Junos® OS

Application Layer Gateways Feature Guide for Security Devices

Release

15.1X49-D70

Modified: 2016-11-16

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS Application Layer Gateways Feature Guide for Security Devices
15.1X49-D70
Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Part 4 **Configuration Statements and Operational Commands**

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- vSRX
- SRX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xvii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xvii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	user@host> **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric* **>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		    route default {
		      nexthop *address*;
		      retain;
		    }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/

- Search for known bugs: http://www2.juniper.net/kb/

- Find product documentation: http://www.juniper.net/techpubs/

- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

- Download the latest versions of software and review release notes:
  http://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications:
  http://kb.juniper.net/InfoCenter/

- Join and participate in the Juniper Networks Community Forum:
  http://www.juniper.net/company/communities/

- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

Introduction to ALGs

ALG Overview

Supported Platforms   SRX Series, vSRX

An Application Layer Gateway (ALG) is a software component that is designed to manage specific protocols such as Session Initiation Protocol (SIP) or FTP on Juniper Networks devices running Junos OS. The ALG module is responsible for Application-Layer aware packet processing.

ALG functionality can be triggered either by a service or application configured in the security policy:

- A service is an object that identifies an application protocol using Layer 4 information (such as standard and accepted TCP and UDP port numbers) for an application service (such as Telnet, FTP, SMTP, and HTTP).

- An application specifies the Layer 7 application that maps to a Layer 4 service.

A predefined service already has a mapping to a Layer 7 application. However, for custom services, you must link the service to an application explicitly, especially if you want the policy to apply an ALG.

ALGs for packets destined to well-known ports are triggered by service type. The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the device:

1. When a packet arrives at the device, the flow module forwards the packet according to the security rule set in the policy.

2. If a policy is found to permit the packet, the associated service type or application type is assigned and a session is created for this type of traffic.

3. If a session is found for the packet, no policy rule match is needed. The ALG module is triggered if that particular service or application type requires the supported ALG processing.

The ALG also inspects the packet for embedded IP address and port information in the packet payload, and performs Network Address Translation (NAT) processing if necessary. The ALG also opens a gate for the IP address and port number to permit data exchange for the session. The control session and data session can be coupled to have the same timeout value, or they can be independent.

ALGs are supported on chassis clusters.

The ALG message buffer optimization is enhanced to reduce high memory consumption. A message buffer is allocated only when the packet is ready to process. The buffer is freed after the packet completes ALG handling, including modifying the payload, performing NAT, opening a pinhole for a new connection between a client and a server, and transferring data between a client and a server located on opposite sides of a Juniper Networks device.

The maximum size of the jbuf is 9 Kb. If the message buffer size is more than 9 Kb, the entire message cannot be transferred to the ALG packet handler. This causes subsequent packets in the session to bypass ALG handling, resulting in a transaction failure.

Starting with Junos OS Release 15.1X49-D60, SRX5400, SRX5600, and SRX5800 devices with the SRX5K-MPC (IOC2), SRX5K-MPC3-100G10G (IOC3), and SRX5K-MPC3-40G10G (IOC3) support Express Path (formerly known as services offloading) for ALG traffic.

The following ALG data traffic supports Express Path—FTP, H.323 (only RTP/RTCP sessions are offloaded), MGCP, MS RPC, RSH, RTSP, SCCP, SIP (only RTP/RTCP sessions are offloaded), Sun RPC, TALK (only TCP sessions are offloaded), and TFTP.

DNS, IKE and ESP, PPTP, and SQL-NET ALG data traffic do not support Express Path.

Once an Express Path session is set up, packets cannot be sent to the SPU again.

Related Documentation

Understanding Custom ALG Services

Supported Platforms   SRX Series, vSRX

By default, ALGs are bound to predefined services. For example, the FTP ALG is bound to junos-ftp, the RTSP ALG is bound to junos-rtsp, and so on.

A predefined service already has a mapping to a Layer 7 application. However, for custom services, you must link the service to an application explicitly, especially if you want the policy to apply an ALG.

When you apply predefined services to your policy, traffic matching the service will be sent to its corresponding ALG for further processing. However, under some circumstances, the customer needs to define custom services in order to achieve the following:

- Utilize the ALG handler to process special traffic, with customer-specified protocols, destination ports and so on.

- Permit traffic but bypass ALG processing, when traffic matches predefined services that bind with ALG.

- Add more applications to the current ALG's application set.

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide.*

The three usages of custom services are illustrated below, considering MS-RPC ALG as an example:

- **Utilize the ALG handler to process special traffic**:

  ```
  [edit]
  user@host# set applications application customer-msrpc application-protocol ms-rpc
  user@host# set applications application customer-msrpc protocol tcp
  user@host# set applications application customer-msrpc destination-port 6000
  ```

  Traffic with TCP destination port 6000 will be sent to MS-RPC ALG for further processing.

- **Permit traffic but bypass ALG processing**:

  ```
  [edit]
  user@host# set applications application customer-ignore application-protocol ignore
  user@host# set applications application customer-ignore protocol tcp
  user@host# set applications application customer-ignore destination-port 135
  ```

  MS-RPC ALG will be ignored by traffic with TCP destination port 135.

- **Add more applications to the current ALG's application set**—To add applications such as MS-RPC or Sun RPC services, which are not predefined on SRX Series devices:

  ```
  [edit]
  user@host# set applications application customer-msrpc term t1 protocol tcp
  user@host# set applications application customer-msrpc term t1 uuid
      e3514235-4b06-11d1-ab04-00c04fc2dcd2
  ```

  MS-RPC data traffic with TCP, uuid e3514235-4b06-11d1-ab04-00c04fc2dcd2, will be permitted, when custom-msrpc is applied to the policy along with other predefined junos-ms-rpc** applications.

Related Documentation

- Understanding VoIP ALG Types on page 141

- ALG Overview on page 3

Understanding IPv6 ALG Support for ICMP

Supported Platforms   SRX Series, vSRX

The Internet Control Message Protocol (ICMP) Application Layer Gateway (ALG) is one of the ALG's that handle ICMP traffic.

IPv6 nodes use the ICMPv6 protocol to report errors encountered in processing packets and to perform other Internet-layer functions such as diagnostics. ICMPv6 is an integral part of IPv6 and must be fully implemented by every IPv6 node; therefore the ALG layer is always enabled for ICMPv6.

ICMP Error Messages

ICMPv6 messages are grouped into two classes:

- ICMPv6 error messages
  - Destination unreachable
  - Packet too big
  - Time exceeded
  - Parameter problem
- ICMPv6 informational (or ping) messages
  - Echo request
  - Echo reply

The ICMP ALG monitors all these messages, and then does the following :

- Closes the session
- Modifies the payload

The ICMP ALG closes a session if it meets the following conditions:

- Receives echo reply message.
- Receives a destination unreachable error message and has not received any replies yet.

> **NOTE:** The ICMP ALG checks if the session has received any replies from destination node. If it has received any reply , the destination should be reachable and the ICMP error message is not credible, therefore it does not close the session. This is to avoid hackers from sniffing the TCP/UDP packet and forging an ICMP destination unreachable packet to kill the session.

ICMP ALG Functionality

ICMP ALG behaves differently in various modes.

ICMP ALG functionality in NAT mode:

1. Close the session.

2. Modify the identifier, the sequence number or both of the echo request.

3. Resume the original identifier and sequence number for the echo reply.

4. NAT translates the embedded IPv6 packet for theICMPv6 error message.

ICMP ALG functionality in NAT-PT support mode:

1. Close the session.

2. Translate the ICMPv4 ping message to the ICMPv6 ping message.

3. Translate the ICMPv6 ping message to the ICMPv4 ping message.

4. Translate the ICMPv4 error message to the ICMPv6 error message and translate its embedded IPv4 packet to an IPv6 packet.

5. Translate the ICMPv6 error message to the ICMPv4 error message and translate its embedded IPv6 packet to an IPv4 packet .

Related Documentation

- *Understanding How SRX Series Devices Handle Packet Fragmentation for IPv6 Flows*

- *Understanding IPv6 Address Space, Addressing, Address Format, and Address Types*

PART 2

Configuring Data ALGs

CHAPTER 2

Data ALG Types

Understanding Data ALG Types

Supported Platforms   SRX Series, vSRX

Junos OS supports the following data ALGs:

- DNS—Provides an ALG for the Domain Name System. The DNS ALG monitors DNS query and reply packets and closes session if the DNS flag indicates the packet is a reply message.

- DDNS—Dynamic DNS (DDNS) is an addition to the DNS standard. DDNS updates a DNS server with new or changed records for IP addresses without the need for human intervention. Unlike DNS that only works with static IP addresses, DDNS is also designed to support dynamic IP addresses, such as those assigned by a DHCP server. DDNS is a good option for home networks, which often receive dynamic public IP addresses from their Internet provider that occasionally changes.

- FTP—Provides an ALG for the File Transfer Protocol (FTP).The FTP ALG monitors PORT, PASV, and 227 commands. It performs NAT on the IP, port, or both in the message and gate opening on the device as necessary.

- IKE and ESP ALG—Monitors IKE traffic between the client and the server and permits only one IKE Phase 2 message exchange between any given client/server pair, not just one exchange between any client and any server.

Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic is exchanged between the clients and the server. However, if the clients do not support NAT-Traversal (NAT-T) and if the device assigns the same NAT-generated IP address to two or more clients, the device will be unable to distinguish and route return traffic properly.

> **i**   NOTE: If the user wants to support both NAT-T-capable and non-NAT-T-capable clients, then some additional configurations are required. If there are NAT-T capable clients, the user must enable the source NAT address persistence.

- TFTP—Provides an ALG for the Trivial File Transfer Protocol (TFTP). The TFTP ALG processes TFTP packets that initiate the request and opens a gate to allow return packets from the reverse direction to the port that sends the request.

- PPTP—Provides an ALG for the Point-to-Point Tunneling Protocol (PPTP). The PPTP is a Layer 2 protocol that tunnels PPP data across TCP/IP networks. The PPTP client is freely available on Windows systems and it is also popularly applied on Linux systems, and is widely deployed for building Virtual Private Networks (VPNs).

- MS-RPC—Provides an ALG for the Microsoft Remote Procedure Call.

- SUNRPC—Provides an ALG for the SUN Remote Procedure Call.

- RSH—Provides an ALG for the Remote Shell (RSH). The RSH ALG handles TCP packets destined for port 514 and processes the RSH port command. The RSH ALG performs NAT on the port in the port command and opens gates as necessary.

- SQL—Provides an ALG for the Structured Query Language (SQL). The SQLNET ALG processes SQL TNS response frame from the server side. It parses the packet and looks for the (HOST=ipaddress), (PORT=port) pattern and performs NAT and gate opening on the client side for the TCP data channel.

- TALK—Provides an ALG for the TALK Protocol. The TALK protocol uses UDP port 517 and port 518 for control channel connections. The talk program consists of a server and a client. The server handles client notifications and helps to establish talk sessions. There are two types of talk servers: ntalk and talkd. The TALK ALG processes packets of both ntalk and talkd formats. It also performs NAT and gate opening as necessary.

- RTSP—Provides an ALG for the Real Time Streaming Protocol (RTSP). RTSP is a standard protocol for streaming media applications. It controls the delivery of data with real-time properties such as audio and video.

For information about enabling and configuring each of these ALGs through J-Web, select the **Configure>Security>ALG** page in the J-Web user interface and click **Help**.

Related Documentation
- ALG Overview on page 3
- Understanding Custom ALG Services on page 4

Configuring the DNS ALG

DNS ALG Overview

Supported Platforms   SRX Series, vSRX

The DNS Application Layer Gateway (ALG) service provides an application-level gateway for use with DNS clients. The DNS ALG service allows a client to access multiple DNS servers in different networks and provides routing to and from those servers. It also supports flexible address translation of the DNS query and response packets. These functions allow the DNS client to query many different domains from a single DNS server instance on the client side of the network.

The DNS server listens through UDP port 53 for incoming queries from DNS resolvers. A resolver communicates with DNS servers by sending DNS queries and handling DNS responses.

> **NOTE:** The default port for DNS ALG is port 53.

The DNS ALG performs the following functions:

- Monitors DNS query and reply packets and closes the session when the DNS reply is received

- Performs DNS doctoring

- Performs the IPv4 and IPv6 address transformations

- Modifies the DNS payload in NAT mode

Dynamic DNS (DDNS) support is now available in addition to the DNS standard. The Domain Name System (DNS) was originally designed to support queries of a static configured database and the data was expected to change.

The main difference between DNS and DDNS is in the message format of the header section and the update message.

DDNS messages are processed differently when compared to DNS messages. Message parsing is rewritten for DDNS. DDNS does NAT and NAT-PT in the query part of the message and DNS does NAT and NAT-PT in the response part of the message.

NOTE: The DNS ALG supports all the new formats and new functionality.

Related Documentation

- *DNS Overview*
- *DNSSEC Overview*

Understanding the IPv6 DNS ALG for Routing, NAT, and NAT-PT

Supported Platforms   SRX Series, vSRX

Domain Name System (DNS) is the part of the ALG that handles DNS traffic, monitors DNS query and reply packets, and closes the session if the DNS flag indicates the packet is a reply message.

The DNS ALG supports IPv4 in route mode for Junos OS Release 10.0 and earlier releases. In Junos OS Release 10.4, this feature implements IPv6 support on the DNS ALG for routing, Network Address Translation (NAT), and Network Address Translation-Protocol Translation (NAT-PT).

When the DNS ALG receives a DNS query from the DNS client, a security check is done on the DNS packet. When the DNS ALG receives a DNS reply from the DNS server, a similar security check is done, and then the session for the DNS traffic closes.

IPv6 DNS ALG Traffic in NAT mode

IPv6 NAT provides address translation between IPv4 and IPv6 addressed network devices. It also provides address translation between IPv6 hosts. NAT between IPv6 hosts is done in a similar manner and for similar purposes as IPv4 NAT.

When the DNS traffic works in NAT mode, the DNS ALG translates the public address in a DNS reply to a private address when the DNS client is on private network, and similarly translates a private address to a public address when the DNS client is on a public network.

In Junos OS Release 10.4 IPv6 NAT supports:

- Source NAT translations
- Destination NAT mappings
- Static NAT mappings

NOTE: The IPv6 DNS ALG NAT supports only static NAT mapping.

IPv6 DNS ALG Traffic in NAT-PT mode

IPv6 NAT-PT provides address allocation and protocol translation between IPv4 and IPv6 addressed network devices. The translation process is based on the Stateless IP/ICMP Translation (SIIT) method; however, the state and the context of each communication is retained during the session lifetime. IPv6 NAT-PT supports Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) packets.

IPv6 NAT-PT supports the following types of NAT-PT:

- Traditional NAT-PT

- Bidirectional NAT-PT

A DNS-based mechanism dynamically maps IPv6 addresses to IPv4-only servers. NAT-PT uses the DNS ALG to transparently do the translations.

For example, a company using an internal IPv6 network needs to be able to communicate with external IPv4 servers that do not have IPv6 addresses.

To support the dynamic address binding, a DNS should be used for name resolution. The IPv4 host looks up the name of the IPv6 node in its local configured IPv4 DNS server, which then passes the query to the IPv6 DNS server through an SRX Series device using NAT-PT.

When DNS traffic works in NAT-PT mode, the DNS ALG translates the IP address in a DNS reply packet between the IPv4 address and the IPv6 address when the DNS client is in an IPv6 network and the server is in an IPv4 network, and vice versa.

NOTE: In NAT-PT mode, only IPV4 to IPV6 addresses translation is supported in the DNS ALG. To support NAT-PT mode in a DNS ALG, the NAT module should support NAT-PT.

When the DNS ALG receives a DNS query from the DNS client, the DNS ALG performs the following security and sanity checks on the DNS packets:

- Enforces the maximum DNS message length (the default is 512 bytes and the maximum length is 8KB)

- Enforces a domain-name length of 255 bytes and a label length of 63 bytes

- Verifies the integrity of the domain-name referred to by the pointer if compression pointers are encountered in the DNS message

- Checks to see if a compression pointer loop exists

Similar sanity checks are done when the DNS ALG receives a DNS reply from the DNS Server, after which the session for this DNS traffic gets closed.

Related Documentation

- DNS ALG Overview on page 13

- *IPv6 NAT Overview*

- *IPv6 NAT PT Overview*

Example: Configuring the DNS ALG

Supported Platforms   SRX Series, vSRX

This example shows how to configure the DNS ALG to pass through DNS traffic with a static NAT pool on Juniper Networks devices.

- Requirements on page 16

- Overview on page 16

- Configuration on page 16

- Verification on page 18

Requirements

Before you begin:

- Configure static NAT pool for all IP address.

- Understand the concepts behind ALG for DNS. See "DNS ALG Overview" on page 13.

Overview

In this example, the ALG for DNS is configured to monitor and allow DNS traffic to be exchanged between the clients and the server located on opposite sides of a Juniper Networks device.

This example shows how to configure a static NAT pool and rule set, and associate the DNS ALG to a policy.

Configuration

- Configuring a NAT Static Pool and Rule Set on page 16

- Configuring and Printing the DNS Trace on page 18

Configuring a NAT Static Pool and Rule Set

CLI Quick Configuration   To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat static rule-set rs1 from zone untrust
set security nat static rule-set rs1 rule r1 match destination-address 1.1.1.1/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 2.2.2.2/32
set security policies from-zone untrust to-zone trust policy u2t match source-address
    any
set security policies from-zone untrust to-zone trust policy u2t match destination-address
    any
```

```
set security policies from-zone untrust to-zone trust policy u2t match application
    junos-dns-udp
set security policies from-zone untrust to-zone trust policy u2t then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a static NAT pool:

1. Create a NAT static rule set.

   ```
   [edit ]
   user@host# set security nat static rule-set rs1 from zone untrust
   user@host# set security nat static rule-set rs1 rule r1 match destination-address
       1.1.1.1/32
   user@host# set security nat static rule-set rs1 rule r1 then static-nat prefix 2.2.2.2/32
   ```

2. Associate the NAT Traversal (NAT-T) application using a policy.

   ```
   [edit]
   user@host# set security policies from-zone untrust to-zone trust policy u2t match
       source-address any
   user@host# set security policies from-zone untrust to-zone trust policy u2t match
       destination-address any
   user@host# set security policies from-zone untrust to-zone trust policy u2t match
       application junos-dns-udp
   user@host# set security policies from-zone untrust to-zone trust policy u2t then
       permit
   ```

Results

From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show security nat
static {
  rule-set rs1 {
    from zone untrust;
    rule r1 {
      match {
        destination-address 1.1.1.1/32;
      }
      then {
        static-nat {
          prefix {
            2.2.2.2/32;
          }
        }
      }
    }
  }
}

[edit]
user@host# show security policies
from-zone untrust to-zone trust {
```

```
        policy u2t {
          match {
            source-address any;
            destination-address any;
            application [ junos-dns-udp];
          }
          then {
            permit;
          }
        }
      }
      default-policy {
        permit-all;
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring and Printing the DNS Trace

Purpose   Print the DNS trace file.

Action   From configuration mode, enter the following command.

```
set security alg traceoptions file alglog
set security alg traceoptions file size 1g
set security alg traceoptions level verbose
set security alg dns traceoptions flag all
```

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying DNS ALG Custom Applications

Purpose   Verify that the custom applications to support the DNS ALG are enabled.

Action   From operational mode, enter the **show security policies** command.

    user@host> **show security policies**

```
Default policy: permit-all
From zone: untrust, To zone: trust
Policy: u2t, State: enabled, Index: 6, Scope Policy: 0, Sequence number: 1
Source addresses: any
Destination addresses: any
Applications: junos-dns-udp
Action: permit
```

Meaning   The sample output shows that the custom applications to support the DNS ALG is enabled.

Verifying DNS ALG

Purpose   Verify that DNS ALG is enabled.

Action   From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status

DNS     : Enabled
FTP     : Enabled
H323    : Enabled
```

Meaning   The output shows the DNS ALG status as follows:

- Enabled—Shows the DNS ALG is enabled.

- Disabled—Shows the DNS ALG is disabled.

Related Documentation   • DNS ALG Overview on page 13

Understanding DNS and DDNS Doctoring

Supported Platforms   SRX Series, vSRX

Junos OS for SRX Series devices provides Domain Name System (DNS) support. The DNS ALG monitors DNS query and reply packets and closes the session if the DNS flag indicates that the packet is a reply message. To configure the DNS ALG, use the **edit security alg dns** statement at the **[edit security alg]** hierarchy level.

DNS provides name-to-address mapping within a routing class, whereas Network Address Translation (NAT) attempts to provide transparent routing between hosts in disparate address realms of the same routing class. As a result, NAT can cause some DNS problems the DNG ALG must handle through a process called DNS doctoring.

The same doctoring feature applies to the dynamic domain name system (DDNS). For DDNS in NAT mode, you also can do the IP translation in the DDNS update.

To resolve the problems introduced by NAT, DNS and DDNS ALG functionality has been extended to support static NAT, allowing the problems to be resolved through DNS doctoring.

> *i* NOTE: The DNS ALG must be enabled on the devices to perform DNS doctoring. With the DNS ALG enabled on SRX5600 and SRX5800 devices, DNS doctoring is enabled by default.

The restoring and doctoring process is performed in two parts:

- **Packet sanity check**
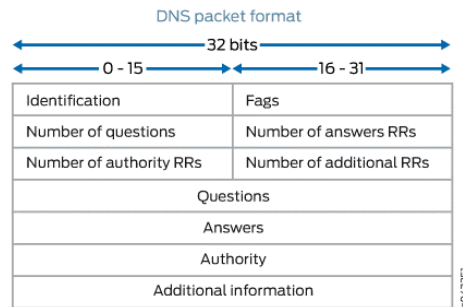
DNS packet format

For the DNS packet, the DNS ALG check fields are questions, answers, authority, and additional information. The DNS ALG drops the packet if the number of questions is more than 1, the domain name is more than 255 bytes, or the label length is more than 63 bytes.

DDNS packet format
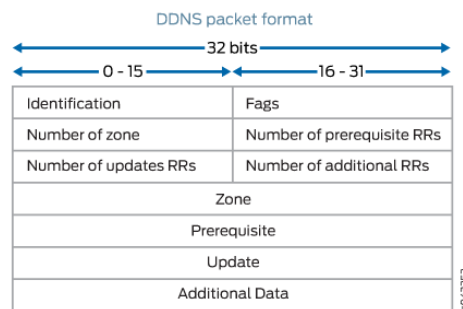
For the DDNS packet, the DNS ALG check fields are zone, prerequisite, update, and additional data. The DNS ALG drops the packet if the number of zones is more than 1, the domain name is more than 255 bytes, or the label length is more than 63 bytes.

For both DNS and DDNS, the DNS ALG drops the packet that does not comply with the standards.

- **NAT**

Figure 1 on page 21 shows how DNS translates a private address to a public address.

Figure 1: DNS Address Translation (Private to Public)
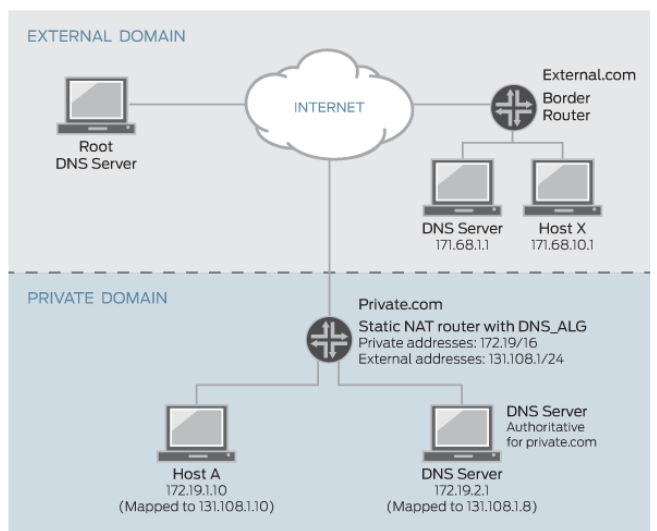
When host X in external.com wants to resolve host A's address through DNS and if the DNS ALG does not support NAT, it takes a private address such as 172.19.1.10, which is invalid to host X. The private address is translated to public address 192.0.5.1 through the DNS ALG.

Figure 2 on page 22 shows how DNS translates a public address to a private address.

Figure 2: DNS Address Translation (Public to Private)
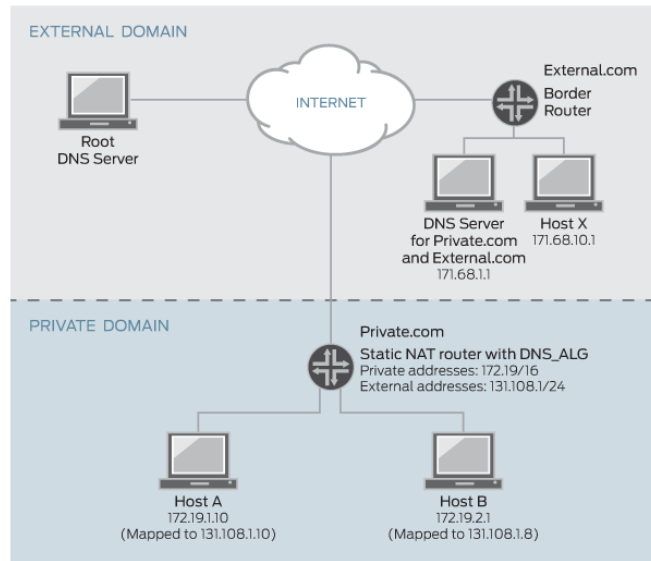
When host A in private.com wants to resolve host B's address through DNS and if the DNS ALG does not support NAT, it takes a public address from the DNS server in external.com, such as 131.108.1.8. If Host A sends traffic to host B with public address 131.108.1.8, which is invalid to host B in the private domain. Hence, the public address in the DNS query A-record is translated to private address 172.19.2.1 through the DNS ALG.

NOTE: The DNS ALG can translate the first 32 A-records in a single DNS reply. A-records after the first 32 records are not handled. Also note that the DNS ALG supports only IPv4 addresses and does not support VPN tunnels.

Related Documentation

- *DNS Overview*
- *IPv6 NAT Overview*
- *IPv6 NAT PT Overview*
- *IPv6 NAT-PT Communication Overview*
- Disabling DNS and DDNS Doctoring on page 22

Disabling DNS and DDNS Doctoring

Supported Platforms   SRX Series, vSRX

The DNS and DDNS doctoring feature is enabled by default. You can disable DNS and DDNS doctoring with the CLI.

To disable DNS and DDNS doctoring:

1. Disable all the doctoring features by specifying the **none** configuration option.

   This command disables all the doctoring features.

   > user@host# **set security alg dns doctoring none**

2. Disable the NAT feature and retain the sanity-check feature by specifying the **sanity-check** configuration option.

   This option disables the NAT feature and retains the sanity-check feature.

   > user@host# **set security alg dns doctoring sanity-check**

3. If you are finished configuring the device, commit the configuration.

4. From configuration mode in the CLI, enter the **show security alg dns doctoring** command to verify the configuration.

Related Documentation

- *DNS Overview*

- *IPv6 NAT Overview*

- *IPv6 NAT PT Overview*

Configuring the FTP ALG

FTP ALG Overview

Supported Platforms   SRX Series, vSRX

The File Transfer Protocol (FTP) is a widely and commonly used method of exchanging files over IP networks. In addition to the main control connection, data connections are also made for any data transfer between the client and the server; and the host, port, and direction are negotiated through the control channel.

For active mode FTP, the Junos OS stateful firewall service scans the client-to-server application data for the PORT command, which provides the IP address and port number to which the server connects. For passive-mode FTP, the Junos OS stateful firewall service scans the client-to-server application data for the PASV command and then scans the server-to-client responses for the 227 response, which contains the IP address and port number to which the client connects.

FTP represents the addresses and port numbers in ASCII. As a result, when addresses and ports are rewritten, the TCP sequence number might be changed, and thereafter the NAT service needs to maintain this delta in SEQ and ACK numbers by performing sequence NAT on all subsequent packets.

The FTP ALG supports the following:

- Automatically allocates data ports and firewall permissions for dynamic data connection

- Monitors the control connection in both active and passive modes

- Rewrites the control packets with the appropriate NAT address and port information

- Network Address Translation, Protocol Translation (NAT-PT)

- Transport Layer Security (TLS) as the security mechanism

Related
Documentation

-

Understanding FTP Commands

Supported Platforms   SRX Series, vSRX

The FTP ALG monitors commands and responses on the FTP control channel for syntactical correctness and opens corresponding pinholes to permit data channel connections to be established. In Junos OS Release 10.4, the FTP ALG supported IPv4 routing and NAT mode, and IPv6 routing mode only. In Junos OS Release 11.2 and later releases, the FTP ALG also supports IPv6 NAT and NAT-PT modes.

PORT Command

The PORT command is used in active FTP mode. The PORT command specifies the address and the port number to which a server should connect. When you use this command, the argument is a concatenation of a 32-bit Internet host address and a 16-bit TCP port address. The address information is broken into 8-bit fields, and the value of each field is transmitted as a decimal number (in character string representation). The fields are separated by commas.

The following is a sample PORT command, where h1 is the highest order 8-bit of the Internet host address:

PORT h1,h2,h3,h4,p1,p2

PASV Command

The PASV command requests a server to listen on a data port that is not the default data port of the server and to wait for a connection, rather than initiating another connection. The response to the PASV command includes the host and port address the server is listening on.

Extended FTP Commands

Extended FTP commands provide a method by which FTP can communicate the data connection endpoint information for network protocols other than IPv4. Extended FTP commands are specified in RFC 2428. In RFC 2428, the extended FTP commands EPRT and EPSV, replace the FTP commands PORT and PASV, respectively.

EPRT Command

The EPRT command allows for the specification of an extended address for the data connection. The extended address must consist of the network protocol as well as the network and transport addresses.

The format of EPRT is:

EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>

Parameter	Description
net-prt	An address family number defined by IANA.
net-addr	A protocol-specific string of the network address.
tcp-port	A TCP port number on which the host is listening for data connection.
Delimiter	The delimiter character must be one of the ASCII characters in range 33 to 126 inclusive. The character "|" (ASCII 124) is recommended.

The following command shows how to specify the server to use an IPv4 address to open a data connection to host 132.235.1.2 on TCP port 6275:

EPRT |1|132.235.1.2|6275|

The following command shows how to specify the server to use an IPv6 network protocol and a network address to open a TCP data connection on port 5282:

EPRT |2|1080::8:800:200C:417A|5282|

In this mode, FTP ALG focuses only on the EPRT command; it extracts the IPv6 address and port from the EPRT command and opens the pinhole.

EPSV mode

The EPSV command requests that a server listen on a data port and wait for a connection. The response to this command includes only the TCP port number of the listening connection.

An example response string is as follows:

```
Entering Extended Passive Mode (|||6446|)
```

> NOTE: The response code for entering passive mode using an extended address must be 229. You should extract the TCP port in 229 payloads and use it to open the pinhole.

Related
Documentation

- FTP ALG Overview on page 25

- Example: Configuring the FTP ALG on page 27

Example: Configuring the FTP ALG

Supported Platforms   SRX Series, vSRX

This example shows how to configure the NAT-PT for FTP ALG.

Requirements

Before you begin:

- Configure proxy ARP for all IP addresses in the source NAT pool.

- Understand the concepts behind ALG for FTP. See "FTP ALG Overview" on page 25.

Overview

In this example, the ALG for FTP is configured to monitor and allow FTP traffic to be exchanged between the clients and the server located on opposite sides of a Juniper Networks device.

This example shows how to configure the NAT-PT for FTP ALG.

Configuration

Configuring a NAT Source Pool, NAT Static Pool and Rule Set

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat static rule-set rs1 from zone untrust
set security nat source rule-set rs-source to zone trust
set security nat source rule-set rs-source rule src-nat match source-address 3333::130/128
set security nat source rule-set rs-source rule src-nat match destination-address
    40.0.0.211/32
set security nat source rule-set rs-source rule src-nat then source-nat interface
set security nat static rule-set rs2 from zone untrust
set security nat static rule-set rs2 rule r2 match destination-address 4444::141/128
set security nat static rule-set rs2 rule r2 then static-nat prefix 40.0.0.211/32
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a source NAT pool:

1. Create a source NAT, static NAT, and interface NAT rule set.

    ```
    [edit ]
    user@host# set security nat source rule-set rs-source from zone untrust
    user@host# set security nat source rule-set rs-source to zone trust
    ```

```
user@host# set security nat source rule-set rs-source rule src-nat match
    source-address 3333::130/128
user@host# set security nat source rule-set rs-source rule src-nat match
    destination-address 40.0.0.211/32
user@host# set security nat source rule-set rs-source rule src-nat then source-nat
    interface
user@host# set security nat static rule-set rs2 from zone untrust
user@host# set security nat static rule-set rs2 rule r2 match destination-address
    4444::141/128
user@host# set security nat static rule-set rs2 rule r2 then static-nat prefix
    40.0.0.211/32
```

2.   Associate the NAT-PT application using a policy.

```
[edit]
user@host# set security policies from-zone trust to-zone untrust policy ftp-basic
    match source-address any
user@host# set security policies from-zone trust to-zone untrust policy ftp-basic
    match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy ftp-basic
    match application junos-ftp
user@host# set security policies from-zone trust to-zone untrust policy ftp-basic
    then permit
```

Results   From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show security nat
static {
  rule-set rs2 {
    from zone untrust;
    rule r2 {
      match {
        destination-address 4444::141/128;
      }
      then {
        static-nat {
          prefix {
            40.0.0.211/32
          }
        }
      }
    }
  }
}

[edit]
user@host# show security policies
from-zone untrust to-zone trust {
  policy ftp-basic {
    match {
      source-address any;
      destination-address any;
      application [ junos-ping junos-mgcp junos-ftp junos-rsh junos-h323 ];
    }
```

```
                    then {
                       permit;
                    }
                 }
              }
              default-policy {
                 permit-all;
              }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring FTP ALG Security Extension

Purpose   Set the security alg ftp extension

Action   From configuration mode, enter the following command.

set security alg ftp ftps-extension

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying the NAT Source Pool, NAT Static Pool Rule Set

Purpose   Verify that the NAT source pool and rule set used to support the FTP ALG are working properly.

Action   From operational mode, enter the **show configuration security nat** command.

Verifying FTP ALGs

Purpose   Verify that FTP ALG is enabled.

Action   From the operational mode, enter the **show security alg status** command.

```
user@host> show security alg status
FTP      : Enabled
```

Meaning   The output shows the FTP ALG status as follows:

- Enabled—Shows the FTP ALG is enabled.

- Disabled—Shows the FTP ALG is disabled.

> **NOTE:** The FTP ALG is enabled by default.

Understanding the IPv6 FTP ALG for Routing

Supported Platforms   SRX Series, vSRX

File Transfer Protocol (FTP) is the part of the ALG that handles FTP traffic. The PORT/PASV requests and corresponding 200/227 responses in FTP are used to announce the TCP port, which the host listens to for the FTP data connection.

EPRT/EPSV/229 commands are used for these requests and responses. FTP ALG supports EPRT/EPSV/229 already, but only for IPv4 addresses.

In Junos OS Release 10.4, EPRT/EPSV/229 commands have been updated to support both IPv4 and IPv6 addresses.

FTP ALG uses preallocated objcache to store its session cookies. When both IPv4 and IPv6 addresses are supported on FTP ALG, the session cookie structure will enlarge by 256 bits (32 bytes) to store IPv6 address.

FTP ALG Support for IPv6

The FTP ALG monitors commands and responses on the FTP control channel for syntactical correctness and opens corresponding pinholes to permit data channel connections to be established. In Junos OS Release 10.4, the FTP ALG supported IPv4 routing, IPv6 routing, and NAT mode only. In Junos OS Release 11.2 and later releases, the FTP ALG also supports IPv6 NAT and NAT-PT modes.

EPRT mode

The EPRT command allows for the specification of an extended address for the data connection. The extended address must consist of the network protocol as well as the network and transport addresses.

The format of EPRT is:

EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>

- <net-prt>: An address family number defined by IANA

- <net-addr>: A protocol specific string of the network address

- <tcp-port>: A TCP port number

The following are sample EPRT commands for IPv6:

EPRT |2|1080::8:800:200C:417A|5282|

In this mode, FTP ALG focuses only on the EPRT command; it extracts the IPv6 address and port from the EPRT command and opens the pinhole.

EPSV mode

The EPSV command requests that a server be listening on a data port and waiting for a connection. The response to this command includes only the TCP port number of the listening connection.

An example response string is follows:

```
Entering Extended Passive Mode (|||6446|)
```

NOTE: The response code for entering passive mode using an extended address must be 229. You should extract the TCP port in 229 payloads and use it to open the pinhole.

Related Documentation

- *IPv6 NAT Overview*
- *IPv6 NAT PT Overview*

CHAPTER 5

Configuring the IKE and ESP ALG

Understanding the ALG for IKE and ESP

Supported Platforms   SRX Series, vSRX

An SRX Series device can be used solely as a Network Address Translation (NAT) device when placed between VPN clients on the private side of the NAT gateway and the virtual private network (VPN) gateways on the public side.

Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic is exchanged between the clients and the server. However, if the clients do not support NAT-Traversal (NAT-T) and if the device assigns the same NAT-generated IP address to two or more clients, the device will be unable to distinguish and route return traffic properly.

> ℹ️ NOTE: If the user wants to support both NAT-T-capable and non-NAT-T-capable clients, then some additional configurations are required. If there are NAT-T capable clients, the user must enable the source NAT address persistence.

The ALG for IKE and ESP monitors IKE traffic between the client and the server and permits only one IKE Phase 2 message exchange between any given client/server pair, not just one exchange between any client and any server.

ALG for IKE and ESP traffic has been created and NAT has been enhanced to implement the following:

- To enable the SRX Series devices to pass IKE and ESP traffic with a source NAT pool
- To allow the device to be configured to return the same NAT-generated IP address for the same IP address without NAT ("address-persistent NAT"). As a result, the device

is able to associate a client's outgoing IKE traffic with its return traffic from the server, especially when the IKE session times out and needs to be reestablished.

- The resulting ESP traffic between the client and the server is also allowed, especially in the direction from the server to the client.

- The return ESP traffic matches the following:

  - The server IP address as source IP

  - The client IP address as destination IP

> **NOTE:** In SRX1500, SRX5600, and SRX5800 devices, IKE negotiations involving NAT traversal do not work if the IKE peer is behind a NAT device that will change the source IP address of the IKE packets during the negotiation. For example, if the NAT device is configured with DIP, it changes the source IP because the IKE protocol switches the UDP port from 500 to 4500.

Related Documentation

- Example: Configuring the IKE and ESP ALG on page 35

Understanding IKE and ESP ALG Operation

Supported Platforms   SRX Series, vSRX

Application Layer Gateway (ALG) for Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic has the following behavior:

- An IKE and ESP ALG monitors IKE traffic between the client and the server, and it permits only one IKE Phase 2 message exchange between the client and the server at any given time.

- For a Phase 2 message:

  - If a Phase 2 message exchange between the client and server does not happen, the IKE ALG gates are opened for the relevant ESP traffic from the client to the server and from the server to the client.

  - If both IKE ALG gates are not opened successfully, or if the Phase 2 message exchange already took place, then the Phase 2 message is dropped.

- When ESP traffic hits the IKE ALG gates, sessions are created to capture subsequent ESP traffic, and to perform the proper NATing (that is, the source IP address translation from the client to the server traffic and the destination IP address translation from the server to the client traffic).

- When the ESP traffic does not hit either one or both of the gates, then the gates naturally time out.

- Once the IKE ALG gates are collapsed or timed out, another IKE Phase 2 message exchange is permitted.

- IKE NAT-T traffic on floating port 4500 is not processed in an IKE ALG. To support a mixture of NAT-T-capable and non-capable clients, you need to enable source NAT address persistent.

Example: Configuring the IKE and ESP ALG

Supported Platforms   SRX Series, vSRX

This example shows how to configure the IKE and ESP ALG to pass through IKE and ESP traffic with a source NAT pool on Juniper Networks devices.

Requirements

Before you begin:

- Configure proxy ARP for all IP addresses in the source NAT pool.

- Understand the concepts behind IKE and ESP ALG. See "Understanding IKE and ESP ALG Operation" on page 34.

Overview

In this example, the ALG for IKE and ESP is configured to monitor and allow IKE and ESP traffic to be exchanged between the clients and the server located on opposite sides of a Juniper Networks device.

This example shows how to configure a source NAT pool and rule set, configure a custom application to support the IKE and ESP ALG, and associate this ALG to a policy.

If you want to support a mixture of NAT-traversal (NAT-T) capable clients and noncapable clients, you must enable persistent source NAT translation (so that once a particular source NAT is associated with a given IP address, subsequent source NAT translations use the same IP address). You also must configure a custom IKE NAT traversal application

to support the encapsulation of IKE and ESP in UDP port 4500. This configuration enables IKE and ESP to pass through the NAT-enabled device.

Configuration

Configuring a NAT Source Pool and Rule Set

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source pool pool1 address 10.10.10.1/32 to 10.10.10.10/32
set security zones security-zone green address-book address sa1 1.1.1.0/24
set security zones security-zone red address-book address da1 2.2.2.0/24
set security nat source rule-set rs1 from zone green
set security nat source rule-set rs1 to zone red
set security nat source rule-set rs1 rule r1 match source-address 1.1.1.0/24
set security nat source rule-set rs1 rule r1 match destination-address 2.2.2.0/24
set security nat source rule-set rs1 rule r1 then source-nat pool pool1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a source NAT pool:

1. Create a NAT source pool.

    ```
    [edit ]
    user@host# set security nat source pool pool1 address 10.10.10.1/32 to 10.10.10.10/32
    ```

2. Configure security zone address book entries.

    ```
    [edit]
    user@host# set security zones security-zone green address-book address sa1
        1.1.1.0/24
    user@host# set security zones security-zone red address-book address da1 2.2.2.0/24
    ```

3. Create a NAT source rule set.

    ```
    [edit security nat source rule-set rs1]
    user@host# set from zone green
    user@host# set to zone red
    user@host# set rule r1 match source-address 1.1.1.0/24
    user@host# set rule r1 match destination-address 2.2.2.0/24
    user@host# set rule r1 then source-nat pool pool1
    ```

Results   From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show security nat
source {
  pool pool1 {
    address {
      10.10.10.1/32 to 10.10.10.10/32;
    }
  }
  rule-set rs1 {
    from zone green;
    to zone red;
    rule r1 {
      match {
        source-address 1.1.1.0/24;
        destination-address 2.2.2.0/24;
      }
      then {
        source-nat {
          pool {
            pool1;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Custom Application and Associating it to a Policy

CLI Quick
Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set applications application custom-ike-alg source-port 500 destination-port 500 protocol
    udp application-protocol ike-esp-nat
set security policies from-zone green to-zone red policy pol1 match destination-address
    da1
set security policies from-zone green to-zone red policy pol1 match application
    custom-ike-alg
set security policies from-zone green to-zone red policy pol1 then permit
```

Step-by-Step
Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a custom application and associate it to a policy:

1.   Configure a custom application.

[edit]

```
user@host# set applications application custom-ike-alg source-port 500
    destination-port 500 protocol udp application-protocol ike-esp-nat
```

2. Associate the custom application to a policy.

```
[edit security policies from-zone green to-zone red policy pol1]
user@host# set match source-address sa1
user@host# set match destination-address da1
user@host# set match application custom-ike-alg
user@host# set then permit
```

Results   From configuration mode, confirm your configuration by entering the **show applications** and **show security zones** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show applications
application custom-ike-alg {
    application-protocol ike-esp-nat;
    protocol udp;
    source-port 500;
    destination-port 500;
}

[edit]
user@host# show security zones
security-zone Trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone green {
    address-book {
        address sa1 1.1.1.0/24;
    }
}
security-zone red {
    address-book {
        address da1 2.2.2.0/24;
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring IKE and ESP ALG Support for Both NAT-T Capable and Noncapable Clients

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source address-persistent
set applications application custom-ike-natt protocol udp source-port 4500
   destination-port 4500
set security policies from-zone green to-zone red policy pol1 match source-address sa1
set security policies from-zone green to-zone red policy pol1 match destination-address
   da1
set security policies from-zone green to-zone red policy pol1 match application
   custom-ike-natt
set security policies from-zone green to-zone red policy pol1 then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure IKE and ESP ALG support for both NAT-T capable and noncapable clients:

1. Globally enable persistent source NAT translation.

    ```
    [edit]
    user@host# set security nat source address-persistent
    ```

2. Configure the IKE NAT-T application.

    ```
    [edit]
    user@host# set applications application custom-ike-natt protocol udp source-port
       4500 destination-port 4500
    ```

3. Associate the NAT-T application using a policy.

    ```
    [edit security policies from-zone green to-zone red policy pol1]
    user@host# set match source-address sa1
    user@host# set match destination-address da1
    user@host# set match application custom-ike-natt
    user@host# set then permit
    ```

Results

From configuration mode, confirm your configuration by entering the **show security nat** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
source {
   address-persistent;
}

[edit]
user@host# show security policies
from-zone green to-zone red {
```

```
        policy pol1 {
          match {
            source-address sa1;
            destination-address da1;
            application [ custom-ike-alg custom-ike-natt ];
          }
          then {
            permit;
          }
        }
      }
      default-policy {
        permit-all;
      }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying IKE and ESP ALG Custom Applications on page 40
- Verifying the Security Polices of ALG on page 41

Verifying IKE and ESP ALG Custom Applications

Purpose   Verify that the custom applications to support the IKE and ESP ALG are enabled.

Action   From operational mode, enter the **show security alg status** command.

user@host> **show security alg status**

```
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Enabled
  MGCP     : Enabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Enabled
  SCCP     : Enabled
  SIP      : Enabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Enabled
```

Meaning   The output shows the ALG status as follows:

- Enabled—Shows the ALG is enabled.
- Disabled—Shows the ALG is disabled.

Verifying the Security Polices of ALG

Purpose   Verify that the application custom IKE ALG and application custom IKE NATT are set.

Action   From operational mode, enter the **show security policies** command.

> user@host> **show security policies**

```
Default policy: permit-all
From zone: green, To zone: red
Policy: pol1, State: enabled, Index: 7, Scope Policy: 0, Sequence number: 1
Source addresses: sa1
Destination addresses: da1
Applications: custom-ike-alg, custom-ike-natt
Action: permit
```

Meaning   The sample output shows that custom IKE ALG and custom IKE NATT applications are set.

Related Documentation

- ALG Overview on page 3
- Understanding the ALG for IKE and ESP on page 33
- Example: Enabling the IKE and ESP ALG and Setting Timeouts on page 41

Example: Enabling the IKE and ESP ALG and Setting Timeouts

Supported Platforms   SRX Series, vSRX

This example shows how to enable the IKE and ESP ALG and set the timeout values to allow time for the ALG to process ALG state information, ESP gates, and ESP sessions.

- Requirements on page 41
- Overview on page 41
- Configuration on page 42
- Verification on page 43

Requirements

Understand the concepts behind ALG for IKE and ESP. See "Understanding IKE and ESP ALG Operation" on page 34.

Overview

The IKE and ESP ALG processes all traffic specified in any policy to which the ALG is attached. In this example, you configure the **set security alg ike-esp-nat enable** statement so the current default IPsec pass-through behavior is disabled for all IPsec pass-through traffic, regardless of policy.

You then set the timeout values to allow time for the IKE and ESP ALG to process ALG state information, ESP gates, and ESP sessions. In this example, you set the timeout of ALG state information. The timeout range is 180 through 86400 seconds. The default

timeout is 14400 seconds. You then set the timeout of the ESP gates created after an IKE Phase 2 exchange has completed. The timeout range is 2 through 30 seconds. The default timeout is 5 seconds. Finally, you set the idle timeout of the ESP sessions created from the IPsec gates. If no traffic hits the session, it is aged out after this period of time. The timeout range is 60 through 2400 seconds. The default timeout is 1800 seconds.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security alg ike-esp-nat enable
set security alg ike-esp-nat esp-gate-timeout 20
set security alg ike-esp-nat esp-session-timeout 2400
set security alg ike-esp-nat state-timeout 360
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To enable the IKE and ESP ALG and set the timeout values:

1. Enable the IKE and ESP ALG.

   ```
   [edit]
   user@host# set security alg ike-esp-nat enable
   ```

2. Set the timeout for the ALG state information.

   ```
   [edit security alg ike-esp-nat]
   user@host# set state-timeout 360
   ```

3. Set the timeout for the ESP gates created after an IKE Phase 2 exchange has completed.

   ```
   [edit security alg ike-esp-nat]
   user@host# set esp-gate-timeout 20
   ```

4. Set the idle timeout for the ESP sessions created from the IPsec gates.

   ```
   [edit security alg ike-esp-nat]
   user@host# set esp-session-timeout 2400
   ```

Results

From configuration mode, confirm your configuration by entering the **show security alg** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security alg
ike-esp-nat {
  enable;
  state-timeout 360;
  esp-gate-timeout 20;
  esp-session-timeout 2400;
```

```
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying the ALG for IKE and ESP and Timeout Settings

Purpose Verify that the ALG for IKE and ESP is enabled and the timeout settings for this feature are correct.

Action From operational mode, enter the **show security alg ike-esp-nat** command.

Related Documentation
- ALG Overview on page 3
- *Introduction to NAT*
- Understanding the ALG for IKE and ESP on page 33
- Understanding IKE and ESP ALG Operation on page 34
- Example: Configuring the IKE and ESP ALG on page 35

CHAPTER 6

Configuring the PPTP ALG

Understanding the PPTP ALG

Supported Platforms   SRX Series, vSRX

The Point-to-Point Tunneling Protocol (PPTP) ALG is used for tunneling Point-to-Point Protocol (PPP) packets over an IP network. The PPTP ALG is often used to implement a client/server architecture, a PPTP network server, and a PPTP access concentrator.

The PPTP ALG processes PPTP packets, performs Network Address Translation (NAT), open pinholes for new data connections between a client and a server, and transfers data between a client and a server located on opposite sides of a Juniper Networks device.

Related Documentation   • Example: Configuring the PPTP ALG on page 46

Understanding IPv6 Support for the PPTP ALG

Supported Platforms   SRX Series, vSRX

IPv6 is supported on the PPTP ALG.

The PPTP ALG supports IPv6 data packets. The PPTP ALG uses TCP port 1723 to connect and disconnect a client and a server.

To support IPv6, the PPTP ALG parses both IPv4 and IPv6 PPTP packets, performs NAT, and then opens a pinhole for the data tunnel. The flow module supports IPv6 to parse the GRE packet and use the GRE call ID as fake port information to search the session table and gate table.

The PPTP ALG with IPv6 support does not support NAT-PT and NAT64, because PPP packets are compressed with Microsoft Point-to-Point Encryption (MPPE) protocol after the tunnel is set up; therefore translation of the IP header in the PPP package cannot be handled.

> **NOTE:** The PPTP ALG can support NAT64 in a specific scenario in which translation of the IP header in the PPP package is not required—that is, if the PPTP client works in dual-stack mode in the IPv6 network and server in the IPv4 network.

- The PPTP ALG with IPv6 support has the following limitation:

  - Because PPP packets are compressed with Microsoft Point-to-Point Encryption (MPPE) protocol after the tunnel is set up, translation of the IP header in the PPP package cannot be handled; therefore, to make sure PPTP connection works well, the PPTP client must be able to work in dual stack mode. So that an IPv6 PPTP client can accept an IPv4 address for PPP tunnel interface, by which it can communicate with the IPv4 PPTP server without IP address translation for PPP packets.

Related Documentation
- Understanding the PPTP ALG on page 45

Example: Configuring the PPTP ALG

Supported Platforms   SRX Series, vSRX

The PPTP ALG processes PPTP packets, performs NAT, and open pinholes for new data connections between a client and a server.

This example shows how to configure the PPTP ALG in route or NAT mode. The configuration allows PPTP traffic to pass through a device, transferring data between a client and a server located on opposite sides of a Juniper Networks device.

- Requirements on page 46
- Overview on page 47
- Configuration on page 48
- Verification on page 56

Requirements

This example uses the following hardware and software components:

- An SRX Series device
- Two PCs (client and server)

Before you begin:

- Understand the concepts behind ALGs. See "ALG Overview" on page 3.
- Understand the basics of PPTP ALG. See "Understanding the PPTP ALG" on page 45.

Overview

In this example, first you configure network interfaces on the device, create security zones and assign interfaces to the zones, and configure a policy to allow PPTP traffic to go through an SRX Series device.

Then you create a static NAT rule set rs1 with a rule r1 to match with the destination address 30.5.2.120/32, and you create a static NAT prefix with address 10.5.1.120/32.

Next you create a source NAT pool src-p1 with a source rule set src-rs1 to translate packets from zone trust to zone untrust. For matching packets, the source address is translated to an IP address in the src-p1 pool.

