not acceptable here		
Server Error	500 Server internal error	501 Not implemented	502 Bad gateway
	502 Service unavailable	504 Gateway time-out	505 SIP version not supported
Global Failure	600 Busy everywhere	603 Decline	604 Does not exist anywhere
	606 Not acceptable		

ALG—Application-Layer Gateway

There are two types of SIP traffic, the signaling and the media stream. SIP signaling traffic consists of request and response messages between client and server and uses transport protocols such as User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). The media stream carries the data (audio data, for example) and uses Application Layer protocols such as Real Time Protocol (RTP) over UDP.

Juniper Networks security devices support SIP signaling messages on port 5060. You can simply create a policy that permits SIP service, and the security device filters SIP signaling traffic like any other type of traffic, permitting or denying it. The media stream, however, uses dynamically assigned port numbers that can change several times during the course of a call. Without fixed ports, it is impossible to create a static policy to control media traffic. In this case, the security device invokes the SIP ALG. The SIP ALG reads SIP messages and their SDP content and extracts the port-number information it needs to dynamically open pinholes and let the media stream traverse the security device.

NOTE: We refer to a pinhole as the limited opening of a port to allow exclusive traffic.

The SIP ALG monitors SIP transactions and dynamically creates and manages pinholes based on the information it extracts from these transactions. The Juniper Networks SIP ALG supports all SIP methods and responses (see “SIP Request Methods” on page 14 and “Classes of SIP Responses” on page 16). You can allow SIP transactions to traverse the Juniper Networks firewall by creating a static policy that permits SIP service. This policy enables the security device to intercept SIP traffic and do one of the following actions: permit or deny the traffic or enable the SIP ALG to open pinholes to pass the media stream. The SIP ALG needs to open pinholes only for the SIP requests and responses that contain media information (SDP). For SIP messages that do not contain SDP, the security device simply lets them through.

The SIP ALG intercepts SIP messages that contain SDP and, using a parser, extracts the information it requires to create pinholes. The SIP ALG examines the SDP portion of the packet, and a parser extracts information such as IP addresses and port numbers, which the SIP ALG records in a pinhole table. The SIP ALG uses the IP addresses and port numbers recorded in the pinhole table to open pinholes and allow media streams to traverse the security device.

NOTE: Juniper Networks security devices do not support encrypted SDP. If a security device receives a SIP message in which SDP is encrypted, the SIP ALG permits it through the firewall but generates a log message informing the user that it cannot process the packet. If SDP is encrypted, the SIP ALG cannot extract the information it needs from SDP to open pinholes. As a result, the media content that SDP describes cannot traverse the security device.

SDP

An SDP session description is text-based and consists of a set of lines. It can contain session-level and media-level information. The session-level information applies to the whole session, while the media-level information applies to a particular media stream. An SDP session description always contains session-level information, which appears at the beginning of the description, and might contain media-level information, which comes after.

NOTE: In the SDP session description, the media-level information begins with the `m =` field.

Of the many fields in the SDP description, two are particularly useful to the SIP ALG because they contain Transport Layer information. The two fields are the following:

- **c =** for connection information

This field can appear at the session or media level. It displays in this format:

- `c = < network type > < address type > < connection address >`

Currently, the security device supports only “IN” (for Internet) as the network type, “IP4” as the address type, and a unicast IP address or domain name as the destination (connection) IP address.

NOTE: Generally, the destination IP address can also be a multicast IP address, but ScreenOS does not currently support multicast with SIP.

If the destination IP address is a unicast IP address, the SIP ALG creates pinholes using the IP address and port numbers specified in the media description field `m =`.

- **m =** for media announcement

This field appears at the media level and contains the description of the media. It displays in this format:

`m = < media > < port > < transport > < fmt list >`

Currently, the security device supports only “audio” as the media and “RTP” as the Application Layer transport protocol. The port number indicates the destination (not the origin) of the media stream. The format list (fmt list) provides information on the Application Layer protocol that the media uses.

In this release of ScreenOS, the security device opens ports only for RTP and RTCP. Every RTP session has a corresponding Real Time Control Protocol (RTCP) session. Therefore, whenever a media stream uses RTP, the SIP ALG must reserve ports (create pinholes) for both RTP and RTCP traffic. By default, the port number for RTCP is one higher than the RTP port number.

NOTE: Generally, the destination IP address can also be a multicast IP address, but ScreenOS does not currently support multicast with SIP.

Pinhole Creation

Both pinholes for the RTP and RTCP traffic share the same destination IP address. The IP address comes from the `c =` field in the SDP session description. Because the `c =` field can appear in either the session-level or media-level portion of the SDP session description, the parser determines the IP address based on the following rules (in accordance with SDP conventions):

- First, the SIP ALG parser verifies if there is a `c =` field containing an IP address in the media level. If there is one, the parser extracts that IP address, and the SIP ALG uses it to create a pinhole for the media.
- If there is no `c =` field in the media level, the SIP ALG parser extracts the IP address from the `c =` field in the session level, and the SIP ALG uses it to create a pinhole for the media. If the session description does not contain a `c =` field in either level, this indicates an error in the protocol stack, and the security device drops the packet and logs the event.

The following lists the information the SIP ALG needs to create a pinhole. This information comes from the SDP session description and parameters on the security device:

- Protocol: UDP.
- Source IP: Unknown.
- Source port: Unknown.
- Destination IP: The parser extracts the destination IP address from the `c =` field in the media or session level.
- Destination port: The parser extracts the destination port number for RTP from the `m =` field in the media level and calculates the destination port number for RTCP using the following formula:

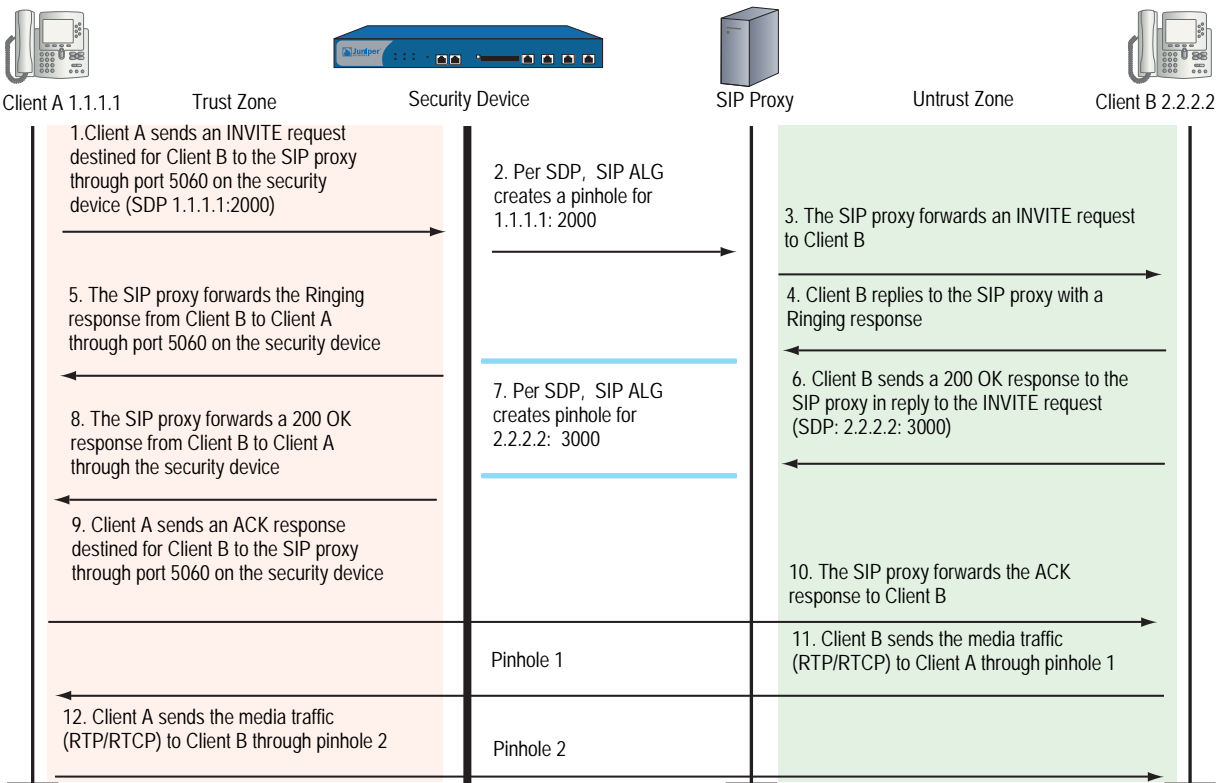
RTP port number + one

- Lifetime: This value indicates the length of time (in seconds) during which a pinhole is open to allow a packet through. A packet must go through the pinhole before the lifetime expires. When the lifetime expires, the SIP ALG removes the pinhole.

When a packet goes through the pinhole within the lifetime period, immediately afterwards the SIP ALG removes the pinhole for the direction from which the packet came.

Figure 7 describes a call setup between two SIP clients and how the SIP ALG creates pinholes to allow RTP and RTCP traffic. The illustration assumes that the security device has a policy that permits SIP, thus opening port 5060 for SIP signaling messages.

Figure 7: SIP ALG Call Setup



NOTE: The SIP ALG does not create pinholes for RTP and RTCP traffic when the destination IP address is 0.0.0.0, which indicates that the session is on hold. To put a session on hold, during a telephone communication, for example, a user (User A) sends the other user (User B) a SIP message in which the destination IP address is 0.0.0.0. Doing so indicates to User B not to send any media until further notice. If User B sends media anyway, the security device drops the packets.

Session Inactivity Timeout

Typically a call ends when one of the clients sends a BYE or CANCEL request. The SIP ALG intercepts the BYE or CANCEL request and removes all media sessions for that call. There could be reasons or problems preventing clients in a call from sending BYE or CANCEL requests, for example, a power failure. In this case, the call might go on indefinitely, consuming resources on the security device. The inactivity-timeout feature helps the security device to monitor the liveliness of the call and terminate it if there is no activity for a specific period of time.

A call can have one or more voice channels. Each voice channel has two sessions (or two media streams), one for RTP and one for RTCP. When managing the sessions, the security device considers the sessions in each voice channel as one group. Settings such as the inactivity timeout apply to a group as opposed to each session.

There are two types of inactivity timeouts that determine the lifetime of a group:

- Signaling-inactivity timeout: This parameter indicates the maximum length of time (in seconds) a call can remain active without any SIP-signaling traffic. Each time a SIP-signaling message occurs within a call, this timeout resets. The default setting is 43200 seconds (12 hours).
- Media-inactivity timeout: This parameter indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTCP) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. The default setting is 120 seconds.

If either of these timeouts expires, the security device removes all sessions for this call from its table, thus terminating the call.

SIP Attack Protection

The ability of the SIP proxy server to process calls can be affected by repeat SIP INVITE requests, whether malicious or through client or server error, that it initially denied. To prevent the SIP proxy server from being overwhelmed by such requests, you can use the **sip protect deny** command to configure the security device to monitor INVITE requests and proxy server replies to them. If a reply contains a 3xx, 4xx, or 5xx response code (see “Classes of SIP Responses” on page 16), the ALG stores the source IP address of the request and the IP address of the proxy server in a table. Subsequently, the security device checks all INVITE requests against this table and, for a configurable number of seconds (the default is 3), discards any packets that match entries in the table. You can also configure the security device to monitor INVITE request to a specific proxy server by specifying the destination IP address. SIP attack protection is configured globally.

Example: SIP Protect Deny

In this example, you configure the security device to protect a single SIP proxy server (1.1.1.3/24) from repeat INVITE requests to which it has already denied service. Packets are dropped for a period of 5 seconds, after which the security device resumes forwarding INVITE requests from those sources.

WebUI

You must use the CLI to protect SIP proxy servers from being inundated by INVITE requests.

CLI

```
set alg sip app-screen protect deny dst-ip 1.1.1.3/24
set alg sip protect deny timeout 5
save
```

Example: Signaling-Inactivity and Media-Inactivity Timeouts

In this example, you configure the signaling-inactivity timeout to 30,000 seconds and the media-inactivity timeout to 90 seconds.

WebUI

NOTE: You must use the CLI to set SIP-signaling and media-inactivity timeouts.

CLI

```
set alg sip signaling-inactivity-timeout 30000
set alg sip media-inactivity-timeout 90
save
```

Example: UDP Flooding Protection

You can protect the security device against UDP flooding by zone and destination address. In this example, you set a threshold of 80,000 per second for the number of UDP packets that can be received on IP address 1.1.1.5, in the Untrust zone, before the security device generates an alarm and drops subsequent packets for the remainder of that second.

NOTE: This example uses a general ScreenOS command and is not necessarily SIP-specific. For more information about UDP flood protection and how to determine effective settings, see “UDP Flood” on page 4-47.

WebUI

Screening > Screen: Enter the following, then click **Apply**:

Zone: Untrust
 UDP Flood Protection (select)

> Destination IP: Enter the following, then click the Back arrow in your browser to return to the Screen configuration page:

Destination IP: 1.1.1.5
 Threshold: 80000
 Add: (select)

CLI

```
set zone untrust screen udp-flood dst-ip 1.1.1.5 threshold 80000
save
```


Example: SIP Connection Maximum

In this example, you prevent flood attacks on the SIP network from attackers in the Untrust zone by setting a maximum of 20 concurrent sessions from a single IP address. If the security device detects more than 20 connection attempts from the same IP address, it begins dropping subsequent attempts until the number of sessions drops below the specified maximum.

NOTE: This example uses a general ScreenOS command and is not necessarily SIP-specific. For more information about source-based session limits and how to determine effective settings, see “Source-Based and Destination-Based Session Limits” on page 4-28.

WebUI

Screening > Screen (Zone: Untrust): Enter the following, then click **OK**:

Source IP Based Session Limit: (select)
Threshold: 20 Sessions

CLI

```
set zone untrust screen limit-session source-ip-based 20
save
```

SIP with Network Address Translation

The Network Address Translation (NAT) protocol enables multiple hosts in a private subnet to share a single public IP address to access the Internet. For outgoing traffic, NAT replaces the private IP address of the host in the private subnet with the public IP address. For incoming traffic, the public IP address is converted back into the private address, and the message is routed to the appropriate host in the private subnet.

Using NAT with the SIP service is more complicated because SIP messages contain IP addresses in the SIP headers as well as in the SIP body. The SIP headers contain information about the caller and the receiver, and the security device translates this information to hide it from the outside network. The SIP body contains the Session Description Protocol (SDP) information, which includes IP addresses and port numbers for transmission of the media. The security device translates SDP information for allocating resources to send and receive the media.

How IP addresses and port numbers in SIP messages are replaced depends on the direction of the message. For an outgoing message, the private IP address and port number of the client are replaced with the public IP address and port number of the Juniper Networks firewall. For an incoming message, the public address of the firewall is replaced with the private address of the client.

When an INVITE message is sent out across the firewall, the SIP ALG collects information from the message header into a call table, which it uses to forward subsequent messages to the correct end point. When a new message arrives, for example an ACK or 200 OK, the ALG compares the “From:”, “To:”, and “Call-ID:” fields against the call table to identify the call context of the message. If a new INVITE message arrives that matches the existing call, the ALG processes it as a REINVITE.

When a message containing SDP information arrives, the ALG allocates ports and creates a NAT mapping between them and the ports in the SDP. Because the SDP requires sequential ports for the Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) channels, the ALG provides consecutive even-odd ports. If it is unable to find a pair of ports it discards the SIP message.

Outgoing Calls

When a SIP call is initiated with a SIP request message from the internal to the external network, NAT replaces the IP addresses and port numbers in the SDP and creates a binding to map the IP addresses and port numbers to the Juniper Networks firewall. Via:, Contact:, Route:, and Record-Route: SIP header fields, if present, are also bound to the firewall IP address. The ALG stores these mappings for use in retransmissions and for SIP response messages.

The SIP ALG then opens pinholes in the firewall to allow media through the security device on the dynamically assigned ports negotiated based on information in the SDP and the Via:, Contact:, and Record-Route: header fields. The pinholes also allow incoming packets to reach the Contact:, Via:, and Record-Route: IP addresses and ports. When processing return traffic, the ALG inserts the original Contact:, Via:, Route:, and Record-Route: SIP fields back into the packets.

Incoming Calls

Incoming calls are initiated from the public network to public mapped IP (MIP) addresses or to interface IP addresses on the security device. MIPs are statically configured IP addresses that point to internal hosts; interface IP addresses are dynamically recorded by the ALG as it monitors REGISTER messages sent by internal hosts to the SIP registrar. (For more information, see “Examples” on page 30.) When the security device receives an incoming SIP packet, it sets up a session and forwards the payload of the packet to the SIP ALG.

The ALG examines the SIP request message (initially an INVITE) and, based on information in the SDP, opens gates for outgoing media. When a 200 OK response message arrives, the SIP ALG performs NAT on the IP addresses and ports and opens pinholes in the outbound direction. (The opened gates have a short time-to-live, and time out if a 200 OK response message is not received quickly.)

When a 200 OK response arrives, the SIP proxy examines the SDP information and reads the IP addresses and port numbers for each media session. The SIP ALG on the security device performs NAT on the addresses and port numbers, opens pinholes for outbound traffic, and refreshes the timeout for gates in the inbound direction.

When the ACK arrives for the 200 OK, it also passes through the SIP ALG. If the message contains SDP information, the SIP ALG ensures that the IP addresses and port numbers are not changed from the previous INVITE—if they are, the ALG deletes old pinholes and creates new pinholes to allow media to pass through. The ALG also monitors the Via:, Contact:, and Record-Route: SIP fields and opens new pinholes if it determines that these fields have changed.

Forwarded Calls

A forwarded call is when, for example, user A outside the network calls user B inside the network, and user B forwards the call to user C outside the network. The SIP ALG processes the INVITE from user A as a normal incoming call. But when the ALG examines the forwarded call from B to C outside the network and notices that B and C are reached using the same interface, it does not open pinholes in the firewall, because media will flow directly between user A and user C.

Call Termination

The BYE message is used to terminate a call. When the security device receives a BYE message, it translates the header fields just as it does for any other message. But because a BYE message must be acknowledged by the receiver with a 200 OK, the ALG delays call teardown for five seconds to allow time for transmission of the 200 OK.

Call Re-INVITE Messages

Re-INVITE messages are used to add new media sessions to a call, and to removing existing media sessions. When new media sessions are added to a call, new pinholes are opened in the firewall and new address bindings created. The process is identical to the original call setup. When one or more media sessions are removed from a call, pinholes are closed and bindings released just as with a BYE message.

Call Session Timers

The SIP ALG uses the Session-Expires value to time out a session if a Re-INVITE or UPDATE message is not received. The ALG gets the Session-Expires value, if present, from the 200 OK response to the INVITE and uses this value for signaling timeout. If the ALG receives another INVITE before the session times out, it resets all timeout values to this new INVITE or to default values, and the process is repeated.

As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist. This ensures that the security device is protected in the event of the following:

- End systems crash during a call and a BYE message is not received.
- Malicious users never send a BYE in an attempt to attack a SIP ALG.
- Poor implementations of sip proxy fail to process Record-Route and never send a BYE message.
- Network failures prevent a BYE message from being received.