Then you create a destination NAT pool des-p1 with a destination rule set des-rs1 to translate packets from zone trust to destination address 30.5.1.120/32. For matching packets, the destination address is translated to an IP address in the des-p1 pool. Finally, you configure PPTP ALG trace options.

Topology

shows the PPTP ALG topology.

Figure 3: PPTP ALG Topology
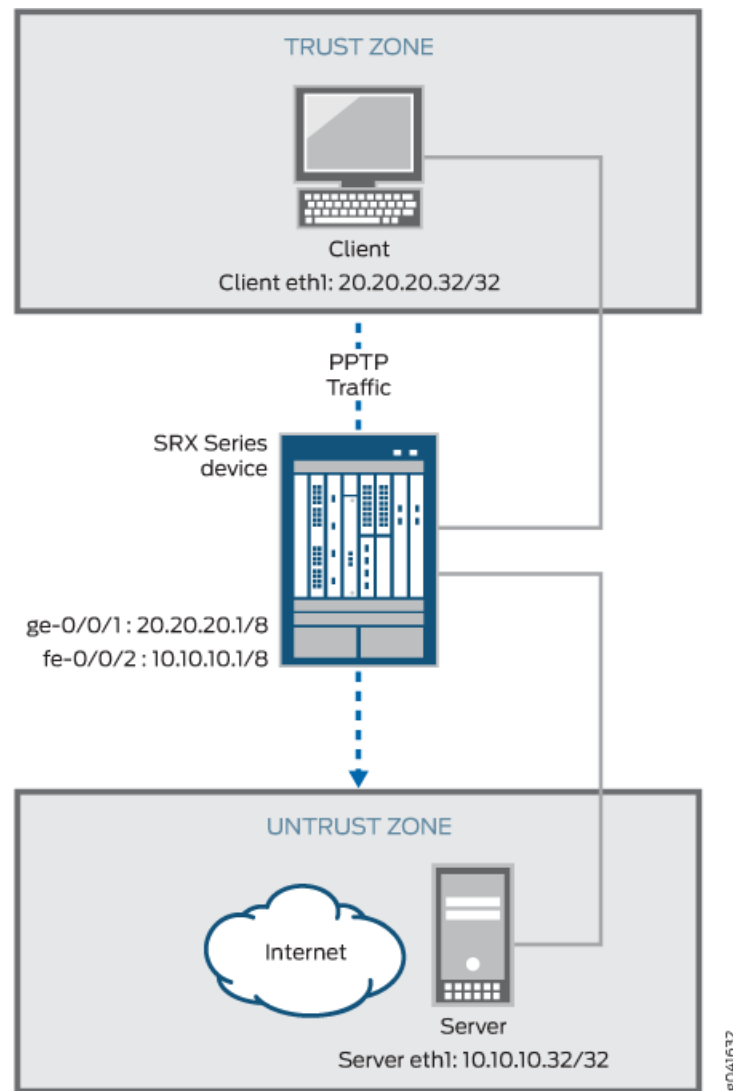
Configuration

To configure the PPTP ALG, perform these tasks:

-
-
-
-
-

Configuring a Route Mode

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/1 unit 0 family inet address 20.20.20.1/8
set interfaces fe-0/0/2 unit 0 family inet address 10.10.10.1/8
set security zones security-zone trust interfaces ge-0/0/1 host-inbound-traffic system-services
 all
set security zones security-zone trust interfaces ge-0/0/1 host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/2 host-inbound-traffic system-services
 all
set security zones security-zone untrust interfaces fe-0/0/2 host-inbound-traffic protocols all
set security policies from-zone trust to-zone untrust policy pptp match source-address any
set security policies from-zone trust to-zone untrust policy pptp match destination-address any
set security policies from-zone trust to-zone untrust policy pptp match application junos-pptp
set security policies from-zone trust to-zone untrust policy pptp then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure route mode:

1. Configure interfaces.

   ```
   [edit interfaces]
   user@host#set ge-0/0/1 unit 0 family inet address 20.20.20.1/8
   user@host#set fe-0/0/2 unit 0 family inet address 10.10.10.1/8
   ```

2. Configure zones and assign interfaces to the zones.

   ```
   [edit security zones security-zone trust]
   user@host#set interfaces ge-0/0/1 host-inbound-traffic system-services all
   user@host#set interfaces ge-0/0/1 host-inbound-traffic protocols all
   [edit security zones security-zone untrust]
   user@host#set interfaces fe-0/0/2 host-inbound-traffic system-services all
   user@host#set interfaces fe-0/0/2 host-inbound-traffic protocols all
   ```

3. Configure a PPTP policy that allows PPTP traffic from the trust zone to the untrust zone.

   ```
   [edit security policies from-zone untrust to-zone trust]
   user@host#set policy pptp match source-address any
   user@host#set policy pptp match destination-address any
   user@host#set policy pptp match application junos-pptp
   user@host#set policy pptp then permit
   ```

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show interfaces
...
   ge-0/0/1 {
   unit 0 {
     family inet {
       address 20.20.20.1/8;
     }
   }
}
fe-0/0/2 {
   unit 0 {
     family inet {
       address 10.10.10.1/8;
     }
   }
}
...

[edit]
user@host# show security zones
security-zone trust {
   ....
     interfaces {
     ge-0/0/1 {
       host-inbound-traffic {
         system-services {
           all;
         }
         protocols {
           all;
         }
       }
     }
   }
}
...
security-zone untrust {
   interfaces {
     fe-0/0/2 {
       host-inbound-traffic {
         system-services {
           all;
         }
         protocols {
           all;
         }
       }
```

```
          }
        }
      }

    [edit]
    user@host# show security policies
    from-zone trust to-zone untrust {
      policy pptp {
        match {
          source-address any;
          destination-address any;
          application junos-pptp;
        }
        then {
          permit;
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Static NAT Rule Set

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat static rule-set rs1 from zone trust
set security nat static rule-set rs1 rule r1 match destination-address 30.5.2.120/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 10.5.1.120/32
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a static NAT rule set:

1. Create a static NAT rule set.

    ```
    [edit security nat static rule-set rs1]
    user@host#set from zone trust
    ```

2. Define the rule to match with the destination address.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 match destination-address 30.5.2.120/32
    ```

3. Define the static NAT prefix for the device.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 then static-nat prefix 10.5.1.120/32
    ```

Results

From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
static {
  rule-set rs1 {
    from zone trust;
    rule r1 {
      match {
        destination-address 30.5.2.120/32;
      }
      then {
        static-nat {
          prefix {
            10.5.1.120/32;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Source NAT Pool and Rule Set

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source pool src-p1 address 30.5.1.120/32
set security nat source rule-set src-rs1 from zone trust
set security nat source rule-set src-rs1 to zone untrust
set security nat source rule-set src-rs1 rule src-r1 match source-address 20.5.1.120/32
set security nat source rule-set src-rs1 rule src-r1 match destination-address 10.5.2.120/32
set security nat source rule-set src-rs1 rule src-r1 then source-nat pool src-p1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a source NAT pool and rule set:

1. Create a source NAT pool.

   ```
   [edit security nat source]
   user@host#set pool src-p1 address 30.5.1.120/32
   ```

2. Create a source NAT rule set.

   ```
   [edit security nat source ]
   user@host# set rule-set src-rs1 from zone trust
   user@host# set rule-set src-rs1 to zone untrust
   ```

3. Configure a rule that matches packets and translates the source address to an address in the source pool.

   ```
   [edit security nat source]
   ```

user@host# **set rule-set src-rs1 rule src-r1 match source-address 20.5.1.120/32**

4. Configure a rule that matches packets and translates the destination address to an address in the source pool.

[edit security nat source]
user@host# **set rule-set src-rs1 rule src-r1 match destination-address 10.5.2.120/32**

5. Configure a source NAT pool in the rule.

[edit security nat source]
user@host# **set rule-set src-rs1 rule src-r1 then source-nat pool src-p1**

Results   From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
source {
  pool src-p1 {
    address {
      30.5.1.120/32;
    }
  }
  rule-set src-rs1 {
    from zone trust;
    to zone untrust;
    rule src-r1 {
      match {
        source-address 20.5.1.120/32;
        destination-address 10.5.2.120/32;
      }
      then {
        source-nat {
          pool {
            src-p1;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Destination NAT Pool and Rule Set

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

set security nat destination pool des-p1 address 10.5.1.120/32
set security nat destination rule-set des-rs1 from zone trust
set security nat destination rule-set des-rs1 rule des-r1 match source-address 20.5.1.120/32
set security nat destination rule-set des-rs1 rule des-r1 match destination-address 30.5.1.120/32
set security nat destination rule-set des-rs1 rule des-r1 then destination-nat pool des-p1

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a destination NAT pool and rule set:

1. Create a destination NAT pool.

    [edit security nat destination]
    user@host#set pool des-p1 address 10.5.1.120/32

2. Create a destination NAT rule set.

    [edit security nat destination]
    user@host# set rule-set des-rs1 from zone trust

3. Configure a rule that matches packets and translates the source address to the address in the pool.

    [edit security nat destination]
    user@host# set rule-set des-rs1 rule des-r1 match source-address 20.5.1.120/32

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

    [edit security nat destination]
    user@host# set rule-set des-rs1 rule des-r1 match destination-address 30.5.1.120/32

5. Configure a source NAT pool in the rule.

    [edit security nat destination]
    user@host# set rule-set des-rs1 rule des-r1 then destination-nat pool des-p1

Results

From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    [edit]
    user@host# show security nat
    destination {
      pool des-p1 {
        address {
          10.5.1.120/32;
        }

```
      }
      rule-set des-rs1 {
        from zone trust;
        rule des-r1 {
          match {
            source-address 20.5.1.120/32;
            destination-address 30.5.1.120/32;
          }
          then {
            destination-nat {
              pool {
                des-p1;
              }
            }
          }
        }
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring PPTP ALG trace options

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security alg pptp traceoptions flag all
set security alg traceoptions file trace
set security alg traceoptions file size 1g
set security alg traceoptions level verbose
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure PPTP ALG trace options:

1. Enable PPTP ALG trace options.

   ```
   [edit security alg]
   user@host#set pptp traceoptions flag all
   ```

2. Configure a filename to receive output from the tracing operation.

   ```
   [edit security alg]
   user@host#set traceoptions file trace
   ```

3. Specify the maximum trace file size.

   ```
   [edit security alg]
   user@host#set traceoptions file size 1g
   ```

4. Specify the level of tracing output.

   ```
   [edit security alg]
   ```

user@host#**set traceoptions level verbose**

Results   From configuration mode, confirm your configuration by entering the **show security alg** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security alg
traceoptions {
   file trace size 1g;
   level verbose;
   }
pptp traceoptions flag all;
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the PPTP ALG Control Session

Purpose   Verify that the PPTP control session is created and all the PPTP control and data sessions are created.

Action   From operational mode, enter the **show security flow session** command.

```
user@host>show security flow session
 SSession ID: 57, Policy name: pptp, Timeout: 1787
Resource information : PPTP ALG, 1, 0
In: 20.20.20.32/3905 --> 10.10.10.32/1723;tcp, If: ge-0/0/1.0 Pkts: 6, Bytes: 584
Out: 10.10.10.32/1723 --> 20.20.20.32/3905;tcp, If: fe-0/0/2.0 Pkts: 4, Bytes:
352

Session ID: 58, Policy name: pptp, Timeout: 1799
In: 20.20.20.32/0 --> 10.10.10.32/256;gre, If: ge-0/0/1.0
Out: 10.10.10.32/256 --> 20.20.20.32/65001;gre, If: fe-0/0/2.0

Session ID: 59, Policy name: pptp, Timeout: 1787
In: .10.10.10.32/0 --> 20.20.20.32/260;gre, If: ge-0/0/1.0
Out: 20.20.20.32/260 --> 10.10.10.32/65000;gre, If: fe-0/0/2.0
```

Meaning
- **Session ID**—Number that identifies the session. Use this ID to get more information about the session such as policy name or number of packets in and out.

- **Policy name**—Policy name that permitted the traffic.

- **In**—Incoming flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and the source interface for this session is ge-0/0/1.0).

- **Out**—Reverse flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and destination interface for this session is fe-0/0/2.0).

Verifying the PPTP ALG Flow Gate Information

Purpose   Verify that the flow gate is opened for TCP data channel connection.

Action   From operational mode, enter the **show security flow gate** command.

```
user@host>show security flow gate

Hole: 20.0.172.24-20.0.172.24/0-0->21.0.172.38-21.0.172.38/25750-25750
Translated: 2015::172:24/65000->2005::172:108/360
Protocol: gre
Application: PPTP ALG/69
Age: 118 seconds
Flags: 0x0080
Zone: trust
Reference count: 1
Resource: 12-1-1

Hole: 2005::172:108-0-0->2015::172:24-2432-2432
Translated: 21.0.172.38/65001->20.0.172.24/2432
Protocol: gre
Application: PPTP ALG/69
```

```
       Age: 120 seconds
       Flags: 0x8080
       Zone: untrust
       Reference count: 1
       Resource: 12-1-2

     Valid gates: 2
     Pending gates: 0
     Invalidated gates: 0
     Gates in other states: 0
     Total gates: 2
```

Verifying PPTP ALG

Purpose   Verify that the PPTP ALG is enabled.

Action   From operational mode, enter the **show security alg status** command.

```
user@host>show security alg status
ALG Status :
   PPTP      : Enabled
   RSH       : Disabled
   RTSP      : Enabled
   SCCP      : Enabled
   SIP       : Enabled
   TALK      : Enabled
   TFTP      : Enabled
   IKE-ESP   : Disabled
```

Meaning   The output shows the PPTP ALG status as follows:

- Enabled—Shows the PPTP ALG is enabled.

- Disabled—Shows the PPTP ALG is disabled.

Verifying the PPTP Resource Manager Group

Purpose   Verify the total number of resource manager groups and active groups that are used by the PPTP ALG.

Action   From operational mode, enter the **show security resource-manager group active** command.

```
user@host>show security resource-manager group active
Group ID 1: Application - PPTP ALG
       Total groups 19763, active groups 1
```

Verifying the PPTP Resource Information

Purpose   Verify the total number of resources and active resources that are used by the PPTP ALG.

Action   From operational mode, enter the **show security resource-manager resource active** command.

```
user@host>show security resource-manager resource active
Resource ID 2: Group ID - 1, Application - PPTP ALG
```



```
                    Resource ID 1: Group ID - 1, Application - PPTP ALG
                    Total Resources 93286, active resources 2
```

Related
Documentation
- Understanding the PPTP ALG on page 45

CHAPTER 7

Configuring the RPC ALG

Understanding RPC ALGs

Supported Platforms   SRX Series, vSRX

Junos OS supports basic Remote Procedure Call Application Layer Gateway (RPC ALG) services. RPC is a protocol that allows an application running in one address space to access the resources of applications running in another address space as if the resources were local to the first address space. The RPC ALG is responsible for RPC packet processing.

The RPC ALG in Junos OS supports the following services and features:

- Sun Microsystems RPC Open Network Computing (ONC)

- Microsoft RPC Distributed Computing Environment (DCE)

- Dynamic port negotiation

- Ability to allow and deny specific RPC services

- Static Network Address Translation (NAT) and source NAT (with no port translation)

- RPC applications in security policies

Use the RPC ALG if you need to run RPC-based applications such as NFS or Microsoft Outlook. The RPC ALG functionality is enabled by default.

Related Documentation

- ALG Overview on page 3
- Understanding Sun RPC ALGs on page 62
- Understanding Microsoft RPC ALGs on page 67

Understanding Sun RPC ALGs

Supported Platforms SRX Series, vSRX

Sun Microsystems Remote Procedure Call (Sun RPC)—also known as Open Network Computing Remote Procedure Call (ONC RPC)—provides a way for a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

Junos OS supports the Sun RPC as a predefined service and allows and denies traffic based on a security policy you configure. The Application Layer Gateway (ALG) provides the functionality for Juniper Networks devices to handle the dynamic transport address negotiation mechanism of the Sun RPC and to ensure program number-based security policy enforcement. You can define a security policy to permit or deny all RPC requests, or to permit or deny by specific program number. The ALG also supports route mode and Network Address Translation (NAT) mode for incoming and outgoing requests.

When an application or a PC client calls a remote service, it needs to find the transport address of the service. In the case of TCP/UDP, the address is a port number. A typical procedure for this case is as follows:

1. The client sends the GETPORT message to the RPCBIND service on the remote machine. The GETPORT message contains the program number, and version and procedure number of the remote service it is attempting to call.

2. The RPCBIND service replies with a port number.

3. The client calls the remote service using the port number returned.

4. The remote service replies to the client.

A client also can use the CALLIT message to call the remote service directly, without determining the port number of the service. In this case, the procedure is as follows:

1. The client sends a CALLIT message to the RPCBIND service on the remote machine. The CALLIT message contains the program number and the version and procedure number of the remote service it attempting to call.

2. RPCBIND calls the service for the client.

3. RCPBIND replies to the client if the call has been successful. The reply contains the call result and the service's port number.

The Sun RPC ALG dynamically allocates new mapping entries instead of using a default size (512 entries). It also offers a flexible time-based RPC mapping entry that removes the mapping entry (auto-clean) without affecting the associated active RPC sessions, including both control session and data session.

You can define the Sun RPC mapping entry ageout value using the **set security alg sunrpc map-entry-timeout value** command. The ageout value ranges from 1 hour to 72 hours, and the default value is 32 hours.

If the Sun RPC ALG service does not trigger the control negotiation even after 72 hours, the maximum RPC ALG mapping entry value times out and the new data connection to the service fails.

Related
Documentation

- Understanding RPC ALGs on page 61

- Enabling Sun RPC ALGs (J-Web Procedure) on page 63

- Enabling Sun RPC ALGs (CLI Procedure) on page 63

- Understanding Sun RPC Services on page 64

- Understanding Microsoft RPC ALGs on page 67

Enabling Sun RPC ALGs (CLI Procedure)

Supported Platforms   SRX Series, vSRX

The Sun RPC ALG is enabled by default and requires no configuration.

To disable the Sun RPC ALG, enter the following command:

    user@host# set security alg sunrpc disable

To re-enable the Sun RPC ALG, enter the following command:

    user@host# delete security alg sunrpc

Related
Documentation

- Understanding Sun RPC ALGs on page 62

- Enabling Sun RPC ALGs (J-Web Procedure) on page 63

Enabling Sun RPC ALGs (J-Web Procedure)

Supported Platforms   SRX Series

The Sun RPC ALG is enabled by default and requires no configuration.

To disable or re-enable the RPC ALG:

1. Select **Configure>Security>ALG**.

2. Select the **Enable SUNRPC** check box.

3. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options**>**Commit**.

Customizing Sun RPC Applications (CLI Procedure)

Supported Platforms   SRX Series

All Sun RPC applications can be customized by using a predefined application set.

For example, an application can be customized to open the control session only and not allow any data sessions:

```
application-set junos-sun-rpc {
    application junos-sun-rpc-tcp;
    application junos-sun-rpc-udp;
}
```

In the following example, the predefined application set allows data sessions only. It will not work without the control session:

```
application-set junos-sun-rpc-portmap {
    application junos-sun-rpc-portmap-tcp;
    application junos-sun-rpc-portmap-udp;
}
```

To customize all Sun RPC applications with predefined application sets, use both application sets in the policy:

```
application-set [junos-sun-rpc junos-sun-rpc-portmap]
```

> **NOTE:** MS RPC applications are customized in the same way as Sun RPC applications.

Understanding Sun RPC Services

Supported Platforms   SRX Series, vSRX

Sun RPC, also known as Open Network computing remote procedure call (ONC RPC), provides a way for a program running on one host to call procedures in a program running on another host. Sun RPC services are defined by a program identifier. The program identifier is independent of any transport address, and most of the Sun RPC sessions are initiated through TCP or UDP port 111. Each host links the required RPC service to a dynamic TCP or UDP port that is negotiated over the port 111 control channel, allowing the client to connect to either TCP or UDP port 111.

Predefined Sun Microsystems remote procedure call (Sun RPC) services include:

- **junos-sun-rpc-tcp**

- **junos-sun-rpc-udp**

The Sun RPC ALG can be applied by using the following methods:

- ALG default application—Use one of the following predefined applications for control and data connections in your policy:

  - **junos-sun-rpc-any-tcp**

  - **junos-sun-rpc-any-udp**

  - **junos-sun-rpc-mountd-tcp**

  - **junos-sun-rpc-mountd-udp**

  - **junos-sun-rpc-nfs-tcp**

  - **junos-sun-rpc-nfs-udp**

  - **junos-sun-rpc-nlockmgr-tcp**

  - **junos-sun-rpc-nlockmgr-udp**

  - **junos-sun-rpc-portmap-tcp**

  - **junos-sun-rpc-portmap-udp**

  - **junos-sun-rpc-rquotad-tcp**

  - **junos-sun-rpc-rquotad-udp**

  - **junos-sun-rpc-ruserd-tcp**

  - **junos-sun-rpc-ruserd-udp**

  - **junos-sun-rpc-sadmind-tcp**

  - **junos-sun-rpc-sadmind-udp**

  - **junos-sun-rpc-sprayd-tcp**

  - **junos-sun-rpc-sprayd-udp**

  - **junos-sun-rpc-status-tcp**

  - **junos-sun-rpc-status-udp**

  - **junos-sun-rpc-walld-tcp**

  - **junos-sun-rpc-walld-udp**

  - **junos-sun-rpc-ypbind-tcp**

  - **junos-sun-rpc-ypbind-udp**

  - **junos-sun-rpc-ypserv-tcp**

  - **junos-sun-rpc-ypserv-udp**

- Default control application—Use the predefined control through **junos-sun-rpc**:

  - Create an application for data (**USER_DEFINED_DATA**). You can make a set of your own data (for example, **my_rpc_application_set**) and use it in the policy.

  - ALG default application set—Use the predefined application set for control and customized data application in the policy:

    - **junos-sun-rpc** (for control sessions)

    - **junos-sun-rpc-any**

    - **junos-sun-rpc-mountd**

    - **junos-sun-rpc-nfs**

    - **junos-sun-rpc-nfs-access**

    - **junos-sun-rpc-nlockmgr**

    - **junos-sun-rpc-portmap** (for data sessions)

    - **junos-sun-rpc-rquotad**

    - **junos-sun-rpc-ruserd**

    - **junos-sun-rpc-sadmind**

    - **junos-sun-rpc-sprayd**

    - **junos-sun-rpc-status**

    - **junos-sun-rpc-walld**

    - **junos-sun-rpc-ypbind**

    - **junos-sun-rpc-ypserv**

- Custom control and custom data application—Use a customized application:

  - Create an application for control (**USER_DEFINED_CONTROL**) and data (**USER_DEFINED_DATA**).

  - In the policy, use the user–defined application set for a control and customized data application:

    - **USER_DEFINED_CONTROL**

    - **USER_DEFINED_DATA**

Table 3 on page 66 lists predefined Sun RPC services, a program identifier associated with each service, and a description of each service.

Table 3: Predefined Sun RPC Services

Service	Program ID	Description
PORTMAP	100000	Sun RPC Portmapper protocol is a TCP or UDP port-based service that includes TCP or UDP port 111.

Table 3: Predefined Sun RPC Services *(continued)*

Service	Program ID	Description
NFS	100003	Sun RPC Network File System.
MOUNT	100005	Sun RPC mount process.
YPBIND	100007	Sun RPC Yellow Page Bind service.
STATUS	100024	Sun RPC status.

Related Documentation

Understanding Microsoft RPC ALGs

Supported Platforms SRX Series, vSRX

Microsoft Remote Procedure Call (MS-RPC) is the Microsoft implementation of the Distributed Computing Environment (DCE) RPC. Like the Sun RPC, MS-RPC provides a way for a program running on one host to call procedures in a program running on another host. Because of the large number of RPC services and the need to broadcast, the transport address of an RPC service is dynamically negotiated based on the service program's universal unique identifier (UUID). The specific UUID is mapped to a transport address.

Junos OS devices running Junos OS support MS-RPC as a predefined service and allow and deny traffic based on a policy you configure. The Application Layer Gateway (ALG) provides the functionality for Juniper Networks devices to handle the dynamic transport address negotiation mechanism of the MS-RPC, and to ensure UUID-based security policy enforcement. You can define a security policy to permit or deny all RPC requests, or to permit or deny by specific UUID number. The ALG also supports route mode and Network Address Translation (NAT) mode for incoming and outgoing requests.

When both the MS-RPC client and MS-RPC server are 64 bit capable (such as MS Exchange 2008), they negotiate to use NDR64 transfer syntax during the network communication. when you use NDR64, the interface parameters should be encoded according to NDR64 syntax, because the packet format for NDR64 is different from the packet format for NDR20 (32 bit version).

In MS-RPC, there is a remote activation interface of the DCOM Remote Protocol called ISystemActivator (also known as IRemoteSCMActivator). It is used by the Windows Management Instrumentation Command-line (WMIC), Internet Information Services (IIS), and many other applications that are used extensively.

The MS-RPC ALG dynamically allocates new mapping entries instead of using a default size (512 entries). It also offers a flexible time-based RPC mapping entry that removes

the mapping entry (auto-clean) without affecting the associated active RPC sessions, including both control session and data session.

You can define the MS-RPC mapping entry ageout value using the **set security alg msrpc map-entry-timeout value** command. The ageout value ranges from 1 hour to 72 hours, and the default value is 32 hours.

If the MS-RPC ALG service does not trigger the control negotiation even after 72 hours, the maximum MS-RPC ALG mapping entry value times out and the new data connection to the service fails.

Related Documentation

- Understanding RPC ALGs on page 61

- Enabling Microsoft RPC ALGs (J-Web Procedure) on page 70

- Enabling Microsoft RPC ALGs (CLI Procedure) on page 70

- Understanding Microsoft RPC Services on page 71

- Understanding Sun RPC ALGs on page 62

- Verifying the Microsoft RPC ALG Tables on page 71

Configuring the Microsoft RPC ALG

Supported Platforms   SRX Series, vSRX

You can configure the Microsoft RPC ALG using the following three methods:

- Configuring the MS-RPC ALG with a Predefined Microsoft Application on page 68
- Configuring the MS-RPC ALG with a Wildcard UUID on page 69
- Configuring the MS-RPC ALG with a Specific UUID on page 69

Configuring the MS-RPC ALG with a Predefined Microsoft Application

There are several predefined MS applications. To view the predefined Microsoft applications from the CLI, enter the **show configuration groups junos-defaults** command.

```
user@host> show security policies
  from-zone trust to-zone untrust {
    policy p1 {
      match {
        source-address any;
        destination-address any;
        application junos-ms-rpc-msexchange;
      }
      then {
        permit;
      }
    }
  }
```

After you commit the configuration, from the CLI, enter the **show security alg msrpc object-id-map** command to view the output.

```
user@host>  show security alg msrpc object-id-map
UUID                                         OID
1544f5e0-613c-11d1-93df-00c04fd7bd09         0x80000001
a4f1db00-ca47-1067-b31f-00dd010662da         0x80000002
f5cc5a18-4264-101a-8c59-08002b2f8426         0x80000003
```

The output shows that the UUID has been applied for the policy.

Configuring the MS-RPC ALG with a Wildcard UUID

To permit the configuration for any MS RPC application, add the **application junos-ms-rpc-any** statement to the Permit configuration.

```
user@host> show security policies
  from-zone trust to-zone untrust {
  policy p1 {
    match {
      source-address any;
      destination-address any;
      application junos-ms-rpc-any;
    }
    then {
      permit;
    }
  }
}
```

After you commit the configuration, from the CLI, enter the **show security alg msrpc object-id-map** command to view the output.

```
user@host>  show security alg msrpc object-id-map
UUID                                         OID
ffffffff-ffff-ffff-ffff-ffffffffffff         0x80000004
```

Configuring the MS-RPC ALG with a Specific UUID

For applications that have not been predefined, you need to manually configure a specific UUID. For example, to permit a NETLOGON application that has not been predefined, you add the **application msrpc-netlogon** statement to the Permit configuration.

```
user@host> show applications
  application msrpc-netlogon {
  term t1 protocol tcp uuid 12345678-1234-abcd-ef00-01234567cffb;
  term t2 protocol udp uuid 12345678-1234-abcd-ef00-01234567cffb;
  term t3 protocol tcp uuid 12345778-1234-abcd-ef00-0123456789ab;
}
user@host> show security policies
  from-zone trust to-zone untrust {
  match {
    source-address any;
    destination-address any;
    application msrpc-netlogon;
  }
  then {
```

```
          permit;
      }
    }
  }
```

After you commit the configuration, from the CLI, enter the **show security alg msrpc object-id-map** command to verify the Microsoft universal unique identifier to Object ID (UUID-to-OID) mapping table. The Microsoft RPC ALG monitors packets on TCP port 135.

```
user@host> show security alg msrpc object-id-map
UUID                                    OID
12345778-1234-abcd-ef00-0123456789ab    0x80000006
12345678-1234-abcd-ef00-01234567cffb    0x80000005
be617c0-31a5-11cf-a7d8-00805f48a135     0x80000020
e3514235-4b06-11d1-ab04-00c04fc2dcd2    0x80000002
67df7c70-0f04-11ce-b13f-00aa003bac6c    0x80000014
```

> **NOTE:** The show security alg msrpc object-id-map CLI command has a chassis cluster node option to permit the output to be restricted to a particular node or to query the entire cluster. The **show security alg msrpc object-id-map node** CLI command options are <node-id | all | local | primary>.

Related Documentation
- Enabling Microsoft RPC ALGs (J-Web Procedure) on page 70
- Enabling Microsoft RPC ALGs (CLI Procedure) on page 70
- Customizing Microsoft RPC Applications (CLI Procedure) on page 73

Enabling Microsoft RPC ALGs (CLI Procedure)

Supported Platforms   SRX Series, vSRX

The MS-RPC ALG is enabled by default and requires no configuration.

To disable the Microsoft RPC ALG, enter the following command:

user@host# **set security alg msrpc disable**

To reenable the Microsoft RPC ALG, enter the following command:

user@host# **delete security alg msrpc**

Related Documentation
- Understanding Microsoft RPC ALGs on page 67
- Enabling Microsoft RPC ALGs (J-Web Procedure) on page 70
- Verifying the Microsoft RPC ALG Tables on page 71

Enabling Microsoft RPC ALGs (J-Web Procedure)

Supported Platforms   SRX Series, vSRX

The MS-RPC ALG is enabled by default and requires no configuration.

To disable or reenable the Microsoft ALG:

1. Select **Configure>Security>ALG**.

2. Select the **Enable MSRPC** check box.

3. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options>Commit**.

Related Documentation
- Understanding Microsoft RPC ALGs on page 67
- Enabling Microsoft RPC ALGs (CLI Procedure) on page 70
- Verifying the Microsoft RPC ALG Tables on page 71

Verifying the Microsoft RPC ALG Tables

Supported Platforms SRX Series, vSRX

Purpose To verify the Microsoft RPC ALG, display the Microsoft universal unique identifier to Object ID (UUID-to-OID) mapping table. The Microsoft RPC ALG monitors packets on TCP port 135.

Action From the CLI, enter the **show security alg msrpc object-id-map** command.

```
user@host> show security alg msrpc object-id-map
UUID                                        OID
1be617c0-31a5-11cf-a7d8-00805f48a135        0x80000020
e3514235-4b06-11d1-ab04-00c04fc2dcd2        0x80000002
67df7c70-0f04-11ce-b13f-00aa003bac6c        0x80000014
```

> **NOTE:** The **show security alg msrpc object-id-map** CLI command has a chassis cluster node option to permit the output to be restricted to a particular node or to query the entire cluster. The **show security alg msrpc object-id-map node** CLI command options are **<node-id | all | local | primary>**.

Related Documentation
- Enabling Microsoft RPC ALGs (J-Web Procedure) on page 70
- Enabling Microsoft RPC ALGs (CLI Procedure) on page 70
- Customizing Microsoft RPC Applications (CLI Procedure) on page 73

Understanding Microsoft RPC Services

Supported Platforms SRX Series, vSRX

MS-RPC is the Microsoft implementation of the Distributed Computing Environment (DCE) RPC. Like the Sun RPC, the MS-RPC provides a way for a program running on one

host to call procedures in a program running on another host. The MS-RPC is dynamically negotiated based on the service program's universal unique identifier (UUID). The specific UUID is mapped to a transport address.

Predefined Microsoft remote procedure call (MS-RPC) services include:

- **junos-ms-rpc-epm**
- **junos-ms-rpc-tcp**
- **junos-ms-rpc-udp**

MS-RPC application defaults include:

- **junos-ms-rpc-iis-com-1**
- **junos-ms-rpc-iis-com-adminbase**
- **junos-ms-rpc-msexchange-directory-nsp**
- **junos-ms-rpc-msexchange-directory-rfr**
- **junos-ms-rpc-msexchange-info-store**
- **junos-ms-rpc-uuid-any-tcp**
- **junos-ms-rpc-uuid-any-udp**
- **junos-ms-rpc-wmic-admin**
- **junos-ms-rpc-wmic-admin2**
- **junos-ms-rpc-wmic-mgmt**
- **junos-ms-rpc-wmic-webm-callresult**
- **junos-ms-rpc-wmic-webm-classobject**
- **junos-ms-rpc-wmic-webm-level1login**
- **junos-ms-rpc-wmic-webm-login-clientid**
- **junos-ms-rpc-wmic-webm-login-helper**
- **junos-ms-rpc-wmic-webm-objectsink**
- **junos-ms-rpc-wmic-webm-refreshing-services**
- **junos-ms-rpc-wmic-webm-remote-refresher**
- **junos-ms-rpc-wmic-webm-services**
- **junos-ms-rpc-wmic-webm-shutdown**

MS-RPC application-set defaults include:

- **junos-ms-rpc**
- **junos-ms-rpc-any**
- **junos-ms-rpc-iis-com**

- **junos-ms-rpc-msexchange**

- **junos-ms-rpc-wmic**

Table 4 on page 73 lists predefined MS-RPC services, UUID values associated with each service, and a description of each service.

Table 4: Predefined MS-RPC services

Service	UUID	Description
EPM	e1af8308-5d1f-11c9-91a4-08002b14a0fa	MS-RPC Endpoint Mapper (EPM) protocol is a TCP/UDP port-based service that includes TCP/UDP port 135.
EXCHANGE-DATABASE	1a190310-bb9c-11cd-90f8-00aa00466520	Microsoft Exchange Database service.
EXCHANGE-DIRECTORY	f5cc5a18-4264-101a-8c59-08002b2f8426 f5cc5a7c-4264-101a-8c59-08002b2f8426 f5cc59b4-4264-101a-8c59-08002b2f8426	Microsoft Exchange Directory service.
WIN-DNS	50abc2a4-574d-40b3-9d66-ee4fd5fba076	Microsoft Windows DNS server.
WINS	5f52c28-7f9f-101a-b52b-08002b2efabe 811109bf-a4e1-11d1-ab54-00a0c91e9b45	Microsoft WINS service.
WMIC-Webm-Level1Login	f309ad18-d86a-11d0-a075-00c04fb68820	This service allows users to connect to the management services interface in a particular namespace.

Related Documentation

- Understanding Microsoft RPC ALGs on page 67

- Customizing Microsoft RPC Applications (CLI Procedure) on page 73

- Understanding Sun RPC Services on page 64

Customizing Microsoft RPC Applications (CLI Procedure)

Supported Platforms SRX Series, vSRX

MS-RPC applications are customized in the same way as SUN RPC applications.

MS-RPC services in security policies are:

- 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde

- 1453c42c-0fa6-11d2-a910-00c04f990f3b

- 10f24e8e-0fa6-11d2-a910-00c04f990f3b

- 1544f5e0-613c-11d1-93df-00c04fd7bd09

The corresponding TCP/UDP ports are dynamic. To permit them, you use the following statement for each number:

  set applications *application-name* term *term-name* uuid *hex-number*

The ALG maps the program numbers into dynamically negotiated TCP/UDP ports based on these four UUIDs and permits or denies the service based on a policy you configure.

Related
Documentation

- Understanding Microsoft RPC Services on page 71
- Customizing Sun RPC Applications (CLI Procedure) on page 64
- Verifying the Microsoft RPC ALG Tables on page 71

CHAPTER 8

Configuring the RSH ALG

Understanding the RSH ALG

Supported Platforms   SRX Series, vSRX

The Remote Shell (RSH) Application Layer Gateway (ALG) processes RSH packets that initiate requests and open two gates to allow return packets from the reverse direction to the client. One gate is used for an identification (ident) session to apply authorization and the other gate is used for a standard error (stderr) session to transfer an error message.

> _**i**_
>
> NOTE: The RSH ALG does not work if Port Address Translation (PAT) is configured. The RSH requires the port range to be between 512 to 1024. The source NAT module cannot match this port range.

Related Documentation   • Example: Configuring the RSH ALG on page 75

Example: Configuring the RSH ALG

Supported Platforms   SRX Series, vSRX

This example shows how to configure the RSH ALG in route or NAT mode. The configuration allows RSH traffic to pass through a device, and it transfers remote commands and results between a client and a server located on opposite sides of a Juniper Networks device.

Requirements

This example uses the following hardware and software components:

- An SRX Series device

- Two PCs (server and client)

Before you begin:

- Understand the concepts behind ALGs. See "ALG Overview" on page 3

- Understand the basics of RSH ALG. See the "Understanding the RSH ALG" on page 75

Overview

In this example, first you configure network interfaces on the device. Create security zones and assign interfaces to the zones, and configure a policy to allow RSH traffic to go through an SRX Series device.

Then you create a static NAT rule set rs1 with a rule r1 to match with the destination address 40.0.172.10/32, and you create a static NAT prefix with address 40.0.172.45/32.

Next you create a source NAT pool src-p1 with a source rule set src-rs1 to translate packets from interface fe-3/0/0.0 to interface fe-3/0/1.0. For matching packets, the source address is translated to an IP address in the src-p1 pool.

Then you create a destination NAT pool des-p1 with a destination rule set des-rs1 to translate packets from zone trust to destination address 40.0.172.10/32. For matching packets, the destination address is translated to an IP address in the des-p1 pool. Finally, you enable RSH ALG trace options.

Topology

shows the RSH ALG topology.

Figure 4: RSH ALG Topology
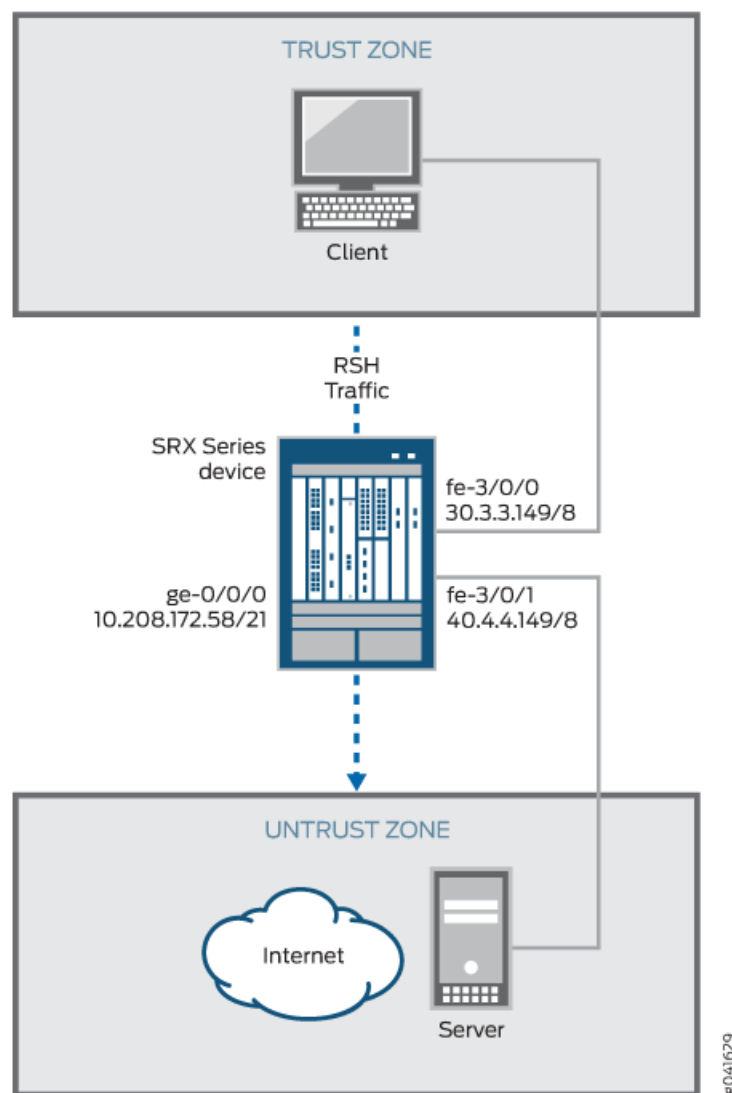
Configuration

To configure the RSH ALG, perform these tasks:

-
-
-
-
-

Configuring a Route Mode

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.208.172.58/21
set interfaces fe-3/0/0 unit 0 family inet address 30.3.3.149/8
set interfaces fe-3/0/1 unit 0 family inet address 40.4.4.149/8
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-3/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-3/0/1.0
set security policies from-zone trust to-zone untrust policy rsh match source-address any
set security policies from-zone trust to-zone untrust policy rsh match destination-address any
set security policies from-zone trust to-zone untrust policy rsh match application junos-rsh
set security policies from-zone trust to-zone untrust policy rsh then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure route mode:

1. Configure interfaces.

    ```
    [edit interfaces]
    user@host#set ge-0/0/0 unit 0 family inet address 10.208.172.58/21
    user@host#set fe-3/0/0 unit 0 family inet address 30.3.3.149/8
    user@host#set fe-3/0/1 unit 0 family inet address 40.4.4.149/8
    ```

2. Configure zones and assign interfaces to the zones.

    ```
    [edit security zones security-zone]
    user@host#set trust host-inbound-traffic system-services all
    user@host#set trust host-inbound-traffic protocols all
    user@host#set trust interfaces fe-3/0/0.0
    user@host#set untrust host-inbound-traffic system-services all
    user@host#set untrust host-inbound-traffic protocols all
    user@host#set untrust interfaces fe-3/0/0.1
    ```

3. Configure an RSH policy that allows RSH traffic from the trust zone to the untrust zone.

    ```
    [edit security policies from-zone trust to-zone untrust]
    user@host#set policy rsh match source-address any
    user@host#set policy rsh match destination-address any
    user@host#set policy rsh match application junos-rsh
    user@host#set policy rsh then permit
    ```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, and **show security policies** commands. If the output does not display

the intended configuration, repeat the configuration instructions in this example for correction.

For brevity, this **show** output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.208.172.58/21;
        }
    }
}
fe-3/0/0 {
    unit 0 {
        family inet {
            address 30.3.3.149/8;
        }
    }
}
fe-3/0/1 {
    unit 0 {
        family inet {
            address 40.4.4.149/8;
        }
    }
}

[edit]
user@host# show security zones
..
    security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-3/0/0.0;
        }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
```

```
      fe-3/0/1.0;
      }
  }
  …

  [edit]
  user@host# show security policies
  from-zone trust to-zone untrust {
    policy rsh {
      match {
        source-address any;
        destination-address any;
        application junos-rsh;
      }
      then {
        permit;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Static NAT Rule Set

CLI Quick
Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat static rule-set rs1 from zone trust
set security nat static rule-set rs1 rule r1 match destination-address 40.0.172.10/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 40.0.172.45/32
```

Step-by-Step
Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a static NAT rule set:

1. Create a static NAT rule set.

    ```
    [edit security nat static rule-set rs1]
    user@host#set from zone trust
    ```

2. Define the rule to match with the destination address.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 match destination-address 40.0.172.10/32
    ```

3. Define the static NAT prefix for the device.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 then static-nat prefix 40.0.172.45/32
    ```

Results From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
static {
  rule-set rs1 {
    from zone trust;
    rule r1 {
      match {
        destination-address 40.0.172.10/32;
      }
      then {
        static-nat {
          prefix {
            40.0.172.45/32;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Source NAT Pool and Rule Set without PAT

CLI Quick Configuration

> NOTE: The RSH ALG does not support PAT configuration. The RSH ALG requires the stderr port range to be between 512 to 1024. The source NAT module cannot match this port range.

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source pool src-p1 address 40.0.172.100/32 to 40.0.172.101/32
set security nat source pool src-p1 port no-translation
set security nat source rule-set src-rs1 from interface fe-3/0/0.0
set security nat source rule-set src-rs1 to interface fe-3/0/1.0
set security nat source rule-set src-rs1 rule r1 match source-address 30.0.0.0/8
set security nat source rule-set src-rs1 rule r1 match destination-address 40.0.0.0/8
set security nat source rule-set src-rs1 rule r1 then source-nat pool src-p1
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a source NAT pool and rule set:

1. Create a source NAT pool.

   ```
   [edit security nat source]
   user@host#set pool src-p1 address 40.0.172.100/32 to 40.0.172.101/32
   ```

2. Create a source NAT pool with no port translation.

   ```
   [edit security nat source ]
   set pool src-p1 port no-translation
   ```

3. Create a source NAT rule set.

   ```
   [edit security nat source]
   user@host# set rule-set src-rs1 from interface fe-3/0/0.0
   user@host# set rule-set src-rs1 to interface fe-3/0/1.0
   ```

4. Configure a rule that matches packets and translates the source address to an address in the source pool.

   ```
   [edit security nat source]
   user@host# set rule-set src-rs1 rule r1 match source-address 30.0.0.0/8
   ```

5. Configure a rule that matches packets and translates the destination address to an address in the source pool.

   ```
   [edit security nat source]
   user@host# set rule-set src-rs1 rule r1 match destination-address 40.0.0.0/8
   ```

6. Configure a source NAT pool in the rule.

   ```
   [edit security nat source]
   user@host# set rule-set src-rs1 rule r1 then source-nat pool src-p1
   ```

Results
From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
source {
  pool src-p1 {
    address {
      40.0.172.100/32 to 40.0.172.101/32;
    }
    port no-translation;
  }
  rule-set src-rs1 {
    from interface fe-3/0/0.0;
    to interface fe-3/0/1.0;
    rule r1 {
      match {
        source-address 30.0.0.0/8;
        destination-address 40.0.0.0/8;
```

```
        }
      then {
        source-nat {
          pool {
            src-p1;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Destination NAT Pool and Rule Set

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat destination pool des-p1 address 40.0.172.45/32
set security nat destination rule-set des-rs1 from zone trust
set security nat destination rule-set des-rs1 rule des-r1 match source-address 30.0.172.12/32
set security nat destination rule-set des-rs1 rule des-r1 match destination-address 40.0.172.10/32
set security nat destination rule-set des-rs1 rule des-r1 then destination-nat pool des-p1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a destination NAT pool and rule set:

1. Create a destination NAT pool.

    ```
    [edit security nat destination]
    user@host#set pool des-p1 address 40.0.172.45/32
    ```

2. Create a destination NAT rule set.

    ```
    [edit security nat destination]
    user@host# set rule-set des-rs1 from zone trust
    ```

3. Configure a rule that matches packets and translates the source address to the address in the pool.

    ```
    [edit security nat destination]
    user@host# set rule-set des-rs1 rule des-r1 match source-address 30.0.172.12/32
    ```

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

    ```
    [edit security nat destination]
    user@host# set rule-set des-rs1 rule des-r1 match destination-address 40.0.172.10/32
    ```

5. Configure a source NAT pool in the rule.

    ```
    [edit security nat destination]
    user@host# set rule-set des-rs1 rule des-r1 then destination-nat pool des-p1
    ```

Results   From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
destination {
  pool des-p1 {
    address {
      40.0.172.45/32;
    }
  }
  rule-set des-rs1 {
    from zone trust;
    rule des-r1 {
      match {
        source-address 30.0.172.12/32;
        destination-address 40.0.172.10/32;
      }
      then {
        destination-nat {
          pool {
            des--p1;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Enabling RSH ALG Trace Options

CLI Quick Configuration   To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security alg rsh traceoptions flag all
set security alg traceoptions file trace
set security alg traceoptions file size 1g
set security alg traceoptions level verbose
```

Step-by-Step Procedure   The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To enable RSH ALG trace options:

1.   Enable RSH ALG trace options.

```
[edit security alg]
user@host#set sql traceoptions flag all
```

2. Configure a filename to receive output from the tracing operation.

[edit security alg]
user@host#**set traceoptions file trace**

3. Specify the maximum trace file size.

[edit security alg]
user@host#**set traceoptions file size 1g**

4. Specify the level of tracing output.

[edit security alg]
user@host#**set traceoptions level verbose**

Results   From configuration mode, confirm your configuration by entering the **show security alg** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security alg
traceoptions {
    file trace size 1g;
    level verbose;
}
rsh traceoptions flag all;
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying the RSH ALG Control Session on page 85
- Verifying the RSH ALG on page 86
- Verifying the RSH ALG Resource Manager Group on page 87
- Verifying the RSH ALG Resource Information on page 87

Verifying the RSH ALG Control Session

Purpose   Verify that the RSH command is executed and all the RSH control and data sessions are created.

Action   From operational mode, enter the **show security flow session** command.

```
user@host>show security flow session
Session ID: 2924, Policy name: rsh/6, Timeout: 2, Valid
Resource information : RSH ALG, 2, 0
  In: 30.0.172.12/1023 --> 40.0.172.45/514;tcp, If: fe-3/0/0.0, Pkts: 7, Bytes:
320
  Out: 40.0.172.45/514 --> 30.0.172.12/1023;tcp, If: fe-3/0/1.0, Pkts: 7, Bytes:
 314

Session ID: 2925, Policy name: rsh/6, Timeout: 2, Valid
Resource information : RSH ALG, 2, 24
  In: 40.0.172.45/44864 --> 30.0.172.12/113;tcp, If: fe-3/0/1.0, Pkts: 5, Bytes:
```

```
278
 Out: 30.0.172.12/113 --> 40.0.172.45/44864;tcp, If: fe-3/0/0.0, Pkts: 5, Bytes:
 345

Session ID: 2926, Policy name: rsh/6, Timeout: 2, Valid
Resource information : RSH ALG, 2, 23
 In: 40.0.172.45/1023 --> 30.0.172.12/1022;tcp, If: fe-3/0/1.0, Pkts: 4, Bytes:
 216
 Out: 30.0.172.12/1022 --> 40.0.172.45/1023;tcp, If: fe-3/0/0.0, Pkts: 3, Bytes:
 164
Total sessions: 3
```

Meaning
- **Session ID**—Number that identifies the session. Use this ID to get more information about the session such as policy name, number of packets in and out.

- **Policy name**—Policy name that permitted the traffic.

- **In**—Incoming flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and source interface for this session is fe-3/0/0.0).

- **Out**—Reverse flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and destination interface for this session is fe-3/0/1.0).

Verifying the RSH ALG

Purpose Verify that the RSH ALG is enabled.

Action From operational mode, enter the **show security alg status** command.

```
user@host>show security alg status
ALG Status :
   PPTP     : Enabled
   RSH      : Disabled
   RTSP     : Enabled
   SCCP     : Enabled
   SIP      : Enabled
   TALK     : Enabled
   TFTP     : Enabled
   IKE-ESP  : Disabled
```

> NOTE: The RSH ALG is disabled by default. To enable the RSH ALG, enter the **set security alg rsh** command in the configuration mode.

Meaning The output shows the RSH ALG status as follows:

- Enabled—Shows the RSH ALG is enabled.

- Disabled—Shows the RSH ALG is disabled.

Verifying the RSH ALG Resource Manager Group

Purpose Verify the total number of resource manager groups and active groups that are used by the RSH ALG.

Action From operational mode, enter the **show security resource-manager group active** command.

```
user@host>show security resource-manager group active
Group ID 1: Application – RSH ALG
    Total groups 677, active groups 1
```

Verifying the RSH ALG Resource Information

Purpose Verify the total number of resources and active resources that are used by the RSH ALG.

Action From operational mode, enter the **show security resource-manager resource active** command.

```
user@host>show security resource-manager resource active
Resource ID 2: Group ID – 1, Application – RSH ALG

    Resource ID 1: Group ID – 1, Application – RSH ALG
   Total Resources 4044, active resources 2
```

Related Documentation
- Understanding the RSH ALG on page 75

Configuring the RTSP ALG

Understanding the RTSP ALG

Supported Platforms   SRX Series, vSRX

Overview

RTSP (Real-Time Streaming Protocol) is an Application Layer protocol for controlling the delivery of data with real-time properties. It is similar in syntax and operation to HTTP/1.1. Unlike SIP and H.323, the purpose of RTSP is to access existing media files over the network and to control the replay of the media. The typical communication is between a client (running RealPlayer for example) and a streaming media server. Commands include the ability to pause and play media files from the remote server.

RTSP is a control channel protocol between the media client and media server. The data channel uses a different protocol, usually Real-Time Transport Protocol (RTP) or RTP Control Protocol (RTCP).

In RTSP standard mode, the client sets up three network channels with the RTSP server when media data is delivered using RTP over UDP.

RTSP runs over TCP. RTP and RTCP run over UDP. The ports for RTP and RTCP packets are dynamically negotiated by the client and server using RTSP. Because RTP and RTCP ports are dynamic, these ports cannot be allowed by a static policy. The main purpose of introducing an RTSP ALG to a firewall is to create dynamic policy (pinhole) according to the result of client/server negotiation so that RTP and RTCP traffic can pass through.

When the client and server reside in different realms, they might not be able to determine how to route to the address of the RTP or RTCP offer given by the peer. In this case, ALG

needs to be involved to do translation for the RTP or RTCP offer address and modify it in the payload.

After the connection is established, the RTSP ALG monitors the messages exchanged between the client and server, tracks the status change of the dialog, and returns all the resources it acquired to support an RTSP dialog back to the system after the dialog has completed or failed.

RTSP Modes

Standard Mode

In RTSP standard mode, the client sets up three network channels with the RTSP server when media data is delivered using RTP over UDP.

A full-duplex TCP connection is used for control and negotiation. A full-duplex UDP channel is used for media data delivery using the RTP packet format. In most cases, RTP is initiated from the server. A full-duplex UDP channel called RTCP is used to provide synchronization information to the client and packet loss information to the server.

Figure 5 on page 90 shows the RTSP ALG standard mode.

Figure 5: RTSP ALG Standard Mode
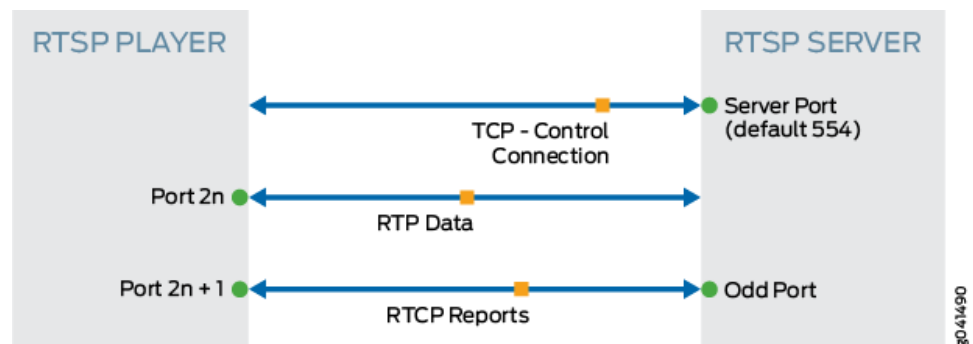
Interleave Mode

In RTSP interleave mode, media data can be made into packets using RTP or RDT over TCP. In this scenario , a single full-duplex TCP connection is used for both control and for media data delivery from the RTSP server to the client. The data stream is interleaved with the RTSP control stream.

Figure 6 on page 90 shows the RTSP ALG interleave mode.

Figure 6: RTSP ALG Interleave Mode
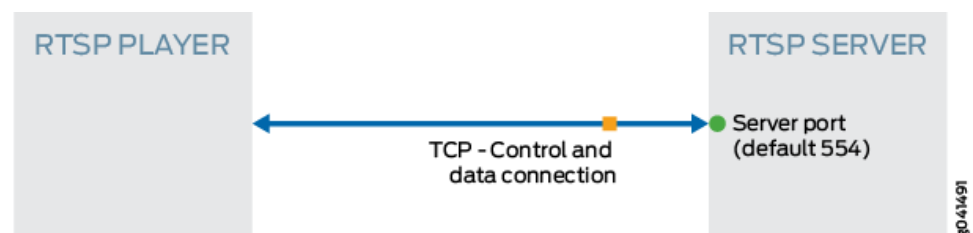
Understanding IPv6 Support for RTSP ALG

Supported Platforms   SRX Series, vSRX

IPv6 is supported on the RTSP ALG along with NAT-PT mode and NAT64 address translation.

This feature enables the RTSP ALG to parse IPv6 RTSP packets, open an IPv6 pattern pinhole, and translate the Layer 7 IPv6 address according to the NAT configuration. Also, support for IPv6 RTSP transaction pass through under permission policy and IPv6 RTSP transaction pass through under NAT-PT and NAT 64 are enabled.

The RTSP ALG with IPv6 support has the following limitations:

- Real-Time Streaming Protocol (RTSP) is an Application Layer protocol for controlling the delivery of data with real-time properties. The RTSP ALG supports a peer client, and the server transmits real-time media; it does not support third-party endpoints involved in the transaction.

- In case of destination NAT or NAT64 for IP address translation, if the RTSP message (including the Session Description Protocol [SDP] application content) length exceeds 2500 bytes, then the RTSP ALG processes only the first 2500 bytes of the message and ignores the rest of the message. In this scenario, the IP address in the RTSP message is not translated if the IP address does not appear in the first 2500 bytes.

Understanding RTSP ALG Messages

Supported Platforms   SRX Series, vSRX

RTSP Messages Format

RTSP is text based and uses the ISO 10646 character set in UTF–8 encoding. Lines are terminated by CRLF, and an empty line is the separator of the message and body.

The first line is called the start-line. For request messages from client to server, the start-line represents the RTSP method. For the response message from server to client,

the start-line represents the RTSP status code as the reply of method. The status code element is a 3-digit integer result code.

RTSP Methods

There are nine types of methods during one transaction.

- **OPTION**—Represents a request for information about the communication options available on the request/response chain identified by the Request-URL. This method allows the client to determine the options, requirements, or both associated with a resource, or the capabilities of a server, without implying a resource action or initiating a resource retrieval.

- **DESCRIBE**—Retrieves the description of a presentation or media object identified by the request URL from a server. This method might use the Accept header to specify the description formats that the client interprets.

- **ANNOUNCE**—Request sent from client to server, this method posts the description of a presentation or media object identified by the request URL to a server. When request sent from server to client, this method updates the session description in real-time.

- **SETUP**—Requests a URI and specifies the transport mechanism to be used for the streamed media.

- **PLAY**—Informs the server to start sending data using the mechanism specified in SETUP.

- **PAUSE**—Requests the stream delivery to be interrupted temporarily.

- **TEARDOWN**—Stops the stream delivery for the given URI, freeing the resource associated with it.

- **GET_PARAMETER**—Retrieves the value of a parameter of a presentation or stream specified in the URI.

- **SET_PARAMETER**—Sets the value of a parameter for a presentation or stream specified by the URI.

RTSP Status Code

The first digit of the status code defines the class of response.

- 1**: Informational—Request received, continuing process.

- 2**: Success

- 3**: Redirection—Further action must be taken in order to complete the request.

- 4**: Client Error—The request contains bad syntax or cannot be fulfilled.

- 5**: Server Error—The server failed to fulfill an apparently valid request.

RTSP Header

The RTSP header consists of the following fields:

- **CSeq**—Specifies the sequence number for an RTSP request-response pair. For every RTSP request containing the given sequence number, there will be a corresponding response having the same number.

- **Content-Length**—Contains the length of the content of the method, that is, after the double CRLF following the last header.

- **TRANSPORT**—Indicates which transport protocol is to be used and configures its parameters.

- **SESSION**—Identifies an RTSP session started by the media server in a SETUP response and concluded by TEARDOWN on the presentation URL.

Related Documentation

- Understanding the RTSP ALG on page 89
- Understanding RTSP ALG Conversation and NAT on page 93
- Example: Configuring the RTSP ALG on page 96

Understanding RTSP ALG Conversation and NAT

Supported Platforms   SRX Series, vSRX

This topic provides details on typical RTSP ALG conversation.

In general, RTP and RTCP packets are bidirectional, which means that either the client or server could initiate an RTP or an RTCP session.

Figure 7 on page 94 describes an example of a sample packet capture in a standard RTSP conversation.

Figure 7: RTSP ALG Conversation
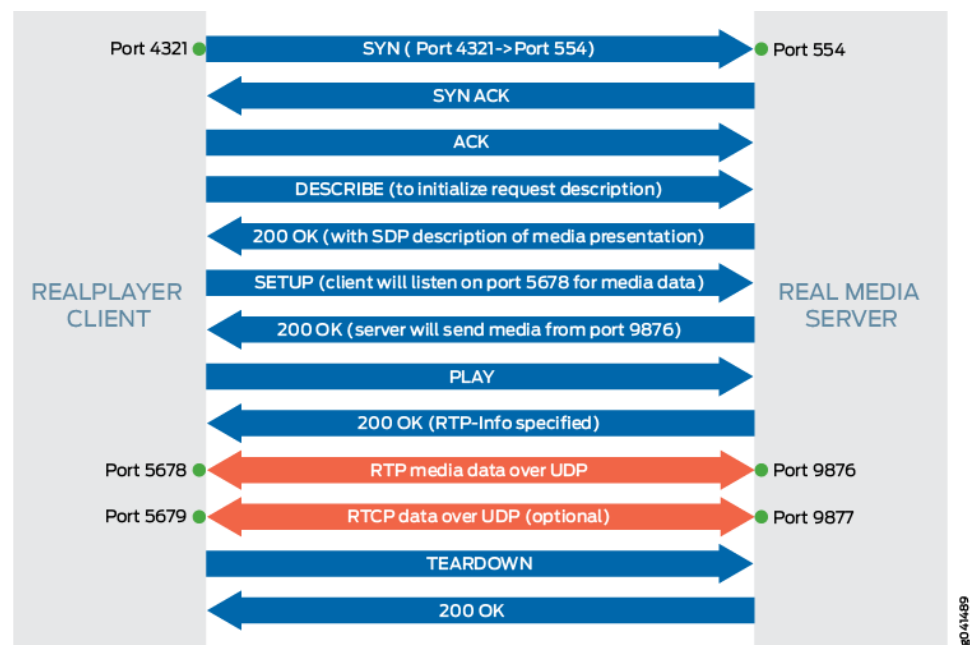
The RTSP ALG performs the following actions for a RTSP sample packet capture in a standard RTSP conversation:

1. Monitors SETUP and 200 OK messages.

2. Receives negotiated ports (6543 and 8765 in this example)

3. Opens a pinhole for UDP media data from server to client.

4. Receives the IP address in payload and translates the address if NAT is required.

   Table 5 on page 94 describes the RTSP payload IP NAT.

Table 5: RTSP Payload IP NAT

	Forward(C->S)	Reverse(S->C)	Pinhole	Payload IP Translate	Payload Port Translate
No NAT	A/4321->B/554	A/4321<-B/554	B/9876->A/5678 A/5678->B/9876	N/A	N/A
Source NAT (IPvx)	A/4321->B/554	A'/P'<-B/554	B/9876->A'/P'' A/5678->B/9876	N/A (*)	5678<->P''
Destination NAT (IPvx)	A/4321->B'/554	A/4321<-B/554	B/9876->A/5678 A/5678->B'/9876	B' -> B (**)	N/A

Table 5: RTSP Payload IP NAT *(continued)*

	Forward(C->S)	Reverse(S->C)	Pinhole	Payload IP Translate	Payload Port Translate
NAT64	A/4321->B''/554	A''/Q'<-B/554	B/9876->A''/Q'' A/5678->B''/9876	B''(IPv6)->B(IPv4)	5678<->Q''
NAT46	A/4321->B'''/554	A'''/R'<-B/554	B/9876->A'''/R'' A/5678->B'''/9876	B'''(IPv4)->B(IPv6)	5678<->R''

In Table 5 on page 94, the following letters and symbols are used:

- A—RTSP client IP address

- A'—Translated IPv4 or IPv6 address of RTSP client

- A''—Translated IPv4 address

- A'''—Translated IPv6 address

- B—RTSP server IP address

- B'—RTSP server IP address before destination NAT

- B''—RTSP server IP address at IPv6 realm

- B'''— RTSP server IP address at IPv4 realm

- P'—Translated Port(translates from 4321) of RTSP client

- P''—Translated Port(translates from 5678 in message payload) of RTSP client

- Q'—Translated (IPv6 to IPv4) Port(translates from 4321) of RTSP client

- Q''—Translated (IPv6 to IPv4) Port (translates from 5678 in message payload) of RTSP client

- R'—Translated (IPv4 to IPv6) Port (translates from 4321) of RTSP client

- R''—Translated (IPv4 to IPv6) Port (translates from 5678 in message payload) of RTSP client

- (*)—RTSP server IP address B appears in payload message; it does not need to translate

- (**)—IP address B' appears in payload message from client to server; it needs to translate to B

Related Documentation

-

-

-

Example: Configuring the RTSP ALG

Supported Platforms   SRX Series, vSRX

This example shows how to configure the RTSP ALG to pass through RTSP traffic with a source NAT pool on Juniper Networks devices.

Requirements

- Configure proxy ARP for all IP addresses in the source NAT pool.

- Enable the RTSP ALG.

- Understand the basics concepts of the RTSP ALG. See "Understanding the RTSP ALG" on page 89.

Overview

In this example, the RTSP ALG is configured to monitor and allow RTSP traffic transferring media between client and server located on opposite sides of a Juniper Networks device.

Configuration

Enabling RTSP ALG

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter **commit** from configuration mode.

To configure proxy ARP for all IP addresses in the source NAT pool and to enable RTSP ALG:

```
set security nat proxy-arp interface <interface-name> address 10.10.10.1/32 to 10.10.10.10/32
set security alg rtsp
```

Enter **commit** from configuration mode.

Configuring a NAT Source Pool and Rule Set and a Policy

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your

network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

set security nat source pool pool1 address 10.10.10.1/32 to 10.10.10.10/32
set security zones security-zone green address-book address sa1 1.1.1.0/24
set security zones security-zone red address-book address da1 2.2.2.0/24
set security nat source rule-set rs1 from zone green
set security nat source rule-set rs1 to zone red
set security nat source rule-set rs1 rule r1 match source-address 1.1.1.0/24
set security nat source rule-set rs1 rule r1 match destination-address 2.2.2.0/24
set security nat source rule-set rs1 rule r1 then source-nat pool pool1

set security policy from-zone green to-zone red policy pol1 match destination-address da1
set security policy from-zone green to-zone red policy pol1 match source-address sa1
set security policy from-zone green to-zone red policy pol1 match application junos-rtsp
set security policy from-zone green to-zone red policy pol1 then permit

Enter **commit** from configuration mode.

> **NOTE:** If you are not sure of the RTSP client and server IP address, you can replace "da1" and "sa1" with "any".

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a source NAT pool:

1. Create a NAT source pool.

   [edit security]
   user@host# **set nat source pool pool1 address 10.10.10.1/32 to 10.10.10.10/32**

2. Configure security zone address book entries.

   [edit security zones security-zone]
   user@host# **set green address-book address sa1 1.1.1.0/24**
   user@host# **set red address-book address da1 2.2.2.0/24**

3. Create a NAT source rule set.

   [edit security nat source rule-set rs1]
   user@host# **set from zone green**
   user@host# **set to zone red**
   user@host# **set rule r1 match source-address 1.1.1.0/24**
   user@host# **set rule r1 match destination-address 2.2.2.0/24**
   user@host# **set rule r1 then source-nat pool pool1**

4. Configure a policy.

   [edit security policies from-zone green to-zone red policy pol1]
   user@host# **set match source-address sa1**
   user@host# **set match destination-address da1**
   user@host# **set match application junos-rtsp**
   user@host# **set then permit**

Results   From configuration mode, confirm your configuration by entering the **show security nat** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit ]
user@host# show security nat
source {
  pool pool1 {
    address {
      10.10.10.1/32 to 10.10.10.10/32;
    }
  }
  rule-set rs1 {
    from zone green;
    to zone red;
    rule r1 {
      match {
        source-address 1.1.1.0/24;
        destination-address 2.2.2.0/24;
      }
      then {
        source-nat {
          pool {
            pool1;
          }
        }
      }
    }
  }
}

[edit]
user@host# show security policies
from-zone green to-zone red {policy pol1 {
  policy pol1 {
    match {
      source-address sa1;
      destination-address da1;
      application [junos-rtsp];
    }
    then {
      permit;
    }
  }
}
default-policy {
  permit-all;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring RTSP ALG trace options

CLI Quick Configuration   To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network

configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

> **set security alg rtsp traceoptions flag all**
> **set security alg traceoptions file trace**
> **set security alg traceoptions file size 1g**
> **set security alg traceoptions level verbose**

Step-by-Step Procedure

To configure RTSP ALG trace options:

1. Enable RTSP ALG trace options.

   > [edit security alg]
   > user@host# **set rtsp traceoptions flag all**

2. Configure a filename to receive output from the tracing operation.

   > [edit security alg]
   > user@host# **set traceoptions file trace**

3. Specify the maximum trace file size.

   > [edit security alg]
   > user@host# **set traceoptions file size 1g**

4. Specify the level of tracing output.

   > [edit security alg]
   > user@host# **set traceoptions level verbose**

Results

From configuration mode, confirm your configuration by entering the **show security alg** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

> [edit]
> user@host# **show security alg**
> traceoptions {
>   file trace size 1g;
>   level verbose;
>   }
> rtsp traceoptions flag all;

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying RTSP ALG on page 100
- Verifying the RTSP ALG Control Session on page 100
- Verifying the RTSP ALG Flow Gate Information on page 101
- Verifying the RTSP Resource Manager Group on page 102
- Verifying the RTSP Resource Information on page 102

Verifying RTSP ALG

Purpose Verify that the RTSP ALG is enabled.

Action From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status

DNS       : Enabled
FTP       : Enabled
H323      : Enabled
RTSP      : Enabled
```

Meaning The output shows the RTSP ALG status as follows:

- Enabled—Shows the RTSP ALG is enabled.

- Disabled—Shows the RTSP ALG is disabled.

Verifying the RTSP ALG Control Session

Purpose Verify that the control session is created and all the RTSP control and data sessions are created.

Action From operational mode, enter the **show security flow session** command.

```
user@host>show security flow session
Flow Sessions on FPC5 PIC0:

Session ID: 100004087, Policy name: dns-alg/4, Timeout: 1798, Valid
Resource information : RTSP ALG, 1, 0
  In: 1.1.0.100/59889 --> 1.1.0.202/554;tcp, If: ge-0/0/1.0, Pkts: 28, Bytes:
7618
  Out: 1.1.0.202/554 --> 1.1.0.100/59889;tcp, If: ge-0/0/2.0, Pkts: 27, Bytes:
24304

Session ID: 100004088, Policy name: dns-alg/4, Timeout: 120, Valid
Resource information : RTSP ALG, 1, 1
  In: 1.1.0.202/5004 --> 1.1.0.100/62092;udp, If: ge-0/0/2.0, Pkts: 19, Bytes:
17013
  Out: 1.1.0.100/62092 --> 1.1.0.202/5004;udp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 100004089, Policy name: dns-alg/4, Timeout: 120, Valid
Resource information : RTSP ALG, 1, 4
  In: 1.1.0.202/5004 --> 1.1.0.100/62094;udp, If: ge-0/0/2.0, Pkts: 433, Bytes:
346183
  Out: 1.1.0.100/62094 --> 1.1.0.202/5004;udp, If: ge-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 100004090, Policy name: dns-alg/4, Timeout: 120, Valid
Resource information : RTSP ALG, 1, 3
  In: 1.1.0.100/62093 --> 1.1.0.202/5005;udp, If: ge-0/0/1.0, Pkts: 2, Bytes: 260

  Out: 1.1.0.202/5005 --> 1.1.0.100/62093;udp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0
Total sessions: 4
```

Meaning
- **Session ID**—Number that identifies the session. Use this ID to get more information about the session such as policy name or number of packets in and out.

- **Policy name**—Policy name that permitted the traffic.

- **In**—Incoming flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and the source interface for this session is ge-0/0/1.0).

- **Out**—Reverse flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and destination interface for this session is fe-0/0/2.0).

Verifying the RTSP ALG Flow Gate Information

Purpose   Verify that the flow gate is opened for TCP data channel connection.

Action   From operational mode, enter the **show security flow gate** command.

```
user@host>show security flow gate

 Flow Gates on FPC5 PIC0:

Hole: 1.1.0.202-1.1.0.202/5005-5005->1.1.0.100-1.1.0.100/62093-62093
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: RTSP ALG/11
  Age: 32 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 4-1-2

Hole: 1.1.0.100-1.1.0.100/62093-62093->1.1.0.202-1.1.0.202/5005-5005
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: RTSP ALG/11
  Age: 32 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 4-1-3

Hole: 1.1.0.202-1.1.0.202/5004-5004->1.1.0.100-1.1.0.100/62094-62094
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: RTSP ALG/11
  Age: 32 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 4-1-4

Hole: 1.1.0.100-1.1.0.100/62094-62094->1.1.0.202-1.1.0.202/5004-5004
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: RTSP ALG/11
  Age: 32 seconds
  Flags: 0x0080
```

```
    Zone: trust
    Reference count: 1
    Resource: 4-1-5

Valid gates: 4
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 4
```

Meaning   The sample output shows that the flow gate is opened for TCP data channel connection.

Verifying the RTSP Resource Manager Group

Purpose   Verify the total number of resource manager groups and active groups that are used by the RTSP ALG.

Action   From operational mode, enter the **show security resource-manager group active** command.

```
user@host>show security resource-manager group active
Group ID 1: Application - RTSP ALG
      Total groups 19763, active groups 1
```

Meaning   The sample output shows the total number of resource manager groups and active groups that are used by the RTSP ALG.

Verifying the RTSP Resource Information

Purpose   Verify the total number of resources and active resources that are used by the RTSP ALG.

Action   From operational mode, enter the **show security resource-manager resource active** command.

```
user@host>show security resource-manager resource active
Resource ID 2: Group ID - 1, Application - RTSP ALG

      Resource ID 1: Group ID - 1, Application - RTSP ALG
      Total Resources 93286, active resources 2
```

Meaning   The sample output shows the total number of resources and active resources that are used by the RTSP ALG.

Related Documentation

- ALG Overview on page 3

- Understanding the RTSP ALG on page 89

- Understanding RTSP ALG Messages on page 91

- Understanding RTSP ALG Conversation and NAT on page 93

Configuring the SQLNET ALG

Understanding the SQLNET ALG

Supported Platforms   SRX Series, vSRX

The SQLNET Application Layer Gateway (ALG) processes Transparent Network Substrate (TNS) REDIRECT packets for IP addresses and port information. The SQLNET ALG performs Network Address Translation (NAT) on the payload of the TNS REDIRECT packet, opens a pinhole for a new connection from a client to a server, and transfers data between a client and a server located on opposite sides of a Juniper Networks device.

SQLNET ALG supports the following types of data transfer modes:

- Redirect mode — connect-redirect type

- Interleave mode — connect-accept type

- Load balance — connect-redirect-connect-redirect type

SQLNET allows remote data access between applications and the Oracle database, or among multiple Oracle databases. SQLNET primarily establishes and maintains connection between a client application and an Oracle database server. SQLNET has several communication layers that enable clients and database servers to share, modify, and manipulate data.

Oracle SQL servers use the SQLNET protocol to execute SQL commands from clients, including load balancing and application-specific services. The SQLNET protocol uses TNS as its networking architecture, and all SQLNET traffic is encapsulated into TNS packet format.

The SQLNET ALG monitors control packets, opens pinhole for data traffic, and performs NAT and port rewrites. Support of stateful firewall and NAT services are required to configure the SQLNET ALG for TCP port 1521.

Related Documentation
- Example: Configuring the SQLNET ALG on page 104

Example: Configuring the SQLNET ALG

Supported Platforms   SRX Series, vSRX

The SQLNET ALG processes TNS REDIRECT packets, performs NAT, and opens a pinhole for a new connection from a client to a server.

This example shows how to configure the SQLNET ALG in route or NAT mode, allow SQLNET traffic to pass through a device, and transfer data between a client and a server located on opposite sides of a Juniper Networks device.

- Requirements on page 104
- Overview on page 104
- Configuration on page 105
- Verification on page 113

Requirements

This example uses the following hardware and software components:

- An SRX Series device
- Two PCs (client and server)

Before you begin:

- Understand the concepts behind ALGs. See "ALG Overview" on page 3.
- Understand the basics of SQLNET ALG . See "Understanding the SQLNET ALG" on page 103.

Overview

In this example, first you configure network interfaces on the device. Create security zones and assign interfaces to the zones, and configure a policy to allow SQLNET traffic to go through an SRX Series device.

Then you create a static NAT rule set rs1 with a rule r1 to match with the destination address 40.0.172.10/32, and you create a static NAT prefix with address 40.0.172.45/32.

Next you create a source NAT pool src-p1 with a source rule set src-rs1 to translate packets from interface fe-3/0/0.0 to interface fe-3/0/1.0. For matching packets, the source address is translated to an IP address in the src-p1 pool.

Then you create a destination NAT pool des-p1 with a destination rule set des-rs1 to translate packets from zone trust to destination address 40.0.172.10/32. For matching packets, the destination address is translated to an IP address in the des-p1 pool. Finally, you enable SQLNET ALG trace options.

Topology

shows the SQLNET ALG topology.

Figure 8: SQLNET ALG Topology
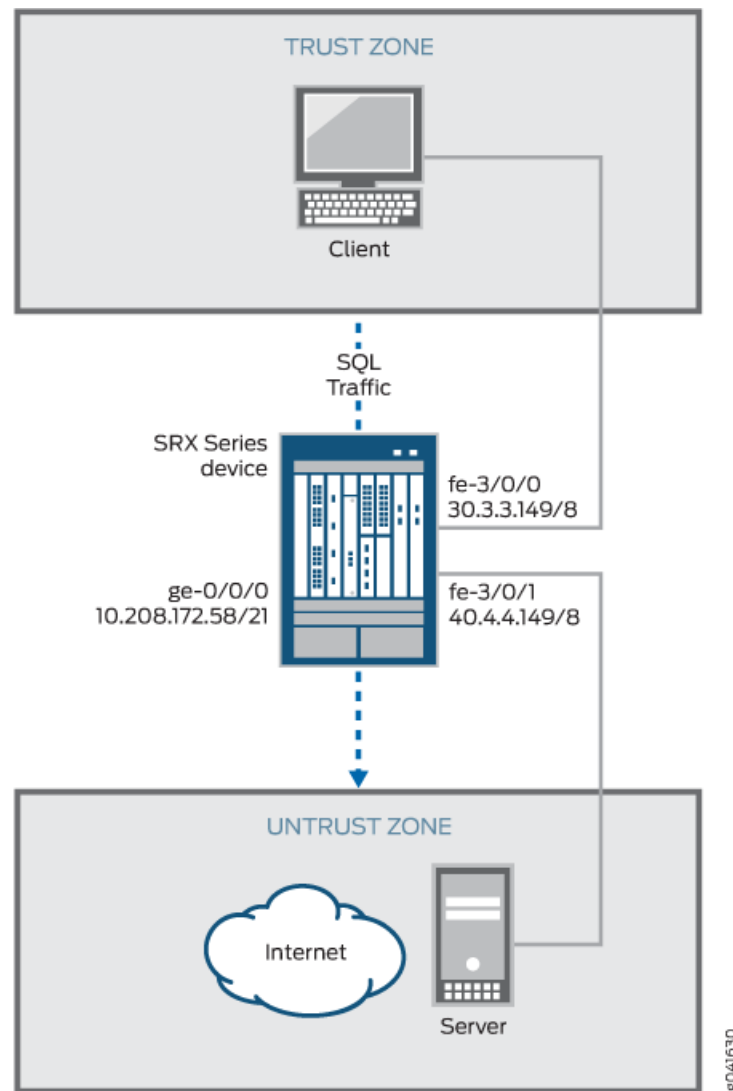
Configuration

To configure the SQLNET ALG, perform these tasks:

-
-
-
-
-

Configuring a Route Mode

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.208.172.58/21
set interfaces fe-3/0/0 unit 0 family inet address 30.3.3.149/8
set interfaces fe-3/0/1 unit 0 family inet address 40.4.4.149/8
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-3/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-3/0/1.0
set security policies from-zone trust to-zone untrust policy sql match source-address any
set security policies from-zone trust to-zone untrust policy sql match destination-address any
set security policies from-zone trust to-zone untrust policy sql match application junos-sqlnet-v2
set security policies from-zone trust to-zone untrust policy sql then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure route mode:

1. Configure interfaces.

    ```
    [edit interfaces]
    user@host# set ge-0/0/0 unit 0 family inet address 10.208.172.58/21
    user@host# set fe-3/0/0 unit 0 family inet address 30.3.3.149/8
    user@host# set fe-3/0/1 unit 0 family inet address 40.4.4.149/8
    ```

2. Configure zones and assign interfaces to the zones.

    ```
    [edit security zones security-zone]
    user@host# set trust host-inbound-traffic system-services all
    user@host# set trust host-inbound-traffic protocols all
    user@host# set trust interfaces fe-3/0/0.0
    user@host# set untrust host-inbound-traffic system-services all
    user@host# set untrust host-inbound-traffic protocols all
    user@host# set untrust interfaces fe-3/0/1.0
    ```

3. Configure a SQL policy that allows SQL traffic from the trust zone to the untrust zone.

    ```
    [edit security policies from-zone trust to-zone untrust ]
    user@host# set policy sql match source-address any
    user@host# set policy sql match destination-address any
    user@host# set policy sql match application junos-sqlnet-v2
    user@host# set policy sql then permit
    ```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, and **show security policies** commands. If the output does not display

the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.208.172.58/21;
        }
    }
}
fe-3/0/0 {
    unit 0 {
        family inet {
            address 30.3.3.149/8;
        }
    }
}
fe-3/0/1 {
    unit 0 {
        family inet {
            address 40.4.4.149/8;
        }
    }
}

[edit]
user@host# show security zones
...
    security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-3/0/0.0;
        }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
```

```
        fe-3/0/1.0;
      }
    }
    …

    [edit]
    user@host# show security policies
    from-zone trust to-zone untrust {
      policy sql {
        match {
          source-address any;
          destination-address any;
          application junos-sqlnet-v2;
        }
        then {
          permit;
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Static NAT Rule Set

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat static rule-set rs1 from zone trust
set security nat static rule-set rs1 rule r1 match destination-address 40.0.172.10/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 40.0.172.45/32
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a static NAT rule set:

1. Create a static NAT rule set.

    ```
    [edit security nat static rule-set rs1]
    user@host#set from zone trust
    ```

2. Define a rule to match with the destination address.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 match destination-address 40.0.172.10/32
    ```

3. Define a static NAT prefix for the device.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 then static-nat prefix 40.0.172.45/32
    ```

Results From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
static {
  rule-set rs1 {
    from zone trust;
    rule r1 {
      match {
        destination-address 40.0.172.10/32;
      }
      then {
        static-nat {
          prefix {
            40.0.172.45/32;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Source NAT Pool and Rule Set

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source pool src-p1 address 40.0.172.100/32 to 40.0.172.101/32
set security nat source rule-set src-rs1 from interface fe-3/0/0.0
set security nat source rule-set src-rs1 to interface fe-3/0/1.0
set security nat source rule-set src-rs1 rule r1 match source-address 30.0.0.0/8
set security nat source rule-set src-rs1 rule r1 match destination-address 40.0.0.0/8
set security nat source rule-set src-rs1 rule r1 then source-nat pool src-p1
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a source NAT pool and rule set:

1. Create a source NAT pool.

    ```
    [edit security nat source]
    user@host#set pool src-p1 address 40.0.172.100/32 to 40.0.172.101/32
    ```

2. Create a source NAT rule set.

    ```
    [edit security nat source]
    user@host# set rule-set src-rs1 from interface fe-3/0/0.0
    user@host# set rule-set src-rs1 to interface fe-3/0/1.0
    ```

3. Configure a rule that matches packets and translates the source address to an address in the source pool.

```
[edit security nat source]
user@host# set rule-set src-rs1 rule r1 match source-address 30.0.0.0/8
```

4. Configure a rule that matches packets and translates the destination address to an address in the source pool.

```
[edit security nat source]
user@host# set rule-set src-rs1 rule r1 match destination-address 40.0.0.0/8
```

5. Configure a source NAT pool in the rule.

```
[edit security nat source]
user@host# set rule-set src-rs1 rule r1 then source-nat pool src-p1
```

Results   From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
source {
    pool src-p1 {
        address {
            40.0.172.100/32 to 40.0.172.101/32;
        }
    }
    rule-set src-rs1 {
        from interface fe-3/0/0.0;
        to interface fe-3/0/1.0;
        rule r1 {
            match {
                source-address 30.0.0.0/8;
                destination-address 40.0.0.0/8;
            }
            then {
                source-nat {
                    pool {
                        src-p1;
                    }
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Destination NAT Pool and Rule Set

CLI Quick   To quickly configure this example, copy the following commands, paste them into a text
Configuration   file, remove any line breaks, change any details necessary to match your network

configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat destination pool des-p1 address 40.0.172.45/32
set security nat destination rule-set des-rs1 from zone trust
set security nat destination rule-set des-rs1 rule des-r1 match source-address 30.0.172.12/32
set security nat destination rule-set des-rs1 rule des-r1 match destination-address 40.0.172.10/32
set security nat destination rule-set des-rs1 rule des-r1 then destination-nat pool des-p1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a destination NAT pool and rule set:

1. Create a destination NAT pool.

   ```
   [edit security nat destination]
   user@host#set pool des-p1 address 40.0.172.45/32
   ```

2. Create a destination NAT rule set.

   ```
   [edit security nat destination]
   user@host# set rule-set des-rs1 from zone trust
   ```

3. Configure a rule that matches packets and translates the source address to the address in the pool.

   ```
   [edit security nat destination]
   user@host# set rule-set des-rs1 rule des-r1 match source-address 30.0.172.12/32
   ```

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

   ```
   [edit security nat destination]
   user@host# set rule-set des-rs1 rule des-r1 match destination-address 40.0.172.10/32
   ```

5. Configure a source NAT pool in the rule.

   ```
   [edit security nat destination]
   user@host# set rule-set des-rs1 rule des-r1 then destination-nat pool des-p1
   ```

Results

From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
destination {
  pool des-p1 {
    address {
      40.0.172.45/32;
    }
  }
  rule-set des-rs1 {
    from zone trust;
    rule des-r1 {
      match {
```

```
                source-address 30.0.172.12/32;
                destination-address 40.0.172.10/32;
            }
            then {
                destination-nat {
                    pool {
                        des-p1;
                    }
                }
            }
        }
    }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Enabling SQLNET ALG Trace Options

CLI Quick Configuration   To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security alg sql traceoptions flag all
set security alg traceoptions file trace
set security alg traceoptions file size 1g
set security alg traceoptions level verbose
```

Step-by-Step Procedure   The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To enable SQLNET ALG trace options:

1. Enable SQLNET ALG trace options.

   [edit security alg]
   user@host#**set sql traceoptions flag all**

2. Configure a filename to receive output from the tracing operation.

   [edit security alg]
   user@host#**set traceoptions file trace**

3. Specify the maximum trace file size.

   [edit security alg]
   user@host#**set traceoptions file size 1g**

4. Specify the level of tracing output.

   [edit security alg]
   user@host#**set traceoptions level verbose**

Results   From configuration mode, confirm your configuration by entering the **show security alg** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security alg
  traceoptions {
    file trace size 1g;
    level verbose;
  }
sql traceoptions flag all;
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

-
-
-
-

Verifying the SQLNET ALG Control Session

Purpose Verify that the SQL command is executed and all the SQL control and data sessions are created.

Action From operational mode, enter the **show security flow session** command.

```
user@host>show security flow session
Session ID: 10880, Policy name: sql, Timeout: 2, Valid
 In: 30.0.172.12/52315 --> 40.0.172.35/1521;tcp, If: fe-3/0/0.0, Pkts: 6, Bytes:
 492
 Out: 40.0.172.35/1521 --> 30.0.172.12/52315;tcp, If: fe-3/0/1.0, Pkts: 4, Bytes:
 227

Session ID: 10881, Policy name: sql, Timeout: 1800, Valid
Resource information : SQLV2 ALG, 5, 18
 In: 30.0.172.12/45944 --> 40.0.172.35/1114;tcp, If: fe-3/0/0.0, Pkts: 18, Bytes:
 4240
 Out: 40.0.172.35/1114 --> 30.0.172.12/45944;tcp, If: fe-3/0/1.0, Pkts: 15,
Bytes: 3989
Total sessions: 2
```

Meaning
- **Session ID**—Number that identifies the session. Use this ID to get more information about the session such as policy name, number of packets in and out.

- **Policy name**—Policy name that permitted the traffic.

- **In**—Incoming flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and source interface for this session is fe-3/0/0.0).

- **Out**—Reverse flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and destination interface for this session is fe-3/0/1.0).

Verifying the SQLNET ALG

Purpose   Verify that the SQLNET ALG is enabled.

Action   From operational mode, enter the **show security alg status** command.

```
user@host>show security alg status
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Disabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

Meaning   The output shows the SQLNET ALG status as follows:

- Enabled—Shows the SQLNET ALG is enabled

- Disabled—Shows the SQLNET ALG is disabled.

Verifying the SQLNET ALG Resource Manager Group

Purpose   Verify the total number of resource manager groups and active groups that are used by the SQLNET ALG.

Action   From operational mode, enter the **show security resource-manager group active** command.

```
user@host>show security resource-manager group active
Group ID 1: Application - SQL ALG
    Total groups 677, active groups 1
```

Verifying the SQLNET ALG Resource Information

Purpose   Verify the total number of resources and active resources that are used by the SQLNET ALG.

Action   From operational mode, enter the **show security resource-manager resource active** command.

```
user@host>show security resource-manager resource active
Resource ID 2: Group ID - 1, Application - SQL ALG

      Resource ID 1: Group ID - 1, Application - SQL ALG
    Total Resources 4044, active resources 2
```

**Related
Documentation**

- Understanding the SQLNET ALG on page 103

CHAPTER 11

Configuring the TALK ALG

Understanding the TALK ALG

Supported Platforms   SRX Series, vSRX

The TALK ALG is a visual communication program used for interactive communication between two users. The TALK ALG processes TALK packets, performs Network Address Translation (NAT), and opens two gates (TCP and UDP) on the receiver side. One gate is used for the next LOOKUP packet. The other gate is used for make a connection from a client to a server and to initiate communication between a client and a server located on opposite sides of a Juniper Networks device.

There are two types of TALK servers: ntalkd and talkd.

The TALK ALG processes both ntalk and talkd packets. The TALK ALG uses port UDP517 and port UDP518 to establish a connection between a client and a server.

Related Documentation

Example: Configuring the TALK ALG

Supported Platforms   SRX Series, vSRX

This example show how to configure the TALK ALG in route or NAT mode, allow the TALK traffic to pass through a device, and initiate communication between a client and a server located on opposite sides of a Juniper Networks device.

Requirements

This example uses the following hardware and software components:

- An SRX Series device
- Two PCs (client and server)

Before you begin:

- Understand the concepts behind ALGs. See "ALG Overview" on page 3.
- Understand the basics of TALK ALG. See "Understanding the TALK ALG" on page 117.

Overview

In this example, first you configure network interfaces on the device, create security zones and assign interfaces to the zones, and configure a policy to allow TALK traffic to go through an SRX Series device.

Then you create a static NAT rule set rs1 with a rule r1 to match the destination address 40.5.2.120/32, and you create a static NAT prefix with address 20.5.2.120/32.

Next you create a source NAT pool src-p1 with a source rule set src-rs1 to translate packets from zone trust to zone untrust. For matching packets, the source address is translated to an IP address in the src-p1 pool.

Then you create a destination NAT pool des-p1 with a destination rule set des-rs1 to translate packets from zone trust to destination address 40.5.2.121/32. For matching packets, the destination address is translated to an IP address in the des-p1 pool. Finally, you configure TALK ALG trace options.

Topology

shows the TALK ALG topology.

Figure 9: TALK ALG Topology
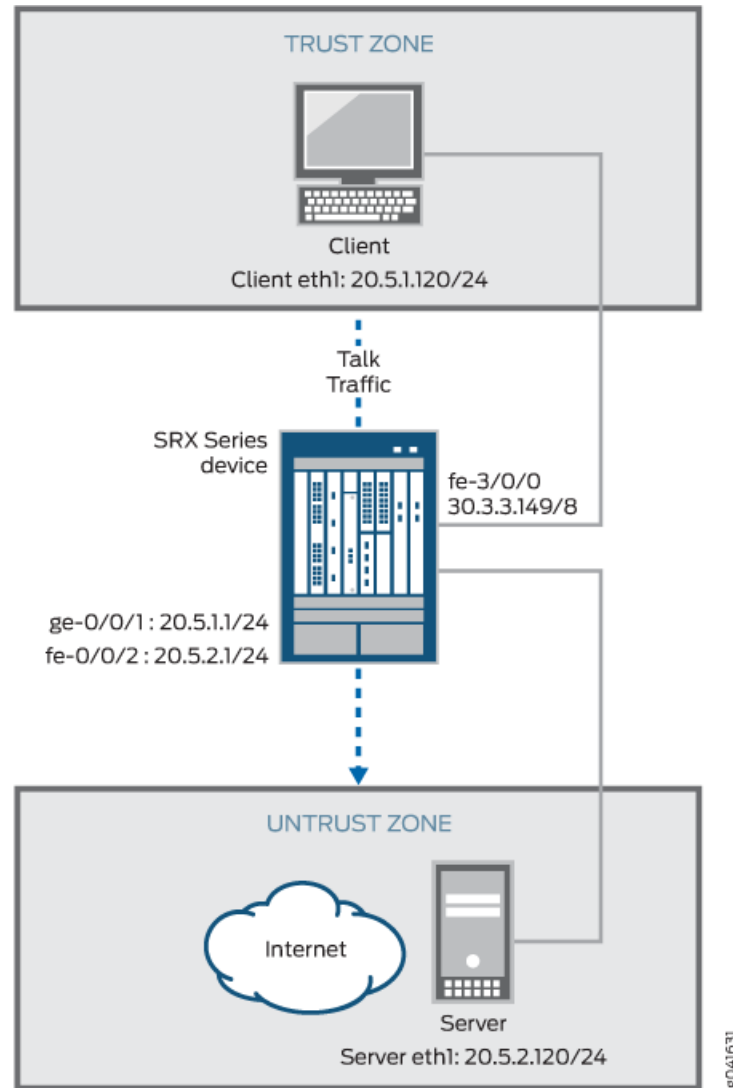
Configuration

To configure the TALK ALG, perform these tasks:

Configuring a Route Mode

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/1 unit 0 family inet address 20.5.1.1/24
set interfaces fe-0/0/2 unit 0 family inet address 20.5.2.1/24
set security zones security-zone trust interfaces ge-0/0/1 host-inbound-traffic system-services
 all
set security zones security-zone trust interfaces ge-0/0/1 host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/2 host-inbound-traffic system-services
 all
set security zones security-zone untrust interfaces fe-0/0/2 host-inbound-traffic protocols all
set security policies from-zone trust to-zone untrust policy talk match source-address any
set security policies from-zone trust to-zone untrust policy talk match destination-address any
set security policies from-zone trust to-zone untrust policy talk match application junos-ntalk
set security policies from-zone trust to-zone untrust policy talk then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure route mode:

1. Configure interfaces.

    ```
    [edit interfaces]
    user@host#set ge-0/0/1 unit 0 family inet address 20.5.1.1/24
    user@host#set fe-0/0/2 unit 0 family inet address 20.5.2.1/24
    ```

2. Configure zones and assign interfaces to the zones.

    ```
    [edit security zones security-zone trust]
    user@host#set interfaces ge-0/0/1 host-inbound-traffic system-services all
    user@host#set interfaces ge-0/0/1 host-inbound-traffic protocols all
    [edit security zones security-zone untrust]
    user@host#set interfaces fe-0/0/2 host-inbound-traffic system-services all
    user@host#set interfaces fe-0/0/2 host-inbound-traffic protocols all
    ```

3. Configure a TALK policy that allows TALK traffic from the trust zone to the untrust zone.

    ```
    [edit security policies from-zone untrust to-zone trust]
    user@host#set policy talk match source-address any
    user@host#set policy talk match destination-address any
    user@host#set policy talk match application junos-ntalk
    user@host#set policy talk then permit
    ```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show interfaces
...
  ge-0/0/1 {
  unit 0 {
    family inet {
      address 20.5.1.1/24;
    }
  }
}
...
fe-0/0/2 {
  unit 0 {
    family inet {
      address 20.5.2.1/24;
    }
  }
}

[edit]
user@host# show security zones
security-zone trust {
  ....
    interfaces {
    ge-0/0/1.0 {
      host-inbound-traffic {
        system-services {
          all;
        }
        protocols {
          all;
        }
      }
    }
  }
}
...
  security-zone untrust {
    interfaces {
      fe-0/0/2.0 {
        host-inbound-traffic {
          system-services {
            all;
          }
          protocols {
            all;
          }
        }
      }
    }
  }
}

[edit]
```

```
user@host# show security policies
from-zone trust to-zone untrust {
  policy talk {
    match {
      source-address any;
      destination-address any;
      application junos-ntalk;
    }
    then {
      permit;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Static NAT Rule Set

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat static rule-set rs1 from zone trust
set security nat static rule-set rs1 rule r1 match destination-address 40.5.2.120/32
set security nat static rule-set rs1 rule r1 then static-nat prefix 20.5.2.120/32
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a static NAT rule set:

1. Create a static NAT rule set.

    ```
    [edit security nat static rule-set rs1]
    user@host#set from zone trust
    ```

2. Define the rule to match with the destination address.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 match destination-address 40.5.2.120/32
    ```

3. Define the static NAT prefix for the device.

    ```
    [edit security nat static rule-set rs1]
    user@host# set rule r1 then static-nat prefix 20.5.2.120/32
    ```

Results
From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
static {
  rule-set rs1 {
```

```
        from zone trust;
        rule r1 {
          match {
            destination-address 40.5.2.120/32
          }
          then {
            static-nat {
              prefix {
                20.5.2.120/32;
              }
            }
          }
        }
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Source NAT Pool and Rule Set

CLI Quick
Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source pool src-p1 address 40.5.1.120/32
set security nat source rule-set src-rs1 from zone trust
set security nat source rule-set src-rs1 to zone untrust
set security nat source rule-set src-rs1 rule src-r1 match source-address 20.5.1.120/32
set security nat source rule-set src-rs1 rule src-r1 match destination-address 20.5.2.120/32
set security nat source rule-set src-rs1 rule src-r1 then source-nat pool src-p1
```

Step-by-Step
Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a source NAT pool and rule set:

1. Create a source NAT pool.

    ```
    [edit security nat source]
    user@host#set pool src-p1 address 40.5.1.120/32
    ```

2. Create a source NAT rule set.

    ```
    [edit security nat source]
    user@host# set rule-set src-rs1 from zone trust
    user@host# set rule-set src-rs1 to zone untrust
    ```

3. Configure a rule that matches packets and translates the source address to an address in the source pool.

    ```
    [edit security nat source]
    user@host# set rule-set src-rs1 rule src-r1 match source-address 20.5.1.120/32
    ```

4. Configure a rule that matches packets and translates the destination address to an address in the source pool.

[edit security nat source]
user@host# **set rule-set src-rs1 rule src-r1 match destination-address 20.5.2.120/32**

5. Configure a source NAT pool in the rule.

    [edit security nat source]
    user@host# **set rule-set src-rs1 rule src-r1 then source-nat pool src-p1**

Results   From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
source {
  pool src-p1 {
    address {
      40.5.1.120/32;
    }
  }
  rule-set src-rs1 {
    from zone trust;
    to zone untrust;
    rule src-r1 {
      match {
        source-address 20.5.1.120/32;
        destination-address 20.5.2.120/32;
      }
      then {
        source-nat {
          pool {
            src-p1;
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring a Destination NAT Pool and Rule Set

CLI Quick
Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

set security nat destination pool des-p1 address 20.5.2.120/32
set security nat destination rule-set des-rs1 from zone trust
set security nat destination rule-set des-rs1 rule des-r1 match source-address 20.5.1.120/32
set security nat destination rule-set des-rs1 rule des-r1 match destination-address 40.5.2.120/32
set security nat destination rule-set des-rs1 rule des-r1 then destination-nat pool des-p1

Step-by-Step
Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a destination NAT pool and rule set:

1. Create a destination NAT pool.

   [edit security nat destination]
   user@host#**set pool des-p1 address 20.5.2.120/32**

2. Create a destination NAT rule set.

   [edit security nat destination]
   user@host# **set rule-set des-rs1 from zone trust**

3. Configure a rule that matches packets and translates the source address to the address in the pool.

   [edit security nat destination]
   user@host# **set rule-set des-rs1 rule des-r1 match source-address 20.5.1.120/32**

4. Configure a rule that matches packets and translates the destination address to the address in the pool.

   [edit security nat destination]
   user@host# **set rule-set des-rs1 rule des-r1 match destination-address 40.5.2.120/32**

5. Configure a source NAT pool in the rule.

   [edit security nat destination]
   user@host# **set rule-set des-rs1 rule des-r1 then destination-nat pool des-p1**

Results

From configuration mode, confirm your configuration by entering the **show security nat** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
destination {
  pool des-p1 {
    address {
      20.5.2.120/32;
    }
```

```
      }
      rule-set des-rs1 {
        from zone trust;
        rule des-r1 {
          match {
            source-address 20.5.1.120/32;
            destination-address 40.5.2.120/32;
          }
          then {
            destination-nat {
              pool {
                des-p1;
              }
            }
          }
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Configuring TALK ALG trace options

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

> set security alg talk traceoptions flag all
> set security alg traceoptions file trace
> set security alg traceoptions file size 1g
> set security alg traceoptions level verbose

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure TALK ALG trace options:

1. Enable TALK ALG trace otpions.

   [edit security alg]
   user@host#**set talk traceoptions flag all**

2. Configure the filename to receive output from the tracing operation.

   [edit security alg]
   user@host#**set traceoptions file trace**

3. Specify the maximum trace file size.

   [edit security alg]
   user@host#**set traceoptions file size 1g**

4. Specify the level of tracing output.

   [edit security alg]
   user@host#**set traceoptions level verbose**

Results From configuration mode, confirm your configuration by entering the **show security alg** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security alg
traceoptions {
   file trace size 1g;
   level verbose;
   }
talk traceoptions flag all;
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the TALK ALG Control Session

Purpose Verify that the TALK control session is created and all the TALK control and data sessions are created.

Action From operational mode, enter the **show security flow session** command.

user@host>**show security flow session**

```
 ession ID: 128570, Policy name: p11/4, Timeout: 56, Valid
Resource information : TALK ALG, 2, 0
  In: 5.1.1.200/1105 --> 6.1.1.200/518;udp, If: ge-0/0/1.0, Pkts: 3, Bytes: 336
  Out: 6.1.1.200/518 --> 5.1.1.200/1105;udp, If: ge-0/0/2.0, Pkts: 3, Bytes: 156

Session ID: 128617, Policy name: p11/4, Timeout: 1796, Valid
Resource information : TALK ALG, 2, 2
  In: 6.1.1.200/42224 --> 5.1.1.200/518;udp, If: ge-0/0/2.0, Pkts: 1, Bytes: 112

  Out: 5.1.1.200/518 --> 6.1.1.200/42224;udp, If: ge-0/0/1.0, Pkts: 1, Bytes: 52

Session ID: 128618, Policy name: p11/4, Timeout: 1796, Valid
Resource information : TALK ALG, 2, 3
  In: 6.1.1.200/51430 --> 5.1.1.200/32905;tcp, If: ge-0/0/2.0, Pkts: 4, Bytes:
219
  Out: 5.1.1.200/32905 --> 6.1.1.200/51430;tcp, If: ge-0/0/1.0, Pkts: 3, Bytes:
167
```

Meaning
- **Session ID**—Number that identifies the session. Use this ID to get more information about the session such as policy name or number of packets in and out.

- **Policy name**—Policy name that permitted the traffic.

- **In**—Incoming flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and the source interface for this session is ge-0/0/1.0).

- **Out**—Reverse flow (source and destination IP addresses with their respective source and destination port numbers, session is TCP, and destination interface for this session is fe-0/0/2.0).

Verifying the TALK Flow Gate Information

Purpose   Verify that the gates are opened for TCP data channel and reverse UDP reply.

Action   From operational mode, enter the **show security flow gate** command.