Call Cancellation

Either party can cancel a call by sending a CANCEL message. Upon receiving a CANCEL message, the SIP ALG closes pinholes through the firewall—if any have been opened—and releases address bindings. Before releasing the resources, the ALG delays the control channel age-out for approximately five seconds to allow time for the final 200 OK to pass through. The call is terminated when the five second timeout expires, regardless of whether a 487 or non-200 response arrives.

Forking

Forking enables a SIP proxy to send a single INVITE message to multiple destinations simultaneously. When the multiple 200 OK response messages arrive for the single call, the SIP ALG parses but updates call information with the first 200 OK message it receives.

SIP Messages

The SIP message format consists of a SIP header section, and the SIP body. In request messages, the first line of the header section is the request line, which includes the method type, Request-URI, and protocol version. In response messages, the first line is the status line, which contains a status code. SIP headers contain IP addresses and port numbers used for signaling. The SIP body, separated from the header section by a blank line, is reserved for session description information, which is optional. Juniper Networks security devices currently support the Session Description Protocol (SDP) only. The SIP body contains IP addresses and port numbers used to transport the media.

In NAT mode, the security device translates information in the SIP headers to hide the information from the outside network. NAT is performed on SIP body information to allocate resources, that is, port numbers where the media is to be received.

SIP Headers

In the following sample SIP request message, NAT replaces the IP addresses in the header fields—shown in bold font—to hide them from the outside network.

```
INVITE bob@10.150.20.5 SIP/2.0
Via: SIP/2.0/UDP 10.150.20.3:5434
From: alice@10.150.20.3
To: bob@10.150.20.5
Call-ID: a12abcde@10.150.20.3
Contact: alice@10.150.20.3:5434
Route: <sip:netscreen@10.150.20.3:5060>
Record-Route: <sip:netscreen@10.150.20.3:5060>
```

How IP address translation is performed depends on the type and direction of the message, which can be any of the following:

- Inbound request
- Outbound response
- Outbound request
- Inbound response

Table 2 shows how NAT is performed in each of these cases. Note that for several of the header fields the ALG must know more than just whether the messages comes from inside or outside the network. It must also know what client initiated the call, and whether the message is a request or response.

Table 2: Requesting Messages with NAT

Message Type	Fields	Action
Inbound Request (from public to private)	To:	Replace ALG address with local address
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	Replace ALG address with local address
	Contact:	None
	Record-Route:	None
	Route:	None
Outbound Response (from private to public)	To:	Replace ALG address with local address
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	N/A
	Contact:	Replace local address with ALG address
	Record-Route:	Replace local address with ALG address
	Route:	None
Outbound Request (from private to public)	To:	None
	From:	Replace local address with ALG address
	Call-ID:	Replace local address with ALG address
	Via:	Replace local address with ALG address
	Request-URI:	None
	Contact:	Replace local address with ALG address
	Record-Route:	Replace local address with ALG address
	Route:	Replace ALG address with local address

Message Type	Fields	Action
Outbound Response (from public to private)	To:	None
	From:	Replace ALG address with local address
	Call-ID:	Replace ALG address with local address
	Via:	Replace ALG address with local address
	Request-URI:	N/A
	Contact:	None
	Record-Route:	Replace ALG address with local address
	Route:	Replace ALG address with local address

SIP Body

The SDP information in the SIP body includes IP addresses the ALG uses to create channels for the media stream. Translation of the SDP section also allocates resources, that is, port numbers to send and receive the media.

The following excerpt from a sample SDP section shows the fields that are translated for resource allocation.

```
o=user 2344234 55234434 IN IP4 10.150.20.3
c=IN IP4 10.150.20.3
m=audio 43249 RTP/AVP 0
```

SIP messages can contain more than one media stream. The concept is similar to attaching multiple files to an email message. For example, an INVITE message sent from a SIP client to a SIP server might have the following fields:

```
c=IN IP4 10.123.33.4
m=audio 33445 RTP/AVP 0
c=IN IP4 10.123.33.4
m=audio 33447 RTP/AVP 0
c=IN IP4 10.123.33.4
m=audio 33449 RTP/AVP 0
```

Juniper Networks security devices support up to 6 SDP channels negotiated for each direction, for a total of 12 channels per call. For more information, see “SDP” on page 18.

SIP NAT Scenario

In Figure 8, ph1 sends a SIP INVITE message to ph2. Note how the IP addresses in the header fields—shown in bold font—are translated by the security device.

The SDP section of the INVITE message indicates where the caller is willing to receive media. Note that the Media Pinhole contains two port numbers, 52002 and 52003, for RTCP and RTP. The Via/Contact Pinhole provides port number 5060 for SIP signaling.

Observe how, in the 200 OK response message, the translations performed in the INVITE message are reversed. The IP addresses in this message, being public, are not translated, but gates are opened to allow the media stream access to the private network.

Figure 8: SIP NAT Scenario 1

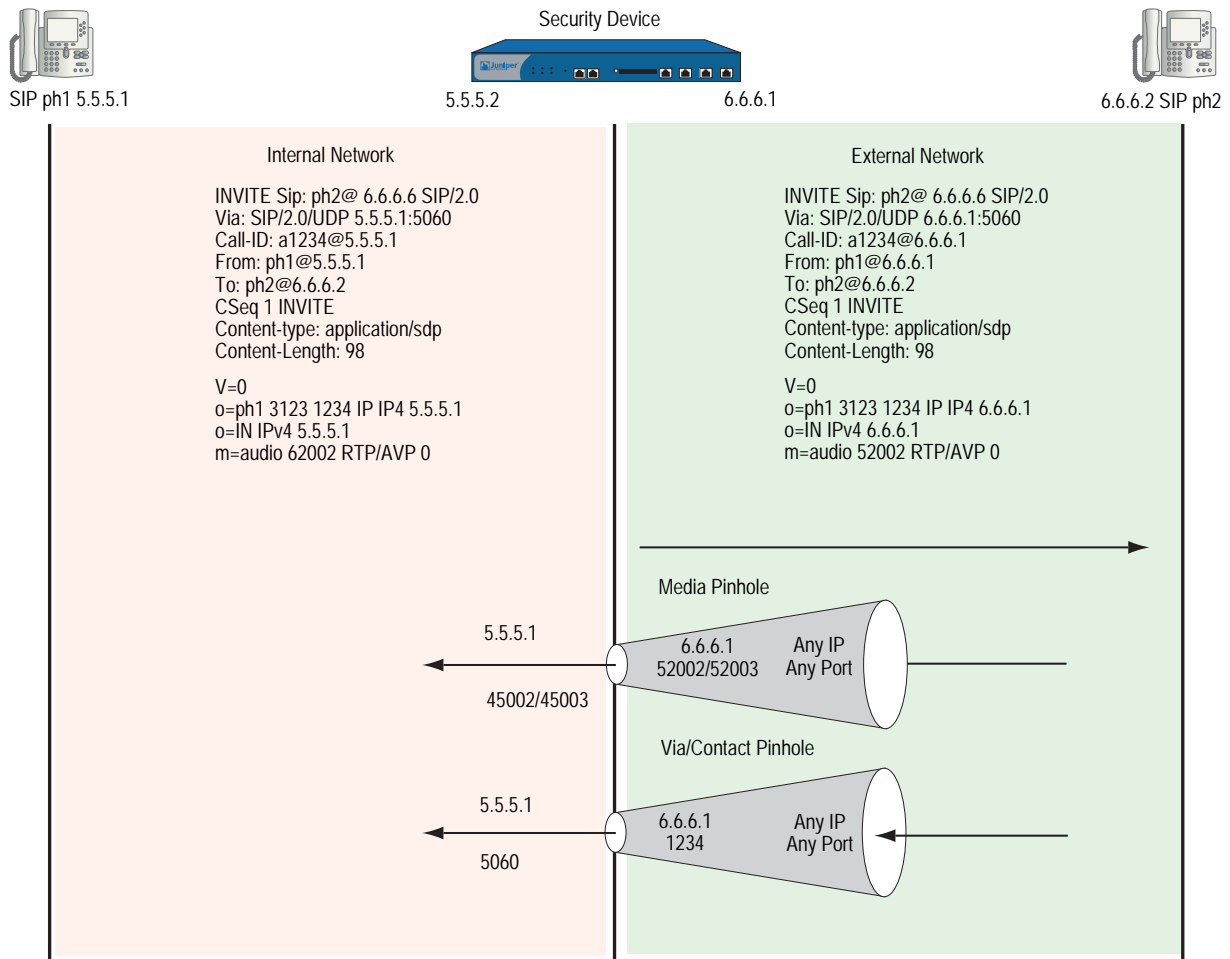
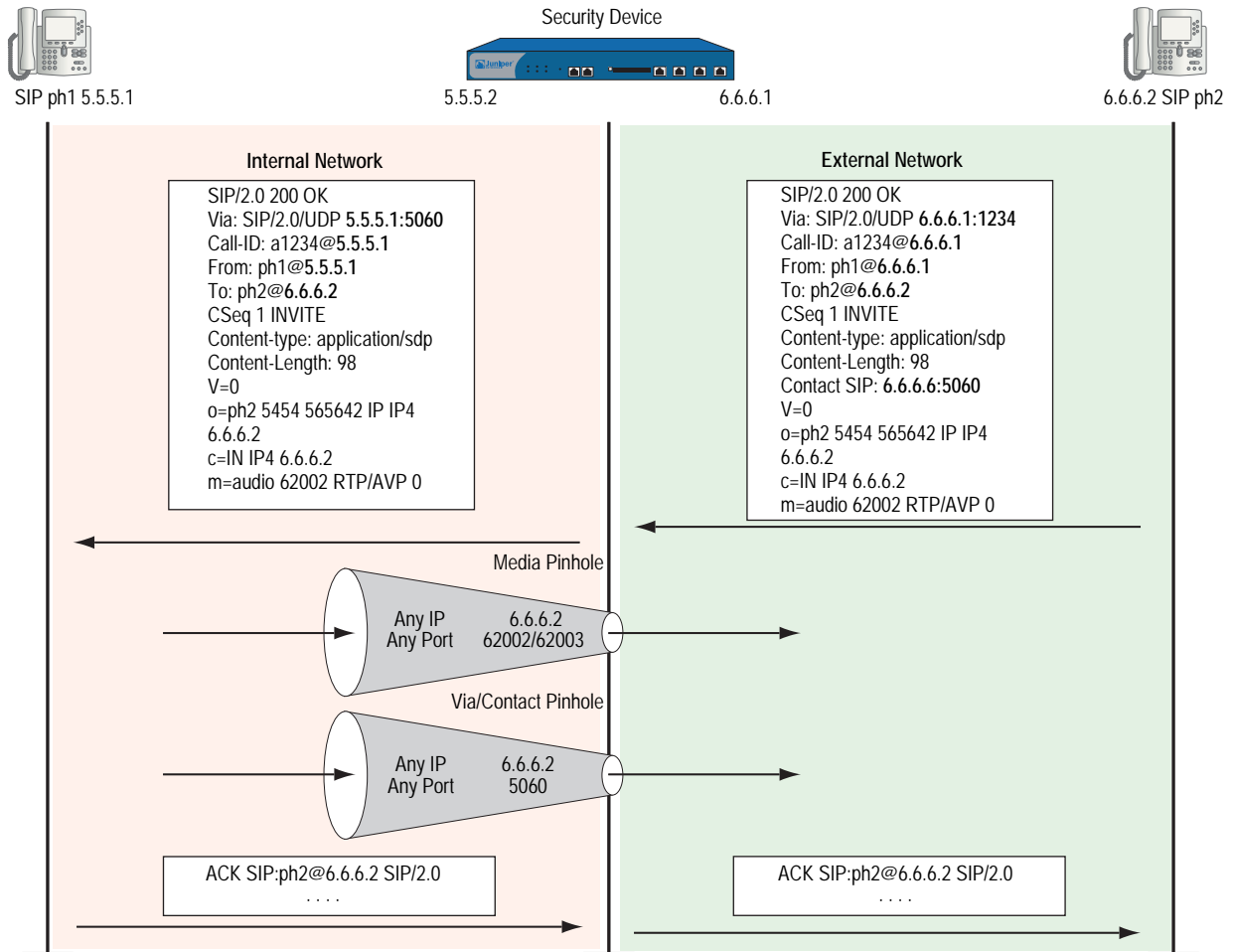


Figure 9: SIP NAT Scenario 2



Examples

This section contains the following sample scenarios:

- “Incoming SIP Call Support Using the SIP Registrar” on page 31
- “Example: Incoming Call with MIP” on page 37
- “Example: Proxy in the Private Zone” on page 39
- “Example: Proxy in the Public Zone” on page 41
- “Example: Three-Zone, Proxy in the DMZ” on page 44
- “Example: Untrust Intrazone” on page 47
- “Example: Trust Intrazone” on page 51
- “Example: Full-Mesh VPN for SIP” on page 53

Incoming SIP Call Support Using the SIP Registrar

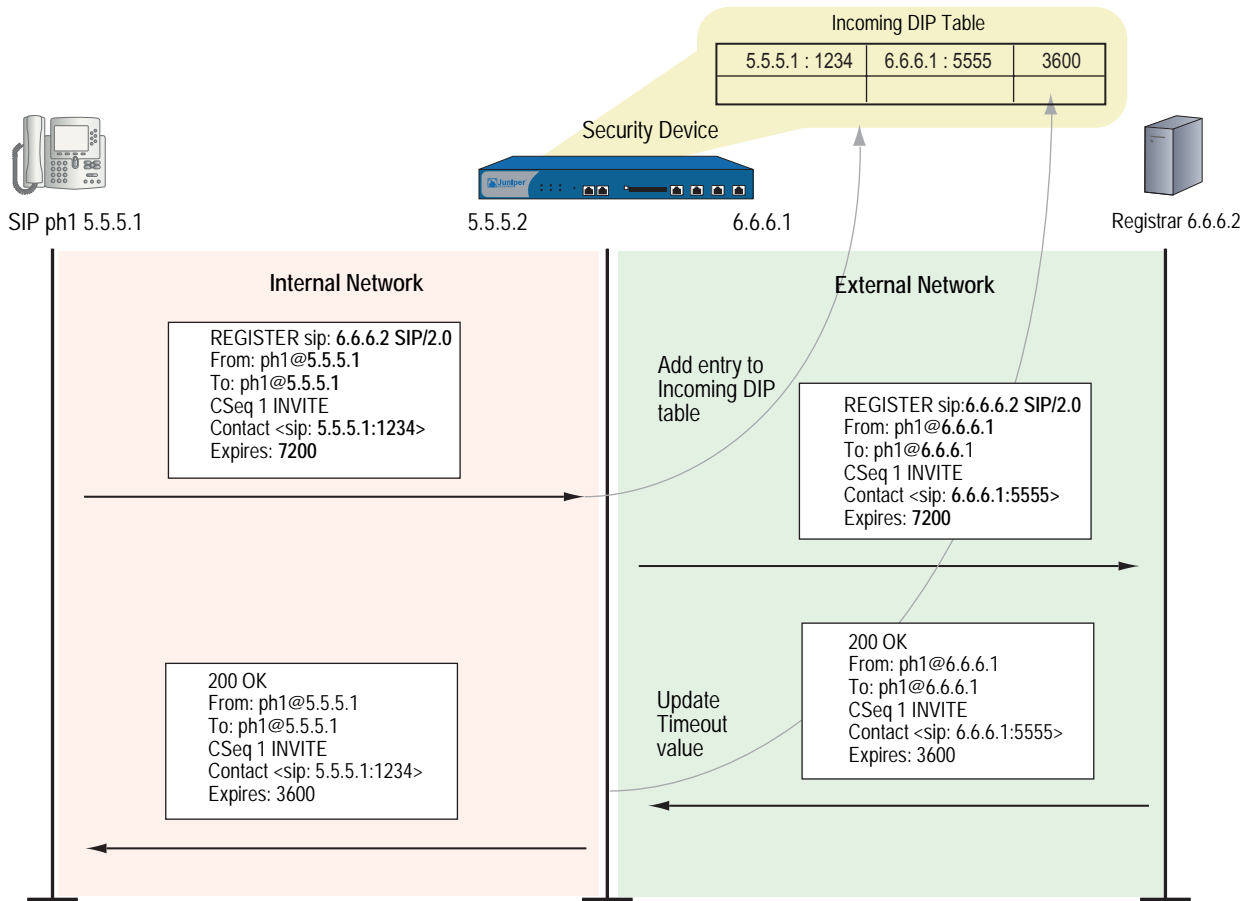
SIP registration provides a discovery capability by which SIP proxies and location servers are able to identify the location or locations where users want to be contacted. A user registers one or more contact locations by sending a REGISTER message to the registrar. The To: and Contact: fields in the REGISTER message contain the address-of-record URI and one or more contact URIs, as shown in Figure 10. Registration creates bindings in a location service that associates the address-of-record with the contact address or addresses.

The security device monitors outgoing REGISTER messages, performs NAT on these addresses, and stores the information in an Incoming DIP table. Then, when an INVITE message is received from outside the network, the security device uses the Incoming DIP table to identify which internal host to route the INVITE message to. You can take advantage of SIP proxy registration service to allow incoming calls by configuring Interface DIP or DIP pools on the egress interface of the security device. Interface DIP is adequate for handling incoming calls in a small office, while we recommend setting up DIP pools for larger networks or an enterprise environment.

NOTE: Incoming call support using Interface DIP or a DIP pool is supported for SIP and H.323 services only.

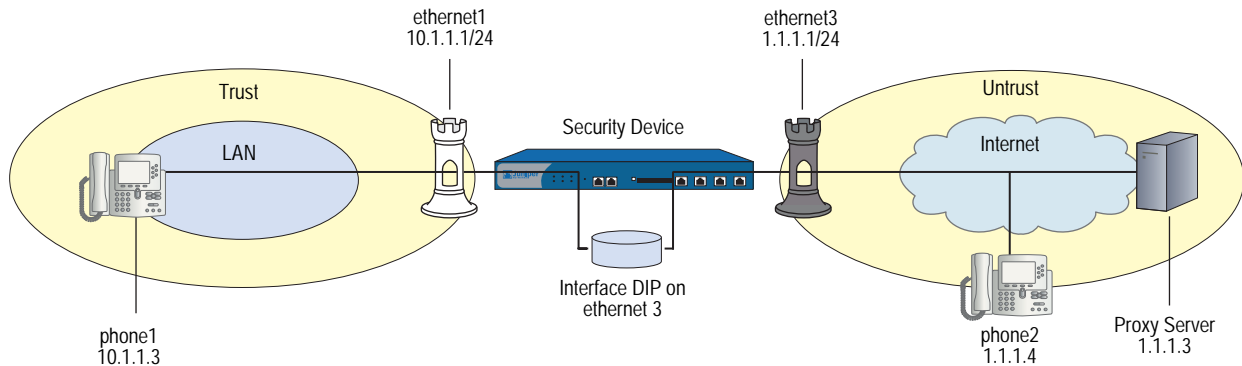
For incoming calls, security devices currently support UDP and TCP only. Domain name resolution is also currently not supported; therefore, URIs must contain IP addresses, as shown in Figure 10.

Figure 10: Incoming SIP



Example: Incoming Call (Interface DIP)

In this example, phone1 is on the ethernet1 interface in the Trust zone, and phone2 and the proxy server are on the ethernet3 interface in the Untrust zone. You set Interface DIP on the ethernet3 interface to do NAT on incoming calls, then create a policy permitting SIP traffic from the Untrust zone to the Trust zone and reference that DIP in the policy. You also create a policy that permits SIP traffic from the Trust to the Untrust zone using NAT Source. This enables phone1 in the Trust zone to register with the proxy in the Untrust zone. For an explanation of how incoming DIP works with the SIP registration service, see “Examples” on page 30.

Figure 11: Incoming Call with Interface DIP on ethernet3 Interface

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 1.1.1.1/24
 Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.3/24
 Zone: Untrust

3. DIP with Incoming NAT

Network > Interface > Edit (for ethernet3) > DIP > New: Select the Incoming NAT option, then click **OK**.

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) phone1
 Destination Address
 Address Book Entry: (select) any
 Service: SIP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: (select)
 (DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select), Any
 Destination Address
 Address Book Entry: (select), DIP(ethernet3)
 Service: SIP
 Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. DIP with Incoming NAT

```
set interface ethernet3 dip interface-ip incoming
set dip sticky
```

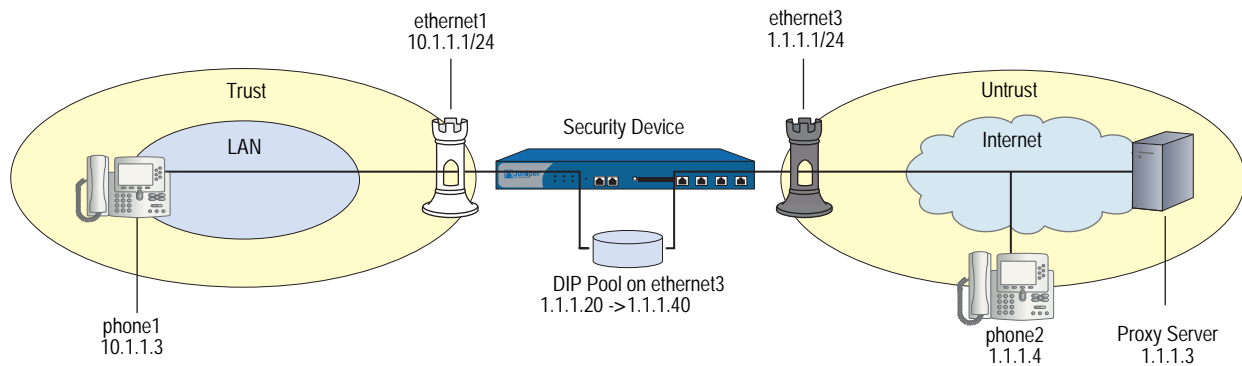
4. Policies

```
set policy from trust to untrust phone1 any sip nat src permit
set policy from untrust to trust any dip(ethernet3) sip permit
save
```

Example: Incoming Call (DIP Pool)

This example, phone1 is in the Trust zone, and phone2 and the proxy server are in the Untrust zone. You set a DIP pool on the ethernet3 interface to do NAT on incoming calls, then set a policy permitting SIP traffic from the Untrust zone to the Trust zone and reference that DIP pool in the policy. You also create a policy that permits SIP traffic from the Trust to the Untrust zone using NAT Source. This enables phone1 in the Trust zone to register with the proxy in the Untrust zone. For an explanation of how DIP works with the SIP registration service, see “Examples” on page 30.

Figure 12: Incoming Call with DIP Pool



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 1.1.1.1/24
 Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.3/24
Zone: Untrust

3. DIP Pool with Incoming NAT

Network > Interface > Edit (for ethernet3) > DIP > New: Enter the following, then click **OK**:

ID: 5
IP Address Range: (select), 1.1.1.20 ~ 1.1.1.40
 Port Translation: (select)
In the same subnet as the interface IP or its secondary IPs: (select)
 Incoming NAT: (select)

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select), phone1
Destination Address
 Address Book Entry: (select), Any
Service: SIP
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: (select)
 (DIP on): 5 (1.1.1.20-1.1.1.40)/port-xlate

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) Any
Destination Address
 Address Book Entry: (select) DIP(5)
Service: SIP
Action: Permit

CLI**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. DIP Pool with Incoming NAT

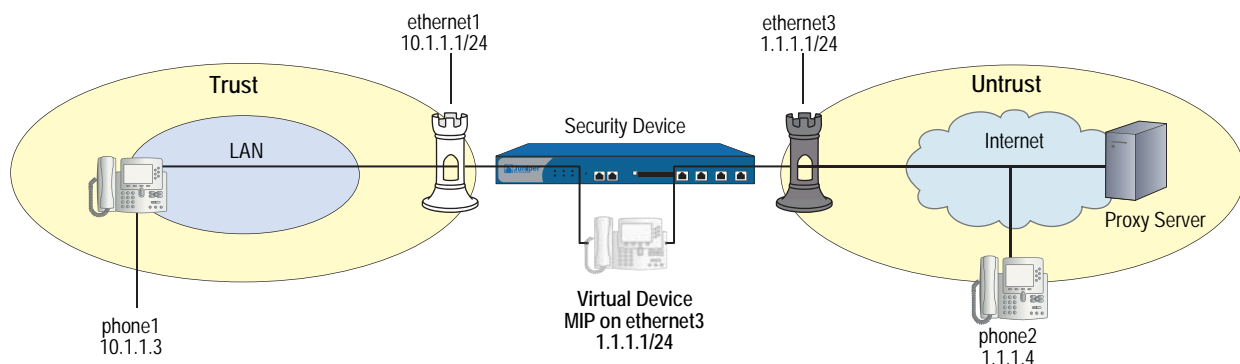
```
set interface ethernet3 dip 5 1.1.1.20 1.1.1.40 incoming
set dip sticky
```

4. Policies

```
set policy from trust to untrust phone1 any sip nat src dip 5 permit
set policy from untrust to trust any dip(5) sip permit
save
```

Example: Incoming Call with MIP

In this example, phone1 is on the ethernet1 interface in the Trust zone, and phone2 and the proxy server are on the ethernet3 interface in the Untrust zone. You put a MIP on the ethernet3 interface to phone1, then create a policy that allows SIP traffic from the Untrust zone to the Trust zone and reference that MIP in the policy. You also create a policy allowing phone1 to register with the proxy server in the Untrust zone. This example is similar to the previous two examples (“Example: Incoming Call (Interface DIP)” on page 32 and “Example: Incoming Call (DIP Pool)” on page 35), except that with a MIP you need one public address for each private address in the Trust zone, while with Interface DIP or a DIP pool a single interface address can serve multiple private addresses.

Figure 13: Incoming Call with MIP

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.1.1.1/24
Enter the following, then click **OK**:
Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
IP Address/Netmask: 1.1.1.1/24
Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.3/24
Zone: Untrust

3. MIP

Network > Interfaces > Edit (for ethernet3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.3
Netmask: 255.255.255.255
Host IP Address: 10.1.1.3

4. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), any
Destination Address:
 Address Book Entry: (select), MIP(1.1.1.3)
Service: SIP
Action: Permit

CLI**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. MIP

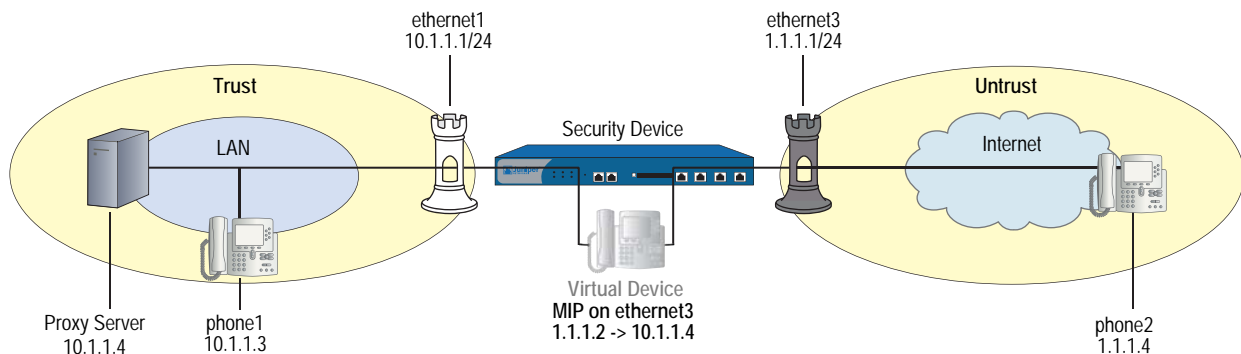
```
set interface ethernet3 mip 1.1.1.3 host 10.1.1.3
```

4. Policy

```
set policy from untrust to trust any mip(1.1.1.3) sip permit
save
```

Example: Proxy in the Private Zone

In this example, phone1 and the SIP proxy server are on the ethernet1 interface in the Trust (private) zone, and phone2 is on the ethernet3 interface in the Untrust zone. You put a MIP on the ethernet3 interface to the proxy server to allow phone2 to register with the proxy, then create a policy allowing SIP traffic from the Untrust to the Trust zone and reference that MIP in the policy. You also create a policy from the Trust to the Untrust zone to allow phone1 to call out.

Figure 14: Proxy in the Private Zone**WebUI****1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

```
Zone: Trust
Static IP: (select this option when present)
IP Address/Netmask: 10.1.1.1/24
Enter the following, then click OK:
Interface Mode: NAT
```

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
IP Address/Netmask: 1.1.1.1/24
Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.3/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (select), 1.1.1.4/24
Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.4/24
Zone: Trust

3. MIP

Network > Interfaces > Edit (for loopback.3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.2
Netmask: 255.255.255.255
Host IP Address: 10.1.1.4
Host Virtual Router Name: trust-vr

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select) any
Destination Address:
Address Book Entry: (select) phone2
Service: SIP
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: (select)
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), phone2
Destination Address:
Address Book Entry: (select), MIP(1.1.1.2)
Service: SIP
Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address trust proxy 10.1.1.4/24
```

3. MIP

```
set interface ethernet3 mip 1.1.1.2 host 10.1.1.4
```

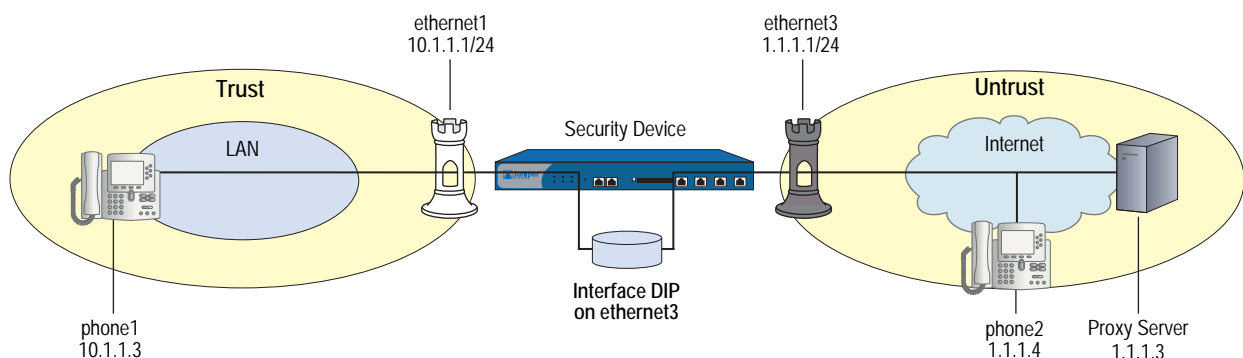
4. Policies

```
set policy from trust to untrust any phone2 sip nat src permit
set policy from untrust to trust phone2 mip(1.1.1.2) sip permit
save
```

Example: Proxy in the Public Zone

In this example, phone1 is on the ethernet1 interface in the Trust zone, and the proxy server and phone2 are on the ethernet3 interface in the Untrust (public) zone. You configure Interface DIP on the Untrust interface, then create a policy permitting SIP traffic from the Untrust zone to the Trust zone and reference that DIP in the policy. You also create a policy from Trust to Untrust to allow phone1 to register with the proxy server in the Untrust zone. This example is similar to the previous incoming call examples (see “Example: Incoming Call (DIP Pool)” on page 35 and “Example: Incoming Call with MIP” on page 37) and, as with those examples, you can use DIP or MIP on the Untrust interface.

Figure 15: Proxy in the Public Zone



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
 IP Address/Netmask: 1.1.1.1/24
 Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.3/24
 Zone: Untrust

3. Interface DIP

Network > Interface > Edit (for ethernet3) > DIP: Select the Incoming NAT checkbox.

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select) phone1
 Destination Address:
 Address Book Entry: (select) Any
 Service: SIP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:

Source Translation: (select)

(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:

Address Book Entry: (select) Any

Destination Address:

Address Book Entry: (select) DIP(ethernet3)

Service: SIP

Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. Interface DIP

```
set interface ethernet3 dip interface-ip incoming
```

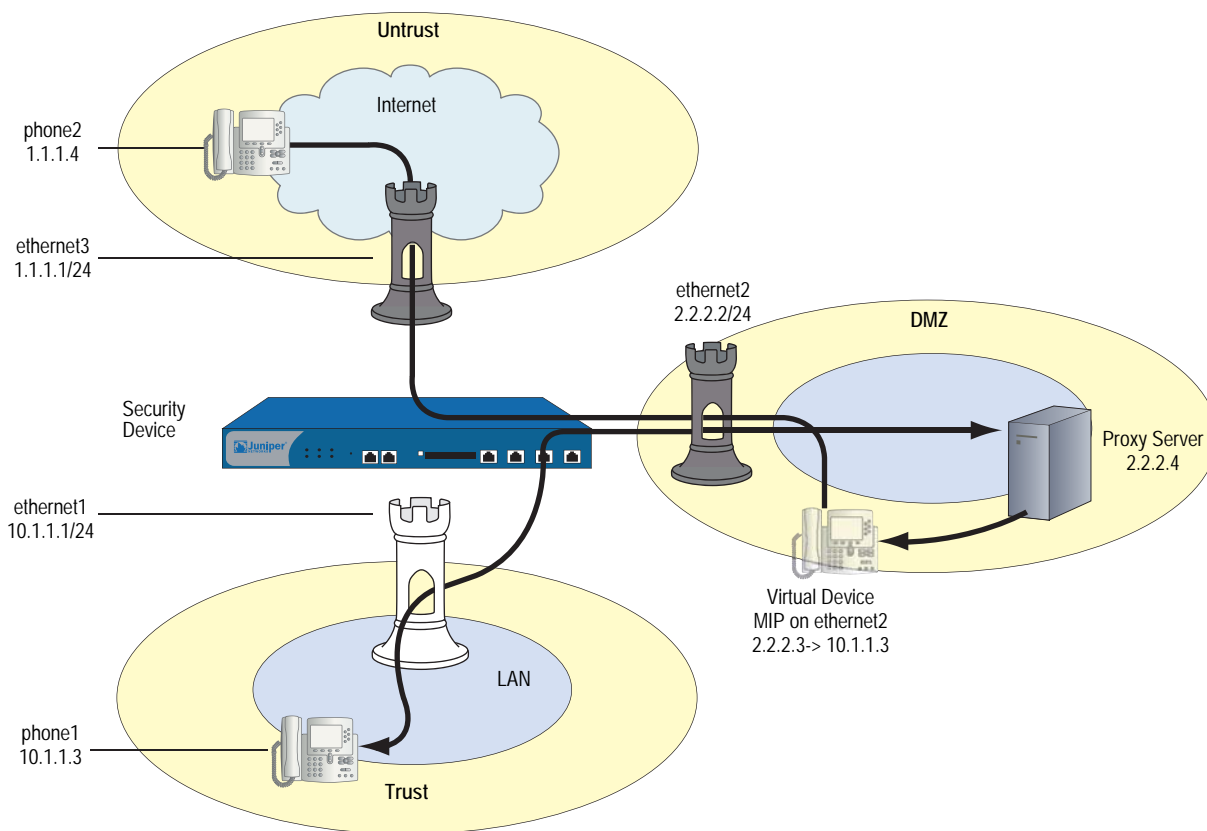
4. Policies

```
set policy from trust to untrust phone1 any sip nat src permit
set policy from untrust to trust any dip(ethernet3) sip permit
save
```

Example: Three-Zone, Proxy in the DMZ

In this example, phone1 is on the ethernet1 interface in the Trust zone, phone2 is on the ethernet3 interface in the Untrust zone, and the proxy server is on the ethernet2 interface in the DMZ. You put a MIP on the ethernet2 interface to phone1 in the Trust zone, and create a policy from the DMZ to the Trust zone and reference that MIP in the policy. In fact, with three zones, you need to create bidirectional policies between each of the zones. The arrows in Figure 16 show the flow of SIP signaling traffic when phone2 in the Untrust zone places a call to phone1 in the Trust zone. After the session is initiated, the media flows directly between phone1 and phone2.

Figure 16: Proxy in the DMZ



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

- Zone: Trust
- Static IP: (select when this option is present)
- IP Address/Netmask: 10.1.1.1/24
- Enter the following, then click **OK**:
- Interface Mode: NAT

Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

Zone Name: DMZ
 Static IP: (select when this option is present)
 IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.1.1/24

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.4/24
 Zone: DMZ

3. MIP

Network > Interfaces > Edit (for ethernet2) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 2.2.2.3
 Netmask: 255.255.255.255
 Host IP Address: 10.1.1.3

4. Policies

Policies > (From: Trust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), phone1
 Destination Address:
 Address Book Entry: (select), proxy
 Service: SIP
 Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

Policies > (From: DMZ, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), proxy
Destination Address:
Address Book Entry: (select), phone2
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), phone2
Destination Address:
Address Book Entry: (select), phone1
Service: SIP
Action: Permit

Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), phone2
Destination Address:
Address Book Entry: (select), proxy
Service: SIP
Action: Permit

Policies > (From: DMZ, To: Trust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), proxy
Destination Address:
Address Book Entry: (select), MIP(2.2.2.3)
Service: SIP
Action: Permit

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), phone1
Destination Address:
Address Book Entry: (select), phone2
Service: SIP
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

CLI**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.2.2.2/24
set interface ethernet2 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address dmz proxy 2.2.2.4
```

3. MIP

```
set interface2 mip 2.2.2.3 host 10.1.1.3
```

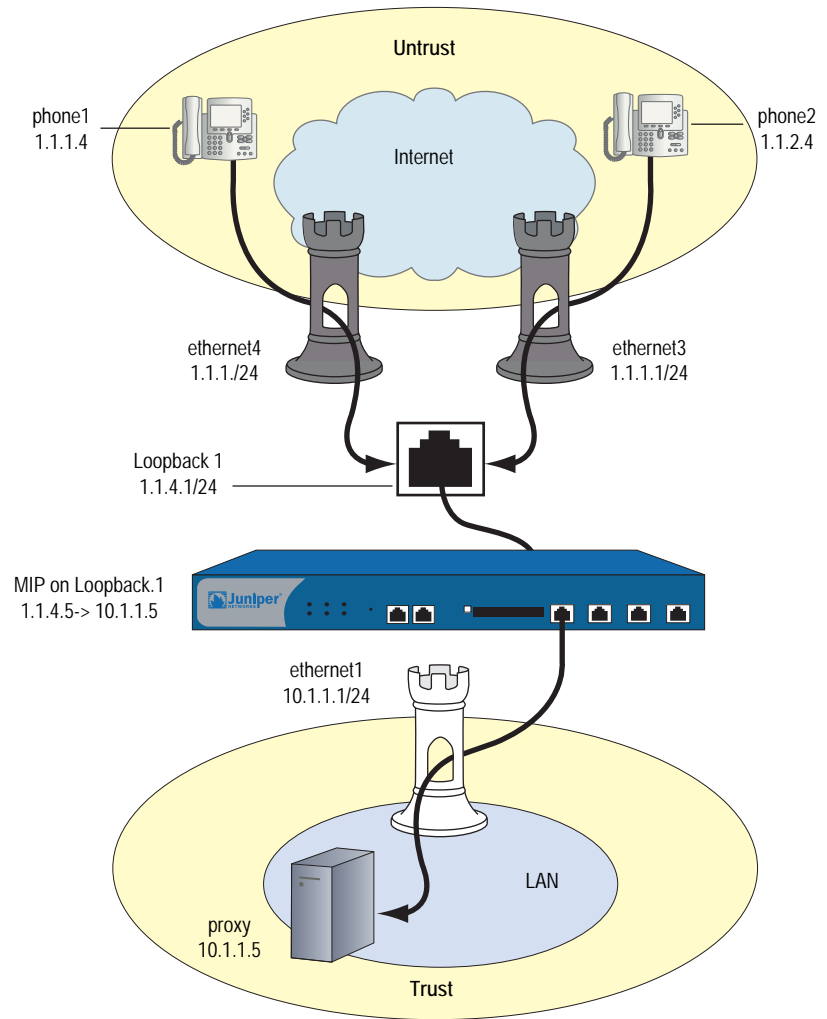
4. Policies

```
set policy from trust to dmz phone1 proxy sip nat src permit
set policy from dmz to untrust proxy phone2 sip permit
set policy from untrust to trust phone2 phone1 sip permit
set policy from untrust to dmz phone2 proxy sip permit
set policy from dmz to trust proxy mip(2.2.2.3) sip permit
set policy from trust to untrust phone1 phone2 sip nat src permit
save
```

Example: Untrust Intrazone

In this example, phone1 is on the ethernet4 interface in the Untrust zone, phone2 is in a subnet on the ethernet3 interface in the Untrust zone, and the proxy server is on the ethernet1 interface in the Trust zone. To allow intrazone SIP traffic between the two phones in the Untrust zone, you create a loopback interface, add ethernet3 and ethernet4 to a loopback group, then put a MIP on the loopback interface to the IP address of the proxy server. Creating a loopback interface enables you to use a single MIP for the proxy server in the Trust zone. Because blocking is on by default in the Untrust zone, you must also turn off blocking to allow intrazone communication. For more information about using loopback interfaces, see “MIP and the Loopback Interface” on page 8-73.