```
user@host>show security flow gate
Hole: 6.1.1.200-6.1.1.200/0-0->5.1.1.200-5.1.1.200/518-518
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: udp
  Application: TALK ALG/65
  Age: 110 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 11-2-2

Hole: 6.1.1.200-6.1.1.200/0-0->5.1.1.200-5.1.1.200/32905-32905
  Translated: 0.0.0.0/0->0.0.0.0/0
  Protocol: tcp
  Application: TALK ALG/65
  Age: 110 seconds
  Flags: 0x0080
  Zone: untrust
  Reference count: 1
  Resource: 11-2-3
```

Meaning
- **Hole**—Range of flows permitted by the pinhole.

- **Translated**—Tuples used to create the session if it matches the pinhole (source and destination IP addresses with their respective source and destination port numbers).

- **Protocol**—Application protocol, such as UDP or TCP.

- **Application**—Name of the application.

- **Age**—Idle timeout for the pinhole.

- **Flags**— Internal debug flags for the pinhole.

- **Zone**—Security zone such as from zone and to zone.

- **Reference count**—Number of resource manager references to the pinhole.

- **Resource**—Resource manager information about the pinhole.

Verifying TALK ALG

Purpose Verify that the TALK ALG is enabled.

Action From operational mode, enter the **show security alg status** command.

```
user@host>show security alg status
ALG Status :
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Enabled
  SCCP     : Enabled
  SIP      : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

Meaning The output shows the TALK ALG status as follows:

- Enabled—Shows the TALK ALG is enabled.

- Disabled—Shows the TALK ALG is disabled.

Verifying the TALK Resource Manager Group

Purpose Verify the total number of resource manager groups and active groups that are used by the TALK ALG.

Action From operational mode, enter the **show security resource-manager group active** command.

```
user@host>show security resource-manager group active
Group ID 2: Application - TALK ALG
      Total groups 3276, active groups 1
```

Verifying the TALK Resource Information

Purpose Verify the total number of resources and active resources that are used by the TALK ALG.

Action From operational mode, enter the **show security resource-manager resource active** command.

```
user@host>show security resource-manager resource active
Resource ID 3: Group ID - 2, Application - TALK ALG

Resource ID 2: Group ID - 2, Application - TALK ALG
Total Resources 6015, active resources 2
```

Related Documentation
- Understanding the TALK ALG on page 117

CHAPTER 12

Configuring the TFTP ALG

Understanding the TFTP ALG

Supported Platforms   SRX Series, vSRX

Overview

Trivial File Transfer Protocol (TFTP) is a simple protocol used for files transfer *(RFC 1350)*. TFTP is implemented on top of UDP, with destination port 69 as the well-known port. The TFTP Application Layer Gateway (ALG) processes TFTP packets that initiate the request and creates pinholes to allow return packets from the reverse direction.

In flow processing there are two sessions for one TFTP conversation, one is the TFTP control session created by a read request (RRQ) or write request (WRQ) packet; the other one is the TFTP data session created by a DATA packet (for RRQ) or acknowledgment (ACK) packet (for WRQ).

In a Junos OS firewall, the TFTP control session is permitted through the junos-tftp application policy. The data session is permitted through the TFTP ALG open pinhole from any port of the server to the TID (port) of the client when the control session packet is received. No NAT translation is required, because the NAT translation has already been performed and the information is available from the session data structure.

On SRX320 and SRX340 devices, broadcast TFTP is not supported when flow is enabled on the device.

TFTP Packets

Any transfer begins with a request to read or write a file. A data packet of less than 512 bytes signals termination of a transfer.

TFTP supports five types of packets:

- Read request (RRQ)

- Write request (WRQ)

- Data (DATA)

- Acknowledgment (ACK)

- Error (ERROR)

TFTP Session

The TFTP ALG is based on UDP, which is a stateless transport protocol. In a firewall, the TFTP ALG acts as a UDP session with timeout. If there is no packet refresh session, the session is terminated after timeout. Although the TFTP client and server determine the termination of a TFTP conversation, they are sometimes unaware of the session in Fireware. Therefore, the client and server could request a new TFTP conversation in this scenario.

The TFTP ALG session can proceed in any of the following ways:

- When the TFTP control session reaches timeout, the session is not terminated if the data session is still alive.

- A TFTP session might terminate or get corrupted by the **clear security flow session all** or the **clear specific session** CLI commands regardless of whether the data session is ongoing or not.

- If a new TFTP session request arrives and reaches the existing session, the TFTP ALG will open the pinhole again for the new request.

- If the pinhole already exists, the TFTP ALG will not open the pinhole again and there will be no packet drop.

- The TFTP ALG will not drop any packet.

Related Documentation

Understanding TFTP ALG Conversation

Supported Platforms   SRX Series, vSRX

By default TFTP servers listen for incoming requests from TFTP clients on port 69. A TFTP client chooses its source tunnel identifier (TID) port and sends its initial request to the server. In response, the server uses the TID chosen as the source port and sends a response to the client's TID as the destination port. The two TIDs ports are then used for the rest of the data transfer.

Read file conversation steps:

1. Host A (client) sends an RRQ packet to host B (server) with A's TID as source and port 69 as destination.

2. Host B (server) sends a DATA packet to host A (client) with B's TID as source and A's TID as destination.

3. Host A (client) sends an ACK packet to host B (server) with A's TID as source and B's TID as destination.

4. DATA and ACK packets conversation continues until file data transferring is complete.

Write file conversation steps:

1. Host A (client) sends a WRQ packet to host B (server) with A's TID as source and port 69 as destination.

2. Host B (server) sends an ACK packet to host A (client) with B's TID as source and A's TID as destination.

3. Host A (client) sends a DATA packet to host B (server) with A's TID as source and B's TID as destination.

4. Host B (server) sends an ACK packet to host A (client) with B's TID as source and A's TID as destination.

Related Documentation
- ALG Overview on page 3
- Understanding IPv6 Support for the TFTP ALG on page 133
- Example: Configuring the TFTP ALG on page 134

Understanding IPv6 Support for the TFTP ALG

Supported Platforms   SRX Series, vSRX

Trivial File Transfer Protocol (TFTP) Application Layer Gateway (ALG) has been enhanced to support IPv6 and IPv4 TFTP conversation, which has IPv6 and IPv4 addresses for both the source IP address and destination IP address.

TFTP ALG processes packets that initiate the routing request and create pinholes to allow return packets from the reverse direction to the port that sent the request.

The data session is set up by the first packet from the client to the server. TFTP ALG monitors the first packet and opens a pinhole from any port on the server to the client. This process helps the return packets from the server and subsequent data packets to pass through.

Related Documentation
- ALG Overview on page 3
- Understanding TFTP ALG Conversation on page 132
- Example: Configuring the TFTP ALG on page 134

Example: Configuring the TFTP ALG

Supported Platforms   SRX Series, vSRX

The TFTP ALG processes TFTP packets that initiate the request and opens a gate to allow return packets from the reverse direction to the port that sends the request.

This example shows how to configure the TFTP ALG to pass through TFTP traffic with a source NAT pool on Juniper Networks devices.

Requirements

- Configure proxy ARP for all IP addresses in the source NAT pool.
- Understand the basic concepts of TFTP ALG. See "Understanding the TFTP ALG" on page 131.

Overview

In this example, the TFTP ALG is configured to monitor and allow TFTP traffic, transferring files between the client and server located on opposite sides of a Juniper Networks device.

Configuration

Configuring a NAT Source Pool, Rule Set, and a Policy

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security nat source pool pool1 address 10.10.10.1/32 to 10.10.10.10/32
set security zones security-zone green address-book address sa1 1.1.1.0/24
set security zones security-zone red address-book address da1 2.2.2.0/24
set security nat source rule-set rs1 from zone green
set security nat source rule-set rs1 to zone red
set security nat source rule-set rs1 rule r1 match source-address 1.1.1.0/24
set security nat source rule-set rs1 rule r1 match destination-address 2.2.2.0/24
set security nat source rule-set rs1 rule r1 then source-nat pool pool1

set security policy from-zone green to-zone red policy pol1 match destination-address da1
set security policy from-zone green to-zone red policy pol1 match source-address sa1
set security policy from-zone green to-zone red policy pol1 match application junos-tftp
set security policy from-zone green to-zone red policy pol1 then permit
```

> NOTE: If you are not sure of the TFTP client and server IP address, you can replace "da1" and "sa1" with "any".

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a source NAT pool:

1. Create a NAT source pool.

    ```
    [edit security]
    user@host# set nat source pool pool1 address 10.10.10.1/32 to 10.10.10.10/32
    ```

2. Configure security zone address book entries.

    ```
    [edit security zones security-zone]
    user@host# set green address-book address sa1 1.1.1.0/24
    user@host# set red address-book address da1 2.2.2.0/24
    ```

3. Create a NAT source rule set.

    ```
    [edit security nat source rule-set rs1]
    user@host# set from zone green
    user@host# set to zone red
    user@host# set rule r1 match source-address 1.1.1.0/24
    user@host# set rule r1 match destination-address 2.2.2.0/24
    user@host# set rule r1 then source-nat pool pool1
    ```

4. Configure a policy

    ```
    [edit security policies from-zone green to-zone red policy pol1]
    user@host# set match source-address sa1
    user@host# set match destination-address da1
    user@host# set match application junos-tftp
    user@host# set then permit
    ```

Results From configuration mode, confirm your configuration by entering the **show security nat** and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security nat
source {
  pool pool1 {
    address {
      10.10.10.1/32 to 10.10.10.10/32;
    }
  }
  rule-set rs1 {
    from zone green;
    to zone red;
    rule r1 {
      match {
        source-address 1.1.1.0/24;
        destination-address 2.2.2.0/24;
      }
      then {
        source-nat {
          pool {
```

```
                                 pool1;
                               }
                             }
                           }
                         }
                       }
         [edit]
         user@host# show security policies
         from-zone green to-zone red {policy pol1 {
           policy pol1 {
             match {
               source-address sa1;
               destination-address da1;
               application [junos-tftp];
             }
             then {
               permit;
             }
           }
         }
         default-policy {
           permit-all;
         }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the NAT Source Pool and Rule Set

Purpose   Verify that the NAT source pool and rule set used to support the TFTP ALG are working properly.

Action   From operational mode, enter the **show security nat static rule r1** command.

Verifying TFTP ALG

Purpose   Verify that the TFTP ALG is enabled.

Action   From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status

DNS      : Enabled
FTP      : Enabled
H323     : Enabled
TFTP     : Enabled
```

Meaning   The output shows the TFTP ALG status as follows:

- Enabled—Shows the TFTP ALG is enabled.

- Disabled—Shows the TFTP ALG is disabled.

Related Documentation

- ALG Overview on page 3

- Understanding TFTP ALG Conversation on page 132

- Understanding IPv6 Support for the TFTP ALG on page 133

PART 3

Configuring VoIP ALGs

VoIP ALG Types

Understanding VoIP ALG Types

Supported Platforms   SRX Series, vSRX

Junos OS supports voice-over-IP Application Layer Gateways (VoIP ALGs) and basic data ALGs. (Note that supported ALG types vary depending on which hardware device you are using.)

VoIP ALGs provide stateful Application Layer inspection and Network Address Translation (NAT) capabilities to VoIP signaling and media traffic. The ALG inspects the state of transactions, or calls, and forwards or drops packets based on those states.

Junos OS supports the following VoIP ALGs:

- H.323—The H.323 ALG provides support for the H.323 legacy VoIP protocol. The ALG lets you secure VoIP communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, the gatekeeper device manages call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones or in the same zone.

- SIP—The SIP ALG provides support for the Session Initiation Protocol (SIP). 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.

- SCCP—The SCCP ALG provides support for Skinny Client Control Protocol (SCCP). SCCP is a Cisco proprietary protocol for call signaling. Skinny is based on a call-agent-based call-control architecture. The control protocol uses binary-coded frames encoded on TCP frames sent to well-known TCP port number destinations to set up and tear down RTP media sessions.

- MGCP—The MGCP ALG provides support for Media Gateway Control Protocol (MGCP). MGCP is a text-based Application Layer protocol used for call setup and call control between the media gateway and the media gateway controller (MGC). .

For information about enabling and configuring each of these ALGs through J-Web, select the **Configure>Security>ALG** page in the J-Web user interface and click **Help**.

Related Documentation

Configuring VoIP Rewrite Rules

Understanding VoIP DSCP Rewrite Rules

Supported Platforms SRX Series, vSRX

This topic describes the voice over IP Application Layer Gateway (VoIP ALG) mechanism for modifying the Differentiated Services Code Point (DSCP) field of Real-Time Transport Protocol (RTP) packets. The VoIP ALG mechanism is applicable for the RTP session, which is recognized by the ALG.

DSCP is a modification of the type of service byte for class of service (CoS). Six bits of this byte are reallocated for use as the DSCP field, where each DSCP specifies a particular per-hop behavior that is applied to a packet.

To avoid VoIP quality degradation caused by network congestion, the RTP packets are required to mark the DSCP bit to ensure they get higher routing priority. A downstream router can put those packets in a higher priority queue for faster forwarding. To provide this functionality, there needs to be a per-VoIP mechanism for modifying the DSCP field of RTP packets according to the specific configuration. This will ensure that all RTP packets based on User Datagram Protocol/Transport Control Protocol (UDP/TCP) that encounter the ALG will be assigned a specific DSCP bit.

A rewrite rule modifies the appropriate CoS bits in an outgoing packet to meet the requirements of the targeted peer. Each rewrite rule reads the current CoS value that is configured at the VoIP ALG level. Every packet that hits the VoIP ALG is marked by this CoS value.

This feature supports ALG DSCP marking for H323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP). It provides a 6-bit DSCP value configuration for each of these. When the first RTP packet hits the ALG, this feature receives the 6-bit DSCP value form the configuration and sets it to the RTP session that the packet has created. This first RTP packet and the following RTP packets passing through the RTP session are marked according to the 6-bit DSCP value in the session.

Example: Configuring VoIP DSCP Rewrite Rules

Supported Platforms   SRX Series, vSRX

This example shows how to configure VoIP DSCP.

- Requirements on page 144
- Overview on page 144
- Configuration on page 144
- Verification on page 144

Requirements

This example uses an SRX320 device. The example assumes that the ALG has been enabled.

Overview

This example shows how to configure four ALG DSCP markings; SIP, H323, MGCP, and SCCP. You set the 6-bit DSCP value configuration for each ALG DSCP.

Configuration

Step-by-Step Procedure   To configure VoIP DSCP rewrite rules:

1. Set the DSCP for each VoIP ALG.

    ```
    [edit]
    user@host# set security alg sip dscp-rewrite code-point 101010
    user@host# set security alg h323 dscp-rewrite code-point 010101
    user@host# set security alg mgcp dscp-rewrite code-point 111000
    user@host# set security alg sccp dscp-rewrite code-point 000111
    ```

2. If you are done configuring the device, commit the configuration.

    ```
    [edit]
    user@host# commit
    ```

Verification

To verify that the configuration is working properly, enter the **show security alg** command.

Configuring the H.323 ALG

Understanding H.323 ALG

Supported Platforms   SRX Series

The H.323 standard is a legacy voice-over-IP (VoIP) protocol defined by the International Telecommunication Union (ITU-T). H.323 consists of a suite of protocols (such as H.225.0 and H.245) that are used for call signaling and call control for VoIP.

H.323 uses the ASN.1 coding format. It sets up the dynamic links for data, video, and audio streams, following the protocols Q.931 (with port number 1720) and H.245. There are three major processes in H.323:

- Gatekeeper Discovery—An endpoint finds its gatekeeper through the gatekeeper discovery process, through broadcast or unicast (to a known IP and the well-known UDP port 1719). (Junos OS supports unicast only.)

- Endpoint Registration, Admission, and Status—An endpoint registers to a gatekeeper and asks for its management. Before making a call, an endpoint asks its gatekeeper

for permission to place the call. In both registration and admission phases, the Registration, Admission, and Status (RAS) channel is used. The Transport Service Access Point (TSAP) can be either the well-known UDP port (1719) or a dynamically assigned port from the discovery or registration phase.

- Call Control and Call Setup—Calls can be established within a zone or across two zones, or even across multiple zones (multipoint conference). The call setup and tear down is performed through the call signaling channel whose TSAP is the well-known TCP port (1720). The call control, including opening/closing media channels between two endpoints, is performed through the call control channel whose TSAP is dynamically assigned from the previous call signaling process. H.245 messages are used in the call control channel, and are encoded using ASN.1.

> **NOTE:** Detailed information on H.323 can be found in ITU-T Recommendation H.323.

The H.323 Application Layer Gateway (ALG) lets you secure VoIP communication between terminal hosts, such as IP phones and multimedia devices. In such a telephony system, the gatekeeper device manages call registration, admission, and call status for VoIP calls. Gatekeepers can reside in the two different zones or in the same zone. (See Figure 10 on page 146.)

Figure 10: H.323 ALG for VoIP Calls
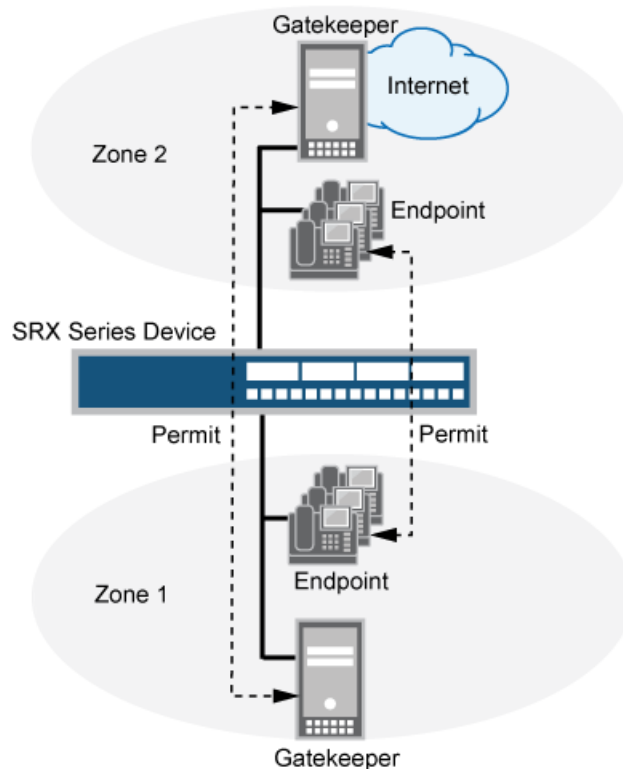
> *i*
>
> NOTE: The illustration uses IP phones for illustrative purposes, although it is possible to make configurations for other hosts that use VoIP, such as Microsoft NetMeeting multimedia devices.

Related Documentation

- ALG Overview on page 3
- Understanding the Avaya H.323 ALG on page 147
- H.323 ALG Configuration Overview on page 149

Understanding the Avaya H.323 ALG

Supported Platforms   SRX Series

The H.323 standard is a legacy voice-over-IP (VoIP) protocol defined by the International Telecommunication Union (ITU-T). H.323 consists of a suite of protocols (such as H.225.0 and H.245) that are used for call signaling and call control for VoIP. The processes for configuring the H.323 standard Application Layer Gateway (ALG) and the proprietary Avaya H.323 ALG are the same.

However, Avaya H.323 ALG has some special features. To understand and configure the Avaya H.323-specific features listed here, see the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

This topic contains the following sections:

- Avaya H.323 ALG-Specific Features on page 147
- Call Flow Details in the Avaya H.323 ALG on page 148

Avaya H.323 ALG-Specific Features

Avaya H.323-specific features are as follows:

- H.323 Fast Connect
- H.323 asymmetric media
- Call waiting
- Call forwarding
- Voice mail
- Call identification
- Conference calling

Call Flow Details in the Avaya H.323 ALG

- Connecting the Phone into the Network—Avaya performs the Q.931 Setup/Connect negotiation when the phone is wired into the network rather than when a call is being initiated.

- Making a call—When a call is made, because the PBX has already stored the capabilities for each phone when the phone is connected to the network, no further Q.931 and PBX negotiations are required to set up the call. It no longer exchanges Q.931 Setup and Connect messages with the PBX. The phone and the PBX exchange H.323 Facility messages to set up the call.

- Registering with a CM—When a call has been made, Avaya H.323 registers with the Avaya Communication Manager (CM). The registration process is similar to a generic H.323 standard registration process.

  NOTE: **The direct mode and tunnel mode are not defined by Avaya H.323 ALG.**

  For a call to work, the CM must be deployed with Avaya Endpoints. During the call, RAS and Q.931 messages are exchanged between the CM and the Avaya Endpoints.

  NOTE: **For Avaya H.323 with a source Network Address Translation (NAT) pool, the registration process allows only one IP address in the pool.**

- Setting up Real-Time Transport Protocol (RTP)/Real-Time Control Protocol (RTCP) ports—The Q.931 Setup, Facility and Information messages are used to set up RTP/RTCP ports. The hierarchy for an Avaya H.323 session is Q.931, RTP/RTCP, Parent, and then Child.

  NOTE: **H.245 ports are not used in an Avaya call flow process.**

- Using Avaya H.323 counters—The counters for calls and active calls are not applicable to the Avaya H.323 ALG. The call creation and tearing down is done by Facility messages afterward. When resources are allocated for a call, all counters for calls and active calls increment. If resources are allocated for a call multiple times, messages belonging to the same call that pass the firewall multiple times will trigger multiple increments of the counters. In other words, messages that belong to the same call and pass the firewall multiple times might trigger multiple increments of the counters if the resource for a call needs to be allocated multiple times.

  For example, in the two-zone case, the setup and connect message pair allocates one call resource. The active call counter is increased once. Each time the setup and connect message pair passes the firewall, a different call resource with unique interfaces and NAT is allocated. Therefore, the counter increments twice in a three-zone scenario.

Related
Documentation

H.323 ALG Configuration Overview

Supported Platforms   SRX Series

The H.323 Application Layer Gateway (ALG) is enabled by default on the device—no action is required to enable it. However, you might choose to fine-tune H.323 ALG operations by using the following instructions:

1. Specify how long an endpoint registration entry remains in the Network Address Translation (NAT) table. For instructions, see "Example: Setting H.323 ALG Endpoint Registration Timeouts" on page 176.

2. Enable media traffic on a narrow or wide range of ports. For instructions, see "Example: Setting H.323 ALG Media Source Port Ranges" on page 177.

3. Protect the H.323 gatekeeper from denial-of-service (DoS) flood attacks. For instructions, see "Example: Configuring H.323 ALG DoS Attack Protection" on page 179.

4. Enable unknown messages to pass when the session is in NAT mode and route mode. For instructions, see "Example: Allowing Unknown H.323 ALG Message Types" on page 180.

Related
Documentation

Example: Passing H.323 ALG Traffic to a Gatekeeper in the Private Zone

Supported Platforms   SRX Series

This example shows how to set up two policies that allow H.323 traffic to pass between IP phone hosts and a gatekeeper in the private zone, and an IP phone host (2.2.2.5/32) in the public zone.

Requirements

Before you begin:

- Understand and configure any Avaya H.323-specific features. See the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

- Configure security zones. See *Understanding Security Zones*.

Overview

This example shows how to set up two policies that allow H.323 traffic to pass between IP phone hosts and a gatekeeper in the private zone, and an IP phone host (2.2.2.5/32) in the public zone. The connection to the device can either be with or without NAT. See Figure 11 on page 150.

Figure 11: H.323 Gatekeeper in the Private Zone
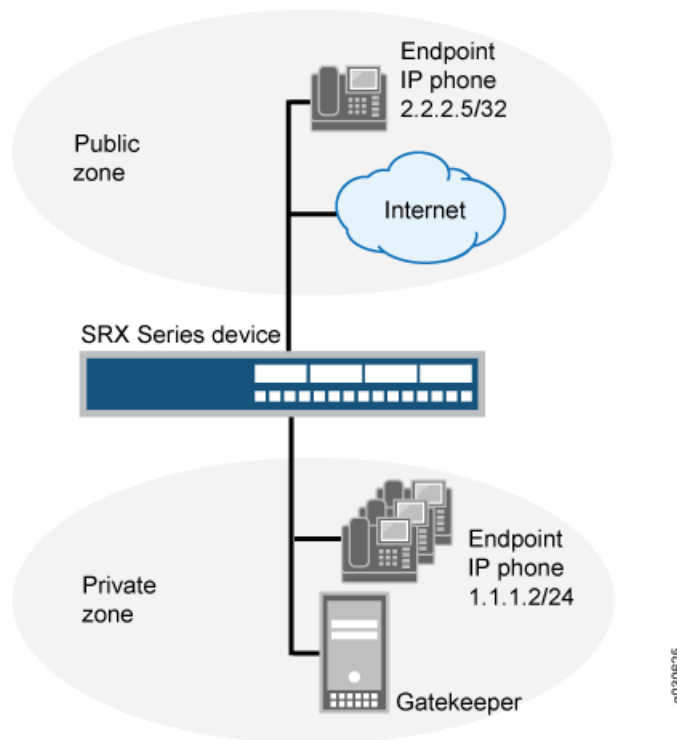
Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

set security zones security-zone public address-book address ip_phone 2.2.2.5/32

set security zones security-zone private address-book address gateway 2.2.2.5/32
set security policies from-zone private to-zone public policy P1 match source-address
   any
set security policies from-zone private to-zone public policy P1 match destination-address
   IP_Phone
set security policies from-zone private to-zone public policy P1 match application
   junos-h323
set security policies from-zone private to-zone public policy P1 then permit
set security policies from-zone public to-zone private policy P2 match source-address
   any
set security policies from-zone public to-zone private policy P2 match destination-address
   gateway
set security policies from-zone public to-zone private policy P2 match application
   junos-h323
set security policies from-zone public to-zone private policy P2 then permit

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure the device to pass H.323 ALG traffic to a gatekeeper in the private zone:

1. Configure two address books.

    [edit]

    user@host# set security zones security-zone public address-book address ip_phone
       2.2.2.5/32

    set security zones security-zone private address-book address gateway 2.2.2.5/32

2. Configure policy P1 from the private zone to the public zone.

    [edit]

    user@host# set security policies from-zone private to-zone public policy P1 match
       source-address any

    user@host# set security policies from-zone private to-zone public policy P1 match
       destination-address IP_Phone

    user@host# set security policies from-zone private to-zone public policy P1 match
       application junos-h323

    user@host# set security policies from-zone private to-zone public policy P1 then
       permit

3. Configure policy P2 from the public zone to the private zone.

    [edit]

    user@host# set security policies from-zone public to-zone private policy P2 match
       source-address any

user@host# **set security policies from-zone public to-zone private policy P2 match destination-address gateway**

user@host# **set security policies from-zone public to-zone private policy P2 match application junos-h323**

user@host# **set security policies from-zone public to-zone private policy P2 then permit**

Results   From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this show output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show security policies
...
from-zone trust to-zone trust {
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone trust to-zone untrust {
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy default-deny {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            deny;
        }
    }
}
from-zone private to-zone public {
    policy P1 {
        match {
```

```
                    source-address any;
                    destination-address IP_Phone;
                    application junos-h323;
                }
                then {
                    permit;
                }
            }
        }
        from-zone public to-zone private {
            policy P2 {
                match {
                    source-address any;
                    destination-address gateway;
                    application junos-h323;
                }
                then {
                    permit;
                }
            }
        }
        ...
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform this task:

Verifying H.323 ALG Configurations

Purpose   Display information about active calls.

NOTE: H.323 counters for calls and active calls in the output to this **show security** command do not apply to the proprietary Avaya implementation of H.323. This is because Q.931 setup and connect messages are exchanged right after the phone is powered up and call creation and tear down is done by Facility messages.

Counters for calls and active calls are increased when the resources allocated for calls are increased—that is, messages belonging to the same call and that pass the firewall multiple times increment the counters. This applies when resources for a call need to be allocated multiple times. For example, in a two-zone scenario the setup and connect message pair allocates one call resource, and the active call counter is increased by one. But in a three-zone scenario the setup and connect message pair passes the firewall twice, each time allocating different call resources. In this case, the counter is incremented.

Action   From the J-Web interface, select **Monitor>ALGs>H323**. Alternatively, from the CLI, enter the **show security alg h323 counters** command.

Counters for H.245 messages received also will not be accurate in the case of H.245 tunneling. Because H.245 messages are encapsulated in Q.931 packets, the counter for H.245 messages received will remain zero even when there are H.245 messages. The **Other H245** counter will, however, reflect these packet transmissions.

```
[edit]
user@host> show security alg h323 counters
H.323 counters summary:
  Packets received        : 0
  Packets dropped         : 0
  RAS message received    : 0
  Q.931 message received  : 0
  H.245 message received  : 0
  Number of calls         : 0
  Number of active calls  : 0
H.323 error counters:
  Decoding errors         : 0
  Message flood dropped   : 0
  NAT errors              : 0
  Resource manager errors : 0
H.323 message counters:
  RRQ      : 0
  RCF      : 0
  ARQ      : 0
  ACF      : 0
  URQ      : 0
  UCF      : 0
  DRQ      : 0
  DCF      : 0
  Oth RAS  : 0
  Setup    : 0
  Alert    : 0
  Connect  : 0
  CallProd : 0
  Info     : 0
  RelCmpl  : 0
  Facility : 0
  Empty    : 0
  OLC      : 0
  OLC-ACK  : 0
  Oth H245 : 0
```

Related Documentation
- Understanding H.323 ALG on page 145
- H.323 ALG Configuration Overview on page 149

Example: Passing H.323 ALG Traffic to a Gatekeeper in the External Zone

Supported Platforms   SRX Series

This example shows how to set up two policies to allow H.323 traffic to pass between IP phone hosts in the internal zone, and the IP phone at IP address 2.2.2.5/32 (and the gatekeeper) in the external zone.

Requirements

Before you begin:

- Understand and configure any Avaya H.323-specific features. See the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

- Configure security zones. See *Understanding Security Zones*.

Overview

Because route mode does not require address mapping of any kind, a device configuration for a gatekeeper in the external, or public, zone is usually identical to the configuration for a gatekeeper in an internal, or private, zone. This example shows how to set up two policies to allow H.323 traffic to pass between IP phone hosts in the internal zone, and the IP phone at IP address 2.2.2.5/32 (and the gatekeeper) in the external zone. The device can be in transparent or route mode. See Figure 12 on page 156.

Figure 12: H.323 Gatekeeper in the External Zone
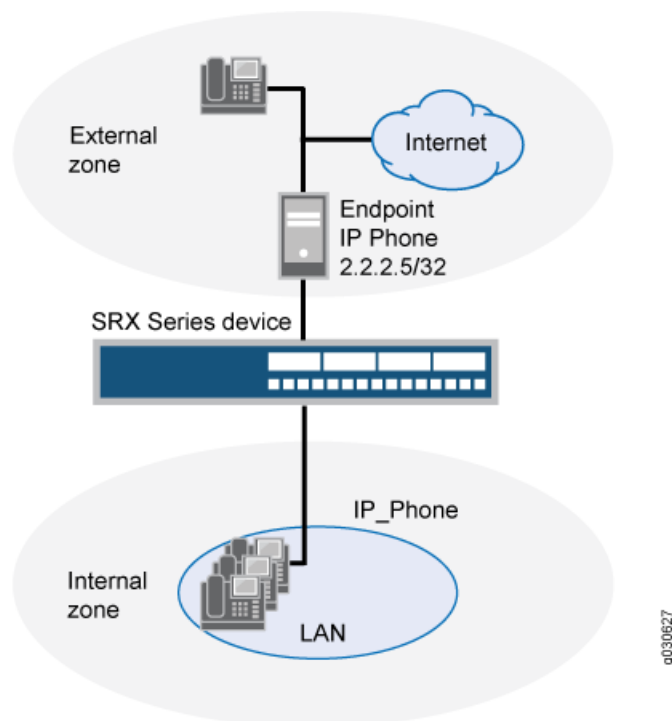
Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone external address-book address IP_Phone 2.2.2.5/32
set security zones security-zone internal address-book address gatekeeper 2.2.2.10/32
set security policies from-zone internal to-zone external policy P1 match source-address
    any
set security policies from-zone internal to-zone external policy P1 match
    destination-address IP_Phone
set security policies from-zone internal to-zone external policy P1 match application
    junos-h323
set security policies from-zone internal to-zone external policy P1 then permit
set security policies from-zone internal to-zone external policy P2 match source-address
    any
set security policies from-zone internal to-zone external policy P2 match
    destination-address gatekeeper
set security policies from-zone internal to-zone external policy P2 match application
    junos-h323
set security policies from-zone internal to-zone external policy P2 then permit
set security policies from-zone external to-zone internal policy P3 match source-address
    IP_Phone
set security policies from-zone external to-zone internal policy P3 match
    destination-address any
```

set security policies from-zone external to-zone internal policy P3 match application
   junos-h323
set security policies from-zone external to-zone internal policy P3 then permit
set security policies from-zone external to-zone internal policy P4 match source-address
   gatekeeper
set security policies from-zone external to-zone internal policy P4 match
   destination-address any
set security policies from-zone external to-zone internal policy P4 match application
   junos-h323
set security policies from-zone external to-zone internal policy P4 then permit

Step-by-Step   The following example requires you to navigate various levels in the configuration
Procedure   hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration
Mode in the CLI User Guide.

To configure the device to pass H.323 ALG traffic to a gatekeeper in the external zone:

1. Configure two address books.

    [edit]
    user@host# set security zones security-zone external address-book address
       IP_Phone 2.2.2.5/32
    user@host# set security zones security-zone internal address-book address
       gatekeeper 2.2.2.10/32

2. Configure policy P1 from the internal zone to the external zone.

    [edit]
    user@host# set security policies from-zone internal to-zone external policy P1 match
       source-address any
    user@host# set security policies from-zone internal to-zone external policy P1 match
       destination-address IP_Phone
    user@host# set security policies from-zone internal to-zone external policy P1 match
       application junos-h323
    user@host# set security policies from-zone internal to-zone external policy P1 then
       permit

3. Configure policy P2 to allow traffic between the internal zone and the gatekeeper
    in the external zone.

    [edit]
    user@host# set security policies from-zone internal to-zone external policy P2 match
       source-address any
    user@host# set security policies from-zone internal to-zone external policy P2 match
       destination-address gatekeeper
    user@host# set security policies from-zone internal to-zone external policy P2 match
       application junos-h323
    user@host# set security policies from-zone internal to-zone external policy P2 then
       permit

4. Configure policy P3 to allow traffic between phones in the internal zone and the
    external zone.

    [edit]
    user@host# set security policies from-zone external to-zone internal policy P3 match
       source-address IP_Phone
    user@host# set security policies from-zone external to-zone internal policy P3 match
       destination-address any

user@host# set security policies from-zone external to-zone internal policy P3 match application junos-h323
user@host# set security policies from-zone external to-zone internal policy P3 then permit

5. Configure policy P4 to allow traffic between phones in the internal zone and the gatekeeper in the external zone.

[edit]
user@host# set security policies from-zone external to-zone internal policy P4 match source-address gatekeeper
user@host# set security policies from-zone external to-zone internal policy P4 match destination-address any
user@host# set security policies from-zone external to-zone internal policy P4 match application junos-h323
user@host# set security policies from-zone external to-zone internal policy P4 then permit

Results From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this show output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
[edit]
user@host# show security policies
...
from-zone internal to-zone external {
    policy P1 {
        match {
            source-address any;
            destination-address IP_Phone;
            application junos-h323;
        }
        then {
            permit;
        }
    }
    policy P2 {
        match {
            source-address any;
            destination-address gatekeeper;
            application junos-h323;
        }
        then {
            permit;
        }
    }
}
from-zone external to-zone internal {
    policy P3 {
        match {
            source-address IP_Phone;
            destination-address any;
            application junos-h323;
        }
        then {
            permit;
```

```
                }
            }
            policy P4 {
                match {
                    source-address gatekeeper;
                    destination-address any;
                    application junos-h323;
                }
                then {
                    permit;
                }
            }
        }
        ...
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform this task:

- Verifying H.323 ALG Configurations on page 159

Verifying H.323 ALG Configurations

Purpose Display information about active calls.

---

i NOTE: H.323 counters for calls and active calls in the output to this **show security** command do not apply to the proprietary Avaya implementation of H.323. This is because Q.931 setup and connect messages are exchanged right after the phone is powered up and call creation and tear down is done by Facility messages.

Counters for calls and active calls are increased when the resources allocated for calls are increased—that is, messages belonging to the same call and that pass the firewall multiple times increment the counters. This applies when resources for a call need to be allocated multiple times. For example, in a two-zone scenario the setup and connect message pair allocates one call resource, and the active call counter is increased by one. But in a three-zone scenario the setup and connect message pair passes the firewall twice, each time allocating different call resources. In this case, the counter is incremented.

Action From the J-Web interface, select **Monitor>ALGs>H323**. Alternatively, from the CLI, enter the **show security alg h323 counters** command.

Counters for H.245 messages received also will not be accurate in the case of H.245 tunneling. Because H.245 messages are encapsulated in Q.931 packets, the counter for

H.245 messages received will remain zero even when there are H.245 messages. The **Other H245** counter will, however, reflect these packet transmissions.

```
[edit]
user@host> show security alg h323 counters
H.323 counters summary:
  Packets received        : 0
  Packets dropped         : 0
  RAS message received    : 0
  Q.931 message received  : 0
  H.245 message received  : 0
  Number of calls         : 0
  Number of active calls  : 0
H.323 error counters:
  Decoding errors         : 0
  Message flood dropped   : 0
  NAT errors              : 0
  Resource manager errors : 0
H.323 message counters:
  RRQ       : 0
  RCF       : 0
  ARQ       : 0
  ACF       : 0
  URQ       : 0
  UCF       : 0
  DRQ       : 0
  DCF       : 0
  Oth RAS   : 0
  Setup     : 0
  Alert     : 0
  Connect   : 0
  CallProd  : 0
  Info      : 0
  RelCmpl   : 0
  Facility  : 0
  Empty     : 0
  OLC       : 0
  OLC-ACK   : 0
  Oth H245  : 0
```

Related Documentation

- Understanding H.323 ALG on page 145
- H.323 ALG Configuration Overview on page 149

Example: Using NAT with the H.323 ALG to Enable Incoming Calls

Supported Platforms   SRX Series

This example shows how to configure NAT with the H.323 ALG to enable calls from a public to a private network.

- Requirements on page 161
- Overview on page 161
- Configuration on page 162
- Verification on page 167

Requirements

Before you begin, understand H.323 ALGs. See "Understanding H.323 ALG" on page 145.

Overview

In a two-zone scenario with a server in the private zone, you can use NAT for incoming calls by configuring a NAT pool on the interface to the public zone.

In this example (see Figure 13 on page 162), IP-Phone1 and a server called gatekeeper are in the private zone, and IP-Phone2 is in the public zone. You configure a static nat rule set and a source NAT pool to do NAT. You also create two policies, private-to-public and public-to-private, to permit ALG H.323 traffic from and to the private and public zones.

Topology

shows NAT with the H.323 ALG incoming calls.

Figure 13: NAT with the H.323 ALG—Incoming Calls
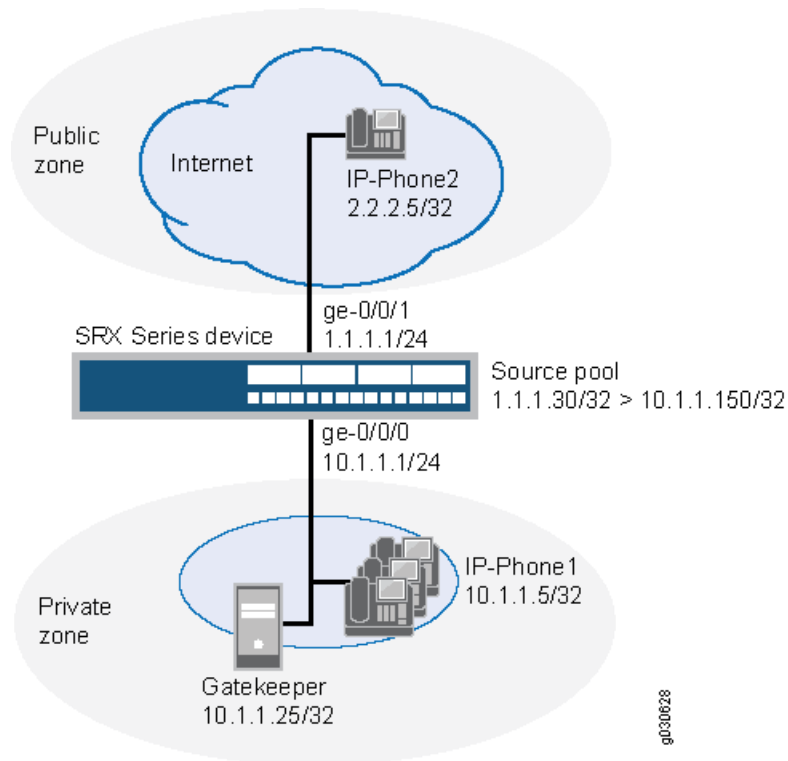
In this example, you configure source NAT as follows:

- Create a static NAT rule set called gatekeeper with a rule called gatekeeper to match packets from the public zone with the destination address 1.1.1.25/32. For matching packets, the destination IP address is translated to the private address 10.1.1.25/32.

- Define a source NAT pool called h323-nat-pool to contain the IP address range from 1.1.1.30/32 through 1.1.1.150/32.

- Create a source NAT rule set called h323-nat with rule h323-r1 to match packets from the private zone to the public zone with the source IP address 10.1.1.0/24. For matching packets, the source address is translated to the IP address in h323-nat-pool.

- Configure proxy ARP for the addresses 1.1.1.30/32 through 1.1.1.150/32 on interface ge-0/0/1.0. This allows the system to respond to ARP requests received on the interface for these addresses.

Configuration

CLI Quick Configuration   To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your

network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private address-book address IP-Phone1 10.1.1.5/32
set security zones security-zone private address-book address gatekeeper 10.1.1.25/32
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public address-book address IP-Phone2 2.2.2.5/32
set security zones security-zone public interfaces ge-0/0/1.0
set security nat source pool h323-nat-pool address 1.1.1.30/32 to 1.1.1.150/32
set security nat source address-persistent
set security nat source rule-set h323-nat from zone private
set security nat source rule-set h323-nat to zone public
set security nat source rule-set h323-nat rule h323-r1 match source-address 10.1.1.0/24
set security nat source rule-set h323-nat rule h323-r1 then source-nat pool h323-nat-pool
set security nat proxy-arp interface ge-0/0/1.0 address 1.1.1.30/32 to 1.1.1.150/32
set security policies from-zone private to-zone public policy private-to-public match
    source-address IP-Phone1
set security policies from-zone private to-zone public policy private-to-public match
    source-address gatekeeper
set security policies from-zone private to-zone public policy private-to-public match
    destination-address IP-Phone2
set security policies from-zone private to-zone public policy private-to-public match
    application junos-h323
set security policies from-zone private to-zone public policy private-to-public then permit
set security policies from-zone public to-zone private policy public-to-private match
    source-address IP-Phone2
set security policies from-zone public to-zone private policy public-to-private match
    destination-address IP-Phone1
set security policies from-zone public to-zone private policy public-to-private match
    destination-address gatekeeper
set security policies from-zone public to-zone private policy public-to-private match
    application junos-h323
set security policies from-zone public to-zone private policy public-to-private then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure NAT with H.323 ALG to enable calls from a public to a private network:

1. Configure interfaces.

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/24
   ```

2. Configure zones and assign addresses to them.

   ```
   [edit security zones]
   user@host# set security-zone private interfaces ge-0/0/0.0
   user@host# set security-zone private address-book address IP-Phone1 10.1.1.5/32
   user@host# set security-zone private address-book address gatekeeper 10.1.1.25/32
   user@host# set security-zone public interfaces ge-0/0/1.0
   user@host# set security-zone public address-book address IP-Phone2 2.2.2.5/32
   ```

3. Create a static NAT rule set.

```
[edit security nat static rule-set ip-phones]
user@host# set from zone public
user@host# set match destination-address 1.1.1.25/32
user@host# set then static-nat prefix 10.1.1.25/32
```

4. Configure proxy ARP.

```
[edit security nat]
user@host# set proxy-arp interface ge-0/0/1.0 address 1.1.1.25/32
```

5. Configure a source NAT rule set.

```
[edit security nat]
set source pool h323-nat-pool address 1.1.1.30/32 to 1.1.1.150/32
set source address-persistent
set source rule-set h323-nat from zone private
set source rule-set h323-nat to zone public
set source rule-set h323-nat rule h323-r1 match source-address 10.1.1.0/24
set source rule-set h323-nat rule h323-r1 then source-nat pool h323-nat-pool
set proxy-arp interface ge-0/0/1.0 address 1.1.1.30/32 to 1.1.1.150/32
```

6. Configure policies for outgoing traffic.

```
[edit security policies from-zone private to-zone public policy private-to-public]
user@host# set match source-address IP-Phone1
user@host# set match source-address gatekeeper
user@host# set match destination-address IP-Phone2
user@host# set match application junos-h323
user@host# set then permit
```

7. Configure policies for incoming traffic.

```
[edit security policies from-zone public to-zone private policy public-to-private]
user@host# set match source-address IP-Phone2
user@host# set match destination-address IP-Phone1
user@host# set match destination-address gatekeeper
user@host# set match application junos-h323
user@host# set then permit
```

Results   From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security nat**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
    ge-0/0/1 {
      unit 0 {
        family inet {
```

```
                    address 1.1.1.1/24;
                }
            }
        }
[edit]
user@host# show security zones
security-zone private {
  address-book {
    address IP-Phone1 10.1.1.5/32;
    address gatekeeper 10.1.1.25/32;
  }
  interfaces {
    ge-0/0/0.0;
  }
}
  security-zone public {
    address-book {
      address IP-Phone2 2.2.2.5/32;
    }
    interfaces {
      ge-0/0/1.0;
    }
  }
[edit]
user@host# show security nat
source {
  pool h323-nat-pool {
    address {
      1.1.1.30/32 to 1.1.1.150/32;
    }
  }
  address-persistent;
  rule-set h323-nat {
    from zone private;
    to zone public;
    rule h323-r1 {
      match {
        source-address 10.1.1.0/24;
      }
      then {
        source-nat {
          pool {
            h323-nat-pool;
          }
        }
      }
    }
  }
}
  proxy-arp {
    interface ge-0/0/1.0 {
      address {
        1.1.1.30/32 to 1.1.1.150/32;
      }
    }
  }
```

```
                                    static {
                                        rule-set ip-phones {
                                            from zone public;
                                            rule gatekeeper {
                                                match {
                                                    destination-address 1.1.1.25/32;
                                                }
                                                then {
                                                    static-nat prefix 10.1.1.25/32;
                                                }
                                            }
                                        }
                                    }
                                    proxy-arp {
                                        interface ge-0/0/1.0 {
                                            address {
                                                1.1.1.25/32;
                                            }
                                        }
                                    }
                                [edit]
                                user@host# show security policies
                                from-zone private to-zone public {
                                    policy private-to-public {
                                        match {
                                            source-address [IP-Phone1 gatekeeper];
                                            destination-address IP-Phone2;
                                            application junos-h323;
                                        }
                                        then {
                                            permit;
                                        }
                                    }
                                }
                                    from-zone public to-zone private {
                                        policy public-to-private {
                                            match {
                                                source-address IP-Phone2;
                                                destination-address [IP-Phone1 gatekeeper];
                                                application junos-h323;
                                            }
                                            then {
                                                permit;
                                            }
                                        }
                                    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying H.323 ALG Status

Purpose   Verify that H.323 ALG is enabled on your system.

Action   From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Enabled
  MGCP     : Enabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Enabled
  SCCP     : Enabled
  SIP      : Enabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

Meaning   The output shows the H323 ALG status as follows:

- Enabled—Shows the H323 ALG is enabled.

- Disabled—Shows the H323 ALG is disabled.

Verifying Security ALG H.323 Counters

Purpose   Verify that there is a security counters for ALG H323.

Action   From operational mode, enter the **show security alg h323 counters** command.

```
user@host> show security alg h323 counters

H.323 counters summary:
Packets received :4060
Packets dropped :24
RAS message received :3690
Q.931 message received :202
H.245 message received :145
Number of calls :25
Number of active calls :0

H.323 Error Counters:
```

```
Decoding errors :24
Message flood dropped :0
NAT errors :0
Resource manager errors :0

H.323 Message Counters:
RRQ : 431
RCF : 49
ARQ : 60
ACF : 33
URQ : 34
UCF : 25
DRQ : 55
DCF : 44
oth RAS : 2942
Setup : 28
Alert : 9
Connect : 25
CallPrcd : 18
Info : 0
RelCmpl : 39
Facility : 14
Progress : 0
Empty : 65
OLC : 20
OLC-ACK : 20
```

Meaning   The sample output gives the rundown of security ALG H.323 counters expressing that, there are security counters for ALG H323.

Verifying Source NAT Rule Usage

Purpose   Verify that there is traffic matching the source NAT rule.

Action   From operational mode, enter the **show security nat source rule all** command. View the Translation hits field to check for traffic that matches the rule.

```
user@host> show security nat source rule all
source NAT rule: h323-r1     Rule-set: h323-nat
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : private
  To zone                   : public
  Match
    Source addresses        : 0.0.0.0        - 255.255.255.255
    Destination port        : 0              - 0
  Action                          : interface
    Persistent NAT type         : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout          : 0
    Max session number          : 0
  Translation hits          : 0
    Successful sessions       : 0
    Failed sessions           : 0
  Number of sessions        : 0
```

Meaning   The **Translation hits** field shows that, there is no traffic matching the source NAT rule.

Example: Using NAT with the H.323 ALG to Enable Outgoing Calls

Supported Platforms SRX Series

This example shows how to configure static NAT with H.323 ALG to enable calls from a private to a public network.

Requirements

Before you begin, understand the H.323 ALG and its processes. See "Understanding H.323 ALG" on page 145.

Overview

In this example (see Figure 14 on page 170), IP-Phone 1 and a server called gatekeeper are in the private zone and IP-Phone2 is in the public zone. You configure static NAT to enable IP-Phone1 and gatekeeper to call IP-Phone2 in the public zone. You then create a policy called public-to-private to allow ALG H.323 traffic from the public zone to the private zone and a policy called private-to-public to allow ALG H.323 traffic from the private zone to the public zone.

Topology

shows NAT with the H.323 ALG outgoing calls.

Figure 14: NAT with the H.323 ALG—Outgoing Calls
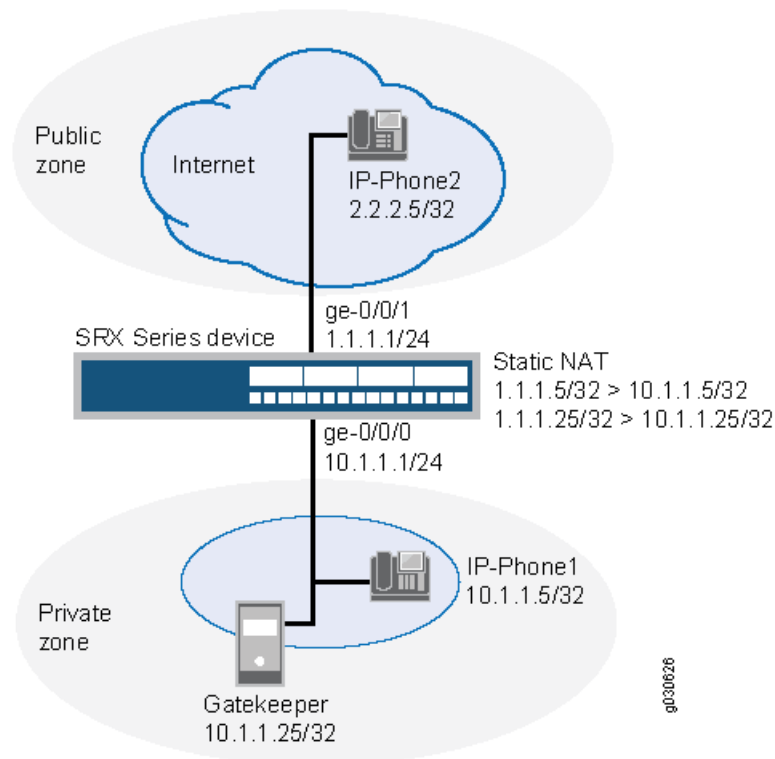
In this example, you configure static NAT as follows:

- Create a static NAT rule set called ip-phones with a rule called phone1 to match packets from the public zone with the destination address 1.1.1.5/32. For matching packets, the destination IP address is translated to the private address 10.1.1.5/32.

- Define a second rule called gatekeeper to match packets from the public zone with the destination address 1.1.1.25/32. For matching packets, the destination IP address is translated to the private address 10.1.1.25/32.

- Create proxy ARP for the addresses 1.1.1.5/32 and 1.1.1.25/32 on interface ge-0/0/1. This allows the system to respond to ARP requests received on the specified interface for these addresses.