Figure 17: Untrust Intrazone



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.1.1/24

Enter the following, then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **OK**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > New Loopback IF: Enter the following, then click **OK**:

Interface Name: loopback.1
 Zone: Untrust (trust-vr)
 IP Address/Netmask: 1.1.4.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.5/32
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/32
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.2.4/32
 Zone: Untrust

3. Loopback Group

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

As member of loopback group: (select) loopback.1
 Zone Name: Untrust

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **OK**:

As member of loopback group: (select) loopback.1
 Zone Name: Untrust

4. MIP

Network > Interfaces > Edit (for loopback.1) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.4.5
 Netmask: 255.255.255.255
 Host IP Address: 10.1.1.5
 Host Virtual Router Name: trust-vr

5. Blocking

Network > Zones > Edit (for Untrust): Enter the following, then click **OK**:

Block Intra-Zone Traffic: (clear)

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), proxy
 Destination Address:
 Address Book Entry: (select), Any
 Service: SIP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: Enable
 (DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), Any
 Destination Address:
 Address Book Entry: (select), MIP(1.1.4.5)
 Service: SIP
 Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.2.1/24
set interface ethernet3 route
set interface ethernet4 zone untrust
set interface ethernet4 ip 1.1.1.1/24
set interface ethernet4 route
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.4.1/24
set interface loopback.1 route
```

2. Addresses

```
set address trust proxy 10.1.1.5/32
set address untrust phone1 1.1.1.4/32
set address untrust phone2 1.1.2.4/32
```

3. Loopback Group

```
set interface ethernet3 loopback-group loopback.1
set interface ethernet4 loopback-group loopback.1
```

4. MIP

```
set interface loopback.1 mip 1.1.4.5 host 10.1.1.5
```

5. Blocking

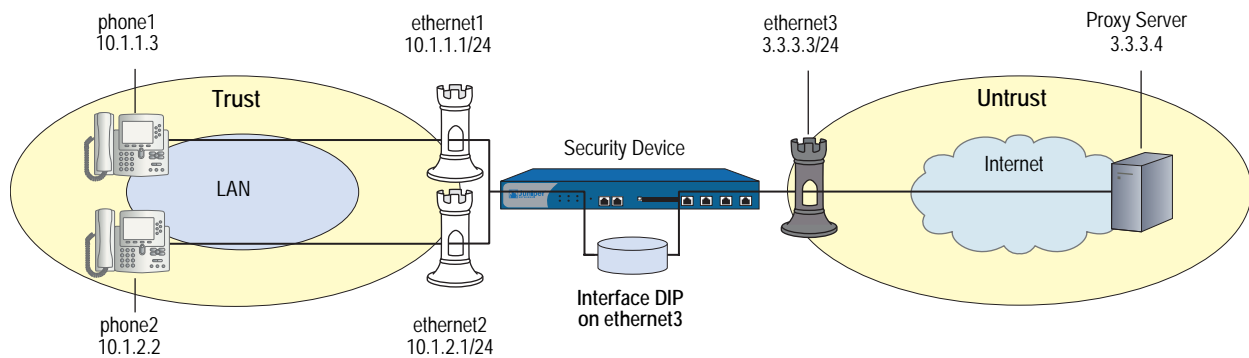
```
unset zone untrust block
```

6. Policies

```
set policy from trust to untrust proxy any sip nat src permit
set policy from untrust to trust any mip(1.1.4.5) sip permit
save
```

Example: Trust Intrazone

In this example, phone1 is on the ethernet1 interface in the Trust zone, phone 2 is on the ethernet2 interface in a subnet in the Trust zone, and the proxy server is on the ethernet3 interface in the Untrust zone. To allow both phones in the Trust zone to communicate with each other, you configure Interface DIP on the ethernet3 interface to allow them to contact the proxy server, then set policies to allow bidirectional SIP traffic between the Trust and the Untrust zones. Blocking is off by default in the Trust zone (as it is in custom zones you define).

Figure 18: Trust Intrazone**WebUI****1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

```
Zone: Trust
Static IP: (select when this option is present)
IP Address/Netmask: 10.1.1.1/24
Enter the following, then click OK:
Interface Mode: NAT
```

Network > Interfaces > Edit (for ethernet2): Enter the following, then click **Apply**:

```
Zone: Trust
Static IP: (select when this option is present)
IP Address/Netmask: 10.1.2.1/24
Enter the following, then click OK:
Interface Mode: NAT
```

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
Static IP: (select when this option is present)
IP Address/Netmask: 3.3.3.3/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
IP Address/Domain Name:
IP/Netmask: (select), 10.1.1.3/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
IP Address/Domain Name:
IP/Netmask: (select), 10.1.2.2/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: proxy
IP Address/Domain Name:
IP/Netmask: (select), 3.3.3.4/24
Zone: Untrust

3. DIP with Incoming NAT

Network > Interface > Edit (for ethernet3) > DIP > New: Enter the following, then click **OK**:

Incoming NAT: (select)

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
Address Book Entry: (select), Any
Destination Address:
Address Book Entry: (select), proxy
Service: SIP
Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) proxy
 Destination Address
 Address Book Entry: (select) Any
 Service: SIP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options:

NAT:
 Source Translation: (select)
 (DIP on): None (Use Egress Interface IP)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.2.1/24
set interface ethernet2 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address trust phone2 10.1.2.2/24
set address untrust proxy 3.3.3.4/24
```

3. Interface DIP

```
set interface ethernet3 dip interface-ip incoming
```

4. Policies

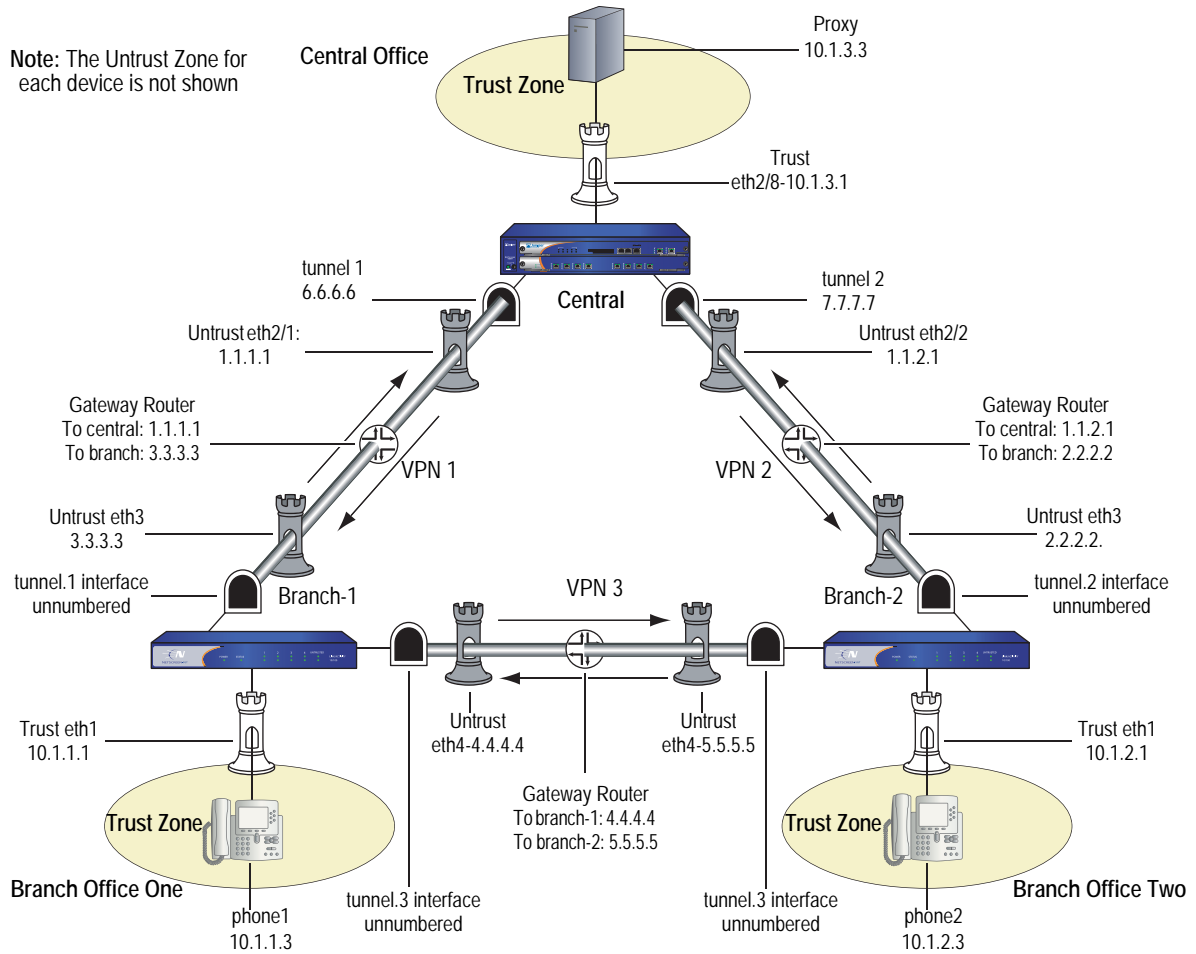
```
set policy from trust to untrust any proxy sip nat src permit
set policy from untrust to trust proxy dip(ethernet3) sip permit
save
```

Example: Full-Mesh VPN for SIP

In this example, the central office and two branch offices are linked by a full-mesh VPN. Each site has a single security device. The proxy server is in the Trust zone at the Central Office, phone1 is in the Trust zone at Branch Office One, and phone2 is in the Trust zone at Branch Office Two. All interfaces connecting the devices are in their respective Untrust zones. On each device, you configure two tunnels, one to each of the other devices, to create a fully meshed network.

NOTE: The security devices used in this example must have at least three independently configurable interfaces available.

Figure 19: Full-Mesh VPN for SIP



WebUI (for Central)

1. Interfaces

Network > Interfaces > Edit (for ethernet2/1): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet2/2): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > Edit (for ethernet2/8): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)

IP Address/Netmask: 10.1.3.1/24
 Enter the following, then click **OK**:
 Interface mode: route

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 1
 Zone (VR): Untrust
 IP Address / Netmask: 6.6.6.6/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 2
 Zone (VR): Untrust
 IP Address / Netmask: 7.7.7.7/24

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: Proxy
 IPv4/Netmask: 10.1.3.3/32
 Zone: Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-branch-1
 Security Level: Standard
 IPv4/v6 Address/Hostname: 3.3.3.3
 Preshare Key: netscreen
 Outgoing Interface: ethernet2/1

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-branch-1

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to: (select) Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-branch-2
 Security Level: Standard
 IPv4/v6 Address/Hostname: 2.2.2.2
 Preshare Key: netscreen
 Outgoing Interface: ethernet2/2

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-branch-2

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to: (select) Tunnel Interface, tunnel.2

4. Routing

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.1.0/24
Interface (select): tunnel.1

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.2.0/24
Interface (select): tunnel.2

5. Policies

Policies > (From: Trust, To: Untrust) New Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Proxy
Destination Address (select) Address Book Entry: Any-IPv4
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Any-IPv4
Destination Address (select) Address Book Entry: Proxy
Service: SIP
Action: Permit

CLI (for Central)

1. Interfaces

```
set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 1.1.1.1/24
set interface ethernet2/2 zone untrust
set interface ethernet2/2 ip 1.1.2.1/24
set interface ethernet2/8 zone trust
set interface ethernet2/8 ip 10.1.3.1/24
set interface ethernet2/8 route
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 6.6.6.6/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 7.7.7.7/24
```

2. Address

```
set address trust proxy 10.1.3.3/32
```

3. VPN

```
set ike gateway to-branch-1 address 3.3.3.3 main outgoing-interface ethernet2/1
  preshare "netscreen" sec-level standard
set ike gateway to-branch-2 address 2.2.2.2 main outgoing-interface ethernet2/2
  preshare "netscreen" sec-level standard
set vpn vpn_branch-1 gateway to-branch-1 no-reply tunnel idletime 0 sec-level
  standard
set vpn vpn_branch-1 id 1 bind interface tunnel.1
set vpn vpn_branch-2 gateway to-branch-2 no-reply tunnel idletime 0 sec-level
  standard
set vpn vpn_branch-2 id 2 bind interface tunnel.2
```

4. Routing

set route 10.1.2.0/24 interface tunnel.2
 set route 10.1.1.0/24 interface tunnel.1

5. Policies

set policy from untrust to trust any proxy sip permit
 set policy from trust to untrust proxy any sip permit
 save

WebUI (for Branch Office 1)**1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.1.1/24
 Interface mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 2
 Zone (VR): Untrust
 Unnumbered (select) Interface: ethernet3

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 3
 Zone (VR): Untrust
 Unnumbered (select) Interface: ethernet4

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IPv4/Netmask: 10.1.1.3/32
 Zone: V1-Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-central

Security Level: Standard
IPv4/v6 Address/Hostname: 1.1.2.1
Preshare Key: netscreen
Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-central

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to (select): Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-ns50
Security Level: Standard
IPv4/v6 Address/Hostname: 5.5.5.5
Preshare Key: netscreen
Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-ns50

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page::

Bind to (select): Tunnel Interface, tunnel.3

4. Routing

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.2.0/24
Interface (select): tunnel.3

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.3.0/24
Interface (select): tunnel.1

5. Policies

Policies > (From: Trust, To: Untrust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: phone2
Destination Address (select) Address Book Entry: Any-IPv4
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Any-IPv4
Destination Address (select) Address Book Entry: phone2
Service: SIP
Action: Permit

CLI (for Branch Office 1)**1. Interfaces**

```

set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4

```

2. Address

```

set address trust phone1 10.1.1.3/32

```

3. VPN

```

set ike gateway to-central address 1.1.1.1 main outgoing-interface ethernet3
  preshare "netscreen" sec-level standard
set ike gateway to-ns50 address 5.5.5.5 main outgoing-interface ethernet4
  preshare "netscreen" sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
set vpn vpncentral bind interface tunnel.1
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 bind interface tunnel.3

```

4. Routes

```

set route 10.1.2.0/24 interface tunnel.3
set route 10.1.3.0/24 interface tunnel.1

```

5. Policies

```

set policy from trust to untrust phone1 any sip permit
set policy from untrust to trust any phone1 sip permit
save

```

WebUI (for Branch Office 2)**1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

```

Zone: Trust
Static IP: (select when this option is present)
IP Address/Netmask: 10.1.2.1/24
Enter the following, then click OK:
Interface mode: NAT

```

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

```

Zone: Untrust
Static IP: (select when this option is present)
IP Address/Netmask: 2.2.2.2/24

```

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **Apply**:

Zone: Untrust
Static IP: (select when this option is present)
IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 2
Zone (VR): Untrust
Unnumbered (select) Interface: ethernet3

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 3
Zone (VR): Untrust
Unnumbered (select) Interface: ethernet4

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
IPv4/Netmask: 10.1.2.3/32
Zone: Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-central
Security Level: Standard
IPv4/v6 Address/Hostname: 1.1.2.1
Preshare Key: netscreen
Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-central

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to (select): Tunnel Interface, tunnel.2

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-ns50
Security Level: Standard
IPv4/v6 Address/Hostname: 4.4.4.4
Preshare Key: netscreen
Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-ns50

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to (select): Tunnel Interface, tunnel.3

4. Routing

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.3.0/24
Interface (select): tunnel.2

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.1.0/24
Interface (select): tunnel.3

5. Policies

Policies > (From: Trust, To: Untrust) New Enter the following, then click **OK**:

Source Address (select) Address Book Entry: phone2
Destination Address (select) Address Book Entry: Any-IPv4
Service: SIP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Any-IPv4
Destination Address (select) Address Book Entry: phone2
Service: SIP
Action: Permit

CLI (for Branch Office 2)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. Address

```
set address trust phone2 10.1.2.3/32
```

3. VPN

```
set ike gateway to-central address 1.1.2.1 Main outgoing-interface ethernet3
  preshare "netscreen" sec-level standard
set ike gateway to-ns50 address 4.4.4.4Main outgoing-interface ethernet4
  preshare "netscreen" sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
set vpn vpncentral id 4 bind interface tunnel.2
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 id 5 bind interface tunnel.3
```

4. Routes

```
set route 10.1.3.0/24 interface tunnel.2
set route 10.1.1.0/24 interface tunnel.3
```

5. Policies

```
set policy from trust to untrust phone2 any sip permit
set policy from untrust to trust any phone2 sip permit
save
```

Bandwidth Management for VoIP Services

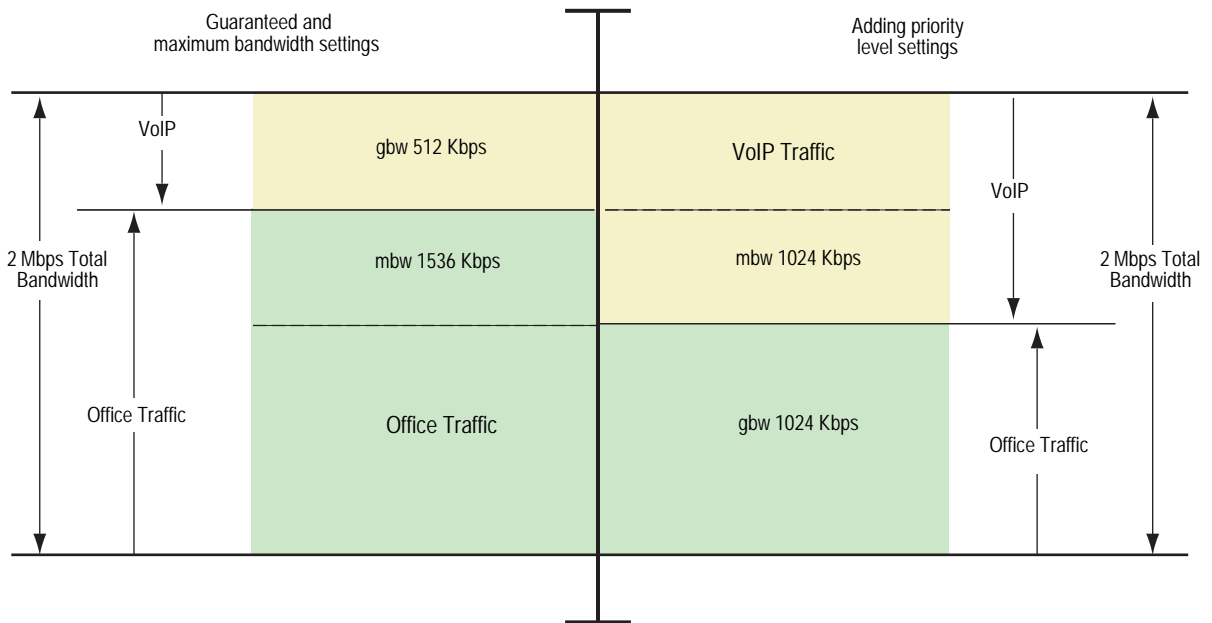
We recommend the following ways to manage bandwidth for VoIP services, using the standard ScreenOS traffic shaping mechanisms:

- **Guarantee bandwidth for VoIP traffic**—The most effective way to ensure quality VoIP service, and still allow other types of traffic on the interface, is to create a policy guaranteeing the minimum bandwidth necessary for the amount of VoIP traffic you expect on the interface and set priority queuing to the highest level. The advantage of this strategy is that VoIP traffic can use additional bandwidth when it is available, and other types of traffic can use bandwidth not guaranteed for VoIP when VoIP traffic is not using it.
- **Limit bandwidth for non-VoIP traffic**—By setting a maximum bandwidth for non-VoIP traffic, you make the remaining bandwidth available to VoIP traffic. You would also set priority queuing to the highest level for VoIP traffic. The disadvantage of this method is that non-VoIP traffic cannot use additional bandwidth even when VoIP traffic is not using it.
- **Use priority queuing and Differentiated Services Codepoint (DSCP) marking**—Guaranteeing bandwidth for VoIP traffic, and limiting bandwidth for non-VoIP traffic, both govern throughput on the security device. DSCP marking enables you to preserve your priority-queuing settings downstream and to keep or change the received DSCP value set by the originating networking device or upstream router so that the next-hop router, typically the LAN or WAN edge router, can enforce Quality of Service (QoS) in its DiffServ domain. In VPN configurations, the security device marks the outer header of the IP packet (if the policy is configured to do so), or leaves the TOS byte as 0, so that the next-hop router can enforce the correct QoS on the encrypted traffic. For information about how DSCP works with priority levels in policies, see “Traffic Shaping” on page 185.

Figure 20 on page 63 shows how priority-level settings can affect guaranteed bandwidth (gbw) and maximum bandwidth (mbw) usage on an ethernet1 (2 Mbps) interface. The illustration assumes you have determined you need to support at least eight VoIP calls (8 x 64 Kbps bandwidth per call, for a total of 512 Kbps) and occasionally as many as 16 calls. You have guaranteed the remaining bandwidth to general office traffic and have set maximum bandwidth for your office traffic to include bandwidth not guaranteed to VoIP. This creates a 512 Kbps overlap of maximum bandwidth for VoIP and office-traffic services, shown by the dashed lines.

The left side of Figure 20 shows what bandwidth usage with these settings looks like with high office-traffic usage and low VoIP traffic usage on the interface. If VoIP traffic suddenly needs more bandwidth, it cannot get it unless it has a higher priority than the office-traffic services. The right side of Figure 20 shows what bandwidth usage looks like in the same circumstance when you give VoIP traffic a higher priority and set office traffic to a lower priority. For more information about configuring bandwidth and priority levels, see “Traffic Shaping” on page 205.

Figure 20: Priority-Level Settings



Chapter 3

Media Gateway Control Protocol Application Layer Gateway

This chapter presents an overview of the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG) and lists the firewall security features of the implementation. Examples of typical scenarios follow a summary of the MGCP architecture. This chapter includes the following sections:

- “Overview” on this page
- “MGCP Security” on page 66
- “About MGCP” on page 66
- “Examples” on page 71

Overview

The Media Gateway Control Protocol (MGCP) is supported on security devices in route mode, transparent mode, and network address translation (NAT) mode. MGCP is a text-based Application Layer protocol used for call setup and control. MGCP is based on a master-slave call control architecture in which the media gateway controller, via the call agent, maintains call control intelligence, while the media gateways carry out the instructions of the call agent.

The MGCP ALG performs the following procedures:

- Conducts VoIP signaling payload inspection. The payload of the incoming VoIP signaling packet is fully inspected based on related RFCs and proprietary standards. Any malformed packet attack is blocked by the ALG.
- Conducts MGCP signaling payload inspection. The payload of the incoming MGCP signaling packet is fully inspected in accordance with RFC3435. Any malformed-packet attack is blocked by the ALG.
- Provides stateful processing. The corresponding VoIP-based state machines are invoked to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.

- Performs Network Address Translation (NAT). Any embedded IP address and port information in the payload is properly translated based on the existing routing information and network topology, and is replaced with the translated IP address and port number, if necessary.
- Manages pinholes for VoIP traffic. To keep the VoIP network secure, the IP address and port information used for media or signaling is identified by the ALG, and any needed pinhole is dynamically created and closed during call setup.

MGCP Security

The MGCP ALG includes the following security features:

- Denial of Service (DoS) attack protection.—the ALG performs stateful inspection at the UDP packet level, the transaction level, and at the call level. MGCP packets matching the RFC3435 message format, transaction state, and call state, are processed. All other messages are dropped.
- Firewall policy enforcement between gateway and gateway controller (signaling policy).
- Firewall policy enforcement between gateways (media policy).
- Per-gateway MGCP message flooding control. Any malfunctioning or hacked gateway will not disrupt the whole VoIP network. Combined with per-gateway flooding control, damage is contained within the impacted gateway.
- Per-gateway MGCP connection flooding control.
- Seamless switchover/failover if calls, including calls in progress, are switched to the standby firewall in case of system failure.

About MGCP

MGCP is a text-based, application layer protocol that can be used for call setup and control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.

Entities in MGCP

There are four basic entities in MGCP:

- “Endpoint” on page 67
- “Connection” on page 67
- “Call” on page 67
- “Call Agent” on page 67

Endpoint

A media gateway (MG) is a collection of endpoints. An endpoint can be an analog line, trunk, or any other access point. An endpoint is named as below:

local-endpoint-name@domain-name

The following are some valid endpoint IDs:

group1/Trk8@mynetwork.net

group2/Trk1/*@[192.168.10.8] (wild-carding)

\$_@voiptel.net (any endpoint within the MG)

*@voiptel.net (all endpoints within the MG)

Connection

Connections are created on each endpoint by a MG during call setup. A typical VoIP call involves two connections. A complex call, for example a three-party call or conference call, might require more connections. The media gateway controller (MGC) can instruct media gateways to create, modify, delete and audit a connection.

A connection is identified by its connection ID which is created by the MG when it is requested to create a connection. Connection ID is presented as a hexadecimal string, and its maximum length is 32 characters

Call

A call is identified by its call ID, which is created by the MGC when establishing a new call. Call ID is a hexadecimal string with a maximum length of 32 characters. Call ID is unique within the MGC. Two or more connections can have the same call ID if they belong to the same call.

Call Agent

One or more call agents (also called media gateway controllers) are supported in MGCP to enhance reliability in VoIP network. The following are two examples of call agent names:

CallAgent@voipCA.mynetwork.com

voipCA.mynetwork.com

Several network addresses can be associated under one domain name in the Domain Name System (DNS). By keeping track of the time to live (TTL) of DNS query/response data and implementing retransmission using other alternative network addresses, switchover and failover is achieved in MGCP.

The concept of *notified entity* is essential in MGCP. The notified entity for an endpoint is the call agent currently controlling that endpoint. An endpoint should send any MGCP command to its notified entity. However, different call agents might send MGCP commands to this endpoint.

The notified entity is set to a provisioned value upon startup, but could be changed by a call agent through the use of a *NotifiedEntity* parameter contained in a MGCP message. If the notified entity for an endpoint is empty or has not been set explicitly, its value defaults to the source address of the last successful non-audit MGCP command received for that endpoint.

Commands

The MGCP protocol defines nine commands for controlling endpoints and connections. All commands are composed of a command header, optionally followed by session description protocol (SDP) information. A command header has the following elements:

- A command line: command verb + transaction ID + endpointId + MGCP version.
- Zero or more parameter lines, composed of a parameter name followed by a parameter value.

Table 3 lists supported MGCP commands, with a description of each, the command syntax, and examples. Refer to RFC 2234 for a complete explanation of command syntax.

Table 3: MGCP Commands

Command Verb	Description	Command Syntax	Examples
EPCF	EndpointConfiguration—used by a call agent to inform a gateway of coding characteristics (a-law or mu-law) expected by the line side of the endpoint.	ReturnCode [PackageList] EndpointConfiguration (EndpointId, [BearerInformation])	EPCF 2012 wxx/T2@mynet.com MGCP 1.0 B: e:mu
CRCX	CreateConnection—used by a call agent to instruct the gateway to create a connection with, and endpoint inside, the gateway.	ReturnCode, [ConnectionId,] [SpecificEndPointId,] [LocalConnectionDescriptor,] [SecondEndPointId,] [SecondConnectionId,][PackageList] CreateConnection (CallId, EndpointId, [NotifiedEntity,] [LocalConnectionOption,] Mode, [RemoteConnectionDescriptor SecondEndPointId},] [encapsulated RQNT,] [encapsulated EPCF])	CRCX 1205 aaIn/1@gw-25.att.net MGCP 1.0 C: A3C47F21456789F0 L: p:10, a:PCMU M: sendrecv X: 0123456789AD R: L/hd S: L/rg v = 0 o = - 25678 753849 IN IP4 128.96.41.1 s = - c = IN IP4 128.96.41.1 t = 0 0 m = audio 3456 RTP/AVP 0

Command Verb	Description	Command Syntax	Examples
MDCX	ModifyConnection—used by a call agent to instruct a gateway to change the parameters for an existing connection.	ReturnCode, [LocalConnectionDescriptor,] [PackageList] ModifyConnection (CallId, EndpointId, ConnectionId, [NotifiedEntity,] [LocalConnectionOption,] [Mode,] [RemoteConnectionDescriptor ,] [encapsulated RQNT,] [encapsulated EPCF])	MDCX 1210 aaln/1@rgw-25.att.net MGCP 1.0 C: A3C47F21456789F0 I: FDE234C8 M: recvonly X: 0123456789AE R: L/hu S: G/rt v = 0 o = - 4723891 7428910 IN IP4 128.96.63.25 S = - c = IN IP4 128.96.63.25 t = 0 0 m = audio 3456 RTP/AVP 0
DLCX	DeleteConnection—used by a call agent to instruct a gateway to delete an existing connection. DeleteConnection can also be used by a gateway to release a connection that can no longer be sustained.	ReturnCode, ConnectionParameters, [PackageList] DeleteConnection (CallId, EndpointId, ConnectionId, [NotifiedEntity,] [encapsulated RQNT,] [encapsulated EPCF])	Example 1: MGC -> MG DLCX 9210 aaln/1@rgw-25.att.net MGCP 1.0 C: A3C47F21456789F0 I: FDE234C8 Example 2: MG -> MGC DLCX 9310 aaln/1@rgw-25.att.net MGCP 1.0 C: A3C47F21456789F0 I: FDE234C8 E: 900 - Hardware error P: PS = 1245, OS = 62345, PR = 780, OR = 45123, PL = 10, JI = 27, LA = 48
RQNT	The NotificationRequest command is used by a call agent to instruct a MG to monitor for certain event(s) or signal(s) for a specific endpoint.	ReturnCode, [PackageList] NotificationRequest (EndpointId, [NotifiedEntity,] [RequestedEvents,] RequestIdentifier, [DigitMap,] [SignalRequests,] [QuarantineHandling,] [DetectEvents,] [encapsulated EPCF])	RQNT 1205 aaln/1@rgw-25.att.net MGCP 1.0 N: ca-new@callagent-ca.att.net X: 0123456789AA R: L/hd(A, E(S(L/dl),R(L/oc,L/hu,D/[0-9#*T](D)))) D: (0T 00T xx 91xxxxxxxxxx 9011x.T) S: T: G/ft
NTFY	Notify—used by a gateway to inform the call agent when requested event(s) or signal(s) occur.	ReturnCode, [PackageList] Notify (EndpointID, [NotifiedEntity,] RequestIdentifier, ObservedEvents)	NTFY 2002 aaln/1@rgw-25.att.net MGCP 1.0 N: ca@ca1.att.net :5678 X: 0123456789AC O: L/hd,D/9,D/1,D/2,D/0,D/1,D/8,D/2,D/9,D/4, D/2,D/6,D/6

Command Verb	Description	Command Syntax	Examples
AUEP	AuditEndpoint—used by a call agent to audit the status of the endpoint.	ReturnCode, EndPointIdList, { [RequestedEvents,] [QuarantineHandling,] [DigitMap,] [SignalRequests,] [RequestedIdentifier,] [NotifiedEntity,] [ConnectionIdentifier,] [DetectEvents,] [ObservedEvents,] [EventStats,] [BearerInformation,] [BearerMethod,] [RestartDelay,] [ReasonCode,] [MaxMGCPDatagram,] [Capabilities]} [PackageList] AuditEndpoint (EndpointId, [RequestedInfo])	Example 1: AUEP 1201 <u>aaln/1@rgw-25.att.net</u> MGCP 1.0 F: A, R,D,S,X,N,I,T,O Example 2: AUEP 1200 * <u>@rgw-25.att.net</u> MGCP 1.0
AUCX	AuditConnection—used by a call agent to collect the parameters applied to a connection.	ReturnCode, [CallId,] [NotifiedEntity,] [LocalConnectionOptions,] [Mode,] [RemoteConnectionDescriptor,] [LocalConnectionDescriptor,] [ConnectionParameters,] [PackageList] AuditConnection (EndpointId, ConnectionId, RequestedInfo)	AUCX 3003 <u>aaln/1@rgw-25.att.net</u> MGCP 1.0 I: 32F345E2 F: C,N,L,M,LC,P
RSIP	RestareInProgress—used by a gateway to notify a call agent that one or more endpoints are being taken out of service or placed back in service.	ReturnCode, [NotifiedEntity,] [PackageList] RestartInProgress (EndpointId, RestartMethod, [RestartDelay,] [ReasonCode])	RSIP 5200 <u>aaln/1@rg2-25.att.net</u> MGCP 1.0 RM: graceful RD: 300

Response Codes

Every command sent by the calling agent or gateway, whether successful or not, requires a response code. The response code is in the header of the response message, and optionally is followed by session description information.

The response header is composed of a response line, followed by zero or more parameter lines, each containing a parameter name letter followed by its value. The response header is composed of a 3-digit response code, transaction ID, and optionally followed by commentary. The response header in the following response message shows the response code 200 (successful completion), followed by ID 1204, and the comment: OK:

```
200 1204 OK
I: FDE234C8
```



```

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 96
a=rtpmap:96 G726-32/8000

```

The ranges of response codes are defined as follows:

- 000 – 099: indicate a response acknowledgement.
- 100 – 199: indicate a provisional response.
- 200 – 299: indicate a successful completion (final response).
- 400 – 499: indicate a transient error (final response).
- 500 – 599: indicate a permanent error (final response).

Refer to RFC 3661 for detailed information about response codes.

A response to a command is sent to the source address of the command, not to the current notified entity. A media gateway can receive MGCP commands from various network addresses simultaneously, and send back responses to corresponding network addresses. However, it sends all MGCP commands to its current notified entity.

Examples

This section includes the following configuration scenarios:

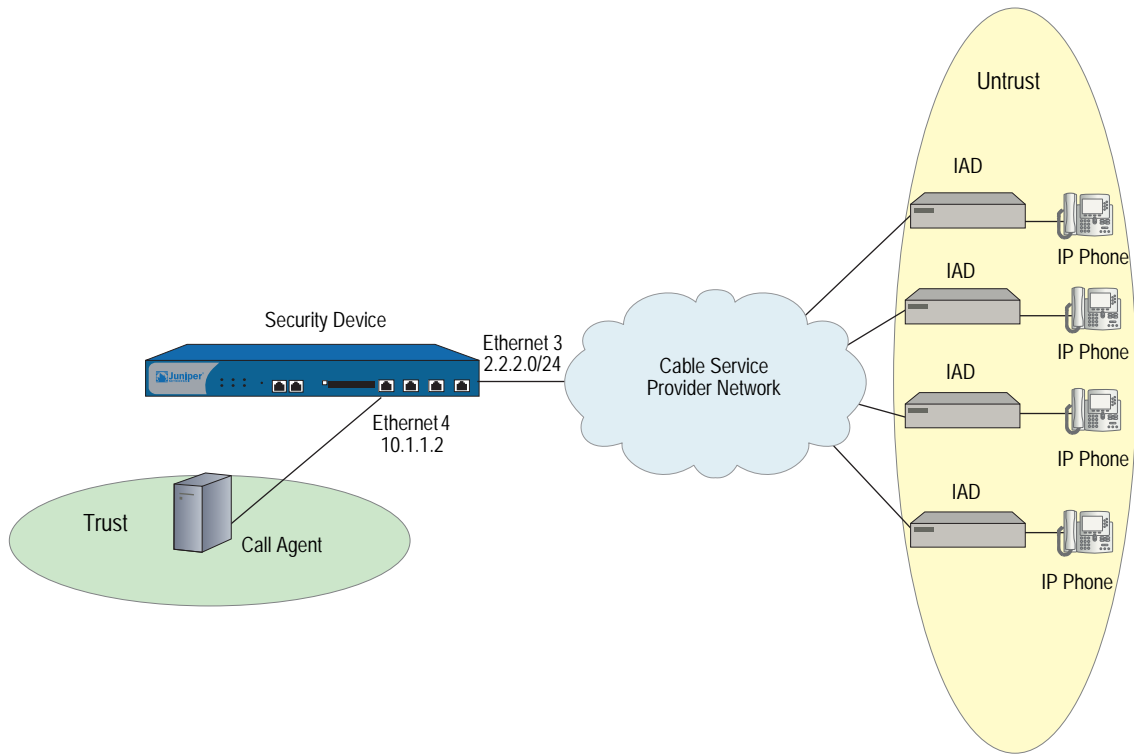
- “Media Gateway in Subscribers’ Homes—Call Agent at the ISP” on this page
- “ISP-Hosted Service” on page 74

Media Gateway in Subscribers’ Homes—Call Agent at the ISP

In this example, (see Figure 21) you configure a security device at a Cable Service Provider to support MGCP for their network of residential subscribers. The security device and the call agent are on the cable service provider’s premises. An integrated Access Device (IAD), or set-top box, is in each subscriber’s home, acting as a gateway—each IAD represents a separate residence. The call agent is in the trust_ca zone; residential customers are in the res_cust zone.