Configuration

CLI Quick Configuration To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24

```
set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private address-book address IP-Phone1 10.1.1.5/32
set security zones security-zone private address-book address gatekeeper 10.1.1.25/32
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public address-book address IP-Phone2 2.2.2.5/32
set security zones security-zone public interfaces ge-0/0/1.0
set security nat static rule-set ip-phones from zone public
set security nat static rule-set ip-phones rule phone1 match destination-address 1.1.1.5/32
set security nat static rule-set ip-phones rule phone1 then static-nat prefix 10.1.1.5/32
set security nat static rule-set ip-phones rule gatekeeper match destination-address
    1.1.1.25/32
set security nat static rule-set ip-phones rule gatekeeper then static-nat prefix 10.1.1.25/32
set security nat proxy-arp interface ge-0/0/1.0 address 1.1.1.5/32
set security nat proxy-arp interface ge-0/0/1.0 address 1.1.1.25/32
set security policies from-zone public to-zone private policy public-to-private match
    source-address IP-Phone2
set security policies from-zone public to-zone private policy public-to-private match
    destination-address gatekeeper
set security policies from-zone public to-zone private policy public-to-private match
    application junos-h323
set security policies from-zone public to-zone private policy public-to-private then permit
set security policies from-zone private to-zone public policy private-to-public match
    source-address IP-Phone1
set security policies from-zone private to-zone public policy private-to-public match
    source-address gatekeeper
set security policies from-zone private to-zone public policy private-to-public match
    destination-address IP-Phone2
set security policies from-zone private to-zone public policy private-to-public match
    application junos-h323
set security policies from-zone private to-zone public policy private-to-public then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure static NAT with the H.323 ALG to enable calls from a private to a public network:

1. Configure interfaces.

   ```
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/24
   ```

2. Create zones and assign addresses to them.

   ```
   [edit security zones]
   user@host# set security-zone private interfaces ge-0/0/0.0
   user@host# set security-zone public interfaces ge-0/0/1.0
   user@host# set security-zone private interfaces ge-0/0/0.0
   user@host# set security-zone private address-book address IP-Phone1 10.1.1.5/32
   user@host# set security-zone private address-book address gatekeeper 10.1.1.25/32
   user@host# set security-zone public interfaces ge-0/0/1.0
   user@host# set security-zone public address-book address IP-Phone2 2.2.2.5/32
   ```

3. Configure static NAT rule set with rules.

   ```
   [edit security nat static rule-set ip-phones]
   ```

```
                                  user@host# set from zone public
                                  user@host# set rule phone1 match destination-address 1.1.1.5/32
                                  user@host# set rule phone1 then static-nat prefix 10.1.1.5/32
                                  user@host# set rule gatekeeper match destination-address 1.1.1.25/32
                                  user@host# set rule gatekeeper then static-nat prefix 10.1.1.25/32
```

4. Configure proxy ARP.

```
    [edit security nat]
    user@host# set proxy-arp interface ge-0/0/1 address 1.1.1.5/32
    user@host# set proxy-arp interface ge-0/0/1 address 1.1.1.25/32
```

5. Configure a security policy for incoming traffic.

```
    [edit security policies from-zone public to-zone private policy public-to-private]
    user@host# set match source-address IP-Phone2
    user@host# set match destination-address gatekeeper
    user@host# set match application junos-h323
    user@host# set then permit
```

6. Configure a security policy for outgoing traffic.

```
    [edit security policies from-zone private to-zone public policy private-to-public]
    user@host# set match source-address IP-Phone1
    user@host# set match source-address gatekeeper
    user@host# set match destination-address IP-Phone2
    user@host# set match application junos-h323
    user@host# set then permit
```

Results   From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security nat**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
    [edit]
    user@host# show interfaces
      ge-0/0/0 {
        unit 0 {
          family inet {
            address 10.1.1.1/24;
          }
        }
      }
        ge-0/0/1 {
          unit 0 {
            family inet {
              address 1.1.1.1/24;
            }
          }
        }
    [edit]
    user@host# show security zones
      security-zone private {
        address-book {
          address IP-Phone1 10.1.1.5/32;
          address gatekeeper 10.1.1.25/32;
        }
```

```
      interfaces {
        ge-0/0/0.0;
      }
    }
    security-zone public {
      address-book {
        address IP-Phone2 2.2.2.5/32;
      }
      interfaces {
        ge-0/0/1.0;
      }
    }
[edit]
user@host# show security nat
  static {
    rule-set ip-phones {
      from zone public;
      rule phone1 {
        match {
          destination-address 1.1.1.5/32;
        }
        then {
          static-nat prefix 10.1.1.5/32;
        }
      }
      rule gatekeeper {
        match {
          destination-address 1.1.1.25/32;
        }
        then {
          static-nat prefix 10.1.1.25/32;
        }
      }
    }
  }
    proxy-arp {
      interface ge-0/0/1.0 {
        address {
          1.1.1.5/32;
          1.1.1.25/32;
        }
      }
    }
[edit]
user@host# show security policies
  from-zone public to-zone private {
    policy public-to-private {
      match {
        source-address IP-Phone2;
        destination-address gatekeeper;
        application junos-h323;
      }
      then {
        permit;
      }
    }
```

```
        }
      from-zone private to-zone public {
        policy private-to-public {
          match {
            source-address [ IP-Phone1 gatekeeper ];
            destination-address IP-Phone2;
            application junos-h323;
          }
          then {
            permit;
          }
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying H.323 ALG Status

Purpose Verify that H.323 ALG is enabled on your system.

Action From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Enabled
  MGCP     : Enabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Enabled
  RTSP     : Enabled
  SCCP     : Enabled
  SIP      : Enabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

Meaning The output shows the H323 ALG status as follows:

- Enabled—Shows the H323 ALG is enabled.

- Disabled—Shows the H323 ALG is disabled.

Verifying Security ALG H.323 Counters

Purpose Verify that there is a security counters for ALG H323.

Action   From operational mode, enter the **show security alg h323 counters** command.

> user@host> **show security alg h323 counters**

```
H.323 counters summary:
Packets received :4060
Packets dropped :24
RAS message received :3690Q.931 message received :202
H.245 message received :145
Number of calls :25
Number of active calls :0

H.323 Error Counters:
Decoding errors :24
Message flood dropped :0
NAT errors :0
Resource manager errors :0

H.323 Message Counters:
RRQ : 431
RCF : 49
ARQ : 60
ACF : 33
URQ : 34
UCF : 25
DRQ : 55
DCF : 44
oth RAS : 2942
Setup : 28
Alert : 9
Connect : 25
CallPrcd : 18
Info : 0
RelCmpl : 39
Facility : 14
Progress : 0
Empty : 65
OLC : 20
OLC-ACK : 20
```

Meaning   The sample output gives the synopsis of security ALG H.323 counters expressing that there are security counters for ALG H.323.

Related   • Example: Passing H.323 ALG Traffic to a Gatekeeper in the External Zone on page 154
Documentation
      • H.323 ALG Configuration Overview on page 149

Understanding H.323 ALG Endpoint Registration Timeouts

Supported Platforms   SRX Series

In Network Address Translation (NAT) mode, when endpoints in the protected network behind the Juniper Networks device register with the H.323 gatekeeper, the device adds an entry to the NAT table containing a mapping of the public-to-private address for each endpoint. These entries make it possible for endpoints in the protected network to receive incoming calls.

You set an endpoint registration timeout to specify how long an endpoint registration entry remains in the NAT table. To ensure uninterrupted incoming call service, set the endpoint registration timeout to a value equal to or greater than the keepalive value the administrator configures on the gatekeeper. The range is 10 to 50,000 seconds, the default value is 3600 seconds.

Related Documentation
- Understanding H.323 ALG on page 145
- H.323 ALG Configuration Overview on page 149
- Example: Setting H.323 ALG Endpoint Registration Timeouts on page 176

Example: Setting H.323 ALG Endpoint Registration Timeouts

Supported Platforms   SRX Series

This example shows how to specify the endpoint registration timeout.

- Requirements on page 176
- Overview on page 176
- Configuration on page 176
- Verification on page 177

Requirements

Before you begin, understand and configure any Avaya H.323-specific features. See the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

Overview

You set an endpoint registration timeout range to specify how long an endpoint registration entry remains in the NAT table. The range is 10 to 50,000 seconds, and the default value is 3600 seconds.

Configuration

GUI Step-by-Step Procedure

To specify the H.323 ALG endpoint registration timeout:

1. Select **Configure>Security>ALG**.

2. Select the **H323** tab.

3. In the Timeout for endpoints box, type **5000**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

1. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Verification

To verify the configuration is working properly, enter the **show security alg h323 counters** command.

Understanding H.323 ALG Media Source Port Ranges

Supported Platforms   SRX Series

The media source port feature enables you to configure the device to allow media traffic on a narrow or wide range of ports. By default, the device listens for H.323 traffic on a wide range of ports. If your endpoint equipment allows you to specify a sending port and a listening port, you might want to narrow the range of ports the device allows media traffic on. This enhances security by opening a smaller pinhole for H.323 traffic.

Example: Setting H.323 ALG Media Source Port Ranges

Supported Platforms   SRX Series

This example shows how to enable the H.323 ALG media source port feature.

Requirements

Before you begin, understand and configure any Avaya H.323-specific features. See the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

Overview

The media source port feature enables you to configure the device to allow media traffic on a narrow or wide range of ports. By default, the device listens for H.323 traffic on a narrow range of ports. This example shows how to configure the device to open a wide gate for media traffic by enabling the media source port feature.

Configuration

GUI Step-by-Step Procedure

To enable the H.323 ALG media source port feature:

1. Select **Configure>Security>ALG**.

2. Select the **H323** tab.

3. Select the **Enable Permit media from any source port** check box.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To enable the H.323 ALG media source port feature:

1. Set a narrow gate for media traffic by disabling the media source port for the H.323 ALG.

   ```
   [edit]
   user@host# delete security alg h323 media-source-port-any
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Verification

To verify the configuration is working properly, enter the **show security alg h323 counters** command.

Related Documentation

- Understanding H.323 ALG Media Source Port Ranges on page 177

- H.323 ALG Configuration Overview on page 149

Understanding H.323 ALG DoS Attack Protection

Supported Platforms SRX Series

You can protect the H.323 gatekeeper from denial-of-service (DoS) flood attacks by limiting the number of Registration, Admission, and Status (RAS) messages per second it will attempt to process. Incoming RAS request messages exceeding the threshold you specify are dropped by H.323 Application Layer Gateway (ALG). The range is 2 to 50,000 messages per second, the default value is 1000.

Related Documentation

- Understanding H.323 ALG on page 145

- H.323 ALG Configuration Overview on page 149

- Example: Configuring H.323 ALG DoS Attack Protection on page 179

Example: Configuring H.323 ALG DoS Attack Protection

Supported Platforms   SRX Series

This example shows how to configure the H.323 ALG DoS attack protection feature.

Requirements

Before you begin, understand and configure any Avaya H.323-specific features. See the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

Overview

You can protect the H.323 gatekeeper from DoS flood attacks by limiting the range of Registration, Admission, and Status (RAS) messages per second it will attempt to process. The range is 2 to 50,000 messages per second, and the default value is 1000. This example limits the number of incoming RAS request messages to 5000 messages per second.

Configuration

GUI Step-by-Step Procedure

To configure the H.323 ALG DoS attack protection feature:

1. Select **Configure>Security>ALG**.

2. Select the **H323** tab.

3. In the Message flood gatekeeper threshold box, type **5000**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure the H.323 ALG DoS attack protection feature:

1. Configure the gatekeeper for the H.323 ALG and set the threshold.

   ```
   [edit]
   user@host# set security alg h323 application-screen message-flood gatekeeper
       threshold 5000
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Verification

To verify the configuration is working properly, enter the **show security alg h323 counters** command.

Understanding H.323 ALG Unknown Message Types

Supported Platforms SRX Series

This feature enables you to specify how unidentified H.323 messages are handled by the device. The default is to drop unknown (unsupported) messages.

You can protect the H.323 gatekeeper from denial-of-service (DoS) flood attacks by limiting the number of Registration, Admission, and Status (RAS) messages per second it will attempt to process. Incoming RAS request messages exceeding the threshold you specify are dropped by the H.323 Application Layer Gateway (ALG). The range is 2 to 50,000 messages per second, the default value is 1000.

We do not recommend permitting unknown messages because they can compromise security. However, in a secure test or production environment, this command can be useful for resolving interoperability issues with disparate vendor equipment. Permitting unknown H.323 messages can help you get your network operational, so that you can analyze your voice-over-IP (VoIP) traffic to determine why some messages were being dropped. The unknown H.323 message type feature enables you to configure the device to accept H.323 traffic containing unknown message types in both Network Address Translation (NAT) mode and route mode.

> **NOTE:** This option applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol and you have configured the device to permit unknown message types, the message is forwarded without processing.

Example: Allowing Unknown H.323 ALG Message Types

Supported Platforms SRX Series

This example shows how to configure the device to allow unknown H.323 message types in both route and NAT modes.

Requirements

Before you begin, understand and configure any Avaya H.323-specific features. See the *Administrator Guide for Avaya Communication Manager*, *Avaya IP Telephony Implementation Guide*, and *Avaya Application Solutions IP Telephony Deployment Guide* at http://support.avaya.com.

Overview

This feature enables you to specify how unidentified H.323 messages are handled by the device. The default is to drop unknown (unsupported) messages. The Enable Permit NAT applied option and the **permit-nat-applied** configuration statement specify that unknown messages be allowed to pass if the session is in NAT mode. The Enable Permit routed option and the **permit-routed** configuration statement specify that unknown messages be allowed to pass if the session is in route mode. (Sessions in transparent mode are treated as route mode.)

Configuration

GUI Step-by-Step Procedure

To configure the device to allow unknown H.323 message types in both route and NAT modes:

1. Select **Configure>Security>ALG**.

2. Select the **H323** tab.

3. Select the **Enable Permit NAT applied** check box.

4. Select the **Enable Permit routed** check box.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure the device to allow unknown H.323 message types in both route and NAT modes:

1. Specify that unknown messages be allowed to pass if the session is in NAT mode.

   [edit]
   user@host# **set security alg h323 application-screen unknown-message permit-nat-applied**

2. Specify that unknown messages be allowed to pass if the session is in route mode.

   [edit]

user@host# **set security alg h323 application-screen unknown-message
permit-routed**

3. If you are done configuring the device, commit the configuration.

    [edit]
    user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg h323** command
and the **show security alg h323 counters** command.

Related
Documentation
- Understanding H.323 ALG Unknown Message Types on page 180
- H.323 ALG Configuration Overview on page 149

Configuring the MGCP ALG

Understanding the MGCP ALG

The Media Gateway Control Protocol (MGCP) is a text-based Application Layer protocol used for call setup and call control between the media gateway and the media gateway controller (MGC).

The protocol is based on a master/slave call control architecture: the MGC (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent. Both signaling packets and media packets are transmitted over UDP. Junos OS supports MGCP in route mode and Network Address Translation (NAT) mode.

The MGCP Application Layer Gateway (ALG) performs the following procedures:

- Conducts voice-over-IP (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 RFC 3435. 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 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 then 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.

This topic contains the following sections:

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 the call level. MGCP packets matching the RFC 3435 message format, transaction state, and call state, are processed. All other messages are dropped.

- Security policy enforcement between gateway and gateway controller (signaling policy).

- Security 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.

Entities in MGCP

There are four basic entities in MGCP:

Endpoint

A media gateway is a collection of endpoints. An endpoint can be an analog line, trunk, or any other access point. An endpoint contains the following elements:

local-endpoint-name@domain-name

The following examples are some valid endpoint IDs:

group1/Trk8@example.net
group2/Trk1/*@[192.168.10.8] (wild-carding)
$@example.net (any endpoint within the media gateway)
*@example.net (all endpoints within the media gateway)

Connection

Connections are created on each endpoint by an 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 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 the VoIP network. The following two examples are of call agent names:

CallAgent@voipCA.example.com
voipCA.example.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 a *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 can be changed by a call agent through the use of the **NotifiedEntity** parameter contained in an 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 6 on page 186 lists supported MGCP commands and includes a description of each, the command syntax, and examples. Refer to RFC 2234 for a complete explanation of command syntax.

Table 6: MGCP Commands

Command	Description	Command Syntax	Example
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@example.com MGCP 1.0B: 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 | SecondEndpoindId},] [encapsulated RQNT,] [encapsulated EPCF])	CRCX 1205 aaln/1@gw-25.example.net MGCP 1.0C: A3C47F21456789F0L: p:10, a:PCMUM: sendrecvX: 0123456789ADR: L/hdS: L/rgv=0o=-25678 753849 IN IP4 128.96.41.1s=-c=IN IP4 128.96.41.1t=0 0m=audio 3456 RTP/AVP 0
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.example.net MGCP 1.0C: A3C47F21456789F0I: FDE234C8M: recvonlyX: 0123456789AER: L/huS: G/rtv=0o=-4723891 7428910 IN IP4 128.96.63.25s=-c=IN IP4 128.96.63.25t=0 0m=audio 3456 RTP/AVP 0

Table 6: MGCP Commands *(continued)*

Command	Description	Command Syntax	Example
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.example.net MGCP 1.0C: A3C47F21456789F0I: FDE234C8 Example 2: MG -> MGC DLCX 9310 aaln/1@rgw-25.example.net MGCP 1.0C: A3C47F21456789F0I: FDE234C8E: 900 - Hardware errorP: PS=1245, OS=62345, PR=780, OR=45123, PL=10, JI=27, LA=48
RQNT	NotificationRequest command—Used by a call agent to instruct an 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.example.net MGCP 1.0N: ca-new@callagent-ca.example.netX: 0123456789AAR: 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.example.net MGCP 1.0N: ca@ca1.example.net:5678X: 0123456789ACO: 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
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 aaln/1@rgw-25.example.net MGCP 1.0F: A, R,D,S,X,N,I,T,O Example 2: AUEP 1200 *@rgw-25.example.net 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 aaln/1@rgw-25.example.net MGCP 1.0I: 32F345E2F: C,N,L,M,LC,P

Table 6: MGCP Commands *(continued)*

Command	Description	Command Syntax	Example
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 aaln/1@rg2-25.example.net MGCP 1.0RM: gracefulRD: 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 three-digit response code, transaction ID, and optionally followed by commentary. The response header in the following response message shows 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.

Related Documentation

- ALG Overview on page 3

- MGCP ALG Configuration Overview on page 189

MGCP ALG Configuration Overview

The Media Gateway Control Protocol (MGCP ALG) is enabled by default on the device—no action is required to enable it. However, you might choose to fine-tune MGCP ALG operations by using the following instructions:

1. Free up bandwidth when calls fail to properly terminate. See "Example: Setting MGCP ALG Call Duration" on page 209.

2. Control how long a call can remain active without any media traffic. See "Example: Setting MGCP ALG Inactive Media Timeout" on page 210.

3. Track and clear signaling traffic when it times out. See "Example: Setting MGCP ALG Transaction Timeout" on page 211.

4. Protect the media gateway from denial-of-service (DoS) flood attacks. See "Example: Configuring MGCP ALG DoS Attack Protection" on page 213.

5. Enable unknown messages to pass when the session is in Network Address Translation (NAT) mode and route mode. See "Example: Allowing Unknown MGCP ALG Message Types" on page 214.

Related Documentation
- Understanding the MGCP ALG on page 183
- Example: Configuring Media Gateways in Subscriber Homes Using MGCP ALGs on page 189
- Example: Configuring Three-Zone ISP-Hosted Service Using MGCP ALG and NAT on page 196

Example: Configuring Media Gateways in Subscriber Homes Using MGCP ALGs

This example shows how to configure media gateways in subscriber homes using MGCP ALGs.

- Requirements on page 189
- Overview on page 190
- Configuration on page 191
- Verification on page 194

Requirements

Before you begin:

- Configure zones. See *Example: Creating Security Zones*.

- Configure addresses and interfaces. See *Example: Configuring Address Books and Address Sets*.

- Configure security policies. See *Security Policies Configuration Overview*.

Overview

When a cable service provider offers MGCP services to residential subscribers, they locate the Juniper Networks device and call agent on their premises and install a set-top box, in each subscriber's home. The set-top boxes act as gateways for the residences.

After creating zones—external_subscriber for the customer and internal_ca for the service provider—you configure addresses, then interfaces, and finally policies to allow signaling between endpoints. Note that although gateways frequently reside in different zones, requiring policies for media traffic, in this example both gateways are in the same subnet. Note also that because RTP traffic between the gateways never passes through the device, no policy is needed for the media. See .

Figure 15: Media Gateway in Subscriber Homes

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set security zones security-zone external-subscriber host-inbound-traffic system-services
    all
set security zones security-zone external-subscriber host-inbound-traffic protocols all
set security zones security-zone internal-ca host-inbound-traffic system-services all
set security zones security-zone internal-ca host-inbound-traffic protocols all
set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.1/24
set interfaces ge-0/0/0 unit 0 family inet
set security zones security-zone external-subscriber interfaces ge-0/0/0
set security zones security-zone internal-ca interfaces ge-0/0/1
set security address-book book1 address ca-agent 110.1.1.101/32
set security address-book book1 attach zone internal-ca
set security address-book book2 address subscriber-subnet 2.2.2.1/24
set security address-book book2 attach zone external-subscriber
set security policies from-zone internal-ca to-zone external-subscriber policy
    ca-to-subscribers match source-address ca-agent-1
set security policies from-zone internal-ca to-zone external-subscriber policy
    ca-to-subscribers match destination-address subscriber-subnet
set security policies from-zone internal-ca to-zone external-subscriber policy
    ca-to-subscribers match application junos-mgcp
set security policies from-zone internal-ca to-zone external-subscriber policy
    ca-to-subscribers then permit
set security policies from-zone external-subscriber to-zone internal-ca policy
    subscriber-to-ca match source-address subscriber-subnet
set security policies from-zone external-subscriber to-zone internal-ca policy
    subscriber-to-ca match destination-address ca-agent-1
set security policies from-zone external-subscriber to-zone internal-ca policy
    subscriber-to-ca match application junos-mgcp
set security policies from-zone external-subscriber to-zone internal-ca policy
    subscriber-to-ca then permit
set security policies from-zone internal-ca to-zone internal-ca policy intra-ca match
    source-address any
set security policies from-zone internal-ca to-zone internal-ca policy intra-ca match
    destination-address any
set security policies from-zone internal-ca to-zone internal-ca policy intra-ca match
    application any
set security policies from-zone internal-ca to-zone internal-ca policy intra-ca then permit
set security policies from-zone external-subscriber to-zone external-subscriber policy
    intra-subscriber match source-address any
set security policies from-zone external-subscriber to-zone external-subscriber policy
    intra-subscriber match destination-address any
set security policies from-zone external-subscriber to-zone external-subscriber policy
    intra-subscriber match application any
set security policies from-zone external-subscriber to-zone external-subscriber policy
    intra-subscriber then permit
```

Step-by-Step Procedure   The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure media gateways in subscriber homes using MGCP ALGs:

1. Create security zones for the customer and the service provider.

   ```
   [edit security zones security-zone external-subscriber]
   user@host# set host-inbound-traffic system-services all
   user@host# set host-inbound-traffic protocols all


   [edit security zones security-zone internal-ca]
   user@host# set host-inbound-traffic system-services all
   user@host# set host-inbound-traffic protocols all
   ```

2. Configure interfaces for the zones.

   ```
   [edit]
   user@host# edit security zones security-zone external-subscriber interfaces
       ge-0/0/0
   user@host# set interfaces ge-0/0/0 unit 0 family inet
   user@host# set security zones security-zone internal-ca interfaces ge-0/0/1
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.1/24
   ```

3. Configure address books and attach zones to them.

   ```
   [edit security address-book book1]
   user@host# set address ca-agent 110.1.1.101/32
   user@host# set attach zone internal-ca

   [edit security address-book book2]
   user@host# set address subscriber-subnet 2.2.2.1/24
   user@host# set attach zone external-subscriber
   ```

4. Configure policies for traffic from the internal to the external zone.

   ```
   [edit security policies from-zone internal-ca to-zone external-subscriber policy
       ca-to-subscribers]
   user@host# edit match source-address ca-agent-1
   user@host# set match destination-address subscriber-subnet
   user@host# set match application junos-mgcp
   user@host# set then permit
   ```

5. Configure policies for traffic from the external to the internal zone.

   ```
   [edit security policies from-zone external-subscriber to-zone internal-ca policy
       subscriber-to-ca]
   user@host# edit match source-address subscriber-subnet
   user@host# set match destination-address ca-agent-1
   user@host# set match application junos-mgcp
   user@host# set then permit
   ```

6. Configure policies for traffic between two internal zones.

   ```
   [edit security policies from-zone internal-ca to-zone internal-ca policy intra-ca]
   user@host# edit match source-address any
   user@host# set match destination-address any
   user@host# set match application any
   user@host# set then permit
   ```

7. Configure policies for traffic between two external zones.

```
[edit security policies from-zone external-subscriber to-zone external-subscriber
    policy intra-subscriber]
user@host# edit match source-address any
user@host# set match destination-address any
user@host# set match application any
user@host# set then permit
```

Results   From configuration mode, confirm your configuration by entering the **show security policies** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
from-zone internal-ca to-zone external-subscriber {
  policy ca-to-subscribers {
    match {
      source-address ca-agent-1;
      destination-address subscriber-subnet;
      application junos-mgcp;
    }
    then {
      permit;
    }
  }
}
from-zone external-subscriber to-zone internal-ca {
  policy subscriber-to-ca {
    match {
      source-address subscriber-subnet;
      destination-address ca-agent-1;
      application junos-mgcp;
    }
    then {
      permit;
    }
  }
}
from-zone internal-ca to-zone internal-ca {
  policy intra-ca {
    match {
      ssource-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone external-subscriber to-zone external-subscriber {
  policy intra-subscriber {
    match {
      source-address any;
      destination-address any;
      application any;
```

```
        }
      then {
        permit;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform this task:

Verifying MGCP ALGs

Purpose   Verify the MGCP ALG verification options.

Action   From operational mode, enter the **show security alg mgcp ?** command.

```
user@host> show security alg mgcp ?
Possible completions:
  calls                  Show MGCP calls
  counters               Show MGCP counters
  endpoints              Show MGCP endpoints
```

Meaning   The output shows a list of all MGCP verification parameters. Verify the following information:

- All MGCP calls
- Counters for all MGCP calls
- Information about all MGCP endpoints

Verifying MGCP ALG Calls

Purpose   Verify information about active MGCP calls.

Action   From operational mode, enter the **show security alg mgcp calls** command.

```
user@host> show security alg mgcp calls
Endpoint@GW                     Zone        Call ID               RM Group
d001@101.50.10.1                Trust       10d55b81140e0f76      512
    Connection Id> 0
    Local SDP>  o: 101.50.10.1              x_o: 101.50.10.1
                c: 101.50.10.1/32206        x_c: 101.50.10.1/32206
    Remote SDP> c: 3.3.3.5/16928            x_c: 3.3.3.5/16928
Endpoint@GW                     Zone        Call ID               RM Group
d001@3.3.3.5                    Untrust     3a104e9b41a7c4c9      511
    Connection Id> 0
```

```
Local SDP>  o: 3.3.3.5                    x_o: 3.3.3.5
            c: 3.3.3.5/16928              x_c: 3.3.3.5/16928
Remote SDP> c: 101.50.10.1/32206          x_c: 101.50.10.1/32206
```

Meaning The output displays information about all MGCP calls. Verify the following information:

- Endpoint

- Zone

- Call identifier

- Resource Manager group

Verifying MGCP ALG Endpoints

Purpose Verify information about MGCP endpoints.

Action From operational mode, enter the **show security alg mgcp endpoints** command.

```
user@host> show security alg mgcp endpoints
Gateway: 101.50.10.1 Zone: Trust IP: 101.50.10.1 -> 101.50.10.1
   Endpoint           Trans #  Call #   Notified Entity
   d001               1        1        0.0.0.0/0->0.0.0.0/0
Gateway: 3.3.3.5 Zone: Untrust IP: 3.3.3.5 -> 3.3.3.5
   Endpoint           Trans #  Call #   Notified Entity
   d001               1        1        0.0.0.0/0->0.0.0.0/0
```

Meaning The output displays information about all MGCP endpoints. Verify the following information:

- Gateway IP address and zone of both endpoints

- Endpoint identifier, transaction number, call number, and notified entity for each gateway

Verifying MGCP ALG Counters

Purpose Verify information about MGCP counters.

Action From operational mode, enter the **show security alg mgcp counters** command.

```
user@host> show security alg mgcp counters
MGCP counters summary:
Packets received            :284
Packets dropped             :0
Message received            :284
Number of connections       :4
Number of active connections :3
Number of calls             :4
Number of active calls      :3
Number of transactions      :121
Number of active transactions:52
Number of re-transmission   :68
MGCP Error Counters:
Unknown-method              :0
Decoding error              :0
```

```
Transaction error         :0
Call error                :0
Connection error          :0
Connection flood drop     :0
Message flood drop        :0
IP resolve error          :0
NAT error                 :0
Resource manager error    :0
MGCP Packet Counters:
CRCX    :4        MDCX     :9      DLCX    :2
AUEP    :1        AUCX     :0      NTFY    :43
RSIP    :79       EPCF     :0      RQNT    :51
000-199 :0        200-299  :95     300-999 :0
```

Meaning   The output displays information about all MGCP counters. Verify the following information:

- Summary of MGCP counters

- MGCP error counters

- MGCP packet counters

Related
Documentation

- Understanding the MGCP ALG on page 183

- MGCP ALG Configuration Overview on page 189

Example: Configuring Three-Zone ISP-Hosted Service Using MGCP ALG and NAT

This example shows how to configure a three-zone configuration using MGCP ALG and NAT.

- Requirements on page 196
- Overview on page 196
- Configuration on page 198
- Verification on page 206

Requirements

Before you begin, understand NAT support with MGCP ALG. See "Understanding the MGCP ALG" on page 183.

Overview

Typically, a three-zone configuration is used when an ISP in one geographical location provides service to two networks in different geographical locations.

In this example (see Figure 16 on page 198), an ISP located on the USA West Coast provides MGCP service to customers in separate networks in Asia and San Francisco. Asia customers are in the asia-3 zone and are supported by the asia-gw gateway; San Francisco customers are in the sf-2 zone and are supported by the sf-gw gateway. A call agent, west-ca, is in the DMZ. The gateways and the call agent are listed in Table 7 on page 198, showing the corresponding IP address, interface, and zone.

In this example, after creating zones and setting addresses for the gateways and the call agent, you associate the zones to interfaces, and then configure static NAT to the call agent and source NAT for communication from an IP phone in the sf-2 zone to phones in the asia-3 zone. You also configure a policy between the zones to allow the communication.

Topology

shows a three-zone ISP-hosted service.

Figure 16: Three-Zone ISP-Hosted Service
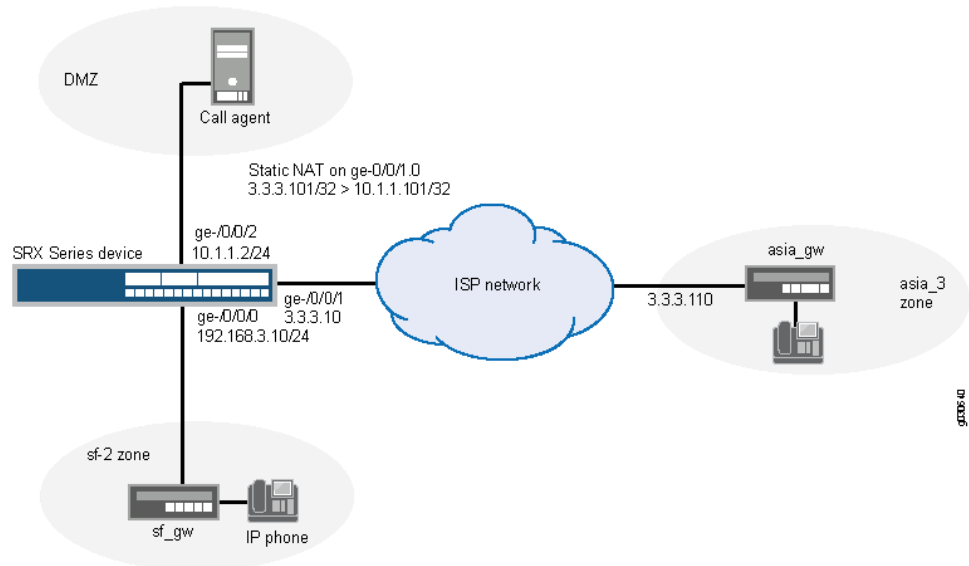
Table 7: Three-Zone ISP-Host Service

Gateway	IP Address	Interface	Zone
sf-gw	192.168.3.201	ge-0/0/0	sf-2
asia-gw	3.3.3.101	ge-0/0/1	asia-3
west-ca	10.1.1.101	ge-0/0/2	DMZ

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 192.168.3.10/24
set interfaces ge-0/0/1 unit 0 family inet address 3.3.3.10/24
set interfaces ge-0/0/2 unit 0 family inet address 10.1.1.2/24
set security zones security-zone sf-2 interfaces ge-0/0/0.0
set security zones security-zone asia-3 interfaces ge-0/0/1.0
set security zones security-zone dmz interfaces ge-0/0/2.0
set security address-book book1 address sf-gw 192.168.3.201/32
set security address-book book1 attach zone sf-2
set security address-book book2 address asia-gw 3.3.3.101/32
set security address-book book2 attach zone asia-3
set security address-book book3 address west-ca 10.1.1.101/32
```

```
set security address-book book3 attach zone dmz
set security nat source pool ip-phone-pool address 3.3.3.20/32
set security nat source rule-set phones from zone sf-2
set security nat source rule-set phones to zone asia-3
set security nat source rule-set phones rule phone1 match source-address 192.168.3.10/32
set security nat source rule-set phones rule phone1 match destination 3.3.3.101/32
set security nat source rule-set phones rule phone1 then source-nat pool ip-phone-pool
set security nat static rule-set to-callagent from zone asia-3
set security nat static rule-set to-callagent rule phone1 match destination-address
    3.3.3.101/32
set security nat static rule-set to-callagent rule phone1 then static-nat prefix 10.1.1.101/32
set security nat proxy-arp interface ge-0/0/1.0 address 3.3.3.101/32
set security nat proxy-arp interface ge-0/0/1.0 address 3.3.3.20/32
set security policies from-zone dmz to-zone asia-3 policy pol-dmz-to-asia-3 match
    source-address west-ca
set security policies from-zone dmz to-zone asia-3 policy pol-dmz-to-asia-3 match
    destination-address asia-gw
set security policies from-zone dmz to-zone asia-3 policy pol-dmz-to-asia-3 match
    application junos-mgcp
set security policies from-zone dmz to-zone asia-3 policy pol-dmz-to-asia-3 then permit
set security policies from-zone asia-3 to-zone dmz policy pol-asia-3-to-dmz match
    source-address asia-gw
set security policies from-zone asia-3 to-zone dmz policy pol-asia-3-to-dmz match
    destination-address west-ca
set security policies from-zone asia-3 to-zone dmz policy pol-asia-3-to-dmz match
    application junos-mgcp
set security policies from-zone asia-3 to-zone dmz policy pol-asia-3-to-dmz then permit
set security policies from-zone sf-2 to-zone dmz policy pol-sf-2-to-dmz match
    source-address sf-gw
set security policies from-zone sf-2 to-zone dmz policy pol-sf-2-to-dmz match
    destination-address west-ca
set security policies from-zone sf-2 to-zone dmz policy pol-sf-2-to-dmz match application
    junos-mgcp
set security policies from-zone sf-2 to-zone dmz policy pol-sf-2-to-dmz then permit
set security policies from-zone dmz to-zone sf-2 policy pol-dmz-to-sf-2 match
    source-address west-ca
set security policies from-zone dmz to-zone sf-2 policy pol-dmz-to-sf-2 match
    destination-address sf-gw
set security policies from-zone dmz to-zone sf-2 policy pol-dmz-to-sf-2 match application
    junos-mgcp
set security policies from-zone dmz to-zone sf-2 policy pol-dmz-to-sf-2 then permit
set security policies from-zone sf-2 to-zone asia-3 policy pol-sf-2-to-asia-3 match
    source-address sf-gw
set security policies from-zone sf-2 to-zone asia-3 policy pol-sf-2-to-asia-3 match
    destination-address asia-gw
set security policies from-zone sf-2 to-zone asia-3 policy pol-sf-2-to-asia-3 match
    application junos-mgcp
set security policies from-zone sf-2 to-zone asia-3 policy pol-sf-2-to-asia-3 then permit
set security policies from-zone asia-3 to-zone sf-2 policy pol-asia-3-to-sf-2 match
    source-address asia-gw
set security policies from-zone asia-3 to-zone sf-2 policy pol-asia-3-to-sf-2 match
    destination sf-gw
set security policies from-zone asia-3 to-zone sf-2 policy pol-asia-3-to-sf-2 match
    application junos-mgcp
set security policies from-zone asia-3 to-zone sf-2 policy pol-asia-3-to-sf-2 then permit
```

set security policies from-zone sf-2 to-zone sf-2 policy pol-intra-sf-2 match source-address
    any
set security policies from-zone sf-2 to-zone sf-2 policy pol-intra-sf-2 match
    destination-address any
set security policies from-zone sf-2 to-zone sf-2 policy pol-intra-sf-2 match application
    any
set security policies from-zone sf-2 to-zone sf-2 policy pol-intra-sf-2 then permit
set security policies from-zone asia-3 to-zone asia-3 policy pol-intra-asia-3 match
    source-address any
set security policies from-zone asia-3 to-zone asia-3 policy pol-intra-asia-3 match
    destination-address any
set security policies from-zone asia-3 to-zone asia-3 policy pol-intra-asia-3 match
    application any
set security policies from-zone asia-3 to-zone asia-3 policy pol-intra-asia-3 then permit

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a three-zone configuration using MGCP ALG and NAT:

1. Configure interfaces.

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.168.3.10/24
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 3.3.3.10/24
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.1.1.2/24
   ```

2. Create security zones.

   ```
   [edit security zones]
   user@host# set security-zone sf-2 interfaces ge-0/0/0
   user@host# set security-zone asia-3 interfaces ge-0/0/1
   user@host# set security-zone dmz interfaces ge-0/0/2
   ```

3. Create address books and assign zones to them.

   ```
   [edit security address-book book1]
   user@host# set address sf-gw 192.168.3.201/32
   user@host# set attach zone sf-2

   [edit security address-book book2]
   user@host# set address asia-gw 3.3.3.101/32
   user@host# set attach zone asia-3

   [edit security address-book book3]
   user@host# set address west-ca 10.1.1.101/32
   user@host# set attach zone dmz
   ```

4. Create a static NAT rule set and set the match conditions and actions for it.

   ```
   [edit security nat static rule-set to-callagent]
   user@host# set from zone asia-3
   user@host# set rule phone1 match destination-address 3.3.3.101/32
   user@host# set rule phone1 then static-nat prefix 10.1.1.101/32
   ```

5. Configure proxy ARP for address **3.3.3.101/32** on interface **ge-0/0/1.0**.

   ```
   [edit security nat ]
   user@host# set proxy-arp interface ge-0/0/1.0 address 3.3.3.101/32
   ```

6. Create a source NAT pool.

    [edit security nat]
    user@host# set source pool ip-phone-pool address 3.3.3.20/32

7. Create a source NAT rule set and set the match conditions and actions for it.

    [edit security nat source rule-set phones]
    user@host# set from zone sf-2
    user@host# set to zone asia-3
    user@host# set rule phone1 match source-address 192.168.3.10/32
    user@host# set rule phone1 match destination-address 3.3.3.101/32
    user@host# set rule phone1 then source-nat pool ip-phone-pool

8. Configure proxy ARP for address **3.3.3.20/32** on interface **ge-0/0/1.0**.

    [edit security nat]
    user@host# set proxy-arp interface ge-0/0/1.0 address 3.3.3.20/32

9. Configure a policy to allow traffic from DMZ to Asia.

    [edit security policies from-zone dmz to-zone asia-3 policy pol-dmz-to-asia-3]
    user@host# set match source-address west-ca
    user@host# set match destination-address asia-gw
    user@host# set match application junos-mgcp
    user@host# set then permit

10. Configure a policy to allow traffic from Asia to DMZ.

    [edit security policies from-zone asia-3 to-zone dmz policy pol-asia-3-to-dmz]
    user@host# set match source-address asia-gw
    user@host# set match destination-address west-ca
    user@host# set match application junos-mgcp
    user@host# set then permit

11. Configure a policy to allow traffic from San Francisco to DMZ.

    [edit security policies from-zone sf-2 to-zone dmz policy pol-sf-2-to-dmz]
    user@host# set match source-address sf-gw
    user@host# set match destination-address west-ca
    user@host# set match application junos-mgcp
    user@host# set then permit

12. Configure a policy to allow traffic from DMZ to San Francisco.

    [edit security policies from-zone dmz to-zone sf-2 policy pol-dmz-to-sf-2]
    user@host# set match source-address west-ca
    user@host# set match destination-address sf-gw
    user@host# set match application junos-mgcp
    user@host# set then permit

13. Configure a policy to allow traffic from San Francisco to Asia.

    [edit security policies from-zone sf-2 to-zone asia-3 policy pol-sf-2-to-asia-3]
    user@host# set match source-address sf-gw
    user@host# set match destination-address asia-gw
    user@host# set match application junos-mgcp
    user@host# set then permit

14. Configure a policy to allow traffic from Asia to San Francisco.

    [edit security policies from-zone asia-3 to-zone sf-2 policy pol-asia-3-to-sf-2]

```
user@host# set match source-address asia-gw
user@host# set match destination-address sf-gw
user@host# set match application junos-mgcp
user@host# set then permit
```

15. Configure a policy to allow traffic on devices within San Francisco.

```
[edit security policies from-zone sf-2 to-zone sf-2 policy pol-intra-sf-2]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application any
user@host# set then permit
```

16. Configure a policy to allow traffic on devices within Asia.

```
[edit security policies from-zone asia-3 to-zone asia-3 policy pol-intra-asia-3]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application any
user@host# set then permit
```

Results   From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security address-book**, **show security nat**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.3.10/24;
      }
    }
  }
    ge-0/0/1 {
      unit 0 {
        family inet {
          address 3.3.3.10/24;
        }
      }
    }
    ge-0/0/2 {
      unit 0 {
        family inet {
          address 10.1.1.2/24;
        }
      }
    }
[edit]
user@host# show security zones
security-zone sf-2 {
  interfaces {
    ge-0/0/0.0;
  }
}
```

```
        security-zone asia-3 {
          interfaces {
            ge-0/0/1.0;
          }
        }
        security-zone dmz {
          interfaces {
            ge-0/0/2.0;
          }
        }
[edit]
user@host# show security address-book
book1 {
  address sf-gw 192.168.3.201/32;
  attach {
    zone sf-2;
  }
}
  book2 {
    address asia-gw 3.3.3.101/32;
    attach {
      zone asia-3;
    }
  }
  book3 {
    address west-ca 10.1.1.101/32;
    attach {
      zone dmz;
    }
  }
[edit]
user@host# show security nat
source {
  pool ip-phone-pool {
    address {
      3.3.3.20/32;
    }
  }
  rule-set phones {
    from zone sf-2;
    to zone asia-3;
    rule phone1 {
      match {
        source-address 192.168.3.10/32;
        destination-address 3.3.3.101/32;
      }
      then {
        source-nat {
          pool {
            ip-phone-pool;
          }
        }
      }
    }
  }
}
```

```
                  static {
                    rule-set to-callagent {
                      from zone asia-3;
                      rule phone1 {
                        match {
                          destination-address 3.3.3.101/32;
                        }
                        then {
                          static-nat prefix 10.1.1.101/32;
                        }
                      }
                    }
                  }
                  proxy-arp {
                    interface ge-0/0/1.0 {
                      address {
                        3.3.3.101/32;
                        3.3.3.20/32;
                      }
                    }
                  }
[edit]
user@host# show security policies
from-zone dmz to-zone asia-3 {
  policy pol-dmz-to-asia-3 {
    match {
      source-address west-ca;
      destination-address asia-gw;
      application junos-mgcp;
    }
    then {
      permit;
    }
  }
}
from-zone asia-3 to-zone dmz {
  policy pol-asia-3-to-dmz {
    match {
      source-address asia-gw;
      destination-address west-ca;
      application junos-mgcp;
    }
    then {
      permit;
    }
  }
}
from-zone sf-2 to-zone dmz {
  policy pol-sf-2-to-dmz {
    match {
      source-address sf-gw;
      destination-address west-ca;
      application junos-mgcp;
    }
    then {
      permit;
```

```
        }
      }
    }
    from-zone dmz to-zone sf-2 {
      policy pol-dmz-to-sf-2 {
        match {
          source-address west-ca;
          destination-address sf-gw;
          application junos-mgcp;
        }
        then {
          permit;
        }
      }
    }
    from-zone sf-2 to-zone asia-3 {
      policy pol-sf-2-to-asia-3 {
        match {
          source-address sf-gw;
          destination-address asia-gw;
          application junos-mgcp;
        }
        then {
          permit;
        }
      }
    }
    from-zone asia-3 to-zone sf-2 {
      policy pol-asia-3-to-sf-2 {
        match {
          source-address asia-gw;
          destination-address sf-gw;
          application junos-mgcp;
        }
        then {
          permit;
        }
      }
    }
    from-zone sf-2 to-zone sf-2 {
      policy pol-intra-sf-2 {
        match {
          source-address any;
          destination-address any;
          application any;
        }
        then {
          permit;
        }
      }
    }
    from-zone asia-3 to-zone asia-3 {
      policy pol-intra-asia-3 {
        match {
          source-address any;
          destination-address any;
```

```
            application any;
          }
          then {
            permit;
          }
        }
      }
    }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying MGCP ALG on page 206
- Verifying MGCP Calls on page 206
- Verifying MGCP ALG Statistics on page 207
- Verifying MGCP Endpoints on page 207

Verifying MGCP ALG

Purpose Verify if the MGCP ALG is enabled.

Action From operational mode, enter the **show security alg status | match mgcp** command.

    user@host> **show security alg status | match mgcp**

```
MGCP      : Enabled
```

Meaning The output shows the MGCPALG status as follows:

- Enabled—Shows the MGCP ALG is enabled.

- Disabled—Shows the MGCP ALG is disabled.

Verifying MGCP Calls

Purpose Verify the MGCP calls that are currently active.

Action From operational mode, enter the **show security alg mgcp calls** command.

    user@host> **show security alg mgcp calls**

```
Endpoint@GW                      Zone         Call ID              RM Group
d001@101.50.10.1                 Trust        10d55b81140e0f76     512
   Connection Id> 0
   Local SDP>  o: 101.50.10.1              x_o: 101.50.10.1
             c: 101.50.10.1/32206          x_c: 101.50.10.1/32206
   Remote SDP> c: 3.3.3.5/16928            x_c: 3.3.3.5/16928
Endpoint@GW                      Zone         Call ID              RM Group
d001@3.3.3.5                     Untrust      3a104e9b41a7c4c9     511
   Connection Id> 0
   Local SDP>  o: 3.3.3.5                  x_o: 3.3.3.5
             c: 3.3.3.5/16928              x_c: 3.3.3.5/16928
   Remote SDP> c: 101.50.10.1/32206        x_c: 101.50.10.1/32206
```

Meaning   The output displays information about all MGCP calls. Verify the following information:

- Endpoint

- Zone

- Call identifier

- Resource Manager group

Verifying MGCP ALG Statistics

Purpose   Verify the MGCP ALG statistics.

Action   From operational mode, enter the **show security alg mgcp counters** command.

```
user@host> show security alg mgcp counters

MGCP counters summary:
Packets received           :284
Packets dropped            :0
Message received           :284
Number of connections      :4
Number of active connections :3
Number of calls            :4
Number of active calls     :3
Number of transactions     :121
Number of active transactions:52
Number of re-transmission  :68
MGCP Error Counters:
Unknown-method             :0
Decoding error             :0
Transaction error          :0
Call error                 :0
Connection error           :0
Connection flood drop      :0
Message flood drop         :0
IP resolve error           :0
NAT error                  :0
Resource manager error     :0
MGCP Packet Counters:
CRCX    :4       MDCX    :9       DLCX     :2
AUEP    :1       AUCX    :0       NTFY     :43
RSIP    :79      EPCF    :0       RQNT     :51
000-199 :0       200-299 :95      300-999  :0
```

Meaning   The output displays information about all MGCP counters. Verify the following information:

- Summary of MGCP counters

- MGCP error counters

- MGCP packet counters

Verifying MGCP Endpoints

Purpose   Verify the MGCP endpoints.

Action   From operational mode, enter the **show security alg mgcp endpoints** command.

> user@host> **show security alg mgcp endpoints**

```
Gateway: 101.50.10.1 Zone: Trust IP: 101.50.10.1 -> 101.50.10.1
    Endpoint              Trans #  Call #   Notified Entity
    d001                   1        1        0.0.0.0/0->0.0.0.0/0
Gateway: 3.3.3.5 Zone: Untrust IP: 3.3.3.5 -> 3.3.3.5
    Endpoint              Trans #  Call #   Notified Entity
    d001                   1        1        0.0.0.0/0->0.0.0.0/0
```

Meaning   The output displays information about all MGCP endpoints. Verify the following information:

- Gateway IP address and zone of both endpoints

- Endpoint identifier, transaction number, call number, and notified entity for each gateway

Related   • *Static NAT Configuration Overview*
Documentation
             • *Understanding Source NAT*

Understanding MGCP ALG Call Duration and Timeouts

The call duration feature gives you control over Media Gateway Control Protocol (MGCP) call activity and helps you to manage network resources.

Typically a Delete Connection (DLCX) message will be sent out to delete a connection. The MCGP Application Layer Gateway (ALG) intercepts it and removes all media sessions for that connection.

A call can have one or more voice channels. Each voice channel has two sessions (or two media streams), one for Real-Time Transport Protocol (RTP) traffic and one for Real-Time Control Protocol (RTCP) signaling. When managing the sessions, the device considers the sessions in each voice channel as one group. Timeouts and call duration settings apply to a group as opposed to each session.

The following parameters govern MGCP call activity:

- **maximum-call-duration**—This parameter sets the absolute maximum length of a call. When a call exceeds this parameter setting, the MGCP ALG tears down the call and releases the media sessions. The default setting is 720 minutes, and the range is 3 through 720 minutes. This setting also frees up bandwidth in cases where calls fail to properly terminate.

- **inactive-media-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. When the period of inactivity exceeds this setting, the MGCP ALG gates opened for media are closed. The default setting is 120 seconds, and the range is 10 through 2550 seconds. Note that upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.

> ℹ️ NOTE: The **inactive-media-timeout** value should be less than the **maximum-call-duration** value.

- **transaction-timeout**—A transaction is a command and its mandatory response. For example, an NTFY from the gateway to the call agent or a 200 OK from the call agent to the gateway. The Juniper Networks device tracks these transactions and clears them when they time out. The timeout range for MGCP transactions is 3 through 50 seconds and the default is 30 seconds.

Example: Setting MGCP ALG Call Duration

This example shows how to set call duration for the MGCP ALG.

Requirements

Before you begin, determine the type of parameter used to control the MGCP call activity and manage its network resources. See "Understanding MGCP ALG Call Duration and Timeouts" on page 208.

Overview

The **maximum-call-duration** parameter governs MGCP call activity and sets the absolute maximum length of a call. When a call exceeds this parameter setting, the MGCP ALG tears down the call and releases the media sessions. The default setting is 720 minutes, and the range is 3 through 720 minutes. This setting also frees up bandwidth in cases where calls fail to properly terminate. In this example, the call duration is set to 600 minutes.

Configuration

GUI Step-by-Step Procedure

To set call duration for the MGCP ALG:

1. Select **Configure** >**Security** >**ALG**.

2. Select the **MGCP** tab.

3. In the Maximum call duration box, enter **600**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options** >**Commit**.

Step-by-Step Procedure
To set call duration for the MGCP ALG:

1. Configure the MGCP ALG call duration.

   [edit]
   user@host# **set security alg mgcp maximum-call-duration 600**

2. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg mgcp** command.

Related Documentation
- Understanding MGCP ALG Call Duration and Timeouts on page 208
- MGCP ALG Configuration Overview on page 189

Example: Setting MGCP ALG Inactive Media Timeout

This example shows how to set the inactive media timeout value for the MGCP ALG.

- Requirements on page 210
- Overview on page 210
- Configuration on page 211
- Verification on page 211

Requirements

Before you begin, determine the type of parameter used to control the MGCP call activity and manage its network resources. See "Understanding MGCP ALG Call Duration and Timeouts" on page 208.

Overview

The **inactive-media-timeout** parameter governs MGCP call activity and 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. When the period of inactivity exceeds this setting, the MGCP ALG gates opened for media are closed. The default setting is 120 seconds, and the range is from 10 to 2550 seconds. Note that upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated. In this example, the inactive media timeout is set to 90 seconds.

Configuration

GUI Step-by-Step Procedure

To set the inactive media timeout for the MGCP ALG:

1. Select **Configure>Security>ALG**.

2. Select the **MGCP** tab.

3. In the Inactive Media Timeout box, enter **90**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To set the inactive media timeout for the MGCP ALG:

1. Configure the MGCP ALG inactive media timeout value.

   ```
   [edit]
   user@host# set security alg mgcp inactive-media-timeout 90
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Verification

To verify the configuration is working properly, enter the **show security alg mgcp** command.

Related Documentation

- Understanding MGCP ALG Call Duration and Timeouts on page 208
- MGCP ALG Configuration Overview on page 189

Example: Setting MGCP ALG Transaction Timeout

This example shows how to set the transaction timeout for the MGCP ALG.

- Requirements on page 211
- Overview on page 211
- Configuration on page 212
- Verification on page 212

Requirements

Before you begin, determine the type of parameter used to control the MGCP call activity and manage its network resources. See "Understanding MGCP ALG Call Duration and Timeouts" on page 208.

Overview

The **transaction-timeout** parameter governs MGCP call activity and is a signaling message; for example, a NTFY from the gateway to the call agent or a 200 OK from the call agent

to the gateway. The Juniper Networks device tracks these transactions, and clears them when they time out. The timeout range for MGCP transactions is from 3 to 50 seconds, and the default is 30 seconds. In this example, the transaction timeout is set to 20 seconds.

Configuration

GUI Step-by-Step Procedure

To set the transaction timeout for the MGCP ALG:

1. Select **Configure>Security>ALG**.

2. Select the **MGCP** tab.

3. In the Transaction Timeout box, enter **20**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To set the transaction timeout for the MGCP ALG:

1. Configure the MGCP ALG transaction timeout value.

   ```
   [edit]
   user@host# set security alg mgcp transaction-timeout 20
   ```

2. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   user@host# commit
   ```

Verification

To verify the configuration is working properly, enter the **show security alg mgcp** command.

Related Documentation

- Understanding MGCP ALG Call Duration and Timeouts on page 208

- MGCP ALG Configuration Overview on page 189

Understanding MGCP ALG DoS Attack Protection

You can protect the Media Gateway Control Protocol (MGCP) media gateway from denial-of-service (DoS) flood attacks by limiting the number of remote access service (RAS) messages and connections per second it will attempt to process.

When you configure MGCP message flood protection, the MGCP Application Layer Gateway (ALG) drops any messages exceeding the threshold you set. The range is 2 to 50,000 messages per second per media gateway, and the default is 1000 messages per second per media gateway.

When you configure MGCP connection flood protection, the MGCP ALG drops any connection request exceeding the threshold you set. This limits the rate of processing of **CreateConnection** (**CRCX**) commands, thereby indirectly limiting pinhole creation. The

range is 2 to 10,000 connection requests per second per media gateway, the default is 200.

Related Documentation

- Understanding the MGCP ALG on page 183

- MGCP ALG Configuration Overview on page 189

- Example: Configuring MGCP ALG DoS Attack Protection on page 213

Example: Configuring MGCP ALG DoS Attack Protection

This example shows how to configure connection flood protection for the MGCP ALG.

- Requirements on page 213
- Overview on page 213
- Configuration on page 213
- Verification on page 214

Requirements

Before you begin, determine whether to protect the MGCP media gateway from DoS flood attacks. See "Understanding MGCP ALG DoS Attack Protection" on page 212.

Overview

In this example, you configure the MGCP ALG to drop any message requests exceeding 10,000 requests per second and to drop any connection requests exceeding 4000 per second.

Configuration

GUI Step-by-Step Procedure

To configure connection flood protection for the MGCP ALG:

1. Select **Configure>Security>ALG**.

2. Select the **MGCP** tab.

3. In the Message flood gatekeeper threshold box, type **10000**.

4. In the Connection flood threshold box, type **4000**.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure connection flood protection for the MGCP ALG:

1. Configure the connection flood threshold value.

   ```
   [edit]
   user@host# set security alg mgcp application-screen message-flood threshold
       10000
   user@host# set security alg mgcp application-screen connection-flood threshold
       4000
   ```

2. If you are done configuring the device, commit the configuration.

[edit]
user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg mgcp** command.

Related
Documentation
- Understanding MGCP ALG DoS Attack Protection on page 212
- MGCP ALG Configuration Overview on page 189

Understanding MGCP ALG Unknown Message Types

To accommodate on-going development of the Media Gateway Control Protocol (MGCP), you might want to allow traffic containing new MGCP message types. The unknown MGCP message type feature enables you to configure the Juniper Networks device to accept MGCP traffic containing unknown message types in both Network Address Translation (NAT) mode and route mode.

This feature enables you to specify how unidentified MGCP messages are handled by the Juniper Networks device. The default is to drop unknown (unsupported) messages. Unknown messages can compromise security. However, in a secure test or production environment, this command can be useful for resolving interoperability issues with disparate vendor equipment. Permitting unknown MGCP messages can help you get your network operational so that you can later analyze your voice-over-IP (VoIP) traffic to determine why some messages were being dropped.

Note that this command applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol and you have configured the device to permit unknown message types, the message is forwarded without processing.

Related
Documentation
- Understanding the MGCP ALG on page 183
- MGCP ALG Configuration Overview on page 189
- Example: Allowing Unknown MGCP ALG Message Types on page 214

Example: Allowing Unknown MGCP ALG Message Types

This example shows how to configure the MGCP ALG to allow unknown MGCP message types in both NAT mode and route mode.

- Requirements on page 215
- Overview on page 215
- Configuration on page 215
- Verification on page 215

Requirements

Before you begin, determine whether to accommodate new and unknown MGCP message types for the device. See "Understanding MGCP ALG Unknown Message Types" on page 214.

Overview

This feature enables you to specify how unidentified MGCP messages are handled by a Juniper Networks device. The default is to drop unknown (unsupported) messages, because unknown messages can compromise security. However, in a secure test or production environment, this command can be useful for resolving interoperability issues with disparate vendor equipment.

Configuration

GUI Step-by-Step Procedure

To configure the MGCP ALG to allow unknown message types:

1. Select **Configure>Security>ALG**.

2. Select the **MGCP** tab.

3. Select the **Enable Permit NAT applied** check box.

4. Select the **Enable Permit routed** check box.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure the MGCP ALG to allow unknown message types:

1. Allow unknown message types to pass if the session is in either NAT mode or in route mode.

   [edit]
   user@host# **set security alg mgcp application-screen unknown-message permit-nat-applied permit-routed**

2. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg mgcp** command.

Related Documentation

- Understanding MGCP ALG Unknown Message Types on page 214

- MGCP ALG Configuration Overview on page 189

Configuring the SCCP ALG

Understanding SCCP ALGs

Supported Platforms   SRX Series, vSRX

Skinny Client Control Protocol (SCCP) is a Cisco proprietary protocol for call signaling. Skinny is based on a call-agent-based call-control architecture. The control protocol uses binary-coded frames encoded on TCP frames sent to well-known TCP port number destinations to set up and tear down RTP media sessions.

The SCCP protocol, in the same way as other call control protocols, negotiates media endpoint parameters—specifically the Real-Time Transport Protocol (RTP) port number and the IP address of media termination—by embedding information in the control packets. The SCCP Application Layer Gateway (ALG) parses these control packets and facilitates media and control packets to flow through the system.

The SCCP ALG also implements rate limiting of calls and helps protect critical resources from overloading and denial-of-service (DoS) attacks.

The following functions are implemented by the SCCP ALG in Junos OS:

- Validation of SCCP protocol data units
- Translation of embedded IP address and port numbers

- Allocation of firewall resources (pinholes and gates) to pass media

- Aging out idle calls

- Configuration API for SCCP ALG parameters

- Operational mode API for displaying counters, status and statistics

In the SCCP architecture, a proxy, known as the Call Manager, does most of the processing. IP phones, also called End Stations, run the SCCP 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 SCCP client, through the Call Manager, to another SCCP client.

- Seamless failover—Switches over all calls in process to the standby firewall during failure of the primary.

- Voice-over-IP (VoIP) signaling payload inspection—Fully inspects the payload of incoming VoIP signaling packets. Any malformed packet attack is blocked by the ALG.

- SCCP signaling payload inspection—Fully inspects the payload of incoming SCCP signaling packets. 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.

This topic includes the following sections:

SCCP Security

The SCCP ALG includes the following security features:

- Stateful inspection of SCCP control messages over TCP and validation of the message format, and message validity for the current call state. Invalid messages are dropped.

- Security policy enforcement between Cisco IP phones and Cisco Call Manager.

- Protect against call flooding by rate limiting the number of calls processed by the ALG.

- Seamless failover of calls, including the ones in progress in case of device failure in a clustered deployment.

SCCP Components

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

- SCCP Client on page 219
- Call Manager on page 219
- Cluster on page 219

SCCP Client

The SCCP client runs on an IP phone, also called an *End Station*, which uses SCCP for signaling and for making calls. For an SCCP 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 implements SCCP call control server software and has 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 detects 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 detects 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 H.323.

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 processes:

Client Initialization

To initialize, the SCCP client needs to determine 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 called sep*macaddr*.cnf. If the TFTP name is not given, the client uses the default filename in the IP phone. The client then downloads the .cnf (xml) configuration file 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 device allows this.

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 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 through RTP/UDP/IP.

SCCP Version

Starting in Junos OS Release 12.1X46-D10, the SCCP ALG supports SCCP versions 16, 17, and 20 and several SCCP messages have been updated with a new format. Cisco Call Manager (CM) version 7 uses SCCP version 20.

SCCP Control Messages and RTP Flow

shows the SCCP control messages used to set up and tear down a simple call between Phone 1 and Phone 2. 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 17: Call Setup and Teardown
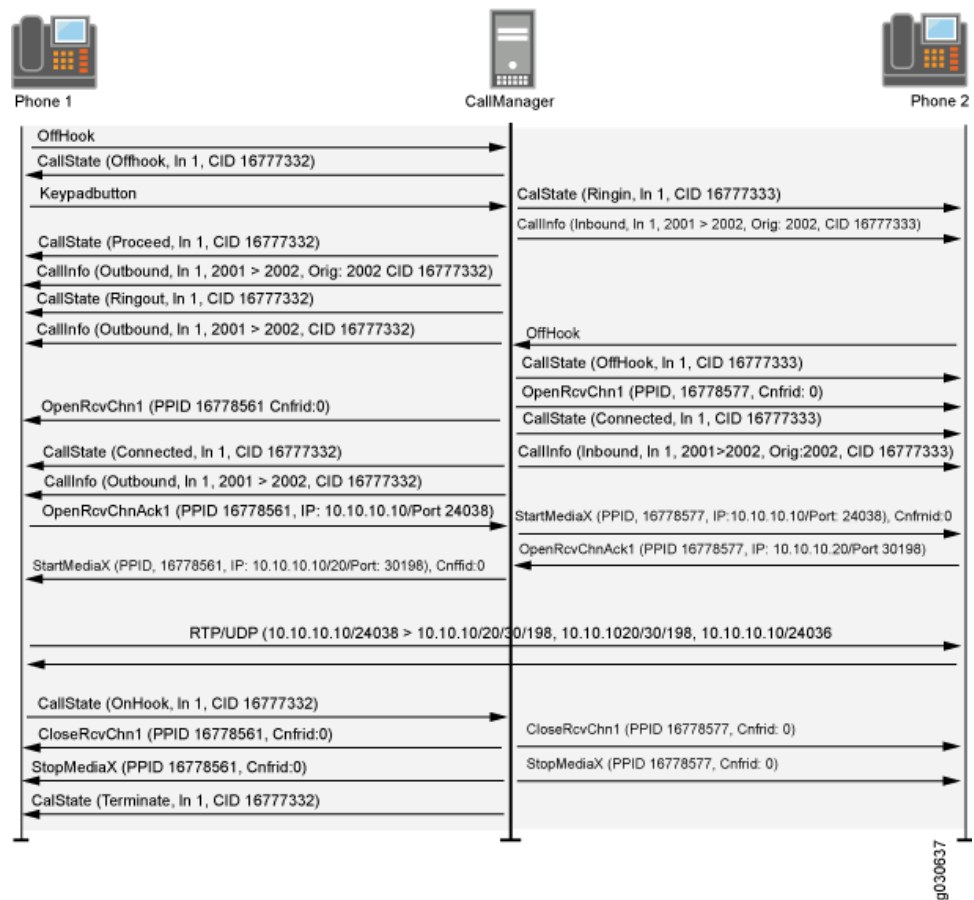
SCCP Messages

, , , and list the SCCP call message IDs in the four intervals allowed by the device.

Table 8: Station to Call Manager Messages

#define STATION_REGISTER_MESSAGE	0x00000001

Table 8: Station to Call Manager Messages *(continued)*

#define STATION_IP_PORT_MESSAGE	0x00000002
#define STATION_ALARM_MESSAGE	0x00000020
#define STATION_OPEN_RECEIVE_CHANNEL_ACK	0x00000022

Table 9: Call Manager to Station Messages

#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 10: Call Manager 4.0 Messages and Post Sccp 6.2

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

Table 11: Call Manager to Station

#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

- The limitations for SCCP ALGs are as follows:

  - The SCCP is a Cisco proprietary protocol. So, any changes to the protocol by Cisco cause the SCCP ALG implementation to break. However, workarounds are provided to bypass strict decoding and allow any protocol changes to be handled gracefully.

  - Any changes to the policies will drop the sessions and impact already established SCCP calls.

- The SCCP ALG opens pinholes that are collapsed during traffic or media inactivity. This means that during a temporary loss of connectivity, media sessions are not reestablished.

- Call Manager (CM) version 6.x and later does not support TCP probe packets in chassis cluster mode. As a result, the existing SCCP sessions will break when there is a failover. You can still create new SCCP sessions during failover.

Related Documentation
- ALG Overview on page 3
- SCCP ALG Configuration Overview on page 223
- Example: Configuring the SCCP ALG Call Manager or TFTP Server in the Private Zone on page 223

SCCP ALG Configuration Overview

The Skinny Client Control Protocol Application Layer Gateway (SCCP ALG) is enabled by default on the device—no action is required to enable it. However, you might choose to fine-tune SCCP ALG operations by using the following instructions:

1. Conserve network resources and maximize throughput. For instructions, see "Example: Setting SCCP ALG Inactive Media Timeouts" on page 233.

2. Enable unknown messages to pass when the session is in Network Address Translation (NAT) mode and route mode. For instructions, see "Example: Allowing Unknown SCCP ALG Message Types" on page 235.

3. Protect the SCCP clients from denial-of-service (DoS) flood attacks. For instructions, see "Example: Configuring SCCP ALG DoS Attack Protection" on page 236.

Related Documentation
- Understanding SCCP ALGs on page 217
- Example: Configuring the SCCP ALG Call Manager or TFTP Server in the Private Zone on page 223
- Verifying SCCP ALG Configurations on page 237

Example: Configuring the SCCP ALG Call Manager or TFTP Server in the Private Zone

This example shows how to configure static NAT on the outgoing interface of a Juniper Networks device to allow callers in a public zone to register with an SCCP ALG Call Manager or a TFTP server located in a private zone.

- Requirements on page 224
- Overview on page 224
- Configuration on page 225
- Verification on page 230

Requirements

Before you begin, understand NAT support with SCCP ALG. See "Understanding SCCP ALGs" on page 217.

Overview

In this example (see Figure 18 on page 225), a single device is serving as a Call Manager or a TFTP server. The Call Manager or TFTP server and phone1 are attached to the private zone, and phone2 is attached to the public zone. You configure a static NAT rule set for the Call Manager or TFTP server so that when phone2 boots up it contacts the TFTP server and obtains the IP address of the Call Manager. You then create a policy called in-pol to allow SCCP traffic from the public to the private zone and a policy called out-pol to allow phone1 to call out.

> **NOTE:** We recommend that you change the IP address of the Call Manager, which resides in the TFTP server configuration file (**sep <mac_addr>.cnf**), to the NAT IP address of the Call Manager.

Topology

shows call manager or TFTP server in the private zone.

Figure 18: Call Manager or TFTP Server in the Private Zone
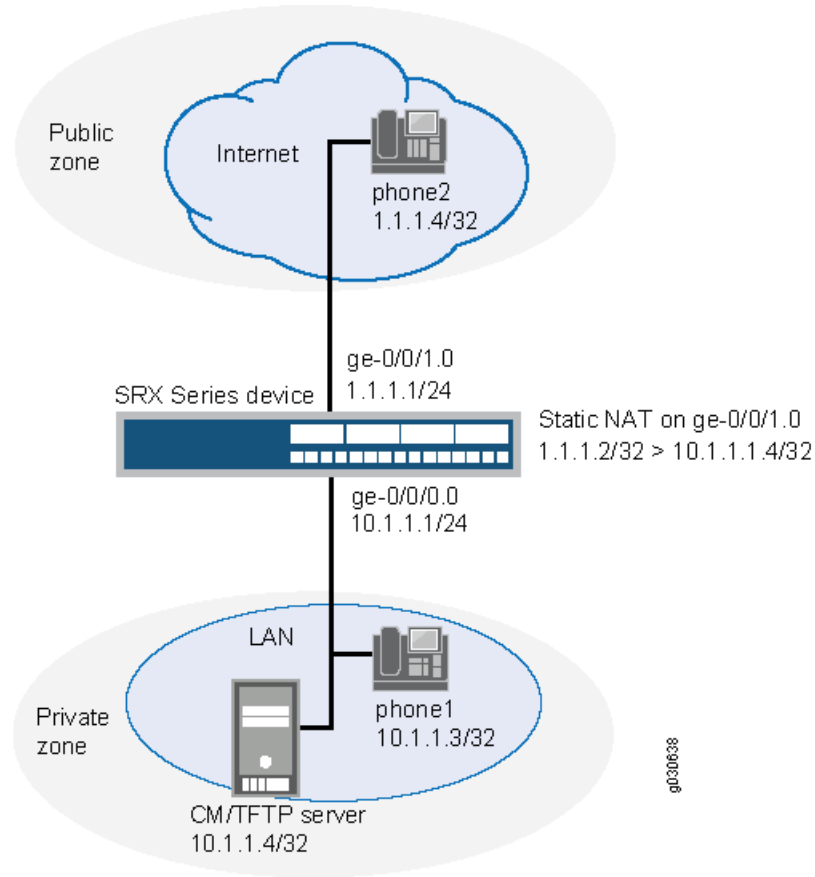
In this example, you configure NAT as follows:

- Create a static NAT rule set called to-proxy with a rule called phone2 to match packets from the public zone with the destination address 1.1.1.2/32. For matching packets, the destination IP address is translated to the private address 10.1.1.4/32.

- Configure proxy ARP for the address 1.1.1.2/32 on interface ge-0/0/1.0. This allows the system to respond to ARP requests received on the interface for these addresses.

- Configure a second rule set called phones with a rule called phone1 to enable interface NAT for communication from phone1 to phone2.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public interfaces ge-0/0/1.0
set security address-book book1 address phone1 10.1.1.3/32
set security address-book book1 address cm-tftp_server 10.1.1.4/32
set security address-book book1 attach zone private
set security address-book book2 address phone2 1.1.1.4/32
set security address-book book2 attach zone public
set security nat source rule-set phones from zone private
set security nat source rule-set phones to zone public
set security nat source rule-set phones rule phone1 match source-address 10.1.1.3/32
set security nat source rule-set phones rule phone1 then source-nat interface
set security nat static rule-set to-proxy from zone public
set security nat static rule-set to-proxy rule phone2 match destination-address 1.1.1.2/32
set security nat static rule-set to-proxy rule phone2 then static-nat prefix 10.1.1.4/32
set security nat proxy-arp interface ge-0/0/1.0 address 1.1.1.2/32
set security policies from-zone public to-zone private policy in-pol match source-address
    phone2
set security policies from-zone public to-zone private policy in-pol match
    destination-address cm-tftp_server
set security policies from-zone public to-zone private policy in-pol match
    destination-address phone1
set security policies from-zone public to-zone private policy in-pol match application
    junos-sccp
set security policies from-zone public to-zone private policy in-pol then permit
set security policies from-zone private to-zone public policy out-pol match source-address
    any
set security policies from-zone private to-zone public policy out-pol match
    destination-address phone2
set security policies from-zone private to-zone public policy out-pol match application
    junos-sccp
set security policies from-zone private to-zone public policy out-pol then permit
set security policies from-zone private to-zone private policy tftp-pol match
    source-address any
set security policies from-zone private to-zone private policy tftp-pol match
    destination-address any
set security policies from-zone private to-zone private policy tftp-pol match application
    junos-tftp
set security policies from-zone private to-zone private policy tftp-pol then permit

Step-by-Step Procedure   The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure NAT for an SCCP ALG Call Manager or a TFTP server located in a private zone:

1.   Configure interfaces.

     [edit]
     user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
     user@host# set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/24

2.   Create security zones.

```
[edit security zones]
user@host# set security-zone private interfaces ge-0/0/0.0
user@host# set security-zone public interfaces ge-0/0/1.0
```

3. Create address books and attach zones to them.

```
[edit security address-book book1]
user@host# set address phone1 10.1.1.3/32
user@host# set address cm-tftp_server 10.1.1.4/32
user@host# set attach zone private

[edits security address-book book2]
user@host# set address phone2 1.1.1.4/32
user@host# set attach zone public
```

4. Create a rule set for static NAT and assign a rule to it.

```
[edit security nat static rule-set to-proxy]
user@host# set from zone public
user@host# set rule phone2 match destination-address 1.1.1.2/32
user@host# set rule phone2 then static-nat prefix 10.1.1.4/32
```

5. Configure proxy ARP.

```
[edit security nat]
user@host# set proxy-arp interface ge-0/0/1.0 address 1.1.1.2/32
```

6. Configure interface NAT for communication from phone1 to phone2.

```
[edit security nat source rule-set phones]
user@host# set from zone private
user@host# set to zone public
user@host# set rule phone1 match source-address 10.1.1.3/32
user@host# set rule phone1 then source-nat interface
```

7. Configure a policy to allow traffic from the public zone to the private zone.

```
[edit security policies from-zone public to-zone private policy in-pol]
user@host# set match source-address phone2
user@host# set match destination-address cm-tftp_server
user@host# set match destination-address phone1
user@host# set match application junos-sccp
user@host# set then permit
```

8. Configure a policy to allow traffic from the private zone to the public zone.

```
[edit security policies from-zone private to-zone public policy out-pol]
user@host# set match source-address any
user@host# set match destination-address phone2
user@host# set match application junos-sccp
user@host# set then permit
```

9. Configure a policy to allow traffic from phone1 to the CM/TFTP server.

```
[edit security policies from-zone private to-zone private policy tftp-pol]
user@host# set match source-address any
user@host# set match destination-address any
user@host# set match application junos-tftp
user@host# set then permit
```

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security address-book**, **show security nat**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
    ge-0/0/1 {
      unit 0 {
        family inet {
          address 1.1.1.1/24;
        }
      }
    }
[edit]
user@host# show security zones
security-zone private {
  interfaces {
    ge-0/0/0.0;
  }
}
  security-zone public {
    interfaces {
      ge-0/0/1.0;
    }
  }
[edit]
user@host# show security address-book
book1 {
  address phone1 10.1.1.3/32;
  address cm-tftp_server 10.1.1.4/32;
  attach {
    zone private;
  }
}
  book2 {
    address phone2 1.1.1.4/32;
    attach {
      zone public;
    }
  }
[edit]
user@host# show security nat
source {
  rule-set phones {
    from zone private;
    to zone public;
    rule phone1 {
```

```
            match {
              source-address 10.1.1.3/32;
            }
            then {
              source-nat {
                interface;
              }
            }
          }
        }
      }
    }
    static {
      rule-set to-proxy {
        from zone public;
        rule phone2 {
          match {
            destination-address 1.1.1.2/32;
          }
          then {
            static-nat prefix 10.1.1.4/32;
          }
        }
      }
    }
    proxy-arp {
      interface ge-0/0/1.0 {
        address {
          1.1.1.2/32;
        }
      }
    }
  }
[edit]
user@host# show security policies
from-zone public to-zone private {
  policy in-pol {
    match {
      source-address phone2;
      destination-address cm-tftp_server;
      destination-address phone1;
      application junos-sccp;
    }
    then {
      permit;
    }
  }
}
  from-zone private to-zone public {
    policy out-pol {
      match {
        source-address any;
        destination-address phone2;
        application junos-sccp;
      }
      then {
        permit;
      }
```

```
            }
          }
          from-zone private to-zone private {
            policy tftp-pol {
              match {
                source-address any;
                destination-address any;
                application junos-tftp;
              }
              then {
                permit;
              }
            }
          }
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Source NAT Rule Usage on page 230
- Verifying Static NAT Configuration on page 231
- Verifying Static NAT Configuration on page 231
- Verifying SCCP ALG on page 232
- Verifying the Security Polices of SIP ALG on page 232

Verifying Source NAT Rule Usage

Purpose   Verify that there is traffic matching the source NAT rule.

Action   From operational mode, enter the **show security nat source rule all** command.

```
    user@host> show security nat source rule all

Total rules: 2
Total referenced IPv4/IPv6 ip-prefixes: 3/0
source NAT rule: r1                    Rule-set: rs1
  Rule-Id                    : 1
  Rule position              : 1
  From interface             : ge-0/0/5.0
                             : ge-0/0/6.0
  To interface               : ge-0/0/2.0
  Match
    Source addresses         : 30.0.0.0        - 30.0.0.255
                               40.0.0.0        - 40.0.0.255
    Destination port         : 0               - 0
  Action                       : interface
    Persistent NAT type        : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout         : 0
    Max session number         : 0
  Translation hits           : 0
source NAT rule: phone1                Rule-set: phones
  Rule-Id                    : 3
  Rule position              : 2
```

```
            From zone                  : private
            To zone                    : public
            Match
              Source addresses         : 10.1.1.3        - 10.1.1.3
              Destination port         : 0               - 0
            Action                        : interface
              Persistent NAT type         : N/A
              Persistent NAT mapping type : address-port-mapping
              Inactivity timeout          : 0
              Max session number          : 0
            Translation hits           : 0
```

Meaning   The **Translation hits** field shows that, there is no traffic matching the source NAT rule.

Verifying Static NAT Configuration

Purpose   Verify that there is traffic matching the static NAT rule set.

Action   From operational mode, enter the **show security nat static rule phone1** command.

> user@host> **show security nat static rule phone1**

```
source NAT rule: phone1                 Rule-set: phones
  Rule-Id                  : 3
  Rule position            : 2
  From zone                : private
  To zone                  : public
  Match
    Source addresses       : 10.1.1.3        - 10.1.1.3
    Destination port       : 0               - 0
  Action                      : interface
    Persistent NAT type         : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout          : 0
    Max session number          : 0
  Translation hits         : 0
```

Meaning   The **Translation hits** field shows that, there is no traffic matching the source NAT rule set.

Verifying Static NAT Configuration

Purpose   Verify that there is traffic matching the static NAT rule set.

Action   From operational mode, enter the **show security nat static rule phone2** command.

> user@host> **show security nat static rule phone2**

```
Static NAT rule: phone2                   Rule-set: to-proxy
  Rule-Id                  : 1
  Rule position            : 1
  From zone                : public
  Destination addresses    : 1.1.1.2
  Host addresses           : 10.1.1.4
  Netmask                  : 32
  Host routing-instance    : N/A
  Translation hits         : 0
```

Meaning The **Translation hits** field shows that, there is no traffic matching the source NAT rule set.

Verifying SCCP ALG

Purpose Verify that the SCCP ALG is enabled.

Action From operational mode, enter the **show security alg status | match sccp** command.

> user@host> **show security alg status | match sccp**

```
SCCP      : Enabled
```

Meaning The output shows the SCCP ALG status as follows:

- Enabled—Shows the SCCP ALG is enabled.

- Disabled—Shows the SCCP ALG is disabled.

Verifying the Security Polices of SIP ALG

Purpose Verify that the static NAT between public zone and private zone is set.

Action From operational mode, enter the **show security policies** command.

> user@host> **show security policies**

```
from-zone private to-zone public {
      policy out-pol {
       match {
           source-address any;
           destination-address phone2;
           application junos-sccp;
       }
       then {
           permit;
       }
    }
}
from-zone public to-zone private {
      policy in-pol {
       match {
           source-address phone2;
           destination-address [ cm-tftp_server phone1 ];
           application junos-sccp;
       }
       then {
           permit;
       }
    }
}
from-zone private to-zone private {
    policy tftp-pol {
        match {
            source-address any;
            destination-address any;
            application junos-tftp;
        }
        then {
```

```
                                permit;
                            }
                        }
                    }
```

Meaning   The sample output shows that the static NAT between public zone and private zone is set.

Related   • SCCP ALG Configuration Overview on page 223
Documentation

Understanding SCCP ALG Inactive Media Timeouts

The inactive media timeout feature helps you to conserve network resources and maximize throughput.

This parameter indicates the maximum length of time (in seconds) a call can remain active without any media traffic within a group. Each time a Real-Time Transport Protocol (RTP) or Real-Time Control Protocol (RTCP) packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the gates the Skinny Client Control Protocol (SCCP) opened for media are closed. The default setting is 120 seconds, and the range is from 10 to 2550 seconds. Note that upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.

Related   • Understanding SCCP ALGs on page 217
Documentation
          • SCCP ALG Configuration Overview on page 223

          • Example: Setting SCCP ALG Inactive Media Timeouts on page 233

Example: Setting SCCP ALG Inactive Media Timeouts

This example shows how to set the inactive media timeout value for the SCCP ALG.

• Requirements on page 233

• Overview on page 233

• Configuration on page 234

• Verification on page 234

Requirements

Before you begin, review the parameter used to indicate the maximum length of time (in seconds) a call can remain active without any media traffic within a group. See "Understanding SCCP ALG Inactive Media Timeouts" on page 233.

Overview

Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the gates the SCCP opened for media are closed. This example sets the media inactivity timeout to 90 seconds.

Configuration

**GUI Step-by-Step
Procedure**

To set the inactive media timeout for the SCCP ALG:

1. Select **Configure>Security>ALG**.

2. Select the **SCCP** tab.

3. In the Inactive Media Timeout box, enter **90**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

**Step-by-Step
Procedure**

To set the inactive media timeout for the SCCP ALG:

1. Configure the SCCP ALG inactive media timeout value.

   [edit]
   user@host# **set security alg sccp inactive-media-timeout 90**

2. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg sccp** command.

**Related
Documentation**

- Understanding SCCP ALG Inactive Media Timeouts on page 233

- SCCP ALG Configuration Overview on page 223

- Verifying SCCP ALG Configurations on page 237

Understanding SCCP ALG Unknown Message Types

To accommodate on-going development of the Skinny Client Control Protocol (SCCP), you might want to allow traffic containing new SCCP message types. The unknown SCCP message type feature enables you to configure the device to accept SCCP traffic containing unknown message types in both Network Address Translation (NAT) mode and route mode.

This feature enables you to specify how unidentified SCCP messages are handled by the device. The default is to drop unknown (unsupported) messages. We do not recommend permitting unknown messages because they can compromise security. However, in a secure test or production environment, this command can be useful for resolving interoperability issues with disparate vendor equipment. Permitting unknown SCCP messages can help you get your network operational so that you can later analyze your voice-over-IP (VoIP) traffic to determine why some messages were being dropped.

Note that this command applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as

a supported protocol and you have configured the device to permit unknown message types, the message is forwarded without processing.

<div style="text-align: right">**Related Documentation**</div>

- Understanding SCCP ALGs on page 217
- SCCP ALG Configuration Overview on page 223
- Example: Allowing Unknown SCCP ALG Message Types on page 235

Example: Allowing Unknown SCCP ALG Message Types

This example shows how to configure the SCCP ALG to allow unknown SCCP message types in both NAT mode and route mode.

- Requirements on page 235
- Overview on page 235
- Configuration on page 235
- Verification on page 236

Requirements

Before you begin, determine whether to accommodate new and unknown SCCP message types for the device. See "Understanding SCCP ALG Unknown Message Types" on page 234.

Overview

This feature enables you to specify how unidentified SCCP messages are handled by a Juniper Networks device. The default is to drop unknown (unsupported) messages because unknown messages can compromise security. However, in a secure test or production environment, this command can be useful for resolving interoperability issues with disparate vendor equipment.

Configuration

GUI Step-by-Step Procedure

To configure the SCCP ALG to allow unknown message types:

1. Select **Configure>Security>ALG**.

2. Select the **SCCP** tab.

3. Select the **Enable Permit NAT applied** check box.

4. Select the **Enable Permit routed** check box.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure the SCCP ALG to allow unknown message types:

1. Allow unknown message types to pass if the session is in either NAT mode or in route mode.

   [edit]

user@host# set security alg sccp application-screen unknown-message
   permit-nat-applied permit-routed

2.   If you are done configuring the device, commit the configuration.

[edit]
user@host# commit

Verification

To verify the configuration is working properly, enter the **show security alg sccp** command.

Related
Documentation

- Understanding SCCP ALG Unknown Message Types on page 234
- SCCP ALG Configuration Overview on page 223
- Verifying SCCP ALG Configurations on page 237

Understanding SCCP ALG DoS Attack Protection

You can protect Skinny Client Control Protocol Application Layer Gateway (SCCP ALG) clients from denial-of-service (DoS) flood attacks by limiting the number of calls they attempt to process.

When you configure SCCP call flood protection, the SCCP ALG drops any calls exceeding the threshold you set. The range is 2 to 1000 calls per second per client, the default is 20.

Related
Documentation

- Understanding SCCP ALGs on page 217
- SCCP ALG Configuration Overview on page 223
- Example: Configuring SCCP ALG DoS Attack Protection on page 236

Example: Configuring SCCP ALG DoS Attack Protection

This example shows how to configure connection flood protection for the SCCP ALG.

- Requirements on page 236
- Overview on page 236
- Configuration on page 237
- Verification on page 237

Requirements

Before you begin, determine whether to protect the SCCP media gateway from DoS flood attacks. See "Understanding SCCP ALG DoS Attack Protection" on page 236.

Overview

In this example, the device is configured to drop any calls exceeding 500 per second per client.

Configuration

GUI Step-by-Step Procedure

To configure call flood protection for the SCCP ALG:

1. Select **Configure>Security>ALG**.

2. Select the **SCCP** tab.

3. In the Call flood threshold box, type **500**.

4. Click **OK** to check your configuration and save it as a candidate configuration.

5. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure call flood protection for the SCCP ALG:

1. Configure the DoS attack protection:

   [edit]
   user@host# **set security alg sccp application-screen call-flood threshold 500**

2. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg sccp** command.

Related Documentation

- Understanding SCCP ALG DoS Attack Protection on page 236
- SCCP ALG Configuration Overview on page 223
- Verifying SCCP ALG Configurations on page 237

Verifying SCCP ALG Configurations

Supported Platforms SRX Series, vSRX

Verifying SCCP ALG

Supported Platforms SRX Series, vSRX

Purpose Display SCCP verification options.

Action From the CLI, enter the **show security alg sccp** command.

user@host> **show security alg sccp ?**

```
Possible completions:
  calls                   Show SCCP calls
  counters                Show SCCP counters
```

Meaning   The output shows a list of all SCCP verification parameters. Verify the following information:

- All SCCP calls

- Counters for all SCCP calls

Verifying SCCP ALG Calls

Supported Platforms   SRX Series, vSRX

Purpose   Display a list of all SCCP calls

Action   From the CLI, enter the **show security alg sccp calls** command.

```
user@host> show security alg sccp calls
Possible completions:
  calls                   Show SCCP calls
  counters                Show SCCP counters
  endpoints               Show SCCP endpoints
```

Meaning   The output shows a list of all SCCP verification parameters. Verify the following information:

- All SCCP calls

- Counters for all SCCP c alls

- Information about all SCCP endpoints

Verifying SCCP ALG Call Details

Supported Platforms   SRX Series, vSRX

Purpose   Display details about all SCCP calls.

Action   From the CLI, enter the **show security alg sccp calls detail** command.

```
user@host> show security alg sccp calls detail
Client IP address: 11.0.102.91
  Client zone: 7
  Call Manager IP: 13.0.99.226
  Conference ID: 16789504
  Resource manager group: 2048
  SCCP channel information:
    Media transmit channel address (IP address/Port): 0.0.0.0:0
    Media transmit channel translated address (IP address/Port): 0.0.0.0:0
    Media transmit channel pass-through party ID (PPID): 0
    Media transmit channel resource ID: 0
    Media receive channel address (IP address/Port): 11.0.102.91:20060
    Media receive channel translated address (IP address/Port): 25.0.0.1:1032
    Media receive channel pass-through party ID (PPID): 16934451
    Media receive channel resource ID: 8185
```

```
        Multimedia transmit channel address (IP address/Port): 0.0.0.0:0
        Multimedia transmit channel translated address (IP address/Port): 0.0.0.0:0
        Multimedia transmit channel pass-through party ID (PPID): 0
        Multimedia transmit channel resource ID: 0
        Multimedia receive channel address (IP address/Port): 0.0.0.0:0
        Multimedia receive channel translated address (IP address/Port): 0.0.0.0:0
        Multimedia receive channel pass-through party ID (PPID): 0
        Multimedia receive channel resource ID: 0
Total number of calls = 1
```

Meaning   The output shows a list of all SCCP verification parameters. Verify the following
           information:

- Client zone

- Call Manager IP address: 13.0.99.226

- Conference ID

- Resource manager group

- SCCP channel information

- Total number of calls

Verifying SCCP ALG Counters

Supported Platforms   SRX Series, vSRX

Purpose   Display a list of all SCCP counters

Action   From the J-Web interface, select **Monitor>ALGs>SCCP>Counters**. Alternatively, from the
          CLI, enter the **show security alg sccp counters** command.

```
user@host> show security alg sccp ounters
SCCP call statistics:
  Active client sessions      : 0
  Active calls                : 0
  Total calls                 : 0
  Packets received            : 0
  PDUs processed              : 0
  Current call rate           : 0
Error counters:
  Packets dropped                     : 0
  Decode errors                       : 0
  Protocol errors                     : 0
  Address translation errors          : 0
  Policy lookup errors                : 0
  Unknown PDUs                        : 0
  Maximum calls exceeded              : 0
  Maximum call rate exceeded          : 0
  Initialization errors               : 0
  Internal errors                     : 0
  Nonspecific error                   : 0
  No active calls to delete           : 0
  No active client sessions to delete : 0
  Session cookie create errors        : 0
  Invalid NAT cookie detected         : 0
```

Meaning The output shows a list of all SCCP verification parameters. Verify the following information:

- SCCP call statistics

- Error counters

Related Documentation
- SCCP ALG Configuration Overview on page 223
- Example: Configuring the SCCP ALG Call Manager or TFTP Server in the Private Zone on page 223

Configuring the SIP ALG

Understanding the SIP ALG

Supported Platforms   SRX Series, vSRX

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.

Junos OS supports SIP as a service, allowing and denying it based on a policy that you configure. SIP is a predefined service in Junos OS and uses port 5060 as the destination port.

One of SIP's 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, signal a call establishment, provide failure indication, and provide methods for endpoint registration.

Session-description information is included in INVITE and 200-OK messages or 200-OK and ACK messages and indicates the multimedia type of the session; for example, whether it is voice or video. Although SIP can use different description protocols to describe the session, the Juniper Networks SIP Application Layer Gateway (ALG) supports only the 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).

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:

- user agent client (UAC), which sends SIP requests on behalf of the user
- user agent server (UAS), which listens to the responses and notifies the user when they arrive

UAC and UAS are defined in relation to the role a particular agent is playing in a negotiation.

Examples of UAs are SIP proxy servers and phones.

This topic contains the following sections:

SIP ALG Operation

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 UDP or TCP. The media stream carries the data (audio data, for example) using transport protocols.

TCP support over SIP ALG reduces traffic to the server by eliminating the need to reregister or refresh the server frequently.

By default, Junos OS supports SIP signaling messages on port 5060. You can configure the port by creating a policy that permits SIP service, and the software 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 insecure to create a static policy to control media traffic. In this case, the device invokes the SIP ALG. The device transport ports used for the media sessions are not known in advance; however, the ports used for the SIP negotiation are well-known (or predefined). The ALG registers interest in packets from the control session, which it can easily distinguish from the other packets, and inspects the negotiation for the transport information used for the media session (both IP addresses and ports).

> **NOTE:** The SIP ALG creates a pinhole when it determines a matching IP, port, transport address, and protocol, which are identified with whatever information is known at the time when the pinhole is opened.

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. You can allow SIP transactions to traverse the Juniper Networks firewall by creating a static policy that permits SIP service. If the policy is configured to inspect SIP traffic (or, more appropriately, if the policy sends some traffic to the SIP ALG for inspection), the allowed actions are to permit the traffic (in which case the appropriate pinholes are opened) or to deny the traffic.

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 device.

> **NOTE:** When the device is performing NAT, the transport addresses that the UAs employ are incorrect. The SIP ALG modifies the transport addresses based on the translated ports and addresses allocated by the device translating network addresses. When SDP is encrypted, the device cannot either extract or modify the contents of the message and therefore cannot correct the transport addresses. To provide a workaround, the STUN protocol has been deployed (requiring NAT devices to do some form of cone-NAT), which allows the clients to determine the translated addresses and use those newly discovered addresses in the SDP messages.

NEC SIP products are conditionally supported.

SDP Session Descriptions

An SDP session description is a well-defined format for conveying sufficient information to discover and participate in a multimedia session. A session is described by a series of attribute/value pairs, one per line. The attribute names are single characters, followed by =, and a value. Optional values are specified with =* Values are either an ASCII string, or a sequence of specific types separated by spaces. Attribute names are only unique within the associated syntactic construct, such as within the session, time, or media only.

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.

- **c=** for connection information

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

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

  Currently, Junos OS supports only "IN" (for Internet) as the network type, "IPv4" and "IPv6" as the address type, and a unicast IP address or domain name as the destination (connection) IP address.

  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 appears in this format:

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

  Currently, Junos OS supports "RTP" as the Application Layer transport protocol. The port number indicates the destination port of the media stream (the origin is allocated by the remote UA). The format list (fmt list) provides information on the Application Layer protocol that the media uses.

  The software opens ports only for RTP and Real-Time Control Protocol (RTCP). Every RTP session has a corresponding 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.

Pinhole Creation

Each pinhole (one for RTP traffic and the other for 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 the 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 looks for a c= field containing an IP address in the media level. If there is such a field, the parser extracts that IP address, and the SIP ALG uses that address 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 that IP address 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 device drops the packet and logs the event.

The SIP ALG also opens pinholes for signal traffic. These signal pinholes are useful after the previous signal session timeout, and they are also useful for the signal traffic sent to a third-party address that does not match with the previous signal session. The SIP ALG signal pinholes never age out, unlike RTP or RTCP pinholes, where only the destination IP and destination port are specified.

The SIP ALG opens signal pinholes for following headers, if needed:

- VIA

- CONTACT

- ROUTE

- RECORD-ROUTE

The SIP ALG needs the following information to create a pinhole. This information either comes from the SDP session description or from the SIP headers (as listed above).

- Protocol—UDP or TCP.

- Source IP—Unknown.

- Source port—Unknown.

- Destination IP—The parser extracts the destination IP address from the c= field at 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.

  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 device has a policy that permits SIP, thus opening port 5060 for SIP signaling messages.

Figure 19: SIP ALG Call Setup
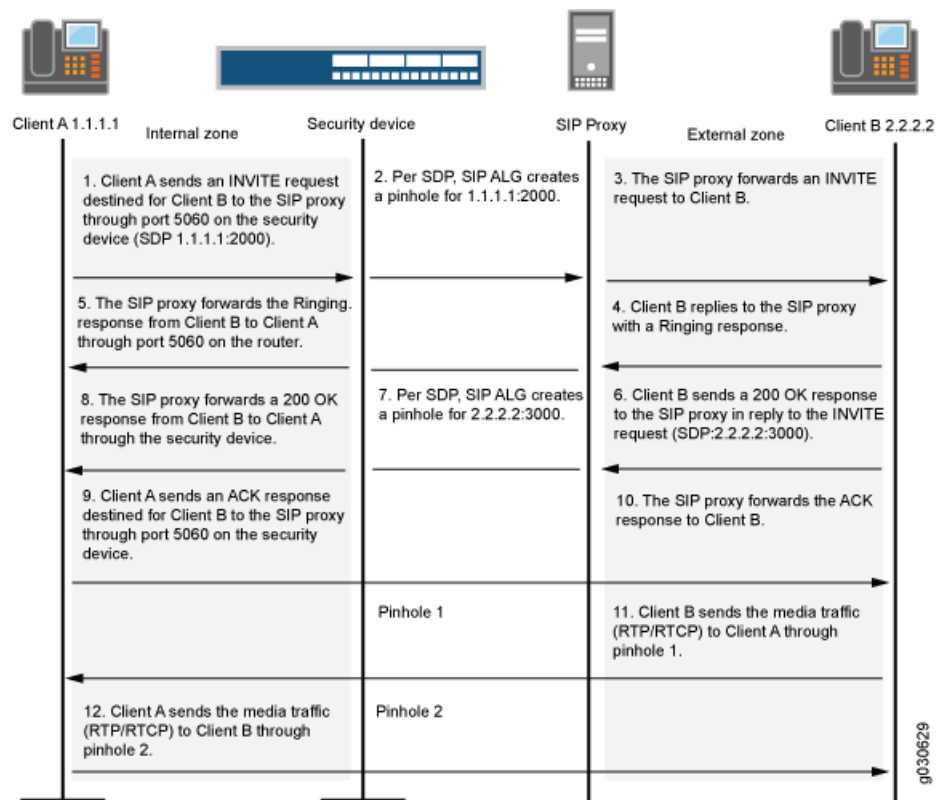
> **NOTE:** The SIP ALG does not create pinholes for RTP and RTCP traffic when the destination IP address is 0.0.0.0, which indicates that the session is on hold. To put a session on hold during a telephone communication, for example, Client A sends Client B a SIP message in which the destination IP address is 0.0.0.0. Doing so indicates to Client B that it should not send any media until further notice. If Client B sends media anyway, the device drops the packets.

Related Documentation

- ALG Overview on page 3
- Understanding SIP ALG Request Methods on page 247
- Understanding the SIP ALG and NAT on page 256
- SIP ALG Configuration Overview on page 248

Understanding IPv6 Support for SIP ALG

Supported Platforms   SRX Series, vSRX

IPv6 is supported on the SIP ALG along with NAT-PT mode and NAT64 address translation.

The SIP ALG processes the IPv6 address in the same way it processes the IPv4 address for updating the payload if NAT is configured and opening pinholes for future traffic.

Special processing occurs for the following formats:

- **IPv6 in SIP URIs**—The SIP URI looks the same as a URI with IPv4 addresses. As in all URIs, an IPv6 address is enclosed in square brackets. The IPv6 address blocks are separated by colons. In many notations, a colon separates the hostname or IP address from the protocol port. To parse the full IPv6 address and separate the port, the address is encapsulated within square brackets

- **IPv6 in SDP**—IPv6 addresses in the Session Description Protocol (SDP) have the IP6 marker.

- The SIP ALG with IPv6 support has the following limitation:

  - When NAT64 with persistent NAT is implemented, the SIP ALG adds the NAT translation to the persistent NAT binding table if NAT is configured on the Address of Record (AOR). Because persistent NAT cannot duplicate the address configured, coexistence of NAT66 and NAT64 configured on the same address is not supported.

    Only one binding is created for the same source IP address.

Related Documentation

- Understanding the SIP ALG on page 241

Understanding SIP ALG Request Methods

Supported Platforms   SRX Series, vSRX

The Session Initiation Protocol (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.

Junos OS 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 can contain the description of the session.

- 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.

- OPTIONS—The User Agent (UA) obtains information about the capabilities of the SIP proxy. A server responds with information about what methods, session description protocols, and message encoding it supports.

- BYE—A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session.

- CANCEL—A user sends 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.

- 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.

- Info—Used to communicate mid-session signaling information along the signaling path for the call.

- Subscribe—Used to request current state and state updates from a remote node.

- Notify—Sent to inform subscribers of changes in state to which the subscriber has a subscription.

- Refer—Used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request.

  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 Application Layer Gateway (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 Network Address Translation (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.

- 1*xx*, 202, 2*xx*, 3*xx*, 4*xx*, 5*xx*, 6*xx* Response Codes—Used to indicate the status of a transaction. Header fields are modified.

Related Documentation

- ALG Overview on page 3
- Understanding the SIP ALG on page 241

SIP ALG Configuration Overview

Supported Platforms   SRX Series

The Session Initiation Protocol Application Layer Gateway (SIP ALG) is disabled by default on high-end devices—it should be enabled using the CLI if required. On other devices, it is enabled by default. To fine-tune SIP ALG operations use the following instructions:

1. Control SIP call activity. For instructions, see "Example: Setting SIP ALG Call Duration and Timeouts" on page 250.

2. Protect the SIP proxy server from denial-of-service (DoS) flood attacks. For instructions, see "Example: Configuring SIP ALG DoS Attack Protection" on page 252.

3. Enable unknown messages to pass when the session is in Network Address Translation (NAT) mode and route mode. For instructions, see "Example: Allowing Unknown SIP ALG Message Types" on page 254.

4. Accommodate proprietary SIP call flows. For instructions, see:

   - Retaining SIP ALG Hold Resources (J-Web Procedure) on page 256

Related
Documentation

Understanding SIP ALG Call Duration and Timeouts

Supported Platforms   SRX Series, vSRX

The call duration and timeout features give you control over Session Initiation Protocol
(SIP) call activity and help you to manage network resources.

Typically a call ends when one of the clients sends a BYE or CANCEL request. The SIP
Application Layer Gateway (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 device.

A call can have one or more voice channels. Each voice channel has two sessions (or two
media streams), one for Real-Time Transport Protocol (RTP) traffic and one for Real-Time
Control Protocol (RTCP) signaling. When managing the sessions, the device considers
the sessions in each voice channel as one group. Timeouts and call duration settings
apply to a group as opposed to each session.

The following parameters govern SIP call activity:

• **inactive-media-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. When
the period of inactivity exceeds this setting, the temporary openings (pinholes) in the
firewall the SIP ALG opened for media are closed. The default setting is 120 seconds,
and the range is 10 through 2550 seconds. Note that upon timeout, resources for media
(sessions and pinholes) are removed and SIP calls on the device will also be terminated
if all the media resources of this call are removed.

• **maximum-call-duration**—This parameter sets the absolute maximum length of a call.
When a call exceeds this parameter setting, the SIP ALG tears down the call and
releases the media sessions. The default setting is 720 minutes, and the range is 3
through 720 minutes.

• **t1-interval**—This parameter specifies the roundtrip time estimate, in seconds, of a
transaction between endpoints. The default is 500 milliseconds. Because many SIP
timers scale with the t1-interval (as described in RFC 3261), when you change the value
of the t1-interval timer, those SIP timers also are adjusted.

• **t4-interval**—This parameter specifies the maximum time a message remains in the
network. The default is 5 seconds and the range is 5 through 10 seconds. Because

many SIP timers scale with the t4-interval (as described in RFC 3261), when you change the value of the t4-interval timer, those SIP timers also are adjusted.

- **c-timeout**—This parameter specifies the INVITE transaction timeout at the proxy, in minutes; the default is 3. Because the SIP ALG is in the middle, instead of using the INVITE transaction timer value B (which is (64 * T1) = 32 seconds), the SIP ALG gets its timer value from the proxy.

Related Documentation

- Understanding the SIP ALG on page 241
- SIP ALG Configuration Overview on page 248
- Example: Setting SIP ALG Call Duration and Timeouts on page 250

Example: Setting SIP ALG Call Duration and Timeouts

Supported Platforms   SRX Series, vSRX

This example shows how to set the call duration and the media inactivity timeout.

Requirements

Before you begin, review the call duration and timeout features used to control SIP call activity. See "Understanding SIP ALG Call Duration and Timeouts" on page 249.

Overview

The call duration and inactivity media timeout features help you to conserve network resources and maximize throughput.

The **maximum-call-duration** parameter sets the maximum allowable length of time a call can be active. When the duration is exceeded, the SIP ALG tears down the call and releases the media sessions. The default setting is 720 minutes, and the range is 3 through 720 minutes. This setting also frees up bandwidth in cases where calls fail to properly terminate.

The **inactive-media-timeout** parameter indicates the maximum length of time (in seconds) a call can remain active without any media (RTP or RTPC) traffic within a group. Each time an RTP or RTCP packet occurs within a call, this timeout resets. When the period of inactivity exceeds this setting, the SIP ALG temporary openings (pinholes) for media in the firewall are closed. The default setting is 120 seconds, and the range is 10 through 2550 seconds. Upon timeout, while resources for media (sessions and pinholes) are removed, the call is not terminated.

In this example, the call duration is set to 36000 seconds and the media inactivity timeout is set to 90 seconds.