After creating zones—untrust_subscriber for the customers and trust_ca for the service provider, you configure addresses, and then policies. Although gateways frequently reside in different zones, requiring policies for media traffic, in this example both gateways are in the same subnet. RTP traffic between the gateways never passes through the firewall, therefore no policy is needed for media.

Figure 21: Media Gateway in Subscribers' Home



WebUI

1. Zones

Network > Zones > New: Enter the following, then click **OK**:

Zone Name: untrust_subscriber

Network > Zones > New: Enter the following, then click **OK**:

Zone Name: trust_ca

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: SubscriberSubNet
 Comment: Our subscribers' network
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.0/24
 Zone: untrust-subscriber

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: call_agent1
 Comment: Our No. 1 call agent
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.101/32
 Zone: trust_ca

3. Interfaces

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

Zone Name: untrust_subscriber
 Static IP: (select this option when present)
 IP Address/Netmask: 2.2.2.0/24
 Enter the following, then click **OK**:
 Interface Mode: route

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **Apply**:

Zone Name: trust_ca
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.101/32
 Enter the following, then click **OK**:
 Interface Mode: route

4. Policies

Policies > (From: trust-ca To: untrust_subscriber) New: Enter the following, then click **OK**:

Name: Pol-CA-To-Subscribers
 Source Address
 Address Book Entry: (select) call_agent1
 Destination Address
 Address Book Entry: (select) SubscriberSubNet
 Service: MGCP-UA
 Action: Permit

Policies > (From: untrust_subscriber To: trust-ca) New: Enter the following, then click **OK**:

Name: Pol-Subscribers-To-CA
 Source Address
 Address Book Entry: (select) SubscriberSubNet
 Destination Address
 Address Book Entry: (select) call_agent1
 Service: MGCP-CA
 Action: Permit

CLI**1. Zones**

```
set zone name untrust_subscriber
set zone name trust_ca
```

2. Addresses

```
set address untrust_subscriber SubscriberSubNet 2.2.2.0 255.255.255.0 "Our
subscribers' network"
set address trust_ca call_agent1 10.1.1.101 255.255.255.255 "Our No. 1 call
agent"
```

3. Interfaces

```
set interface ethernet3 zone untrust_subscriber "Our subscribers' network"
set interface ethernet3 ip 2.2.2.0/24
set interface ethernet3 route
```

```
set interface ethernet4 zone trust_ca "Our No. 1 call agent"
set interface ethernet4 ip 10.1.1.2/24
set interface ethernet4 route
```

4. Policies

```
set policy name Pol-CA-TO-Subscribers from trust_ca to untrust_subscriber
  call_agent1 SubscriberSubNet mgcp-ua permit
set policy name Pol-Subscribers-To-CA from untrust_subscriber to trust_ca
  SubscriberSubNet call_agent1 mgcp-ca permit
```

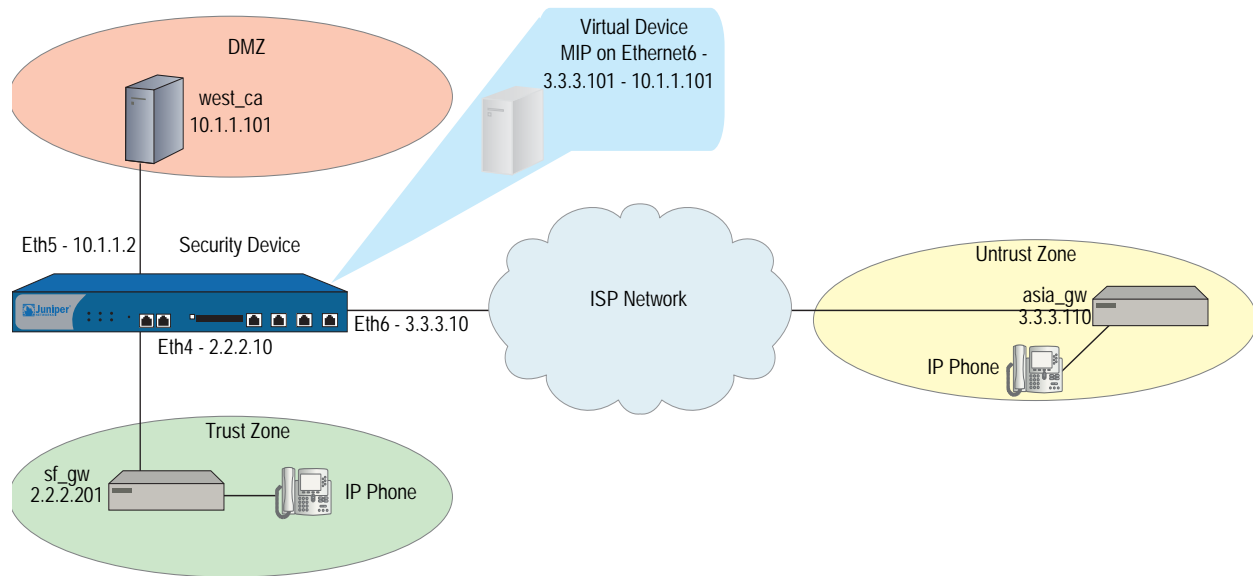
ISP-Hosted Service

In this example, (see Figure 22) an ISP located on the American west coast provides MGCP service to customers in Asia and San Francisco. Asia customers are in the Untrust zone, and supported by the gateway: asia_gw (3.3.3.110); San Francisco customers are in the Trust zone, and supported by the gateway: sf_gw (2.2.2.201). The call agent: west_ca (10.1.1.101) is in the DMZ.

After setting addresses for the gateways and the call agent, you configure the interfaces, putting ethernet4 and ethernet5, which are trusted, in route mode to allow them to stream media directly after call setup. To protect the IP address of the call agent in the DMZ from exposure, you place a MIP on ethernet6, that is, you map the IP address of the call agent (10.1.1.101) to an IP address from the pool of addresses on the ethernet6 interface, in this case: 3.3.3.101.

Finally, you create policies. To allow MGCP signaling between the call agent in the DMZ and the gateway in the Untrust zone, you create one policy for each direction, referencing the MIP that protects the call agent. You create another pair of policies to allow signaling between the call agent and the gateway in the Trust zone. A single policy is sufficient to allow bidirectional communication between gateways in the Trust and Untrust zones.

Figure 22: ISP-Hosted Service



WebUI

1. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: sf_gw
 Comment: gateway in asia
 IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.201/32
 zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: asia_gw
 Comment: gateway in asia
 IP Address/Domain Name:
 IP/Netmask: (select), 3.3.3.110/32
 zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: west_ca
 Comment: ca in west coast
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.101/32
 zone: DMZ

2. Interfaces

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 2.2.2.10/24
 Enter the following, then click **OK**:
 Interface Mode: route

Network > Interfaces > Edit (for ethernet5): Enter the following, then click **Apply**:

Zone Name: DMZ
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.2/24
 Enter the following, then click **OK**:
 Interface Mode: route

Network > Interfaces > Edit (for ethernet6): Enter the following, then click **Apply**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 3.3.3.10/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

3. MIP

Network > Interfaces > Edit (for ethernet6) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 3.3.3.101
 Netmask: 255.255.255.255
 Host IP Address: 10.1.1.101
 Host Virtual Router Name: trust-vr

4. Policies

Policies > (From: DMZ To: Untrust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) west_ca
 Destination Address
 Address Book Entry: (select) asia_gw
 Service: MGCP-UA
 Action: Permit

Policies > (From: Untrust To: DMZ) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) asia_gw
 Destination Address
 Address Book Entry: (select) west_ca
 Service: MGCP-CA
 Action: Permit

Policies > (From: Trust To: DMZ) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) sf_gw
 Destination Address
 Address Book Entry: (select) west_ca
 Service: MGCP-CA
 Action: Permit

Policies > (From: DMZ To: Trust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) west_ca
 Destination Address
 Address Book Entry: (select) sf_gw
 Service: MGCP-UA
 Action: Permit

Policies > (From: Trust To: Untrust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) sf_gw
 Destination Address
 Address Book Entry: (select) asia_gw
 Service: MGCP-UA
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: (select)
 DIP on): None (Use Egress Interface IP)

CLI

1. Addresses

```
set address trust sf_gw 2.2.2.201/32 "gateway in s.f."
set address untrust asia_gw 3.3.3.110/32 "gateway in asia"
set address dmz west_ca 10.1.1.101/32 "ca in west coast"
```

2. Interfaces

```
set interface ethernet4 ip 2.2.2.10/24
set interface ethernet4 route
set interface ethernet4 zone trust
```

```
set interface ethernet5 ip 10.1.1.2/24
set interface ethernet5 route
set interface ethernet5 zone dmz
```

```
set interface ethernet6 ip 3.3.3.10/24
set interface ethernet6 zone untrust
```

3. Mapped IP Address

```
set interface ethernet6 mip 3.3.3.101 host 10.1.1.101 netmask
255.255.255.255 vrouter trust-vr
```

4. Policies

```
set policy from dmz to untrust west_ca asia_gw mgcp-ua permit  
set policy from untrust to dmz asia_gw mip(3.3.3.101) mgcp-ca permit
```

```
set policy from trust to dmz sf_gw west_ca mgcp-ca permit  
set policy from dmz to trust west_ca sf_gw mgcp-ua permit
```

```
set policy from trust to untrust sf_gw asia_gw mgcp-ua nat src permit
```


Chapter 4

Skinny Client Control Protocol Application Layer Gateway

This chapter presents an overview of the Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) and lists the firewall security features of the implementation. Examples of typical scenarios follow a summary of the SCCP architecture. This chapter includes the following sections:

- “Overview” on this page
- “SCCP Security” on page 80
- “Examples” on page 85

Overview

Skinny Client Control Protocol (SCCP) is supported on security devices in Route, Transparent, and Network Address Translation (NAT) modes. SCCP is a binary-based Application-Layer protocol used for Voice-over-Internet Protocol (VoIP) call setup and control. In the SCCP architecture, a Cisco H.323 proxy, known as the Call Manager, does most of the processing. IP phones, also called End Stations, run the Skinny client and connect to a primary (and, if available, a secondary) Call Manager over TCP on port 2000 and register with the primary Call Manager. This connection is then used to establish calls coming to or from the client.

The SCCP ALG supports the following:

- Call flow from a Cisco IP phone to the Call Manager, another Cisco IP phone, and to a Cisco H.323 proxy server.
- Call from a Cisco IP phone to an H.323 terminal.
- Advanced calling features, including call hold, call forwarding, call park, call transfer, and call conferencing.
- Seamless failover—switches over all calls in process to the standby firewall during failure of the primary.
- VoIP signaling payload inspection—fully inspects the payload of incoming VoIP signaling packets based on related RFCs and proprietary standards. Any malformed packet attack is blocked by the ALG.

- SCCP signaling payload inspection—fully inspects the payload of incoming SCCP signaling packets in accordance with RFC 3435. Any malformed-packet attack is blocked by the ALG.
- Stateful processing—invokes the corresponding VoIP-based state machines to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.
- Network Address Translation (NAT)—translates any embedded IP address and port information in the payload, based on the existing routing information and network topology, with the translated IP address and port number, if necessary.
- Pinhole creation and management for VoIP traffic—identifies IP address and port information used for media or signaling and dynamically opens (and closes) pinholes to securely stream the media.

SCCP Security

The SCCP ALG includes the following security features:

- Denial of Service (DoS) attack protection. The ALG performs stateful inspection at the UDP packet level, the transaction level, and the call level. Packets matching the SCCP message format, transaction state, and call state are processed. All other messages are dropped.
- Firewall policy enforcement between Cisco IP phones and the Call Manager (Intra-Cluster).
- Firewall policy enforcement between Call Managers (Inter-Cluster).
- Call Manager flood control. Protects the Call Manager from being flooded with new calls either by an already compromised connected client or by a faulty device.
- Firewall policy enforcement between gateways (media policy).
- Per-gateway SCCP connection flooding control.
- Seamless switchover/failover if calls, including calls in progress, are switched to the standby firewall in case of system failure.

About SCCP

The following sections give a brief overview of SCCP and how it works:

- “SCCP Components” on this page
- “SCCP Transactions” on page 82
- “SCCP Messages” on page 85

SCCP Components

The principle components of the SCCP VoIP architecture include the following:

- SCCP Client
- Call Manager
- Cluster

SCCP Client

The SCCP client runs on an IP phone, also called an End Station, which uses SCCP for signaling and for making calls. In order for a Skinny client to make a call, it must first register with a Primary Call Manager (and a secondary, if available). The connection between the client and the Call Manager is over TCP on port 2000. This connection is then used to establish calls to or from the client. Transmission of media is over RTP, UDP, and IP.

Call Manager

The Call Manager is a Cisco H.323 server with overall control of all devices and communication in the SCCP VoIP network. Its functions include defining, monitoring and controlling SCCP groups, regions of numbers, and route plans; providing initialization, admission and registration of devices on the network; providing a redundant database that contains addresses, phone numbers, and number formats; and initiating contact with called devices or their agents to establish logical sessions in which voice communication can flow.

Cluster

A Cluster is a collection of SCCP clients and a Call Manager. The Call Manager in the cluster knows about all SCCP clients in the cluster. There can be more than one Call Manager for backup in a cluster. Call Manager behavior varies in each of the following cluster scenarios:

- Intra-Cluster, in which the Call Manager knows about each SCCP client, and the call is between SCCP clients of the same cluster.
- Inter-Cluster, in which the Call Manager needs to communicate with another Call Manager using H.323 for call setup.
- Inter-Cluster calls using the gatekeeper for admission control and address resolution.

Call Manager behavior also varies with calls between an SCCP client and a phone in a Public Switched Telephone Network (PSTN), and with calls between an SCCP client and a phone in another administrative domain that is using H323.

SCCP Transactions

SCCP transactions are the processes that need to take place in order for an SCCP call to proceed. SCCP transactions include the following:

- Client Initialization
- Client Registration
- Call Setup
- Media Setup

Client Initialization

To initialize, the SCCP client needs to know the IP address of the Call Manager, its own IP address, and other information about the IP gateway and DNS servers. Initialization takes place on the local LAN. The client sends a Dynamic Host Control Protocol (DHCP) request to get an IP address, the DNS server address, and the TFTP server name and address. The client needs the TFTP server name to download the configuration file: *sepmacaddr.cnf*. If the TFTP name is not given, the client uses the default filename in the IP phone. The client then downloads the configuration file: *.cnf (xml)* from TFTP server. CNF files contain the IP address or addresses of the primary and secondary Cisco Call Manager. With this information, the client contacts the Call Manager to register.

Client Registration

The SCCP client, after initialization, registers with the Call Manager over a TCP connection on well-known default port 2000. The client registers by providing the Call Manager with its IP address, the MAC address of the phone, and other information, such as protocol and version. The client cannot initiate or receive calls until it is registered. Keepalive messages keep this TCP connection open between the client and Call Manager so that the client can initiate or receive calls at any time, provided that a policy on the security device allows this.

Table 4 lists SCCP messages and indicates messages that are of interest to the security device.

Table 4: SCCP Registration Messages

From Client	From Call Manager	Of Interest to Security Device
RegisterMessage		✓
IPortMessage		✓
	RegisterAckMessage	✓
	CapabilitiesRequest	
CapabilitiesResMessage		
ButtonTemplateReqMessage		
	ButtonTemplateResMessage	
SoftKeyTemplateReqMessage		
	SoftKeyTemplateResMessage	
LineStatReqMessage		✓
	LineStatMessage	✓

Call Setup

IP phone-to-IP phone call-setup using SCCP is always handled by the Call Manager. Messages for call setup are sent to the Call Manager, which returns messages appropriate to the status of the call. If call setup is successful, and a policy on the security device allows the call, the Call Manager sends the media setup messages to the client.

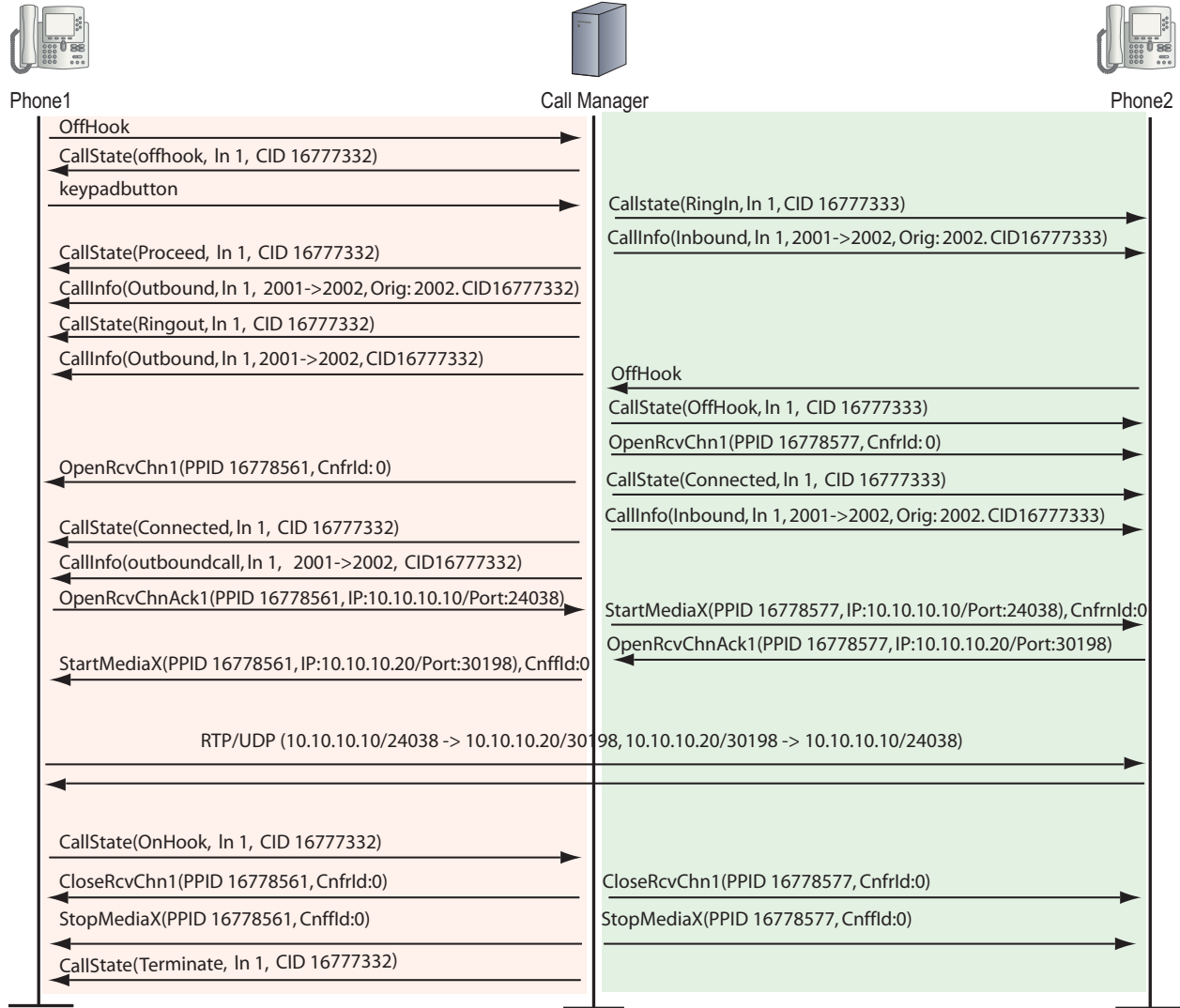
Media Setup

The Call Manager sends the IP address and port number of the called party to the calling party. The Call Manager also sends the media IP address and port number of the calling party to the called party. After media setup, media is transmitted directly between clients. When the call ends, the Call Manager is informed and terminates the media streams. At no time during this process does the Call Manager hand over call-setup function to the client. Media is streamed directly between clients via RTP/UDP/IP.