Configuration

GUI Step-by-Step Procedure

To set the SIP ALG call duration and the media inactivity timeout:

1. Select **Configure** >**Security** >**ALG**.

2. Select the **SIP** tab.

3. In the Maximum call duration field, type **600**.

4. In the Inactive media timeout field, enter **90**.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options** >**Commit**.

Step-by-Step Procedure

To set the SIP ALG call duration and the media inactivity timeout:

1. Configure the SIP ALG call duration.

   [edit]
   user@host# **set security alg sip maximum-call-duration 600**

2. Configure the SIP ALG inactivity media timeout.

   [edit]
   user@host# **set security alg sip inactive-media-timeout 90**

3. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg sip** command.

Related Documentation

- SIP ALG Configuration Overview on page 248
- Verifying SIP ALG Configurations on page 303

Understanding SIP ALG DoS Attack Protection

Supported Platforms   SRX Series, vSRX

The ability of the Session Initiation Protocol (SIP) proxy server to process calls can be impacted by repeat SIP INVITE requests—requests that it initially denied. The denial-of-service (DoS) protection feature enables you to configure the device to monitor INVITE requests and proxy server replies to them. If a reply contains a 3*xx, 4xx*, or 5*xx* response code other than 401, 407, 487, and 488 that are not real failure responses, then the request should not be blocked. See "Classes of SIP Responses" on page 264. The ALG stores the source IP address of the request and the IP address of the proxy server in a table. Subsequently, the 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 configure the device to monitor and deny repeat INVITE

requests to all proxy servers, or you can protect a specific proxy server by specifying the destination IP address. SIP attack protection is configured globally.

> **NOTE:** IPv6 is supported on the SIP ALG along with Network Address Translation Protocol Translation (NAT-PT) mode and NAT64 address translation.
>
> The type of the <destination-ip-address> is changed from IPv4 address to IP prefix to support all kinds of IP addresses, and correspondingly a prefix is supported to allow multiple IP addresses.

Related Documentation

- Understanding the SIP ALG on page 241
- SIP ALG Configuration Overview on page 248
- Example: Configuring SIP ALG DoS Attack Protection on page 252

Example: Configuring SIP ALG DoS Attack Protection

Supported Platforms SRX Series, vSRX

This example shows how to configure the DoS attack protection feature.

Requirements

Before you begin, review the DoS attack protection feature used to control SIP call activity. See "Understanding SIP ALG DoS Attack Protection" on page 251.

Overview

The ability of the SIP proxy server to process calls can be impacted by repeat SIP INVITE requests—requests that the server initially denied. The DoS protection feature enables you to configure the device to monitor INVITE requests and proxy server replies to them.

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

Configuration

GUI Step-by-Step Procedure

To configure SIP ALG DoS attack protection:

1. Select **Configure>Security>ALG**.

2. Select the **SIP** tab.

3. In the Enable attack protection area, click the **Selected servers** option.

4. In the Destination IP box, enter **1.1.1.3** and click **Add**.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To configure SIP ALG DoS attack protection:

1. Configure the device to protect a single SIP proxy server.

   [edit]
   user@host# **set security alg sip application-screen protect deny destination-ip 1.1.1.3**

   > *i* NOTE: IPv6 is supported on the SIP ALG along with Network Address Translation Protocol Translation (NAT-PT) mode and NAT64 address translation.
   >
   > The type of the <destination-ip-address> is changed from IPv4 address to IP prefix to support all kinds of IP addresses, and correspondingly a prefix is supported to allow multiple IP addresses.

2. Configure the device for the deny timeout period.

   [edit]
   user@host# **set security alg sip application-screen protect deny timeout 5**

3. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg sip** command.

Related Documentation

Understanding SIP ALG Unknown Message Types

Supported Platforms   SRX Series, vSRX

This feature enables you to specify how unidentified Session Initiation Protocol (SIP) messages are handled by the device. The default is to drop unknown (unsupported) messages.

We do not recommend permitting unknown messages because they can compromise security. However, in a secure test or production environment, this command can be useful for resolving interoperability issues with disparate vendor equipment. Permitting unknown SIP messages can help you get your network operational so you can later analyze your voice-over-IP (VoIP) traffic to determine why some messages were being dropped. The unknown SIP message type feature enables you to configure the device

to accept SIP traffic containing unknown message types in both Network Address Translation (NAT) mode and route mode.

> **NOTE:** This option applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol and you have configured the device to permit unknown message types, the message is forwarded without processing.

Related Documentation

- Understanding the SIP ALG on page 241

- SIP ALG Configuration Overview on page 248

- Example: Allowing Unknown SIP ALG Message Types on page 254

Example: Allowing Unknown SIP ALG Message Types

Supported Platforms   SRX Series, vSRX

This example shows how to allow unknown message types.

Requirements

Before you begin, review how unidentified SIP messages are handled by the device. See "Understanding SIP ALG Unknown Message Types" on page 253.

Overview

In this example, you configure the device to allow unknown message types in SIP traffic in both NAT mode and route mode. The default is to drop unknown (unsupported) messages.

Configuration

GUI Step-by-Step Procedure

To allow unknown SIP ALG message types:

1. Select **Configure>Security>ALG**.

2. Select the **SIP** tab.

3. Select the **Enable Permit NAT applied** check box.

4. Select the **Enable Permit routed** check box.

5. Click **OK** to check your configuration and save it as a candidate configuration.

6. If you are done configuring the device, click **Commit Options>Commit**.

Step-by-Step Procedure

To allow unknown SIP ALG message types:

1.   Configure the device to allow unknown message types in SIP traffic.

[edit]

> user@host# **set security alg sip application-screen unknown-message**
> **permit-nat-applied permit-routed**

2. If you are done configuring the device, commit the configuration.

   [edit]
   user@host# **commit**

Verification

To verify the configuration is working properly, enter the **show security alg sip** command.

Related
Documentation

- SIP ALG Configuration Overview on page 248

- Verifying SIP ALG Configurations on page 303

Understanding SIP ALG Hold Resources

Supported Platforms   SRX Series, vSRX

When a user puts a call on hold, the Session Initiation Protocol Application Layer Gateway (SIP ALG) releases Session Description Protocol (SDP) media resources, such as pinholes and translation contexts. When the user resumes the call, an INVITE request message negotiates a new SDP offer and answer and the SIP ALG reallocates resources for the media stream. This can result in new translated IP address and port numbers for the media description even when the media description is the same as the previous description. This is compliant with *RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP)*.

Some proprietary SIP implementations have designed call flows so that the User Agent (UA) module ignores the new SDP INVITE offer and continues to use the SDP offer of the previous negotiation. To accommodate this functionality, you must configure the device to retain SDP media resources when a call is put on hold for reuse when the call is resumed.

Related
Documentation

- Understanding the SIP ALG on page 241

- SIP ALG Configuration Overview on page 248

- Retaining SIP ALG Hold Resources (J-Web Procedure) on page 256

- Retaining SIP ALG Hold Resources (CLI Procedure) on page 255

Retaining SIP ALG Hold Resources (CLI Procedure)

Supported Platforms   SRX Series

To accommodate proprietary SIP call flows:

> user@host# **set security alg sip retain-hold-resource**

Related
Documentation

- Understanding SIP ALG Hold Resources on page 255

- SIP ALG Configuration Overview on page 248

Retaining SIP ALG Hold Resources (J-Web Procedure)

Supported Platforms   SRX Series

To accommodate proprietary SIP call flows:

1. Select **Configure>Security>ALG**.

2. Select the **SIP** tab.

3. Select the **Enable retail hold resource** check box.

4. Click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options**>**Commit**.

Related Documentation
- Understanding SIP ALG Hold Resources on page 255
- SIP ALG Configuration Overview on page 248
- Retaining SIP ALG Hold Resources (CLI Procedure) on page 255
- Verifying SIP ALG Configurations on page 303

Understanding the SIP ALG and NAT

Supported Platforms   SRX Series, vSRX

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 Session Initiation Protocol (SIP) service is more complicated because SIP messages contain IP addresses in the SIP headers as well as in the SIP body. When using NAT with the SIP service, the SIP headers contain information about the caller and the receiver, and the 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 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 Application Layer Gateway (ALG) collects information from the message header into a call table, which it uses to forward subsequent messages to the correct endpoint. 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 Transport 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.

IPv6 is supported on the SIP ALG along with NAT-PT mode and NAT64 address translation.

This topic contains the following sections:

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 binds 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 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 packets.

Incoming Calls

Incoming calls are initiated from the public network to public static NAT addresses or to interface IP addresses on the device. Static NATs 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. When the 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 they 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 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 terminates a call. When the 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 5 seconds to allow time for transmission of the 200 OK.

Call Re-INVITE Messages

Re-INVITE messages add new media sessions to a call and remove existing media sessions. When new media sessions are added to a call, new pinholes are opened in the

firewall and new address bindings are created. The process is identical to the original call setup. When all the media sessions or media pinholes are removed from a call, the call is removed when a BYE message is received.

Call Session Timers

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 device is protected should one of the following events occur:

- 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 5 seconds to allow time for the final 200 OK to pass through. The call is terminated when the 5-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 messages 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. Junos OS currently supports the SDP only. The SIP body contains IP addresses and port numbers used to transport the media.

SIP Headers

In the following sample SIP request message, NAT replaces the IP addresses in the header fields 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. A message can be any of the following:

- Inbound request

- Outbound response

- Outbound request

- Inbound response

Table 12 on page 260 shows how NAT is performed in each of these cases. Note that for several of the header fields the ALG determine more than just whether the messages comes from inside or outside the network. It must also determine what client initiated the call, and whether the message is a request or response.

Table 12: Requesting Messages with NAT Table

Inbound Request	To:	Replace domain with local address
(from public to private)	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	Replace ALG address with local address
	Contact:	None
	Record-Route:	None
	Route:	None

Table 12: Requesting Messages with NAT Table *(continued)*

Outbound Response	To:	Replace ALG address with local address
(from private to public)	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	To:	None
(from private to public)	From:	Replace local address with ALG address
	Call-ID:	None
	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 local address with ALG address
Outbound Response	To:	None
(from public to private)	From:	Replace ALG address with local address
	Call-ID:	None
	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 e-mail 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
```

Junos OS supports up to 6 SDP channels negotiated for each direction, for a total of 12 channels per call. For more information, see "SDP Session Descriptions" on page 244.

SIP NAT Scenario

Figure 20 on page 263 and Figure 21 on page 264 show a SIP call INVITE and 200 OK. In Figure 20 on page 263, 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 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 in Figure 21 on page 264, 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 20: SIP NAT Scenario 1
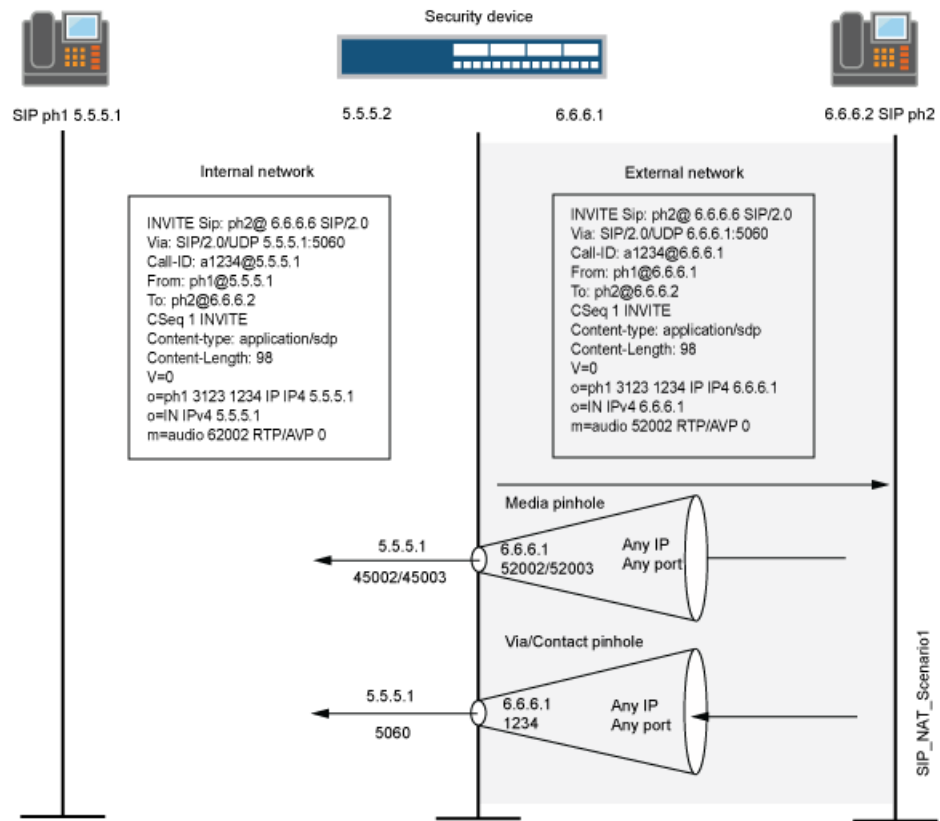
Figure 21: SIP NAT Scenario 2
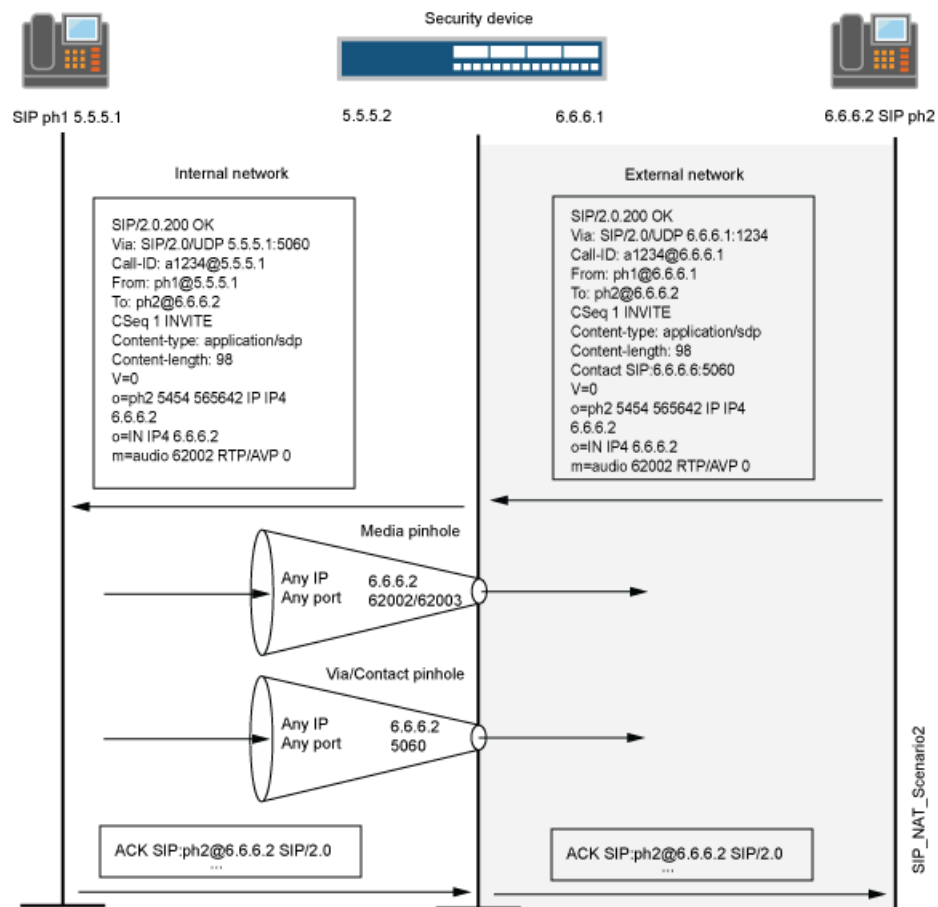
Classes of SIP Responses

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 13 on page 265 provides a complete list of current SIP responses.

Table 13: SIP Responses

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		

NAT Mode in Pure IPv6 Mode (NAT66) for SIP IPv6 ALG

The SIP IPv6 ALG supports NAT66 just like NAT44. NAT66 (IPv6 NAT) provides source NAT and static NAT functions similar to NAT44 (IPv4 NAT).

NAT-PT

Network Address Translation Protocol Translation (NAT-PT) (RFC 2766) is a protocol translation mechanism that allows communication between IPv6-only and IPv4-only nodes through protocol-independent translation of IPv4 and IPv6 datagrams, requiring no state information for the session.

NAT-PT is implemented by normal NAT from IPv6 address to IPv4 address and vice versa. The SIP ALG processes those address translations in the payload just as the addresses are processed in normal NAT.

NAT-PT binds the addresses in the IPv6 network with addresses in the IPv4 network and vice versa to provide transparent routing for the datagrams traversing between address realms.

The main advantage of NAT-PT is that the end devices and networks can run either IPv4 addresses or IPv6 addresses and traffic can be started from any side.

NAT64

NAT64 is a mechanism to allow IPv6 hosts to communicate with IPv4 servers. NAT64 is required to keep the IPv6 to IPv4 address mapping. Such address mapping is either statically configured by the system administrator (stateless translation), or more frequently, created automatically when the first packet from the IPv6 network reaches NAT64 to be translated (stateful).

On SRX Series devices, NAT64 is implemented by persistent NAT. When the first SIP request message (first packet should be only from IPv6) transverses the DUT, address binding is created and then the packets can flow in both directions.

The NAT64 mechanism translates IPv6 packets to IPv4 packets and vice versa, which allows IPv6 clients to contact to the IPv4 servers using unicast UDP, TCP, or ICMP. The NAT-PT and NAT64 behavior seems similar, but these mechanisms are implemented differently.

When NAT64 with persistent NAT is implemented, the SIP ALG with IPv6 support adds the NAT translation to the persistent NAT binding table if NAT is configured on the address of record. Because persistent NAT cannot duplicate the address configured, coexistence of NAT66 and NAT64 configured on the same address is not supported.

Only one binding is created for the same source IP address.

STUN and SIP ALG

Session Traversal Utilities for NAT (STUN) is a solution to make VoIP work through NAT and firewall.

Previously STUN worked without the SIP ALG. This means that the SIP ALG was not involved when persistent NAT was configured.

STUN can coexist with the SIP ALG and SIP ALG is involved when persistent NAT is configured.

Related Documentation

- Understanding the SIP ALG on page 241

- Understanding Incoming SIP ALG Call Support Using the SIP Registrar and NAT on page 267

- Example: Configuring Interface Source NAT for Incoming SIP Calls on page 268

Understanding Incoming SIP ALG Call Support Using the SIP Registrar and NAT

Supported Platforms   SRX Series, vSRX

Session Initiation Protocol (SIP) registration provides a discovery capability by which SIP proxies and location servers can 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 Uniform Resource Identifier (URI) and one or more contact URIs, as shown in Figure 22 on page 268. Registration creates bindings in a location service that associates the address-of-record with the contact address or addresses.

The device monitors outgoing REGISTER messages, performs Network Address Translation (NAT) on these addresses, and stores the information in an Incoming NAT table. Then, when an INVITE message is received from outside the network, the device uses the Incoming NAT 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 source NAT or NAT pools on the egress interface of the device. Interface source NAT is adequate for handling incoming calls in a small office, whereas we recommend setting up source NAT pools for larger networks or an enterprise environment.

> *i*
>
> NOTE: Incoming call support using interface source NAT or a source NAT pool is supported for SIP and H.323 services only. For incoming calls, Junos OS currently supports UDP and TCP only. Domain name resolution is also currently not supported; therefore, URIs must contain IP addresses, as shown in Figure 22 on page 268.

Figure 22: Using the SIP Registrar
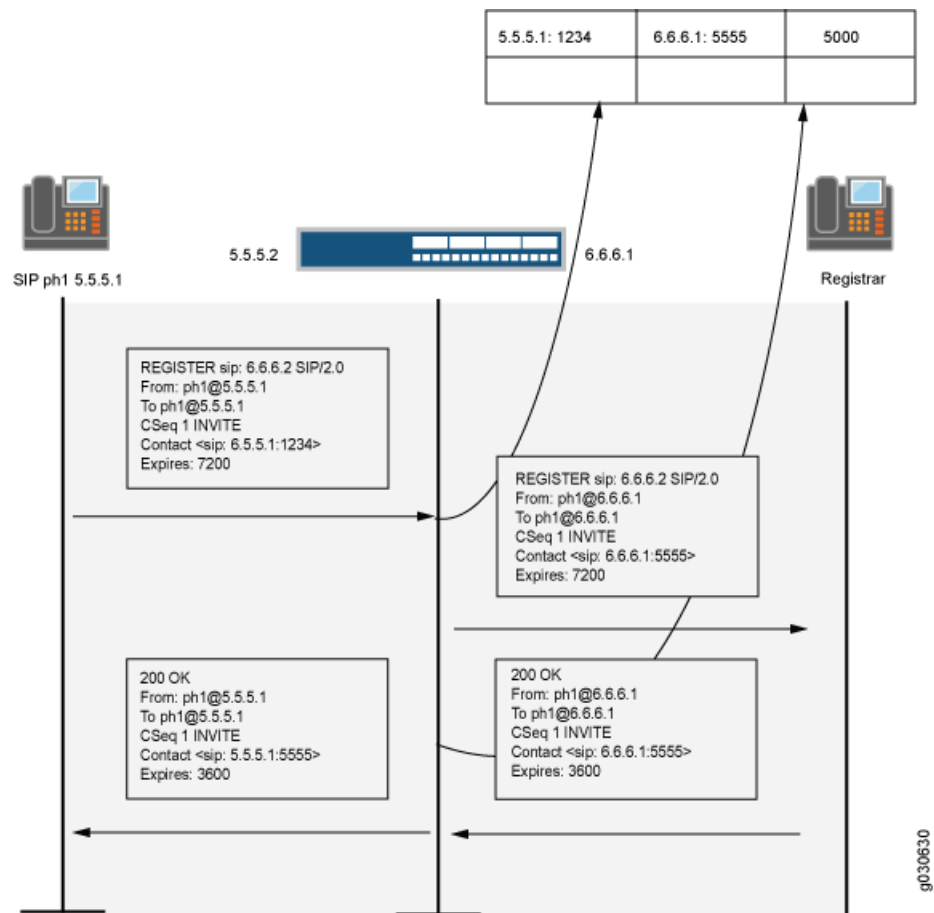
Example: Configuring Interface Source NAT for Incoming SIP Calls

Supported Platforms   SRX Series, vSRX

This example shows how to configure a source NAT rule on a public zone interface allowing NAT to be used for incoming SIP calls.

Requirements

Before you begin, understand how NAT works with the SIP ALG. See "Understanding the SIP ALG and NAT" on page 256.

Overview

In a two-zone scenario with the SIP proxy server in an external zone, you can use NAT for incoming calls by configuring a source NAT rule on the interface in the public or external zone.

In this example (see Figure 23 on page 269), phone1 is on the ge-0/0/0 interface in the private zone, and phone2 and the proxy server are on the ge-0/0/2 interface in the public zone. You configure a source NAT rule on the public interface ge-0/0/2.0.

Topology

Figure 23 on page 269 shows source NAT for incoming SIP calls.

Figure 23: Source NAT for Incoming SIP Calls
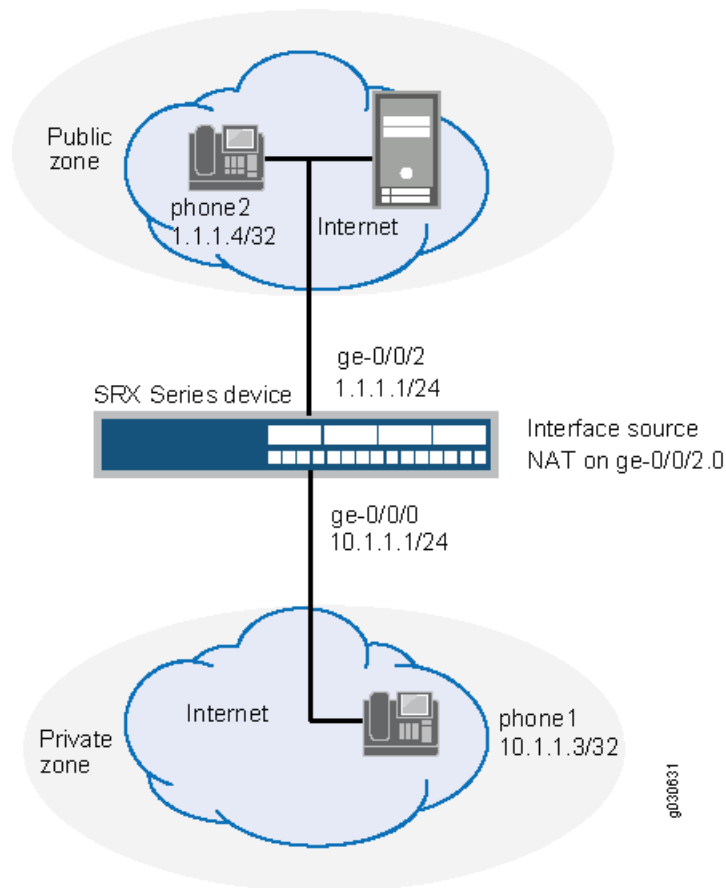
In this example, after creating zones called private and public and assigning them to interfaces, you configure address books to be used in the source NAT rule set. Then you configure source NAT by defining a rule set called sip-phones and a rule called phone1 that matches any packets from the source address 10.1.1.3/32.

Finally, you create security policies to allow all SIP traffic between the private and public zones.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private address-book address phone1 10.1.1.3/32
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public address-book address proxy 1.1.1.3/32
set security zones security-zone public address-book address phone2 1.1.1.4/32
set security zones security-zone public interfaces ge-0/0/2.0
set security nat source rule-set sip-phones from zone private
set security nat source rule-set sip-phones to zone public
set security nat source rule-set sip-phones rule phone1 match source-address 10.1.1.3/32
set security nat source rule-set sip-phones rule phone1 then source-nat interface
set security policies from-zone private to-zone public policy outgoing match
    source-address phone1
set security policies from-zone private to-zone public policy outgoing match
    destination-address phone2
set security policies from-zone private to-zone public policy outgoing match
    destination-address proxy
set security policies from-zone private to-zone public policy outgoing match application
    junos-sip
set security policies from-zone private to-zone public policy outgoing then permit
set security policies from-zone public to-zone private policy incoming match
    source-address phone2
set security policies from-zone public to-zone private policy incoming match
    destination-address phone1
set security policies from-zone public to-zone private policy incoming match
    source-address proxy
set security policies from-zone public to-zone private policy incoming match application
    junos-sip
set security policies from-zone public to-zone private policy incoming then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a source NAT rule on a public zone interface:

1.   Configure interfaces.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
```

```
                        user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
```

2. Configure zones and assign them to the interfaces.

   ```
   [edit security zones]
   user@host# set security-zone private interfaces ge-0/0/0.0
   user@host# set security-zone public interfaces ge-0/0/2.0
   ```

3. Configure address books and create addresses.

   ```
   [edit security zones]
   user@host# set security-zone private address-book address phone1 10.1.1.3/32
   user@host# set security-zone public address-book address proxy 1.1.1.3/32
   user@host# set security-zone public address-book address phone2 1.1.1.4/32
   ```

4. Configure a source NAT rule set.

   ```
   [edit security nat source]
   user@host# set rule-set sip-phones from zone private
   user@host# set rule-set sip-phones to zone public
   user@host# set rule-set sip-phones rule phone1 match source-address 10.1.1.3/32
   user@host# set rule-set sip-phones rule phone1 then source-nat interface
   ```

5. Enable persistent source NAT translation.

   ```
   [edit security nat source]
   user@host# set address-persistent
   ```

6. Configure a security policy to allow outgoing SIP traffic.

   ```
   [edit security policies from-zone private to-zone public policy outgoing]
   user@host# set match source-address phone1
   user@host# set match destination-address phone2
   user@host# set match destination-address proxy
   user@host# set match application junos-sip
   user@host# set then permit
   ```

7. Configure a security policy to allow incoming SIP traffic.

   ```
   [edit security policies from-zone public to-zone private policy incoming]
   user@host# set match source-address phone2
   user@host# set match destination-address phone1
   user@host# set match source-address proxy
   user@host# set match application junos-sip
   user@host# set then permit
   ```

Results   From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security policies**, and **show security nat** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 10.1.1.1/24;
    }
  }
```

```
        }
      ge-0/0/2 {
        unit 0 {
          family inet {
            address 1.1.1.1/24;
          }
        }
      }

[edit]
user@host# show security zones
security-zone private {
  address-book {
    address phone1 10.1.1.3/32;
  }
  interfaces {
    ge-0/0/0.0;
  }
}
  security-zone public {
    address-book {
      address proxy 1.1.1.3/32;
      address phone2 2.2.2.4/32;
    }
    interfaces {
      ge-0/0/2.0;
    }
  }
}
[edit]
user@host# show security nat
source {
  rule-set sip-phones {
    from zone private;
    to zone public;
    rule phone1 {
      match {
        source-address 10.1.1.3/32;
      }
      then {
        source-nat {
          interface;
        }
      }
    }
  }
}
[edit]
user@host# show security policies
from-zone private to-zone public {
  policy outgoing {
    match {
      source-address phone1;
      destination-address [ phone2 proxy ];
      application junos-sip;
    }
    then {
```

```
                    permit;
                  }
                }
              }
              from-zone public to-zone private {
                policy incoming {
                  match {
                    source-address [ phone2 proxy ];
                    destination-address phone1 ;
                    application junos-sip;
                  }
                  then {
                    permit;
                  }
                }
              }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying Source NAT Rule Usage

Purpose   Verify that there is traffic matching the source NAT rule.

Action   From operational mode, enter the **show security nat source rule all** command. View the Translation hits field to check for traffic that matches the rule.

```
user@host> show security nat source rule all
source NAT rule: phone1        Rule-set: sip-phones
  Rule-Id                      : 1
  Rule position                : 1
  From zone                    : private
  To zone                      : public
  Match
    Source addresses           : 0.0.0.0          - 255.255.255.255
    Destination port           : 0                - 0
  Action                          : interface
    Persistent NAT type          : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout           : 0
    Max session number           : 0
  Translation hits             : 0
    Successful sessions          : 0
    Failed sessions              : 0
  Number of sessions           : 0
```

Meaning   The **Translation hits** field shows that, there is no traffic matching the source NAT rule.

Verifying SIP ALG Status

Purpose   Verify that SIP ALG is enabled on your system.

Action   From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

Meaning   The output shows the SIP ALG status as follows:

- Enabled—Shows the SIP ALG is enabled.

- Disabled—Shows the SIP ALG is disabled.

Related Documentation
- Verifying SIP ALG Configurations on page 303

Decreasing Network Complexity by Configuring a Source NAT Pool for Incoming SIP Calls

Supported Platforms   SRX Series, vSRX

This example shows how to decrease network complexity by configuring a source NAT pool on an external interface to enable NAT for incoming SIP calls.

- Requirements on page 274
- Overview on page 275
- Configuration on page 276
- Verification on page 280

Requirements

Before you begin, understand how NAT works with the SIP ALG. See "Understanding the SIP ALG and NAT" on page 256.

Overview

In a two-zone scenario with the SIP proxy server in an external or public zone, you can use NAT for incoming calls by configuring a NAT pool on the interface to the public zone.

In this example (see Figure 24 on page 276), phone1 is in the private zone, and phone2 and the proxy server are in the public zone. You configure a source NAT pool to do NAT. You also create a policy that permits SIP traffic from the private to the public zone. This enables phone1 in the private zone to register with the proxy server in the public zone, and it also enables incoming calls from the public zone to the private zone.

Topology

shows source NAT pool for incoming calls.

Figure 24: Source NAT Pool for Incoming SIP Calls
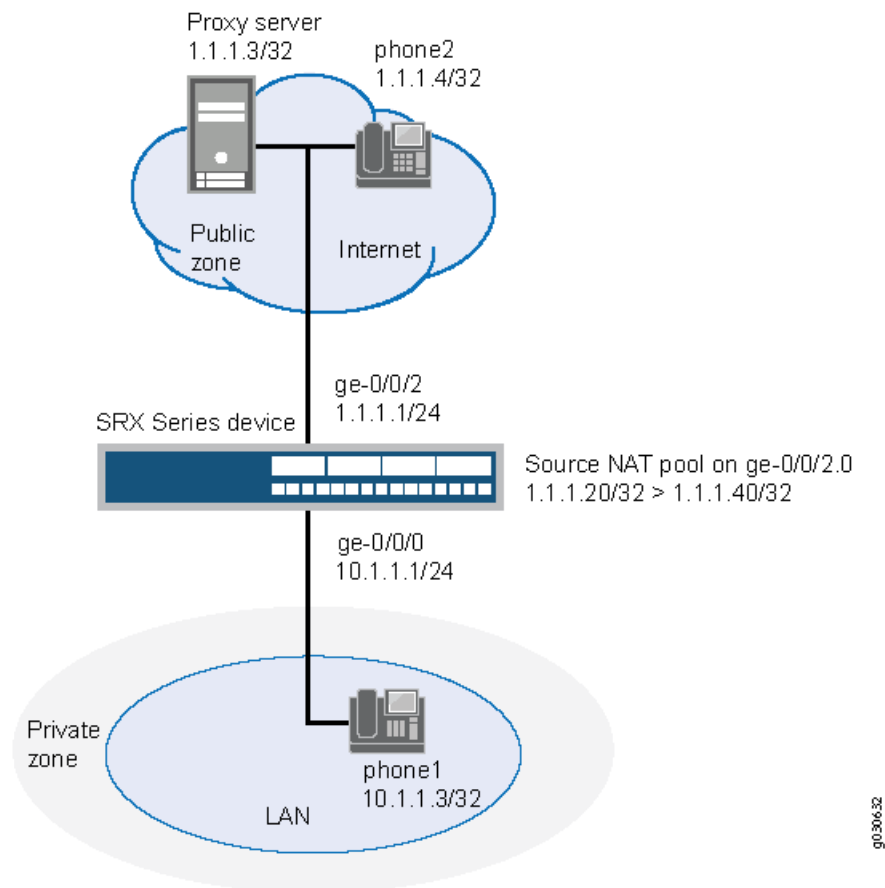
In this example, you configure source NAT as follows:

- Define source NAT pool called sip-nat-pool to contain the IP address range from 1.1.1.20/32 through 1.1.1.40/32.

- Create a source NAT rule set called sip-nat with a rule sip-r1 to match packets from the private zone to the public zone with the source IP address 10.1.1.3/24. For matching packets, the source address is translated to one of the IP address in sip-nat-pool.

- Configure proxy ARP for the addresses 1.1.1.20/32 through 1.1.1.40/32 on interface ge-0/0/2.0. This allows the system to respond to ARP requests received on the interface for these addresses.

Configuration

CLI Quick Configuration To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your

network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy
level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private address-book address phone1 10.1.1.3/32
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public address-book address proxy 1.1.1.3/32
set security zones security-zone public address-book address phone2 1.1.1.4/32
set security zones security-zone public interfaces ge-0/0/2.0
set security nat source pool sip-nat-pool address 1.1.1.20/32 to 1.1.1.40/32
set security nat source address-persistent
set security nat source rule-set sip-nat from zone private
set security nat source rule-set sip-nat to zone public
set security nat source rule-set sip-nat rule sip-r1 match source-address 10.1.1.3/24
set security nat source rule-set sip-nat rule sip-r1 then source-nat pool sip-nat-pool
set security nat proxy-arp interface ge-0/0/2.0 address 1.1.1.20/32 to 1.1.1.40/32
set security policies from-zone private to-zone public policy outgoing match
    source-address phone1
set security policies from-zone private to-zone public policy outgoing match
    destination-address any
set security policies from-zone private to-zone public policy outgoing match application
    junos-sip
set security policies from-zone private to-zone public policy outgoing then permit
set security policies from-zone public to-zone private policy incoming match
    source-address phone2
set security policies from-zone public to-zone private policy incoming match
    destination-address phone1
set security policies from-zone public to-zone private policy incoming match application
    junos-sip
set security policies from-zone public to-zone private policy incoming then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration
hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration
Mode in the CLI User Guide.

To configure a source NAT pool for incoming calls:

1. Configure interfaces.

    ```
    [edit]
    user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
    user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
    ```

2. Configure zones and assign interfaces to them.

    ```
    [edit security zones]
    user@host# set security-zone private interfaces ge-0/0/0.0
    user@host# set security-zone public interfaces ge-0/0/2.0
    ```

3. Configure address books.

    ```
    [edit security zones]
    user@host# set security-zone private address-book address phone1 10.1.1.3/32
    user@host# set security-zone public address-book address proxy 1.1.1.3/32
    user@host# set security-zone public address-book address phone2 1.1.1.4/32
    ```

4. Configure a source NAT pool.

   [edit security nat]
   user@host# **set source pool sip-nat-pool address 1.1.1.20/32 to 1.1.1.40/32**

5. Configure a source NAT rule set with a rule.

   [edit security nat source rule-set sip-nat]
   user@host# **set from zone private**
   user@host# **set to zone public**
   user@host# **set rule sip-r1 match source-address 10.1.1.3/24**
   user@host# **set rule sip-r1 then source-nat pool sip-nat-pool**

6. Enable persistent NAT.

   [edit security nat]
   user@host# **set source address-persistent**

7. Configure proxy ARP.

   [edit security nat]
   user@host# **set proxy-arp interface ge-0/0/2.0 address 1.1.1.20/32 to 1.1.1.40/32**

8. Configure a security policy to allow outgoing SIP traffic.

   [edit security policies from-zone private to-zone public policy outgoing]
   set match source-address phone1
   set match destination-address any
   set match application junos-sip
   set then permit

9. Configure a security policy to allow incoming SIP traffic.

   [edit security policies from-zone public to-zone private policy incoming]
   set match source-address phone2
   set match destination-address phone1
   set match application junos-sip
   set then permit

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security nat**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
  ge-0/0/2 {
    unit 0 {
      family inet {
        address 1.1.1.1/24;
      }
    }
```

```
        }
      [edit]
      user@host# show security zones
        security-zone private {
          address-book {
            address phone1 10.1.1.3/32;
          }
          interfaces {
            ge-0/0/0.0;
          }
        }
          security-zone public {
            address-book {
              address proxy 1.1.1.3/32;
              address phone2 1.1.1.4/32;
            }
            interfaces {
              ge-0/0/2.0;
            }
          }
      user@host# show security nat
        source {
          pool sip-nat-pool {
            address {
              1.1.1.20/32 to 1.1.1.40/32;
            }
          }
          address-persistent;
          rule-set sip-nat {
            from zone private;
            to zone public;
            rule sip-r1 {
              match {
                source-address 10.1.1.3/24;
              }
              then {
                source-nat {
                  pool {
                    sip-nat-pool;
                  }
                }
              }
            }
          }
        }
          proxy-arp {
            interface ge-0/0/2.0 {
              address {
                1.1.1.20/32 to 1.1.1.40/32;
              }
            }
          }
      [edit]
      user@host# show security policies
        from-zone private to-zone public {
          policy outgoing {
```

```
                    match {
                        source-address phone1;
                        destination-address any;
                        application junos-sip;
                    }
                    then {
                        permit;
                    }
                }
            }
            from-zone public to-zone private {
                policy incoming {
                    match {
                        source-address phone2;
                        destination-address phone1;
                        application junos-sip;
                    }
                    then {
                        permit;
                    }
                }
            }
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying Source NAT Pool Usage

Purpose   Verify that there is traffic using IP addresses from the source NAT pool.

Action   From operational mode, enter the **show security nat source pool all** command.

> user@host> **show security nat source pool all**

```
Total pools: 1
Pool name          : sip-nat-pool
Pool id            : 4
Routing instance   : default
Host address base  : 0.0.0.0
Port               : [1024, 63487]
port overloading   : 1
Total addresses    : 21
Translation hits   : 0
Address range                        Single Ports    Twin Ports
        1.1.1.20 - 1.1.1.40               0               0
```

Meaning   The **Translation hits** field shows that there is no traffic used by IP addresses from the source NAT pool.

Verifying Source NAT Rule Usage

Purpose   Verify that there is traffic matching the source NAT rule.

Action   From operational mode, enter the **show security nat source rule all** command.

user@host> **show security nat source rule all**

```
source NAT rule: sip-r1      Rule-set: sip-nat
  Rule-Id                   : 1
  Rule position             : 1
  From zone                 : private
  To zone                   : public
  Match
    Source addresses        : 0.0.0.0          - 255.255.255.255
    Destination port        : 0                - 0
  Action                       : interface
    Persistent NAT type        : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout         : 0
    Max session number         : 0
  Translation hits          : 0
    Successful sessions     : 0
    Failed sessions         : 0
  Number of sessions        : 0
```

Meaning   The **Translation hits** field shows that, there is no traffic matching the source NAT rule.

Verifying SIP ALG Status

Purpose   Verify that SIP ALG is enabled on your system.

Action   From operational mode, enter the **show security alg status** command.

user@host> **show security alg status**

```
ALG Status :
  DNS     : Enabled
  FTP     : Enabled
  H323    : Disabled
  MGCP    : Disabled
  MSRPC   : Enabled
  PPTP    : Enabled
  RSH     : Disabled
  RTSP    : Disabled
  SCCP    : Disabled
  SIP     : Enabled
  SQL     : Enabled
  SUNRPC  : Enabled
  TALK    : Enabled
  TFTP    : Enabled
  IKE-ESP : Disabled
```

Meaning   The output shows the SIP ALG status as follows:

- ·Enabled—Shows the SIP ALG is enabled.

- ·Disabled—Shows the SIP ALG is disabled.

Verifying the Security Polices of SIP ALG

Purpose Verify that the source NAT between public zone and private zone is set.

Action From operational mode, enter the **show security policies** command.

user@host> **show security policies**

```
from-zone private to-zone public {
    policy outgoing {
        match {
            source-address phone1;
            destination-address any;
            application junos-sip;
        }
        then {
            permit;
        }
    }
}

from-zone public to-zone private {
    policy incoming {
        match {
            source-address phone2;
            destination-address phone1;
            application junos-sip;
        }
        then {
            permit;
        }
    }
}
```

Meaning The sample output shows that the source NAT between public zone and private zone is set.

Related Documentation

- Verifying SIP ALG Configurations on page 303

Example: Configuring Static NAT for Incoming SIP Calls

Supported Platforms SRX Series, vSRX

This example shows how to configure a static NAT mapping that allows callers in the private zone to register with the proxy server in the public zone.

- Requirements on page 283
- Overview on page 283
- Configuration on page 284
- Verification on page 288

Requirements

Before you begin, understand how NAT works with the SIP ALG. See "Understanding the SIP ALG and NAT" on page 256.

Overview

When a SIP proxy server is located in an external or public zone, you can configure static NAT on the public interface to enable callers in the private zone to register with the proxy server.

In this example (see Figure 25 on page 284), phone1 is on the ge-0/0/0 interface in the private zone, and phone2 and the proxy server are on the ge-0/0/2 interface in the public zone. You create a static NAT rule set called incoming-sip with a rule called phone1 to match packets from the public zone with the destination address 1.1.1.3/32. For matching packets, the destination IP address is translated to the private address 10.1.1.3/32. You also create proxy ARP for the address 1.1.1.3/32 on interface ge-0/0/2.0. This allows the system to respond to ARP requests received on the interface for these addresses. Finally, you create a security policy called incoming that allows SIP traffic from the public zone to the private zone.

> **NOTE:** When configuring static NAT for incoming SIP calls, make sure to configure one public address for each private address in the private zone.

Topology

shows static NAT for incoming calls.

Figure 25: Static NAT for Incoming Calls

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone private address-book address phone1 10.1.1.5/32
set security zones security-zone public interfaces ge-0/0/2.0
set security zones security-zone public address-book address proxy 1.1.1.3/32
set security zones security-zone public address-book address phone2 1.1.1.4/32
set security nat static rule-set incoming-sip from zone public
set security nat static rule-set incoming-sip rule phone1 match destination-address
    1.1.1.3/32
set security nat static rule-set incoming-sip rule phone1 then static-nat prefix 10.1.1.3/32
set security nat proxy-arp interface ge-0/0/2.0 address 1.1.1.3/32
set security policies from-zone public to-zone private policy incoming match
    source-address phone2
```

set security policies from-zone public to-zone private policy incoming match
    source-address proxy
set security policies from-zone public to-zone private policy incoming match
    destination-address phone1
set security policies from-zone public to-zone private policy incoming match application
    junos-sip
set security policies from-zone public to-zone private policy incoming then permit
set security policies from-zone private to-zone public policy outgoing match
    source-address phone1
set security policies from-zone private to-zone public policy outgoing match
    destination-address phone2
set security policies from-zone private to-zone public policy outgoing match
    destination-address proxy
set security policies from-zone private to-zone public policy outgoing match application
    junos-sip
set security policies from-zone private to-zone public policy outgoing then permit

**Step-by-Step
Procedure**

The following example requires you to navigate various levels in the configuration
hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration
Mode in the CLI User Guide.

To configure static NAT for incoming calls:

1. Configure interfaces.

   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24

2. Create security zones.

   [edit security zones]
   user@host# set security-zone private interfaces ge-0/0/0.0
   user@host# set security-zone public interfaces ge-0/0/2.0

3. Assign addresses to the security zones.

   [edit security zones]
   user@host# set security-zone private address-book address phone1 10.1.1.5/32
   user@host# set security-zone public address-book address proxy 1.1.1.3/32
   user@host# set security-zone public address-book address phone2 1.1.1.4/32

4. Create a static NAT rule set with a rule.

   [edit security nat static rule-set incoming-sip]
   user@host# set from zone public
   user@host# set rule phone1 match destination-address 1.1.1.3/32
   user@host# set rule phone1 then static-nat prefix 10.1.1.3/32

5. Configure proxy ARP.

   [edit security nat]
   user@host# set proxy-arp interface ge-0/0/2.0 address 1.1.1.3/32

6. Define a security policy to allow incoming SIP traffic.

   [edit security policies from-zone public to-zone private policy incoming]
   user@host# set match source-address phone2
   user@host# set match source-address proxy
   user@host# set match destination-address phone1

```
                                user@host# set match application junos-sip
                                user@host# set then permit
```

7. Define a security policy to allow outgoing SIP traffic.

```
    [edit security policies from-zone private to-zone public policy outgoing]
    user@host#  set match source-address phone1
    user@host# set match destination-address phone2
    user@host# set match destination-address proxy
    user@host# set match application junos-sip
    user@host# set then permit
```

Results   From configuration mode, confirm your configuration by entering the **show interfaces**,
             show security zones, **show security nat**, and **show security policies** commands. If the output
             does not display the intended configuration, repeat the configuration instructions in this
             example to correct it.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
   unit 0 {
      family inet {
         address 10.1.1.1/24;
      }
   }
}
   ge-0/0/2 {
      unit 0 {
         family inet {
            address 1.1.1.1/24;
         }
      }
   }

[edit]
user@host# show security zones
security-zone private {
   address-book {
      address phone1 10.1.1.5/32;
   }
   interfaces {
      ge-0/0/0.0;
   }
}
   security-zone public {
      address-book {
         address proxy 1.1.1.3/32;
         address phone2 1.1.1.4/32;
      }
      interfaces {
         ge-0/0/2.0;
      }
   }

[edit]
user@host# show security nat
```

```
                static {
                  rule-set incoming-sip {
                    from zone public;
                    rule phone1 {
                      match {
                        destination-address 1.1.1.3/32;
                      }
                      then {
                        static-nat prefix 10.1.1.3/32;
                      }
                    }
                  }
                }
                  proxy-arp {
                    interface ge-0/0/2.0 {
                      address {
                        1.1.1.3/32;
                      }
                    }
                  }

                [edit]
                user@host# show security policies
                from-zone public to-zone private {
                  policy incoming {
                    match {
                      source-address phone2;
                      destination-address phone1;
                      application junos-sip;
                    }
                    then {
                      permit;
                    }
                  }
                }
                from-zone private to-zone public {
                  policy outgoing {
                    match {
                      source-address phone1;
                      destination-address [phone2 proxy];
                      application junos-sip;
                    }
                    then {
                      permit;
                    }
                  }
                }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying Static NAT Configuration

Purpose   Verify that there is traffic matching the static NAT rule set.

Action   From operational mode, enter the **show security nat static rule all** command.

```
user@host> show security nat static rule all

Static NAT rule: phone1 Rule-set: incoming-sip
Rule-Id : 1
Rule position : 1
From zone : trust
Source addresses : 40.10.10.0 - 40.10.10.3
: addr1
Source ports : 200 - 300
Destination addresses : 20.1.1.0
Host addresses : 3.3.3.0
Netmask : 24
Host routing-instance : N/A
Translation hits : 4
Successful sessions : 4
Failed sessions : 0
Number of sessions : 4
```

Meaning   The **Translation hits** field shows that there is traffic matching the static NAT rule set.

Verifying SIP ALG Status

Purpose   Verify that SIP ALG is enabled on your system.

Action   From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status

ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
```

```
TFTP    : Enabled
IKE-ESP : Disabled
```

Meaning The output shows the SIP ALG status as follows:

- ·Enabled—Shows the SIP ALG is enabled.

- ·Disabled—Shows the SIP ALG is disabled.

Verifying the Security Polices of SIP ALG

Purpose Verify that the static NAT between public zone and private zone is set.

Action From operational mode, enter the **show security policies** command.

user@host> **show security policies**

```
from-zone public to-zone private {
    policy incoming {
        match {
            source-address [ phone2 proxy ];
            destination-address phone1;
            application junos-sip;
        }
        then {
            permit;
        }
    }
}
  from-zone private to-zone public {
    policy outgoing {
        match {
            source-address phone1;
            destination-address [ phone2 proxy ];
            application junos-sip;
        }
        then {
            permit;
        }
    }
}
```

Meaning The sample output shows that the static NAT between public zone and private zone is set.

Related Documentation
-

Example: Configuring the SIP Proxy in the Private Zone and NAT in the Public Zone

Supported Platforms SRX Series, vSRX

This example shows how to configure a SIP proxy server in a private zone and static NAT in a public zone to allow callers in the public zone to register with the proxy server.

- Requirements on page 290
- Overview on page 290
- Configuration on page 291
- Verification on page 295

Requirements

Before you begin, understand how NAT works with the SIP ALG. See "Understanding the SIP ALG and NAT" on page 256.

Overview

With the SIP proxy server in the private zone, you can configure static NAT on the external, or public, interface to allow callers in the public zone to register with the proxy server.

In this example (see Figure 26 on page 291), phone1 and the SIP proxy server are on the ge-0/0/0 interface in the private zone, and phone2 is on the ge-0/0/2 interface in the public zone. You configure a static NAT rule for the proxy server to allow phone2 to register with the proxy server, and then create a policy called outgoing that allows SIP traffic from the public to the private zone to enable callers in the public zone to register with the proxy server. You also configure a policy called incoming from the private to the public zone to allow phone1 to call out.

Topology

Figure 26 on page 291 shows configuring SIP proxy in the private zone and NAT in a public zone.

Figure 26: Configuring SIP Proxy in the Private Zone and NAT in a Public Zone
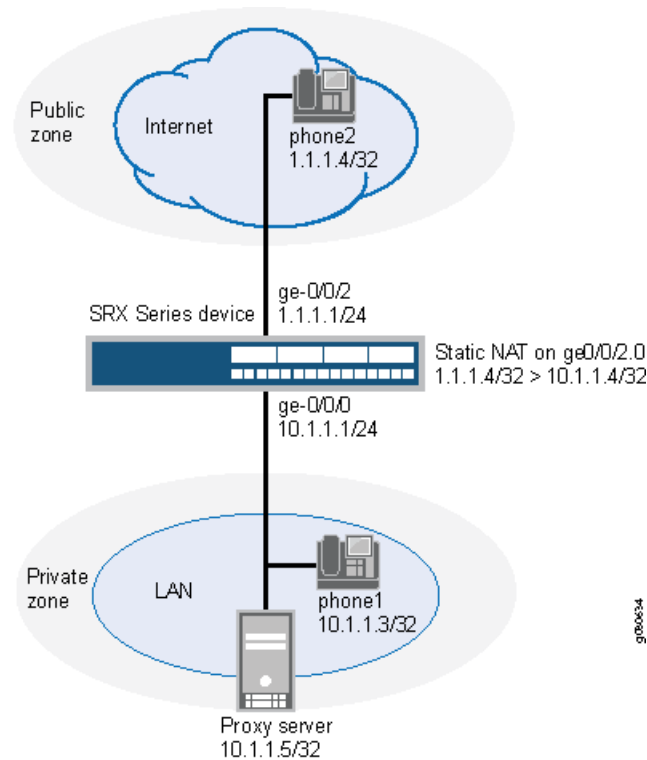
In this example, you configure NAT as follows:

- Configure static NAT on the ge-0/0/2 interface to the proxy server with a rule set called incoming-sip with a rule called proxy to match packets from the public zone with the destination address 1.1.1.4/32. For matching packets, the destination IP address is translated to the private address 10.1.1.4/32.