SCCP Control Messages and RTP Flow

Figure 23 shows the SCCP control messages used to set up and tear down a simple call between *Phone1* and *Phone2*. Except for the OffHook message initiating the call from *Phone1* and the OnHook message signaling the end of the call, all aspects of the call are controlled by the Call Manager.

Figure 23: Call Setup and Teardown



SCCP Messages

Table 5, Table 6, Table 7, and Table 8 list the SCCP call message IDs in the four intervals allowed by the security device.

Table 5: Station to Call Manager Messages

Message	Range
#define STATION_REGISTER_MESSAGE	0x00000001
#define STATION_IP_PORT_MESSAGE	0x00000002
#define STATION_ALARM_MESSAGE	0x00000020
#define STATION_OPEN_RECEIVE_CHANNEL_ACK	0x00000022

Table 6: Call Manager to Station Messages

Message	Range
#define STATION_START_MEDIA_TRANSMISSION	0x00000001
#define STATION_STOP_MEDIA_TRANSMISSION	0x00000002
#define STATION_CALL_INFO_MESSAGE	0x00000020
#define STATION_OPEN_RECEIVE_CHANNEL_ACK	0x00000022
#define STATION_CLOSE_RECEIVE_CHANNEL	0x00000106

Table 7: Call Manager 4.0 Messages and Post Skinny 6.2

Message	Range
#define STATION_REGISTER_TOKEN_REQ_MESSAGE	0x00000029
#define STATION_MEDIA_TRANSMISSION_FAILURE	0x0000002A
#define STATION_OPEN_MULTIMEDIA_RECEIVE_CHANNEL_ACK	0x00000031

Table 8: Call Manager to Station

Message	Range
#define STATION_OPEN_MULTIMEDIA_RECEIVE_CHANNEL	0x00000131
#define STATION_START_MULTIMEDIA_TRANSMISSION	0x00000132
#define STATION_STOP_MULTIMEDIA_TRANSMISSION	0x00000133
#define STATION_CLOSE_MULTIMEDIA_RECEIVE_CHANNEL	0x00000136

Examples

This section contains the following sample scenarios:

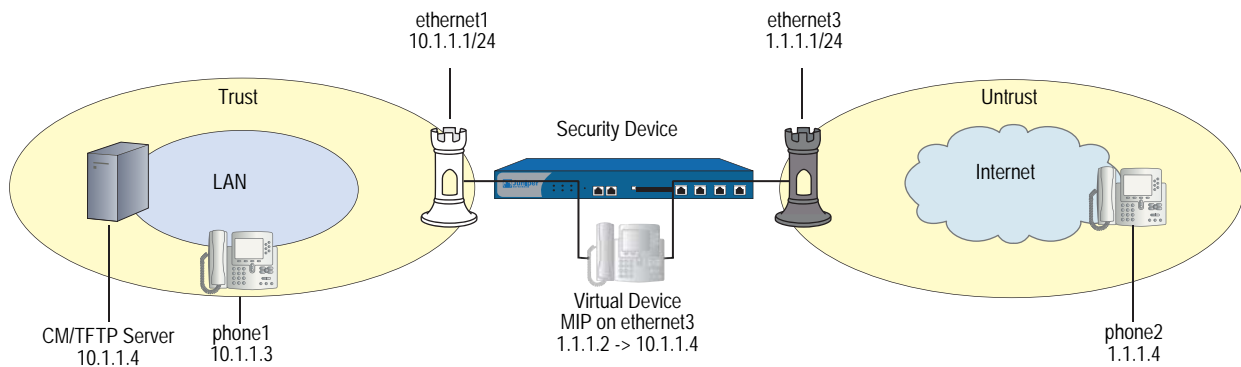
- “Example: Call Manager/TFTP Server in the Trust Zone” on page 86
- “Example: Call Manager/TFTP Server in the Untrust Zone” on page 88
- “Example: Three-Zone, Call Manager/TFTP Server in the DMZ” on page 90

- “Example: Intrazone, Call Manager/TFTP Server in Trust Zone” on page 93
- “Example: Intrazone, Call Manager/TFTP Server in Untrust Zone” on page 97
- “Example: Full-Mesh VPN for SCCP” on page 99

Example: Call Manager/TFTP Server in the Trust Zone

In this example, phone1 and the Call Manager/TFTP Server are on the ethernet1 interface in the Trust (private) zone, and phone2 is on the ethernet3 interface in the Untrust zone. You put a MIP for the Call Manager/TFTP Server on the ethernet3 interface, so that when phone2 boots up it can contact the TFTP Server and obtain the IP address of the Call Manager. (We recommend that you change the IP address of the Call Manager in the TFTP Server config file (sep < mac_addr > .cnf) to the MIP IP address of the Call Manager.) You then create a policy allowing SCCP traffic from the Untrust to the Trust zone and reference that MIP in the policy. You also create a policy from the Trust to the Untrust zone to allow phone1 to call out.

Figure 24: Call Manager/TFTP Server in the Private Zone



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **OK**:

Zone: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: route

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
 IP Address/Netmask: 1.1.1.1/24
 Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: CM-TFTP_Server
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.4/24
 Zone: Trust

3. MIP

Network > Interfaces > Edit (for loopback.3) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.1.2
 Netmask: 255.255.255.255
 Host IP Address: 10.1.1.4
 Host Virtual Router Name: trust-vr

4. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select) any
 Destination Address:
 Address Book Entry: (select) phone2
 Service: SCCP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: (select)
 (DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), phone2
 Destination Address:
 Address Book Entry: (select), MIP(1.1.1.2)
 Service: SCCP
 Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address trust cm-tftp_server 10.1.1.4/24
```

3. MIP

```
set interface ethernet3 mip 1.1.1.2 host 10.1.1.4
```

4. Policies

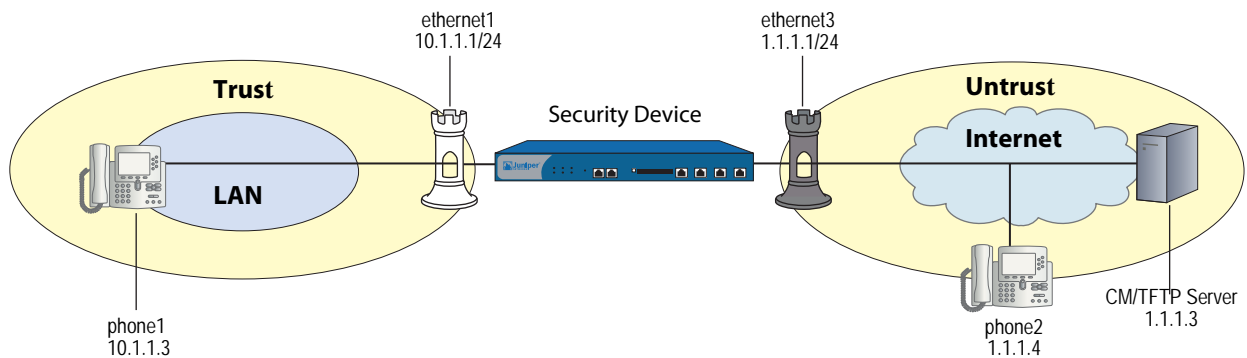
```
set policy from trust to untrust any phone2 sccp nat src permit
set policy from untrust to trust phone2 mip(1.1.1.2) sccp permit
save
```

NOTE: It is always more secure to specify a service explicitly, as shown in this example configuration, than to use the keyword any.

Example: Call Manager/TFTP Server in the Untrust Zone

In this example, phone1 is on the ethernet1 interface in the Trust zone, and phone2 and the Call Manager/TFTP Server are on the ethernet3 interface in the Untrust zone. After configuring interfaces and addresses, you create policy from the Trust zone to the Untrust. This allows phone1 to register with the Call Manager/TFTP Server in the Untrust zone.

Figure 25: Call Manager/TFTP Server in the Untrust Zone



WebUI**1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone Name: Trust
 Static IP: (select this option when present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: route

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select this option when present)
 IP Address/Netmask: 1.1.1.1/24
 Interface Mode: Route

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: CM/TFTP Server
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.3/24
 Zone: Untrust

3. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address
 Address Book Entry: (select) phone1
 Destination Address
 Address Book Entry: (select) any
 Service: SCCP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: (select)
 (DIP on): None (Use Egress Interface IP)

CLI**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust cm-tftp_server 1.1.1.3/24
```

3. Policies

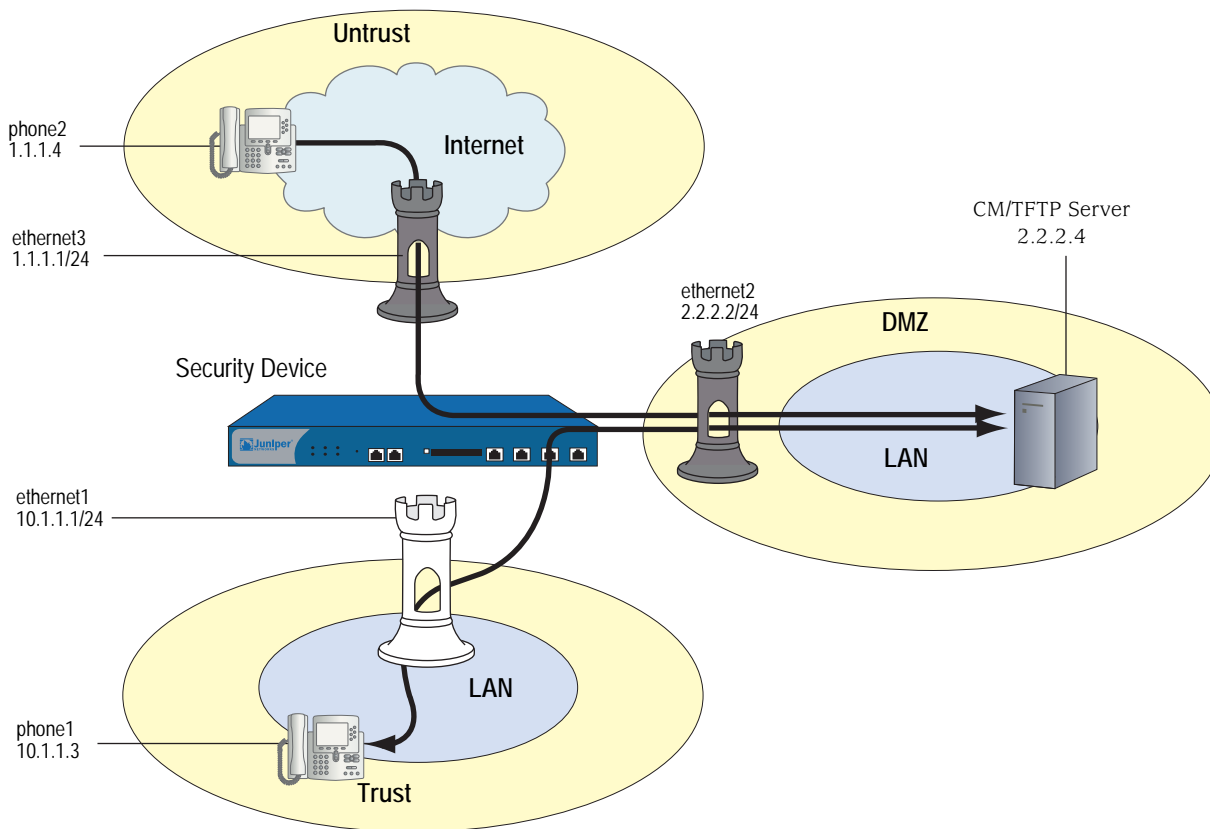
```
set policy from trust to untrust phone1 any sccp nat src permit
save
```

NOTE: It is always more secure to specify a service explicitly, as shown in this example configuration, than to use the keyword `any`.

Example: Three-Zone, Call Manager/TFTP Server in the DMZ

In this example, phone1 is on the ethernet1 interface in the Trust zone, phone2 is on the ethernet3 interface in the Untrust zone, and the Call Manager/TFTP Server is on the ethernet2 interface in the DMZ. For signalling, you create a policy from the Trust zone to the DMZ to allow phone1 to communicate with the Call Manager/TFTP Server, and you create a policy from the Untrust zone to the DMZ to allow phone2 to communicate with the Call Manager/TFTP Server. For transmission of media, you create a policy from Trust to Untrust to allow phone1 and phone2 to communicate directly. The arrows in Figure 26 show the flow of SCCP signaling traffic when phone2 in the Untrust zone places a call to phone1 in the Trust zone. After the session is initiated, the media flows directly between phone1 and phone2.

Figure 26: Call Manager/TFTP Server in the DMZ



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.1.1/24
 Enter the following, then click **OK**:
 Interface Mode: NAT

Network > Interfaces > Edit (for ethernet2): Enter the following, then click **OK**:

Zone Name: DMZ
 Static IP: (select when this option is present)
 IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone Name: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.1.1/24

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/24
Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: CM-TFTP_Server
IP Address/Domain Name:
 IP/Netmask: (select), 2.2.2.4/24
Zone: DMZ

3. Policies

Policies > (From: Trust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), phone1
Destination Address:
 Address Book Entry: (select), CM-TFTP_Server
Service: SCCP
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

NAT:
Source Translation: Enable
 (DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: DMZ) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), phone2
Destination Address:
 Address Book Entry: (select), CM-TFTP_Server
Service: SCCP
Action: Permit

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), phone1
Destination Address:
 Address Book Entry: (select), phone2
Service: SCCP
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

```
NAT:
Source Translation: Enable
(DIP on): None (Use Egress Interface IP)
```

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.2.2.2/24
set interface ethernet2 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address dmz cm-tftp_server 2.2.2.4
```

3. Policies

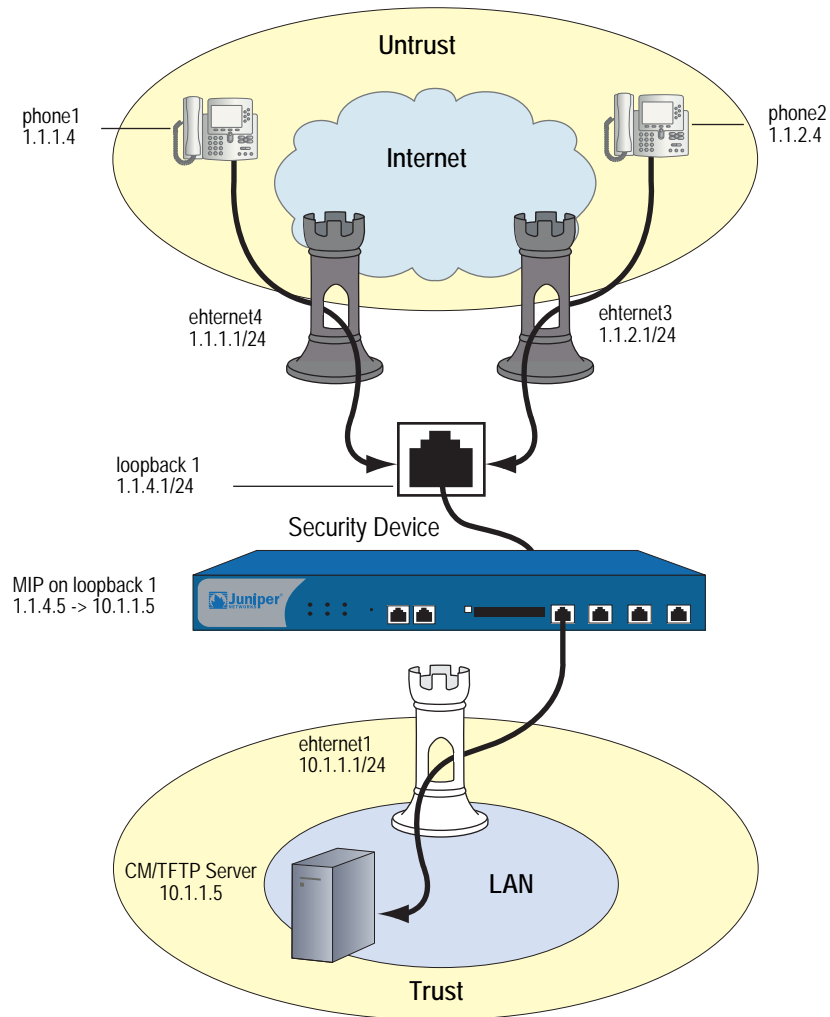
```
set policy from trust to dmz phone1 cm-tftp_server sccp nat src permit
set policy from untrust to dmz phone2 cm-tftp_server sccp permit
set policy from trust to untrust phone1 phone2 sccp nat src permit
save
```

NOTE: It is always more secure to specify a service explicitly, as shown in this example configuration, than to use the keyword `any`.

Example: Intrazone, Call Manager/TFTP Server in Trust Zone

In this example, phone1 is on the ethernet4 interface in the Untrust zone, phone2 is in a subnet on the ethernet3 interface in the Untrust zone, and the Call Manager/TFTP Server is on the ethernet1 interface in the Trust zone. To allow intrazone SCCP traffic between the two phones in the Untrust zone, you create a loopback interface, add ethernet3 and ethernet4 to a loopback group, then put a MIP on the loopback interface to the IP address of the Call Manager/TFTP Server. Creating a loopback interface enables you to use a single MIP for the Call Manager/TFTP Server in the Trust zone. (For more information about using loopback interfaces, see “MIP and the Loopback Interface” on page 8-73.) And finally, because intrazone blocking is on by default, you unset blocking in the Untrust zone to allow intrazone communication.

Figure 27: Intrazone, Call Manager/TFTP Server in Trust Zone



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.1.1/24

Enter the following, then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **OK**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > New Loopback IF: Enter the following, then click **OK**:

Interface Name: loopback.1
 Zone: Untrust (trust-vr)
 IP Address/Netmask: 1.1.4.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: CM-TFTP_Server
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.5/32
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.1.4/32
 Zone: Untrust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 1.1.2.4/32
 Zone: Untrust

3. Loopback Group

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

As member of loopback group: (select) loopback.1
 Zone Name: Untrust

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **OK**:

As member of loopback group: (select) loopback.1
 Zone Name: Untrust

4. MIP

Network > Interfaces > Edit (for loopback.1) > MIP > New: Enter the following, then click **OK**:

Mapped IP: 1.1.4.5
 Netmask: 255.255.255.255
 Host IP Address: 10.1.1.5
 Host Virtual Router Name: trust-vr

5. Blocking

Network > Zones > Edit (for Untrust): Enter the following, then click **OK**:

Block Intra-Zone Traffic: (clear)

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:

Address Book Entry: (select), CM-TFTP_Server

Destination Address:

Address Book Entry: (select), Any

Service: SCCP

Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:

Source Translation: Enable

(DIP on): None (Use Egress Interface IP)

Policies > (From: Untrust, To: Trust) New: Enter the following, then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), MIP(1.1.4.5)

Service: SCCP

Action: Permit

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.2.1/24
set interface ethernet3 route
set interface ethernet4 zone untrust
set interface ethernet4 ip 1.1.1.1/24
set interface ethernet4 route
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.4.1/24
set interface loopback.1 route
```

2. Addresses

```
set address trust cm-tftp_server 10.1.1.5/32
set address untrust phone1 1.1.1.4/32
set address untrust phone2 1.1.2.4/32
```

3. Loopback Group

```
set interface ethernet3 loopback-group loopback.1
set interface ethernet4 loopback-group loopback.1
```

4. MIP

```
set interface loopback.1 mip 1.1.4.5 host 10.1.1.5
```

5. Blocking

```
unset zone untrust block
```

6. Policies

```
set policy from trust to untrust cm/tftp_server any sccp nat src permit
set policy from untrust to trust any mip(1.1.4.5) sccp permit
save
```

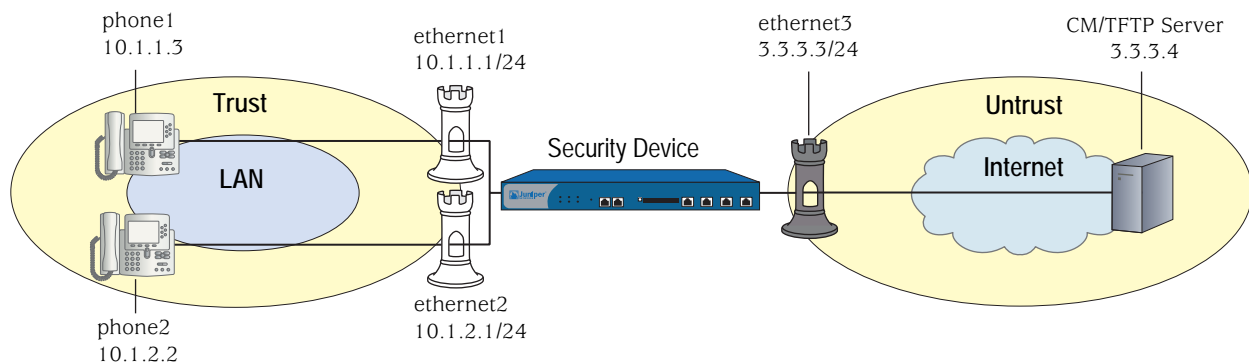
NOTE: Although, in this example, you unset blocking in the Untrust zone to allow intrazone communication, you can accomplish the same thing by creating the following policy:

```
set policy from untrust to untrust any any sccp permit
```

Note, also, that it is always more secure to specify a service explicitly, as shown in this example configuration, than to use the keyword **any**.

Example: Intrazone, Call Manager/TFTP Server in Untrust Zone

In this example, phone1 is on the ethernet1 interface in the Trust zone, phone 2 is on the ethernet2 interface in a subnet in the Trust zone, and the Call Manager/TFTP Server is on the ethernet3 interface in the Untrust zone. After configuring interfaces and addresses, you create a policy from Trust to Untrust to allow phone1 and phone2 to register with the Call Manager/TFTP Server in the Untrust zone. Blocking is off by default in the Trust zone (as it is in custom zones you define), so it is not necessary to create. However, for greater security, you could optionally turn blocking off, and create a policy from Trust to Trust. This would allow you to specify the SCCP service, and restrict intrazone calls to phone1 and phone2.

Figure 28: Intrazone, Call Manager/TFTP Server in Trust Zone**WebUI****1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

```
Zone: Trust
Static IP: (select when this option is present)
IP Address/Netmask: 10.1.1.1/24
Enter the following, then click OK:
Interface Mode: route
```

Network > Interfaces > Edit (for ethernet2): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.2.1/24
 Enter the following, then click **OK**:
 Interface Mode: route

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **OK**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 3.3.3.3/24

2. Addresses

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.1.3/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IP Address/Domain Name:
 IP/Netmask: (select), 10.1.2.2/24
 Zone: Trust

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: CM/TFTP Server
 IP Address/Domain Name:
 IP/Netmask: (select), 3.3.3.4/24
 Zone: Untrust

3. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

Source Address:
 Address Book Entry: (select), Any
 Destination Address:
 Address Book Entry: (select), CM/TFTP Server
 Service: SCCP
 Action: Permit

> Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

NAT:
 Source Translation: Enable
 (DIP on): None (Use Egress Interface IP)

CLI**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet3 route
```

2. Addresses

```
set address trust phone1 10.1.1.3/24
set address trust phone2 10.1.2.2/24
set address untrust cm-tftp_server 3.3.3.4/24
```

3. Policies

```
set policy from trust to untrust any cm-tftp_server sccp nat src permit
save
```

NOTE: It is always more secure to specify a service explicitly, as shown in this example configuration, than to use the keyword `any`.

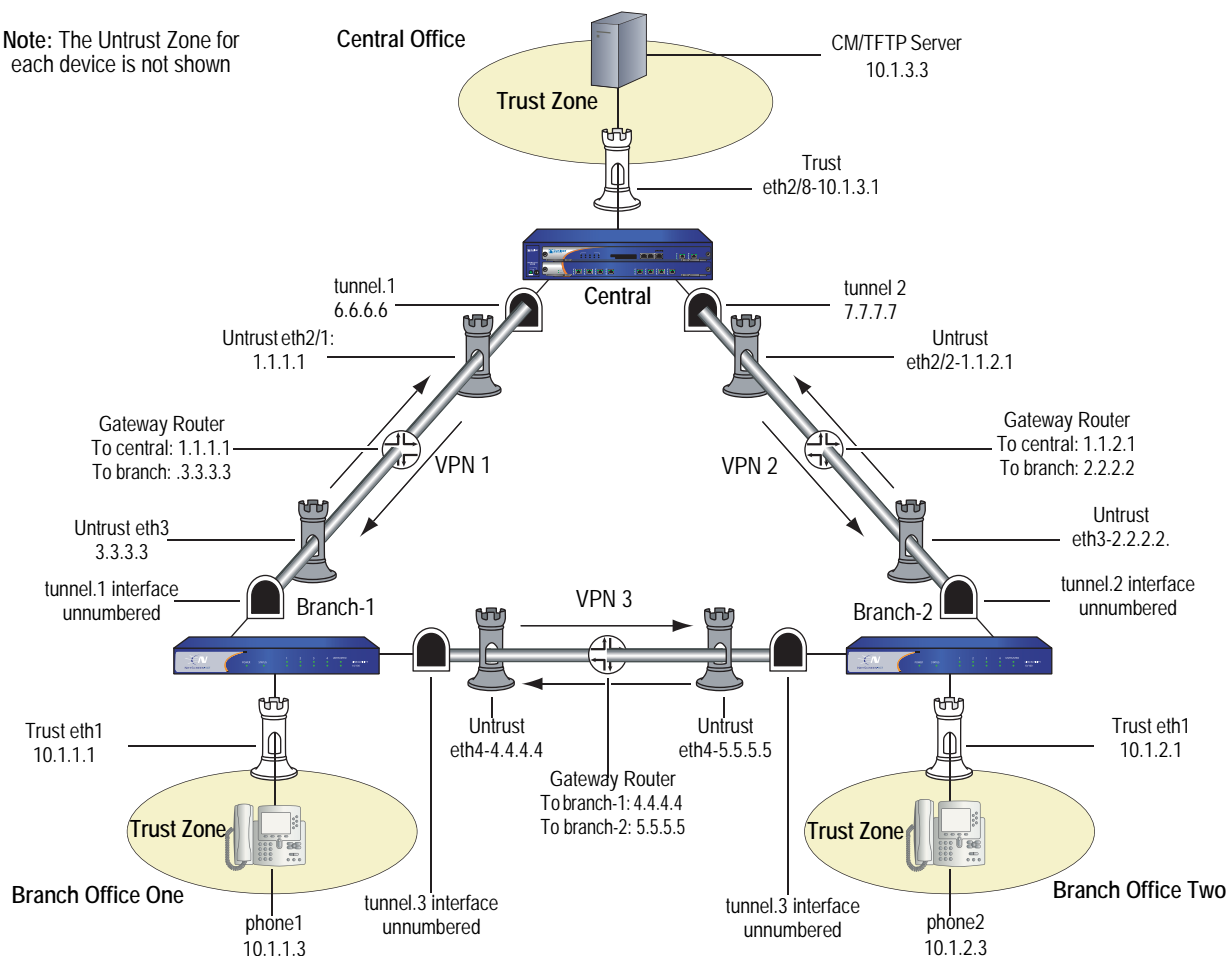
Example: Full-Mesh VPN for SCCP

In this example, the central office and two branch offices are linked by a full-mesh VPN. Each site has a single security device. The Call Manager/TFTP Server is in the Trust zone at the Central Office, phone1 is in the Trust zone at Branch Office One, and phone2 is in the Trust zone at Branch Office Two. All interfaces connecting the devices are in their respective Untrust zones. On each device, you configure two tunnels, one to each of the other devices, to create a fully meshed network.

NOTE: The security devices used in this example must have at least three independently configurable interfaces available.

Figure 29: Full-Mesh VPN for SCCP

Note: The Untrust Zone for each device is not shown



NOTE: It is always more secure to explicitly specify a service, as shown in this example configuration, than to use the keyword any.

WebUI (for Central)

1. Interfaces

Network > Interfaces > Edit (for ethernet2/1): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (for ethernet2/2): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 1.1.2.1/24

Network > Interfaces > Edit (for ethernet2/8): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.3.1/24
 Enter the following, then click **OK**:
 Interface mode: route

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 1
 Zone (VR): Untrust
 IP Address / Netmask: 6.6.6.6/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 2
 Zone (VR): Untrust
 IP Address / Netmask: 7.7.7.7/24

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: CM/TFTP Server
 IPv4/Netmask: 10.1.3.3/32
 Zone: Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-branch-1
 Security Level: Standard
 IPv4/v6 Address/Hostname: 3.3.3.3
 Preshare Key: netscreen
 Outgoing Interface: ethernet2/1

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-branch-1

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to: (select) Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-branch-2
 Security Level: Standard
 IPv4/v6 Address/Hostname: 2.2.2.2
 Preshare Key: netscreen
 Outgoing Interface: ethernet2/2

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-branch-2

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to: (select) Tunnel Interface, tunnel.2

4. Routing

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.1.0/24
Interface (select): tunnel.1

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.2.0/24
Interface (select): tunnel.2

5. Policies

Policies > (From: Trust, To: Untrust) New Enter the following, then click **OK**:

Source Address (select) Address Book Entry: CM/TFTP Server
Destination Address (select) Address Book Entry: Any-IPv4
Service: SCCP
Action: Permit

Policies > (From: Untrust, To: Trust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Any-IPv4
Destination Address (select) Address Book Entry: CM/TFTP Server
Service: SCCP
Action: Permit

CLI (for Central)

1. Interfaces

```
set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 1.1.1.1/24
set interface ethernet2/2 zone untrust
set interface ethernet2/2 ip 1.1.2.1/24
set interface ethernet2/8 zone trust
set interface ethernet2/8 ip 10.1.3.1/24
set interface ethernet2/8 route
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 6.6.6.6/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip 7.7.7.7/24
```

2. Address

```
set address trust cm-tftp_server 10.1.3.3/32
```


3. VPN

```

set ike gateway to-branch-1 address 3.3.3.3 main outgoing-interface ethernet2/1
  preshare "netscreen" sec-level standard
set ike gateway to-branch-2 address 2.2.2.2 main outgoing-interface ethernet2/2
  preshare "netscreen" sec-level standard
set vpn vpn-branch-1 gateway to-branch-1 no-reply tunnel idletime 0 sec-level
  standard
set vpn vpn-branch-1 id 1 bind interface tunnel.1
set vpn vpn-branch-2 gateway to-branch-2 no-reply tunnel idletime 0 sec-level
  standard
set vpn vpn-branch-2 id 2 bind interface tunnel.2

```

4. Routing

```

set route 10.1.2.0/24 interface tunnel.2
set route 10.1.1.0/24 interface tunnel.1

```

5. Policies

```

set policy from trust to untrust cm-tftp_server any sccp permit
set policy from untrust to trust any cm-tftp_server sccp permit
save

```

WebUI (for Branch Office 1)**1. Interfaces**

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

```

Zone: Trust
Static IP: (select when this option is present)
IP Address/Netmask: 10.1.1.1/24
Interface mode: route

```

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

```

Zone: Untrust
Static IP: (select when this option is present)
IP Address/Netmask: 3.3.3.3/24

```

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **Apply**:

```

Zone: Untrust
Static IP: (select when this option is present)
IP Address/Netmask: 4.4.4.4/24

```

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

```

Tunnel Interface Name: 2
Zone (VR): Untrust
Unnumbered (select) Interface: ethernet3

```

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

```

Tunnel Interface Name: 3
Zone (VR): Untrust
Unnumbered (select) Interface: ethernet4

```

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone1
IPv4/Netmask: 10.1.1.3/32
Zone: V1-Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-central
Security Level: Standard
IPv4/v6 Address/Hostname: 1.1.2.1
Preshare Key: netscreen
Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-central

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to (select): Tunnel Interface, tunnel.1

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-ns50
Security Level: Standard
IPv4/v6 Address/Hostname: 5.5.5.5
Preshare Key: netscreen
Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-ns50

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page::

Bind to (select): Tunnel Interface, tunnel.3

4. Routing

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.2.0/24
Interface (select): tunnel.3

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.3.0/24
Interface (select): tunnel.1

5. Policies

Policies > (From: Trust, To: Untrust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: phone2
 Destination Address (select) Address Book Entry: Any-IPv4
 Service: SCCP
 Action: Permit

Policies > (From: Untrust, To: Trust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Any-IPv4
 Destination Address (select) Address Book Entry: phone2
 Service: SCCP
 Action: Permit

CLI (for Branch Office 1)**1. Interfaces**

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. Address

```
set address trust phone1 10.1.1.3/32
```

3. VPN

```
set ike gateway to-central address 1.1.1.1 main outgoing-interface ethernet3
  preshare "netscreen" sec-level standard
set ike gateway to-ns50 address 5.5.5.5 main outgoing-interface ethernet4
  preshare "netscreen" sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
set vpn vpncentral bind interface tunnel.1
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 bind interface tunnel.3
```

4. Routes

```
set route 10.1.2.0/24 interface tunnel.3
set route 10.1.3.0/24 interface tunnel.1
```

5. Policies

```
set policy from trust to untrust phone1 any sccp permit
set policy from untrust to trust any phone1 sccp permit
save
```

WebUI (for Branch Office 2)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, then click **Apply**:

Zone: Trust
 Static IP: (select when this option is present)
 IP Address/Netmask: 10.1.2.1/24
 Enter the following, then click **OK**:
 Interface mode: route

Network > Interfaces > Edit (for ethernet3): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Edit (for ethernet4): Enter the following, then click **Apply**:

Zone: Untrust
 Static IP: (select when this option is present)
 IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 2
 Zone (VR): Untrust
 Unnumbered (select) Interface: ethernet3

Network > Interfaces > New Tunnel IF: Enter the following, then click **Apply**:

Tunnel Interface Name: 3
 Zone (VR): Untrust
 Unnumbered (select) Interface: ethernet4

2. Address

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: phone2
 IPv4/Netmask: 10.1.2.3/32
 Zone: Trust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-central
 Security Level: Standard
 IPv4/v6 Address/Hostname: 1.1.2.1
 Preshare Key: netscreen
 Outgoing Interface: ethernet3

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-central

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to (select): Tunnel Interface, tunnel.2

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

Gateway Name: to-ns50

Security Level: Standard

IPv4/v6 Address/Hostname: 4.4.4.4

Preshare Key: netscreen

Outgoing Interface: ethernet4

VPNs > AutoKey IKE > New: Enter the following, then click **OK**:

VPN Name: vpn-ns50

Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Bind to (select): Tunnel Interface, tunnel.3

4. Routing

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.3.0/24

Interface (select): tunnel.2

Network > Routing > Destination > New: Enter the following, then click **OK**:

Network Address / Netmask: 10.1.1.0/24

Interface (select): tunnel.3

5. Policies

Policies > (From: Trust, To: Untrust) New Enter the following, then click **OK**:

Source Address (select) Address Book Entry: phone2

Destination Address (select) Address Book Entry: Any-IPv4

Service: SCCP

Action: Permit

Policies > (From: Untrust, To: Trust) > New: Enter the following, then click **OK**:

Source Address (select) Address Book Entry: Any-IPv4

Destination Address (select) Address Book Entry: phone2

Service: SCCP

Action: Permit

CLI (for Branch Office 2)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.2.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. Address

```
set address trust phone1 10.1.2.3/32
```

3. VPN

```
set ike gateway to-central address 1.1.1.1 Main outgoing-interface ethernet3
  preshare "netscreen" sec-level standard
set ike gateway to-ns50 address 4.4.4.4 Main outgoing-interface ethernet4
  preshare "netscreen" sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level standard
set vpn vpncentral id 4 bind interface tunnel.2
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 id 5 bind interface tunnel.3
```

4. Routes

```
set route 10.1.3.0/24 interface tunnel.1
set route 10.1.2.0/24 interface tunnel.3
```

5. Policies

```
set policy from trust to untrust phone2 any sccp permit
set policy from untrust to trust any phone2 sccp permit
save
```

Index

A

ALG.....	17
SIP.....	13
SIP NAT.....	23

G

gatekeeper devices.....	1
-------------------------	---

M

multimedia sessions, SIP.....	13
-------------------------------	----

P

pinholes.....	19
---------------	----

S

SDP.....	17 to 18
service book, service groups (WebUI).....	63
SIP	
ALG.....	17, 20
connection information.....	18
defined.....	13
media announcements.....	18
messages.....	14
multimedia sessions.....	13
pinholes.....	17
request methods.....	14
response codes.....	16
RTCP.....	18
RTP.....	18
SDP.....	17 to 18
signaling.....	17

SIP NAT

call setup.....	23, 28
defined.....	23
DIP pool, using a.....	35
DIP, using incoming.....	31
DIP, using interface.....	32
incoming, with MIP.....	35, 37
proxy in DMZ.....	44
proxy in private zone.....	39, 86
proxy in public zone.....	41
trust intrazone.....	51
untrust intrazone.....	47, 93
VPN, using full-mesh.....	53, 99

SIP timeouts

inactivity.....	20
media inactivity.....	21, 22
session inactivity.....	20
signaling inactivity.....	21, 22

V

voice-over IP	
bandwidth management.....	62