- Configure a second rule set called sip-phones with a rule called phone1 to enable interface NAT for communication from phone1 to phone2.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private address-book address phone1 10.1.1.3/32
set security zones security-zone private address-book address proxy 10.1.1.5/32
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public address-book address phone2 1.1.1.4/32
set security zones security-zone public interfaces ge-0/0/2.0
set security nat source rule-set sip-phones from zone private
set security nat source rule-set sip-phones to zone public
```

```
set security nat source rule-set sip-phones rule phone1 match source-address 10.1.1.3/32
set security nat source rule-set sip-phones rule phone1 then source-nat interface
set security nat static rule-set incoming-sip from zone public
set security nat static rule-set incoming-sip rule proxy match destination-address 1.1.1.4/32
set security nat static rule-set incoming-sip rule proxy then static-nat prefix 10.1.1.4/32
set security policies from-zone private to-zone public policy outgoing match
    source-address any
set security policies from-zone private to-zone public policy outgoing match
    destination-address phone2
set security policies from-zone private to-zone public policy outgoing match application
    junos-sip
set security policies from-zone private to-zone public policy outgoing then permit
set security policies from-zone public to-zone private policy incoming match
    source-address phone2
set security policies from-zone public to-zone private policy incoming match
    destination-address proxy
set security policies from-zone public to-zone private policy incoming match application
    junos-sip
set security policies from-zone public to-zone private policy incoming then permit
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure static NAT for incoming calls:

1. Configure interfaces.

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
   ```

2. Configure security zones.

   ```
   [edit security zones]
   user@host# set security-zone private interfaces ge-0/0/0.0
   user@host# set security-zone public interfaces ge-0/0/2.0
   ```

3. Assign addresses to the security zones.

   ```
   [edit security zones]
   user@host# set security-zone private address-book address phone1 10.1.1.3/32
   user@host# set security-zone private address-book address proxy 10.1.1.5/32
   user@host# set security-zone public address-book address phone2 1.1.1.4/32
   ```

4. Create a rule set for static NAT and assign a rule to it.

   ```
   [edit security nat static rule-set incoming-sip]
   user@host# set from zone public
   user@host# set rule proxy match destination-address 1.1.1.4/32
   user@host# set rule proxy then static-nat prefix 10.1.1.4/32
   ```

5. Configure the second rule set and assign a rule to it.

   ```
   [edit security nat source rule-set sip-phones]
   user@host# set from zone private
   user@host# set to zone public
   user@host# set rule phone1 match source-address 10.1.1.3/32
   user@host# set rule phone1 then source-nat interface
   ```

6. Configure a security policy for outgoing traffic.

```
[edit security policies from-zone private to-zone public policy outgoing]
user@host# set match source-address any
user@host# set match destination-address phone2
user@host# set match application junos-sip
user@host# set then permit
```

7. Configure a security policy for incoming traffic.

```
[edit security policies from-zone public to-zone private policy incoming]
user@host# set match source-address phone2
user@host# set match destination-address proxy
user@host# set match application junos-sip
user@host# set then permit
```

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show security zones**, **show security nat**, and **show security policies** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 10.1.1.1/24;
    }
  }
}
  ge-0/0/2 {
    unit 0 {
      family inet {
        address 1.1.1.1/24;
      }
    }
  }
[edit]
user@host# show security zones
security-zone private {
  address-book {
    address phone1 10.1.1.3/32;
    address proxy 10.1.1.5/32;
  }
  interfaces {
    ge-0/0/0.0;
  }
}
  security-zone public {
    address-book {
      address phone2 1.1.1.4/32;
    }
    interfaces {
      ge-0/0/2.0;
    }
  }
```

```
[edit]
user@host# show security nat
source {
  rule-set sip-phones {
    from zone private;
    to zone public;
    rule phone1 {
      match {
        source-address 10.1.1.3/32;
      }
      then {
        source-nat {
          interface;
        }
      }
    }
  }
}
  static {
    rule-set incoming-sip {
      from zone public;
      rule proxy {
        match {
          destination-address 1.1.1.4/32;
        }
        then {
          static-nat prefix 10.1.1.4/32;
        }
      }
    }
  }
[edit]
user@host# show security policies
from-zone private to-zone public {
  policy outgoing {
    match {
      source-address any;
      destination-address phone2;
      application junos-sip;
    }
    then {
      permit;
    }
  }
}
  from-zone public to-zone private {
    policy incoming {
      match {
        source-address phone2;
        destination-address proxy;
        application junos-sip;
      }
      then {
        permit;
      }
    }
```

```
        }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying Static NAT Configuration

Purpose Verify that there is traffic matching the static NAT rule set.

Action From operational mode, enter the **show security nat static rule all** command. View the Translation hits field to check for traffic that matches the rule.

```
user@host> show security nat source rule all
source NAT rule: phone1       Rule-set: sip-phones
  Rule-Id                     : 1
  Rule position               : 1
  From zone                   : private
  To zone                     : public
  Match
    Source addresses          : 0.0.0.0          - 255.255.255.255
    Destination port          : 0                - 0
  Action                      : interface
    Persistent NAT type       : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout        : 0
    Max session number        : 0
  Translation hits            : 0
    Successful sessions       : 0
    Failed sessions           : 0
  Number of sessions          : 0
```

Meaning The **Translation hits** field shows that, there is no traffic matching the source NAT rule.

Verifying SIP ALG Status

Purpose Verify that SIP ALG is enabled on your system.

Action From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
```

```
SQL      : Enabled
SUNRPC   : Enabled
TALK     : Enabled
TFTP     : Enabled
IKE-ESP  : Disabled
```

Meaning   The output shows the SIP ALG status as follows:

- Enabled—Shows the SIP ALG is enabled.

- Disabled—Shows the SIP ALG is disabled.

Related   • Verifying SIP ALG Configurations on page 303
Documentation

Example: Configuring a Three-Zone SIP ALG and NAT Scenario

Supported Platforms   SRX Series, vSRX

This example shows how to configure a SIP proxy server in a private zone and static NAT in a public zone to allow callers in the public zone to register with the proxy server.

- Requirements on page 296
- Overview on page 296
- Configuration on page 297
- Verification on page 302

Requirements

Before you begin, understand how NAT works with the SIP ALG. See "Understanding the SIP ALG and NAT" on page 256.

Overview

In a three-zone SIP configuration, the SIP proxy server is typically in a different zone from the calling and called systems. Such a scenario requires additional address and zone configuration, and policies to ensure that all systems have access to each other and to the proxy server.

In this example, phone1 is on the ge-0/0/0.0 interface in the private zone, phone2 is on the ge-0/0/2.0 interface in the public zone, and the proxy server is on the ge-0/0/1.0 interface in the DMZ. You configure static NAT rule for phone1 in the private zone. You then create policies for traffic traversing from the private zone to the DMZ and from the DMZ to the private zone, from the public zone to the DMZ and from the DMZ to the public zone, and from the private zone to the public zone. The arrows in Figure 27 on page 297 show the flow of SIP signaling traffic when phone2 in the public zone places a call to phone1 in the private zone. After the session is initiated, the data flows directly between phone1 and phone2.

Figure 27: Three-Zone SIP Configuration with Proxy in the DMZ
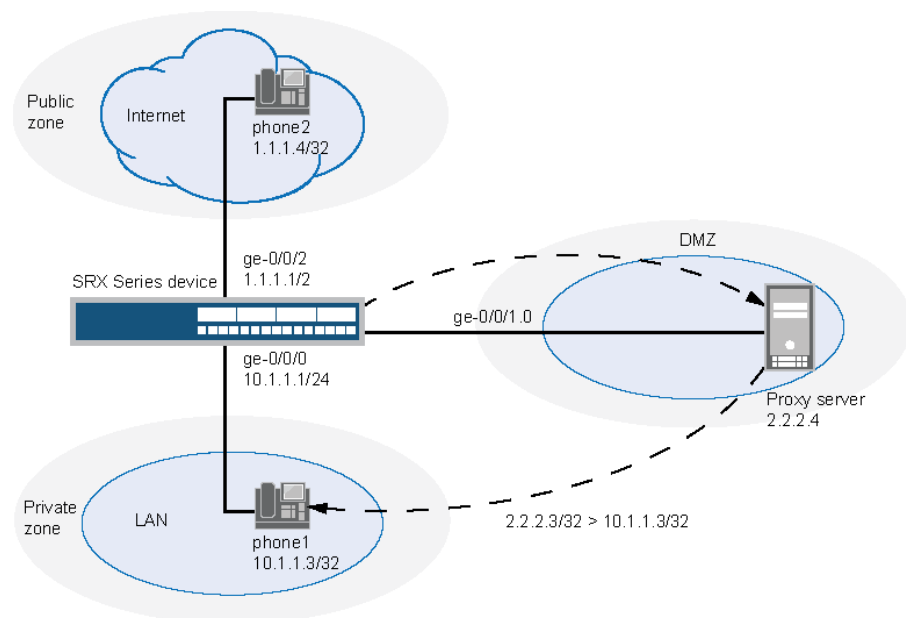
In this example, you configure NAT as follows:

- Configure a static NAT rule set called incoming-sip with a rule phone1 to match packets from the public zone with the destination address 2.2.2.3/32. For matching packets, the destination IP address is translated to the private address 10.1.1.3/32.

- Configure proxy ARP for the address 2.2.2.3/32 on interface ge-0/0/1.0 allowing the system to respond to ARP requests received on the interface for this address.

- Configure a second rule set called sip-phones with a rule r1 to enable interface NAT for communication from phone1 to the proxy server and from phone1 to phone2.

Configuration

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24
set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
set security zones security-zone private address-book address phone1 10.1.1.3/32
set security zones security-zone private interfaces ge-0/0/0.0
set security zones security-zone public address-book address phone2 1.1.1.4/32
set security zones security-zone public interfaces ge-0/0/2.0
set security zones security-zone dmz address-book address proxy 2.2.2.4/32
set security zones security-zone dmz interfaces ge-0/0/1.0
set security nat source rule-set sip-phones from zone private
set security nat source rule-set sip-phones to zone dmz
set security nat source rule-set sip-phones rule r1 match source-address 10.1.1.3/32
set security nat source rule-set sip-phones rule r1 then source-nat interface
```

set security policies from-zone private to-zone dmz policy private-to-proxy match
    source-address phone1
set security policies from-zone private to-zone dmz policy private-to-proxy match
    destination-address proxy
set security policies from-zone private to-zone dmz policy private-to-proxy match
    application junos-sip
set security policies from-zone private to-zone dmz policy private-to-proxy then permit
set security policies from-zone public to-zone dmz policy public-to-proxy match
    source-address phone2
set security policies from-zone public to-zone dmz policy public-to-proxy match
    destination-address proxy
set security policies from-zone public to-zone dmz policy public-to-proxy match application
    junos-sip
set security policies from-zone public to-zone dmz policy public-to-proxy then permit
set security policies from-zone private to-zone public policy private-to-public match
    source-address phone1
set security policies from-zone private to-zone public policy private-to-public match
    destination-address phone2
set security policies from-zone private to-zone public policy private-to-public match
    application junos-sip
set security policies from-zone private to-zone public policy private-to-public then permit
set security policies from-zone dmz to-zone private policy proxy-to-private match
    source-address proxy
set security policies from-zone dmz to-zone private policy proxy-to-private match
    destination-address phone1
set security policies from-zone dmz to-zone private policy proxy-to-private match
    application junos-sip
set security policies from-zone dmz to-zone private policy proxy-to-private then permit
set security policies from-zone dmz to-zone public policy proxy-to-public match
    source-address proxy
set security policies from-zone dmz to-zone public policy proxy-to-public match
    destination-address phone2
set security policies from-zone dmz to-zone public policy proxy-to-public match application
    junos-sip
set security policies from-zone dmz to-zone public policy proxy-to-public then permit

Step-by-Step Procedure   The following example requires you to navigate various levels in the configuration
hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration
Mode* in the CLI User Guide.

To configure a SIP proxy server in a private zone and static NAT in a public zone:

1. Configure interfaces.

    [edit]
    user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
    user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/24
    user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24

2. Configure security zones.

    [edit security zones]
    user@host# set security-zone private interfaces ge-0/0/0.0
    user@host# set security-zone public interfaces ge-0/0/2.0
    user@host# set security-zone dmz interfaces ge-0/0/1.0

3. Assign addresses to the security zones.

[edit security zones]
user@host# set security-zone private address-book address phone1 10.1.1.3/32
user@host# set security-zone public address-book address phone2 1.1.1.4/32
user@host# set security-zone dmz address-book address proxy 2.2.2.4/32

4. Configure interface NAT for communication from phone1 to proxy.

[edit security nat source rule-set sip-phones]
user@host# set from zone private
user@host# set to zone dmz
user@host# set rule r1 match source-address 10.1.1.3/32
user@host# set rule r1 then source-nat interface

5. Configure a security policy to allow traffic from zone private to zone DMZ.

[edit security policies from-zone private to-zone dmz policy private-to-proxy]
user@host# set match source-address phone1
user@host# set match destination-address proxy
user@host# set match application junos-sip
user@host# set then permit

6. Configure a security policy to allow traffic from zone public to zone DMZ.

[edit security policies from-zone public to-zone dmz policy public-to-proxy]
user@host# set match source-address phone2
user@host# set match destination-address proxy
user@host# set match application junos-sip
user@host# set then permit

7. Configure a security policy to allow traffic from zone private to zone public.

[edit security policies from-zone private to-zone public policy private-to-public]
user@host# set match source-address phone1
user@host# set match destination-address phone2
user@host# set match application junos-sip
user@host# set then permit

8. Configure a security policy to allow traffic from zone DMZ to zone private.

[edit security policies from-zone dmz to-zone private policy proxy-to-private]
user@host# set match source-address proxy
user@host# set match destination-address phone1
user@host# set match application junos-sip
user@host# set then permit

9. Configure a security policy to allow traffic from zone DMZ to zone public.

[edit security policies from-zone dmz to-zone public policy proxy-to-public]
user@host# set match source-address proxy
user@host# set match destination-address phone2
user@host# set match application junos-sip
user@host# set then permit

Results   From configuration mode, confirm your configuration by entering the **show interfaces**,
show security zones, **show security nat**, and **show security policies** commands. If the output
does not display the intended configuration, repeat the configuration instructions in this
example to correct it.

[edit]

```
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 10.1.1.1/24;
    }
  }
}
  ge-0/0/1 {
    unit 0 {
      family inet {
        address 2.2.2.2/24;
      }
    }
  }
  ge-0/0/2 {
    unit 0 {
      family inet {
        address 1.1.1.1/24;
      }
    }
  }

[edit]
user@host# show security zones
security-zone private {
  address-book {
    address phone1 10.1.1.3/32;
  }
  interfaces {
    ge-0/0/0.0;
  }
  }
  security-zone public {
    address-book {
      address phone2 1.1.1.4/32;
    }
    interfaces {
      ge-0/0/2.0;
    }
  }
  security-zone dmz {
    address-book {
      address proxy 2.2.2.4/32;
    }
    interfaces {
      ge-0/0/1.0;
    }
  }
[edit]
user@host# show security nat
source {
  rule-set sip-phones {
    from zone private;
    to zone dmz;
    rule r1 {
```

```
                match {
                    source-address 10.1.1.3/32;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
proxy-arp {
    interface ge-0/0/1.0 {
        address {
            2.2.2.3/32;
        }
    }
}

[edit]
user@host# show security policies
from-zone private to-zone dmz {
    policy private-to-proxy {
        match {
            source-address phone1;
            destination-address proxy;
            application junos-sip;
        }
        then {
            permit;
        }
    }
}
    from-zone public to-zone dmz {
        policy public-to-proxy {
            match {
                source-address phone2;
                destination-address proxy;
                application junos-sip;
            }
            then {
                permit;
            }
        }
    }
    from-zone private to-zone public {
        policy private-to-public {
            match {
                source-address phone1;
                destination-address phone2;
                application junos-sip;
            }
            then {
                permit;
            }
        }
```

```
            }
            from-zone dmz to-zone private {
              policy proxy-to-private {
                match {
                  source-address proxy;
                  destination-address phone2;
                  application junos-sip;
                }
                then {
                  permit;
                }
              }
            }
          }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying Source NAT Rule Usage

Purpose   Verify that there is traffic matching the source NAT rule.

Action   From operational mode, enter the **show security nat source rule all** command. View the Translation hits field to check for traffic that matches the rule.

```
user@host> show security nat source rule all
source NAT rule: r1       Rule-set: sip-phones
  Rule-Id                     : 1
  Rule position               : 1
  From zone                   : private
  To zone                     : public
  Match
    Source addresses          : 0.0.0.0          - 255.255.255.255
    Destination port          : 0                - 0
  Action                      : interface
    Persistent NAT type       : N/A
    Persistent NAT mapping type : address-port-mapping
    Inactivity timeout        : 0
    Max session number        : 0
  Translation hits            : 0
    Successful sessions       : 0
    Failed sessions           : 0
  Number of sessions          : 0
```

Verifying Static NAT Configuration

Purpose   Verify that there is traffic matching the static NAT rule set.

Action   From operational mode, enter the **show security nat static rule r1** command. View the Translation hits field to check for traffic that matches the rule.

Verifying SIP ALG Status

Purpose   Verify that SIP ALG is enabled on your system.

Action   From operational mode, enter the **show security alg status** command.

```
user@host> show security alg status
ALG Status :
  DNS      : Enabled
  FTP      : Enabled
  H323     : Disabled
  MGCP     : Disabled
  MSRPC    : Enabled
  PPTP     : Enabled
  RSH      : Disabled
  RTSP     : Disabled
  SCCP     : Disabled
  SIP      : Enabled
  SQL      : Enabled
  SUNRPC   : Enabled
  TALK     : Enabled
  TFTP     : Enabled
  IKE-ESP  : Disabled
```

Related Documentation
- Verifying SIP ALG Configurations on page 303

Verifying SIP ALG Configurations

Supported Platforms   SRX Series, vSRX

- Verifying SIP ALG on page 303
- Verifying SIP ALG Calls on page 304
- Verifying SIP ALG Call Details on page 304
- Verifying SIP ALG Counters on page 305
- Verifying the Rate of SIP ALG Messages on page 306

Verifying SIP ALG

Supported Platforms   SRX Series, vSRX

Purpose   Verify SIP ALG verification options.

Action   From the CLI, enter the **show security alg sip ?** command.

```
user@host> show security alg sip ?
Possible completions:
  calls              Show SIP calls
  counters           Show SIP counters
  rate               Show SIP rate
```

Meaning   The output shows a list of all SIP verification parameters. Verify the following information:

- Calls—Lists all SIP calls.

- Counters—Provides counters of response codes for each SIP request method and error type.

- Rate—Provides speed and periodicity of SIP signaling messages.

Verifying SIP ALG Calls

Supported Platforms   SRX Series, vSRX

Purpose   Display information about active calls.

Action   From the J-Web interface, select **Monitor>ALGs>SIP>Calls**. Alternatively, from the CLI, enter the **show security alg sip calls** command.

```
user@host> show security alg sip calls
Total number of calls: 1
        Call ID: 47090a32@30.2.20.5
   Method: INVITE
```

Meaning   The output shows a list of all active SIP calls. Verify the User Agent Server (UAS) call ID and local and remote tags, and the state of the call.

Verifying SIP ALG Call Details

Supported Platforms   SRX Series, vSRX

Purpose   Display address and SDP about active calls.

Action   From the J-Web interface, select **Monitor>ALGs>SIP>Details**. Alternatively, from the CLI, enter the **show security alg sip calls detail** command.

```
user@host> show security alg sip calls detail
Total number of calls: 1
        Call ID    : 47090a32@30.2.20.5
Method    : INVITE
   State    : SETUP
   Group ID : 24575
```

Meaning   The output provides details about all active SIP calls. Verify the following information:

- The total number of calls, their ID and tag information, and state

- Remote group ID

- The IP addresses and port numbers and SDP connection and media details

Verifying SIP ALG Counters

Supported Platforms   SRX Series, vSRX

Purpose   Display information about SIP counters.

Action   From the J-Web interface, select **Monitor>ALGs>SIP>Counters**. Alternatively, from the
CLI, enter the **show security alg sip counters** command.

```
user@host> show security alg sip counters
Method        T        1xx       2xx       3xx       4xx       5xx       6xx
              RT        RT        RT        RT        RT        RT        RT
INVITE        4         4         3         0         0         0         0
              0         0         0         0         0         0         0
CANCEL        0         0         0         0         0         0         0
              0         0         0         0         0         0         0
ACK           3         0         0         0         0         0         0
              0         0         0         0         0         0         0
BYE           3         0         3         0         0         0         0
              0         0         0         0         0         0         0
REGISTER      7         0         7         0         0         0         0
              0         0         0         0         0         0         0
OPTIONS       0         0         0         0         0         0         0
              0         0         0         0         0         0         0
INFO          0         0         0         0         0         0         0
              0         0         0         0         0         0         0
MESSAGE       0         0         0         0         0         0         0
              0         0         0         0         0         0         0
NOTIFY        0         0         0         0         0         0         0
              0         0         0         0         0         0         0
PRACK         0         0         0         0         0         0         0
              0         0         0         0         0         0         0
PUBLISH       0         0         0         0         0         0         0
              0         0         0         0         0         0         0
REFER         0         0         0         0         0         0         0
              0         0         0         0         0         0         0
SUBSCRIBE     0         0         0         0         0         0         0
              0         0         0         0         0         0         0
UPDATE        0         0         0         0         0         0         0
              0         0         0         0         0         0         0
BENOTIFY      0         0         0         0         0         0         0
              0         0         0         0         0         0         0
SERVICE       0         0         0         0         0         0         0
              0         0         0         0         0         0         0
OTHER         0         0         0         0         0         0         0
              0         0         0         0         0         0         0
        SIP Error Counters
        ----------------------------
          Total Pkt-in                    :34
          Total Pkt dropped on error      :0
                Call error                      :0
          IP resolve error                :0
          NAT error                       :0
          Resource manager error          :0
          RR header exceeded max          :0
          Contact header exceeded max     :0
          Call Dropped due to limit       :0
          SIP stack error                 : 0
          SIP decode error                : 0
```

```
SIP unknown method error              : 0
 RTO message sent                     : 0
 RTO message received                 : 0
 RTO buffer allocation failure        : 0
 RTO buffer transmit failure          : 0
 RTO send processing error            : 0
  RTO receive processing error         : 0
 RTO receive invalid length           : 0
  RTO receive call process error        : 0
  RTO receive call allocation error     : 0
  RTO receive call register error       : 0
  RTO receive invalid status error      : 0
```

Meaning The output provides a count of all SIP response codes transmitted and received, and of SIP errors. Verify the following information:

- A count of transmissions of response codes for each SIP request method

- A count of all possible error types

Verifying the Rate of SIP ALG Messages

Supported Platforms SRX Series, vSRX

Purpose Display information about SIP message rate.

Action From the J-Web interface, select **Monitor>ALGs>SIP>Rate**. Alternatively, from the CLI, enter the **show security alg sip rate** command.

```
user@host> show security alg sip rate
CPU ticks per microseconds is 3735928559
    Time taken for the last message is 0 microseconds
    Total time taken for 0 messages is 0 microseconds(in less than 10 minutes)
    Rate: 3735928559 messages/second
```

Meaning The output provides information about CPU usage for messages, and speed and periodicity of SIP signaling messages. Verify the following information:

- CPU ticks per US

- Passage time for last message, for all messages, and the rate at which messages transit the network

Related Documentation
- SIP ALG Configuration Overview on page 248

- Example: Configuring Interface Source NAT for Incoming SIP Calls on page 268

- Decreasing Network Complexity by Configuring a Source NAT Pool for Incoming SIP Calls on page 274

- Example: Configuring Static NAT for Incoming SIP Calls on page 282

- Example: Configuring the SIP Proxy in the Private Zone and NAT in the Public Zone on page 289

- Example: Configuring a Three-Zone SIP ALG and NAT Scenario on page 296

PART 4

Configuration Statements and Operational Commands

Configuration Statements

address (Security Destination NAT)

Supported Platforms SRX Series, vSRX

Syntax
```
address <ip-address> {
    (port port-number | to ip-address);
}
```

Hierarchy Level [edit security nat destination pool pool-name]

Release Information Statement modified in Junos OS Release 9.6.

Description Specify a single address or an address range of the destination NAT pool.

Options
- *ip-address* —IP address of a pool.
- **port** *port-number*—Specify the port number.
- **to**—Specify the upper limit of the address range.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

alg

Supported Platforms   SRX Series, vSRX

Syntax
```
alg {
    alg-manager {
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    alg-support-lib {
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    dns {
        disable;
        doctoring (none | sanity-check);
        maximum-message-length number;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    ftp {
        allow-mismatch-ip-address;
        disable;
        ftps-extension;
        line-break-extension;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    h323 {
        application-screen {
            message-flood {
                gatekeeper {
                    threshold rate;
                }
            }
            unknown-message {
                permit-nat-applied;
                permit-routed;
            }
        }
        disable;
        dscp-rewrite {
            code-point string;
```

```
        }
        endpoint-registration-timeout value-in-seconds;
        media-source-port-any;
        traceoptions {
            flag flag <detail | extensive | terse>;
        }
    }
    ike-esp-nat {
        enable;
        esp-gate-timeout value-in-seconds;
        esp-session-timeout value-in-seconds;
        state-timeout value-in-seconds;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    mgcp {
        application-screen {
            connection-flood {
                threshold rate;
            }
            message-flood {
                threshold rate;
            }
            unknown-message {
                permit-nat-applied;
                permit-routed;
            }
        }
        disable;
        dscp-rewrite {
            code-point string;
        }
        inactive-media-timeout value-in-seconds;
        maximum-call-duration value-in-minutes;
        traceoptions {
            flag flag <extensive>;
        }
        transaction-timeout value-in-seconds;
    }
    msrpc {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    pptp {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
```

```
              }
            }
            real {
              disable;
              traceoptions {
                flag {
                  all <extensive>;
                }
              }
            }
            rsh {
              disable;
              traceoptions {
                flag {
                  all <extensive>;
                }
              }
            }
            rtsp {
              disable;
              traceoptions {
                flag {
                  all <extensive>;
                }
              }
            }
            sccp {
              application-screen {
                call-flood {
                  threshold rate;
                }
                unknown-message {
                  permit-nat-applied;
                  permit-routed;
                }
              }
              disable;
              dscp-rewrite {
                code-point string;
              }
              inactive-media-timeout value-in-seconds;
              traceoptions {
                flag flag <extensive>;
              }
            }
            sip {
              application-screen {
                protect {
                  deny {
                    all {
                      timeout value-in-seconds;
                    }
                    destination-ip address;
                    timeout value-in-seconds;
                  }
                }
```

```
            unknown-message {
                permit-nat-applied;
                permit-routed;
            }
        }
        c-timeout value-in-minutes;
        disable;
        dscp-rewrite {
            code-point string;
        }
        inactive-media-timeout value-in-seconds;
        maximum-call-duration value-in-minutes;
        retain-hold-resource;
        t1-interval value-in-milliseconds;
        t4-interval value-in-seconds;
        traceoptions {
            flag flag <detail | extensive | terse>;
        }
    }
    sql {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    sunrpc {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    talk {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    tftp {
        disable;
        traceoptions {
            flag {
                all <extensive>;
            }
        }
    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
```

```
              (no-world-readable | world-readable);
              size maximum-file-size;
            }
            level (brief | detail | extensive | verbose);
            no-remote-trace;
        }
    }
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure an Application Layer Gateway (ALG) on the device. An ALG runs as a service and can be associated in policies with specified types of traffic. ALGs are enabled by default.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

alg (Applications)

Supported Platforms   SRX Series, vSRX

Syntax   alg *application*;

Hierarchy Level   [edit applications application *application-name* <term *term-name*>]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Define individual Application Layer Gateway (ALG).

Options   *application* —Name of the application. The following protocols are supported:

- **dns** —Domain Name Service
- **ftp** —File Transfer Protocol
- **http** —Hypertext Transfer Protocol
- **https** —Hypertext Transfer Protocol
- **ignore**—Ignore application type
- **ike-esp-nat** —IKE ESP NAT application protocol
- **mgcp-ca** —Media Gateway Control Protocol with Call Agent
- **mgcp-ua** —MGCP with User Agent
- **ms-rpc** —Microsoft RPC
- **pptp** —Point-to-Point Tunneling Protocol
- **q931** —ISDN connection control protocol (Q.931)
- **ras** —Remote Access Service
- **realaudio** —RealAudio
- **rsh** —UNIX remote shell services
- **rtsp** —Real-Time Streaming Protocol
- **sccp** —Skinny Client Control Protocol
- **sip**—Session Initiation Protocol
- **smtp** —Simple Mail Transfer Protocol
- **sqlnet-v2** —Oracle SQLNET v2
- **ssh** —Secure Shell Protocol
- **sun-rpc** —Sun Microsystems RPC
- **talk**—TALK program
- **telnet** —Telnet Protocol
- **tftp** —Trivial File Transfer Protocol

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	• term (Applications) on page 384

alg-manager

Supported Platforms	SRX Series, vSRX
Syntax	```alg-manager {` ` traceoptions {` ` flag {` ` all <extensive>;` ` }` ` }` `}```
Hierarchy Level	[edit security alg]
Description	Configure the Application Layer Gateway (ALG) manager.
Options	The remaining statements are explained separately. See CLI Explorer.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• traceoptions (Security ALG) on page 386

allow-dns-reply

Supported Platforms	SRX Series, vSRX
Syntax	allow-dns-reply;
Hierarchy Level	[edit security flow]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Allow an incoming Domain Name Service (DNS) reply packet without a matched request. By default, if an incoming UDP first-packet has dst-port 53, the device checks the DNS message packet header to verify that the query bit (QR) is 0, which denotes a query message. If the QR bit is 1, which denotes a response message, the device drops the packet, does not create a session, and increments the illegal packet flow counter for the interface. Using the **allow-dns-reply** statement directs the device to skip the check.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• *Juniper Networks Devices Processing Overview*

application (Security Policies)

Supported Platforms   SRX Series, vSRX

Syntax
```
application {
    [application];
    any;
}
```

Hierarchy Level   [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify the IP or remote procedure call (RPC) application or set of applications to be used as match criteria.

Options   *application-name-or-set*—Name of the predefined or custom application or application set used as match criteria.

any—Any predefined or custom applications or application sets.

> *i* NOTE: A custom application that does not use a well-known destination port for the application will not be included in the any option, and must be named explicitly.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation   • *Security Policies Overview*

application-protocol (Applications)

Supported Platforms SRX Series, vSRX

Syntax application-protocol (dns | ftp | http | https | ignore | ike-esp-nat | mgcp-ca | mgcp-ua | ms-rpc | pptp | q931 | ras | realaudio | rsh | rtsp | sccp | sip | smtp | sqlnet-v2 | ssh | sun-rpc | talk | telnet | tftp);

Hierarchy Level [edit applications application *application-name*]

Release Information Statement modified in Junos OS Release 8.5. The **ike-esp-nat** option introduced in Junos OS Release 10.2.

Description Identify the application protocol name. The following protocols are supported:

- **dns** —Domain Name Service

- **ftp** —File Transfer Protocol

- **http** —Hypertext Transfer Protocol

- **https** —Hypertext Transfer Protocol

- **ignore** —Ignore application type

- **ike-esp-nat** —IKE ESP NAT application protocol

- **mgcp-ca** —Media Gateway Control Protocol with Call Agent

- **mgcp-ua** —MGCP with User Agent

- **ms-rpc** —Microsoft RPC

- **pptp** —Point-to-Point Tunneling Protocol

- **q931** —ISDN connection control protocol (Q.931)

- **ras** —Remote Access Service

- **realaudio** —RealAudio

- **rsh** —UNIX remote shell services

- **rtsp**—Real-Time Streaming Protocol

- **sccp** —Skinny Client Control Protocol

- **sip**—Session Initiation Protocol

- **smtp** —Simple Mail Transfer Protocol

- **sqlnet-v2** —Oracle SQLNET v2

- **ssh** —Secure Shell Protocol

- **sun-rpc** —Sun Microsystems RPC

- **talk**—TALK program

- **telnet** —Telnet Protocol

- **tftp** —Trivial File Transfer Protocol

Required Privilege Level   system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation   • *Policy Application Sets Overview*

application-screen (Security H323)

Supported Platforms   SRX Series

Syntax
```
application-screen {
    message-flood {
        gatekeeper {
            threshold rate;
        }
    }
    unknown-message {
        permit-nat-applied;
        permit-routed;
    }
}
```

Hierarchy Level   [edit security alg h323]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure the security screens for the H.323 protocol Application Layer Gateway (ALG).

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation   • h323 on page 344

application-screen (Security MGCP)

Supported Platforms SRX Series, vSRX

Syntax

```
application-screen {
    connection-flood {
        threshold rate;
    }
    message-flood {
        threshold rate;
    }
    unknown-message {
        permit-nat-applied;
        permit-routed;
    }
}
```

Hierarchy Level [edit security alg mgcp]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure the security screens for the Media Gateway Control Protocol (MGCP) Application Layer Gateway (ALG).

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- mgcp on page 354

application-screen (Security SCCP)

Supported Platforms	SRX Series, vSRX

Syntax

```
application-screen {
    call-flood {
        threshold rate;
    }
    unknown-message {
        permit-nat-applied;
        permit-routed;
    }
}
```

Hierarchy Level   [edit security alg sccp]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure the security screens for the Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG).

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related
Documentation
- sccp on page 370

application-screen (Security SIP)

Supported Platforms   SRX Series, vSRX

Syntax
```
application-screen {
    protect {
        deny {
            all {
                timeout value-in-seconds;
            }
            destination-ip address;
            timeout value-in-seconds;
        }
    }
    unknown-message {
        permit-nat-applied;
        permit-routed;
    }
}
```

Hierarchy Level   [edit security alg sip]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure the security screens for the Session Initiation Protocol (SIP) Application Layer Gateway (ALG).

> **NOTE:** IPv6 is supported on the SIP ALG along with Network Address Translation Protocol Translation (NAT-PT) mode and NAT64 address translation.
>
> The type of the <destination-ip-address> is changed from IPv4 address to IP prefix to support all kinds of IP addresses, and correspondingly a prefix is supported to allow multiple IP addresses.

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation   • sip (Security) on page 373

alg-support-lib

Syntax
```
alg-support-lib {
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg-support-lib]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configures the Application Layer Gateway (ALG) support library.

Options The remaining statements are explained separately.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

banner (Access FTP HTTP Telnet Authentication)

Supported Platforms SRX Series, vSRX

Syntax
```
banner {
    fail string;
    login string;
    success string;
}
```

Hierarchy Level [edit access firewall-authentication pass-through (ftp | http | telnet)]

Release Information Statement introduced in Junos OS Release 8.5.
HTTPS for Web authentication is supported on high-end SRX Series Services Gateways from Junos OS Release 12.1X44-D10 and on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways from Junos OS Release 15.1X49-D40.

Description Configure the banners that appear to users during the FTP, HTTP, HTTPS, and Telnet firewall authentication process. The banners appear during login, after successful authentication, and after failed authentication.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation
- *Understanding Firewall Authentication Banner Customization*

call-flood

Supported Platforms	SRX Series, vSRX

Syntax	call-flood {
	    threshold *rate*;
	}

Hierarchy Level	[edit security alg sccp application-screen]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Limit the number of calls per second allowed to Skinny Client Control Protocol (SCCP) client. Calls exceeding the threshold are dropped by the SCCP Application Layer Gateway (ALG).
Options	**threshold** *rate*—Number of calls per second per client. **Range:** 2 through 1000 **Default:** 20
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• sccp on page 370

c-timeout

Supported Platforms	SRX Series, vSRX
Syntax	c-timeout *value-in-minutes*;
Hierarchy Level	[edit security alg sip]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the timeout interval for Session Initiation Protocol (SIP) transactions in minutes.
Options	*value-in-minutes*—Timeout interval. **Range:** 3 through 10 minutes **Default:** 3 minutes
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• sip (Security) on page 373

deny (Security SIP)

Supported Platforms   SRX Series, vSRX

Syntax
```
deny {
    all {
        timeout value-in-seconds;
    }
    destination-ip address;
    timeout value-in-seconds;
}
```

Hierarchy Level   [edit security alg sip application-screen protect]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Protect servers against INVITE attacks.

Options
- **all**—Configure the Session Initiation Protocol (SIP) application screen to protect servers at all destination IP addresses against INVITE attacks.

- **destination-ip** *address*—Configure the SIP application screen to protect the server at this destination IP address against INVITE attacks. You can include up to 16 destination IP addresses of servers to be protected. Enabling this option disables the all option.

- **timeout** *value-in-seconds*—Amount of time (in *seconds*) to make an attack table entry for each INVITE, which is listed in the application screen.

Range: 1 through 3600 seconds
Default: 5 seconds

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- sip (Security) on page 373

destination-address (Security Destination NAT)

Supported Platforms   SRX Series, vSRX

Syntax   destination-address <*ip-address*>;

Hierarchy Level   [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

Release Information   Statement modified in Junos OS Release 9.6.

Description   Specify a destination address to match the rule. You can configure one address or a subnet.

> **NOTE:**
>
> - If the destination address is IPv4 and the pool is an IPv6 prefix, the length of the IPv6 prefix must be 96.
>
> - If the destination address is an IPv6 prefix and the pool is an IPv6 prefix, their length must be the same.

Options   *ip-address*— Destination address or a subnet.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

destination-address (Security Policies)

Supported Platforms	SRX Series, vSRX

Syntax	destination-address {
	  [*address*];
	  any;
	  any-ipv4;
	  any-ipv6;
	}

Hierarchy Level	[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match] [edit security policies global policy *policy-name* match]
Release Information	Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1.
Description	Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.
Options	*address*—IP address (**any**, **any-ipv4**, **any-ipv6**), IP address set, or address book entry, or wildcard address (represented as A.B.C.D/wildcard-mask). You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• *Security Policies Overview*

destination-address (Security Source NAT)

Supported Platforms	SRX Series, vSRX
Syntax	destination-address <*ip-address*>;
Hierarchy Level	[edit security nat source rule-set *rule-set-name* rule *rule-name* match]
Release Information	Statement modified in Junos OS Release 9.6.
Description	Specify a destination address to match the rule. You can configure multiple addresses or subnets.
Options	*ip-address*—Destination address or a subnet.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

destination-address (Security Static NAT)

Supported Platforms	SRX Series, vSRX
Syntax	destination-address <*ip-address*>;
Hierarchy Level	[edit security nat static rule-set *rule-set-name* rule *rule-name* match]
Release Information	Statement modified in Junos OS Release 9.6.
Description	Specify a destination address to match the rule. You can configure one address or a subnet.
Options	*ip-address*—Destination address or a subnet.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

destination-nat

Supported Platforms	SRX Series, vSRX
Syntax	destination-nat (off	pool *pool-name*	rule-session-count-alarm (clear-threshold *value* | raise-threshold *value*));
Hierarchy Level	[edit security nat destination rule-set *rule-set-name* rule *rule-name* then]
Release Information	Statement modified in Junos OS Release 9.6. The **rule-session-count-alarm** option added in Junos OS Release 12.1X45-D10.
Description	Specify the action of the destination NAT rule.
Options	**off**—Do not perform destination NAT operation.
	pool—Use user-defined destination NAT pool to perform destination NAT.
	rule-session-count-alarm—Define session count alarm thresholds for a specific destination NAT rule. When the session count exceeds the upper (raise) threshold or falls below the lower (clear) threshold, an SNMP trap is triggered.

> **NOTE:** If you enter a value for **raise-threshold** but not for **clear-threshold**, **clear-threshold** is automatically set to 80 percent of raise-threshold.

Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.

destination-port (Applications)

Supported Platforms   SRX Series, vSRX

Syntax   destination-port *port-identifier*;

Hierarchy Level   [edit applications application *application-name*],
[edit applications application *application-name* term *term-name*]

Release Information   Statement modified in Junos OS Release 8.5.

Description   Specify a TCP or UDP destination port number.

Options   *port-identifier* —Range of ports. You can use a numeric value or one of the text synonyms listed in Table 14 on page 332.

Table 14: Port Supported by Services Interfaces

Port Name	Corresponding Port Number
afs	1483
bgp	179
biff	512
bootpc	68
bootps	67
cmd	514
cvspserver	2401
dhcp	67
domain	53
eklogin	2105
ekshell	2106
excc	512
finger	79
ftp	21
ftp-data	20
http	80
https	443
ident	113
imap	143
kerberos-sec	88
klogin	543
kpasswd	761
krb-prop	754
krbupdate	760

Table 14: Port Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
kshell	544
ldap	389
ldp	646
login	513
mobileip-agent	434
mobilip-mn	435
msdp	639
netbios-dgm	138
netbios-ns	137
netbios-ssn	139
nfsd	2049
nntp	119
ntalk	518
ntp	123
pop3	110
pptp	1723
printer	515
radacct	1813
radius	1812
rip	520
rkinit	2108
smtp	25
snmp	161
snmp-trap	162

Table 14: Port Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
snpp	444
socks	1080
ssh	22
sunrpc	111
syslog	514
tacacs	49
tacacs-ds	65
talk	517
telnet	23
tftp	69
timed	525
who	513
xdmcp	177

Required Privilege Level   system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation   • *Policy Application Sets Overview*

dns

Supported Platforms	SRX Series, vSRX

Syntax

```
dns {
    disable;
    doctoring (none | sanity-check);
    maximum-message-length number;
    oversize-message-drop
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the Domain Name System (DNS) Application Layer Gateway (ALG) on the device.

Options
- **disable**—Disable the DNS ALG. By default, the DNS ALG is enabled. This option will enable or disable the DNS ALG for both IPv4 and IPv6 mode.

- **doctoring**—Configure DNS ALG doctoring.

    - **none**— Disable all DNS ALG doctoring.

    - **sanity-check**—Perform only DNS ALG sanity checks.

- **maximum-message-length**—A limit imposed on the size of individual DNS messages.

- **oversize-message-drop**—Configure to drop the oversized DNS packets.

- **traceoptions**— Configure SQL ALG tracing options.

    - **flag**—Trace operation to perform.

        - **all**—Trace all events.

        - *extensive*—Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *DNS Overview*

dns (System Services)

Supported Platforms   SRX Series, vSRX

Syntax
```
dns {
    dns-proxy {
        cache hostname inet ip-address;
        default-domain domain-name {
            forwarders ip-address;
        }
        interface interface-name;
        propogate-setting (enable | disable);
        view view-name {
            domain domain-name {
                forward-only;
                forwarders ip-address;
            }
            match-clients subnet-address;
        }
    }
}
dnssec {
    disable;
    dlv {
        domain-name domain-name trusted-anchor  trusted-anchor;
    }
secure-domains domain-name;
    trusted-keys (key dns-key | load-key-file url);
forwarders {
    ip-address;
}
max-cache-ttl seconds;
max-ncache-ttl seconds;
traceoptions {
    category {
        category-type;
    }
    debug-level level;
    file {
        filename;
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
    }
}
```

Hierarchy Level   [edit system services]

Release Information   Statement introduced in Junos OS Release 10.2.

Description   Configure the DNS server.

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege   system—To view this statement in the configuration.
Level   system-control—To add this statement to the configuration.

Related   • *DNS Overview*
Documentation

dscp-rewrite

Supported Platforms   SRX Series, vSRX

Syntax   dscp-rewrite {
            code-point *6 bit patterns*;
        }

Hierarchy Level   [edit security alg sip]
            [edit security alg h323]
            [edit security alg mgcp]
            [edit security alg sccp]

Release Information   Statement introduced in Junos OS Release 10.4.

Description   Specify a rewrite-rule for the traffic that passes through a voice over IP Application Layer
            Gateway (VoIP ALG).

Options   **6-bit patterns**—Value of the code point in binary form.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related   • Understanding VoIP DSCP Rewrite Rules on page 143
Documentation

endpoint-registration-timeout

Supported Platforms	SRX Series, vSRX
Syntax	endpoint-registration-timeout *value-in-seconds*;
Hierarchy Level	[edit security alg h323]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the timeout value in seconds for entries in the NAT table.
Options	*value-in-seconds*—Timeout value. **Range:** 10 through 50,000 seconds **Default:** 3600 seconds
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• h323 on page 344

family inet (Interfaces)

Supported Platforms   SRX Series, vSRX

Syntax
```
inet {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
    address (source–address/prefix) {
        arp destination-address {
            (mac mac-address | multicast-mac multicast-mac-address);
            publish publish-address;
        }
        broadcast address;
        preferred;
        primary;
        vrrp-group group-id {
            (accept-data | no-accept-data);
            advertise-interval seconds;
            advertisements-threshold number;
            authentication-key key-value;
            authentication-type (md5 | simple);
            fast-interval milliseconds;
            inet6-advertise-interval milliseconds
            (preempt <hold-time seconds> | no-preempt );
            priority value;
            track {
                interface interface-name {
                    bandwidth-threshold bandwidth;
                    priority-cost value;
                }
                priority-hold-time seconds;
                route route-address{
                    routing-instance routing-instance;
                    priority-cost value;
                }
            }
            virtual-address [address];
            virtual-link-local-address address;
            vrrp-inherit-from {
                active-group value;
                active-interface interface-name;
            }
        }
        web-authentication {
            http;
            https;
            redirect-to-https;
        }
    }
    dhcp {
```

```
                              client-identifier {
                                 (ascii string | hexadecimal string);
                              }
                              lease-time (length | infinite);
                              retransmission-attempt value;
                              retransmission-interval seconds;
                              server-address server-address;
                              update-server;
                              vendor-id vendor-id ;
                           }
                           dhcp-client {
                              client-identifier {
                                 prefix {
                                    host-name;
                                    logical-system-name;
                                    routing-instance-name;
                                 }
                                 use-interface-description (device | logical);
                                 user-id (ascii string| hexadecimal string);
                              }
                              lease-time (length | infinite);
                              retransmission-attempt value;
                              retransmission-interval seconds;
                              server-address server-address;
                              update-server;
                              vendor-id vendor-id ;
                           }
                           filter {
                              group number;
                              input filter-name;
                              input-list [filter-name];
                              output filter-name;
                              output-list [filter-name];
                           }
                           mtu value;
                           no-neighbor-learn;
                           no-redirects;
                           policer {
                              arp arp-name;
                              input input-name;
                              output output-name;
                           }
                           primary;
                           rpf-check {
                              fail-filter filter-name;
                              mode {
                                 loose;
                              }
                           }
                           sampling {
                              input;
                              output;
                              simple-filter;
                           }
                           targeted-broadcast {
                              (forward-and-send-to-re |forward-only);
```

```
    }
  unnumbered-address {
    interface-name;
    preferred-source-address preferred-source-address;
  }
}
```

Hierarchy Level   [edit interfaces *interface* unit *unit*]

Release Information   Statement supported in Junos 10.2 for SRX Series devices.

Description   Assign an IP address to a logical interface.

Options   *ipaddress*—Specify the IP address for the interface. The remaining statements are explained separately.

> ⓘ **NOTE:** You use family **inet** to assign an IPv4 address. You use family **inet6** to assign an IPv6 address. An interface can be configured with both an IPv4 and IPv6 address.

Required Privilege Level   **interface**—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation   • *Understanding Interfaces*

ftp (Access)

Supported Platforms   SRX Series, vSRX

Syntax
```
ftp {
  banner {
    fail string;
    login string;
    success string;
  }
}
```

Hierarchy Level   [edit access firewall-authentication pass-through]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure banners for the FTP login prompt, successful authentication, and failed authentication.

Options   The remaining statements are explained separately.

Required Privilege Level   **access**—To view this statement in the configuration.
access-control—To add this statement to the configuration.

ftp (Security ALG)

Supported Platforms SRX Series, vSRX

Syntax
```
ftp {
    allow-mismatch-ip-address;
    disable;
    ftps-extension;
    line-break-extension;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Junos OS Release 11.4.

Description Specify the FTP ALG on the device.

Options
- **disable**—Disable the FTP ALG. By default, the FTP ALG is enabled. This option will enable or disable FTP ALG for both IPV4 and IPV6 mode.

- **ftps-extension**—Enable secure FTP and FTP SSL protocols.

- **line-break-extension**—Enable line-break-extension. This option will enable the FTP ALG to recognize the LF as line break in addition to the standard CR+LF (carriage return, followed by line feed).

- **traceoptions**—Configure FTP ALG tracing options. To specify more than one trace operation, include multiple flag statements.

  - **flag**—Trace operation to perform.

    - **all**—Trace all events.

    - **extensive**—(Optional) Display extensive amount of data.

Required Privilege
Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related
Documentation

- FTP ALG Overview on page 25

gatekeeper

Supported Platforms SRX Series, vSRX

Syntax
```
gatekeeper {
    threshold rate;
}
```

Hierarchy Level [edit security alg h323 application-screen message-flood]

Release Information Statement introduced in Junos OS Release 8.5.

Description Limit the rate at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped.

Options threshold *rate*—Threshold measured in messages per second.

Range: 1 through 50,000

Default: 1000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- h323 on page 344

h323

Supported Platforms   SRX Series

Syntax
```
h323 {
    application-screen {
        message-flood {
            gatekeeper {
                threshold rate;
            }
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    disable;
    dscp-rewrite {
        code-point string;
    }
    endpoint-registration-timeout value-in-seconds;
    media-source-port-any;
    traceoptions {
        flag flag <detail | extensive | terse>;
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify the H.323 Application Layer Gateway (ALG) on the device. H.323 is a control-signaling protocol used to exchange messages between H.323 endpoints.

Options   disable—Disable the H.323 ALG. By default, H.323 ALG is enabled.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- application-screen (Security H323) on page 321
- endpoint-registration-timeout on page 338
- dscp-rewrite on page 337

host-inbound-traffic

Supported Platforms SRX Series, vSRX

Syntax

```
host-inbound-traffic {
    protocols protocol-name {
        except;
    }
    system-services service-name {
        except;
    }
}
```

Hierarchy Level [edit security zones functional-zone management],
[edit security zones functional-zone management interfaces *interface-name*],
[edit security zones security-zone *zone-name*],
[edit security zones security-zone *zone-name* interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 8.5.

Description Control the type of traffic that can reach the device from interfaces bound to the zone.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Understanding How to Control Inbound Traffic Based on Traffic Types*
- *Understanding How to Control Inbound Traffic Based on Protocols*

ike-esp-nat

Supported Platforms   SRX Series, vSRX

Syntax
```
ike-esp-nat {
    enable;
    esp-gate-timeout seconds;
    esp-session-timeout seconds;
    state-timeout seconds;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure Application Layer Gateway (ALG) for Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) traffic with Network Address Translation (NAT).

Options
- **Enable** —Enable the IKE-ESP ALG.

- **esp-gate-timeout** *seconds*—Set the timeout for the ESP gates created after an IKE Phase 2 exchange has completed.

  Range: 2 through 30 seconds.

  Default: 5 seconds.

- **esp-session-timeout** *seconds*—Set the idle timeout for the ESP sessions created from the IPsec gates.

  Range: 60 through 2400 seconds.

  Default: 1800 seconds.

- **state-timeout** *seconds*—Set the timeout for the ALG state information.

  Range: 180 through 86,400 seconds.

  Default: 14,400 seconds.

- **traceoptions**—Set the IKE-ESP ALG trace options.

  - **flag** —Specify which tracing operation to perform.

    - **all**—Trace all operations.

      - **extensive**—Set trace verbosity level to extensive.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

ike (Security)

Supported Platforms   SRX Series, vSRX

Syntax
```
ike {
    gateway gateway-name {
        address [ip-address-or-hostname];
        advpn {
            suggester {
                disable;
            }
            partner {
                connection-limit <number>;
                idle-threshold <packets/sec>;
                idle-time <seconds>;
                disable;
            }
        }
        dead-peer-detection {
            (always-send | optimized | probe-idle-tunnel);
            interval seconds;
            threshold number;
        }
        dynamic {
            connections-limit number;
            (distinguished-name <container container-string> <wildcard wildcard-string> |
                hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname
                e-mail-address);
            ike-user-type (group-ike-id | shared-ike-id);
        }
        external-interface external-interface-name;
        fragmentation {
            enable:
            size bytes;
        }
        general-ikeid;
        ike-policy policy-name;
        local-address (ipv4-address | ipv6-address);
        local-identity {
            (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address |
                user-at-hostname e-mail-address);
        }
        nat-keepalive seconds;
        no-nat-traversal;
        remote-identity {
            (distinguished-name <container container-string> <wildcard wildcard-string> |
                hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname
                e-mail-address);
        }
        version (v1-only | v2-only);
        xauth {
            access-profile profile-name;
        }
    }
    policy policy-name {
```

```
            certificate {
               local-certificate certificate-id;
               peer-certificate-type (pkcs7 | x509-signature);
               policy-oids [ oid ];
            }
            description description;
            mode (aggressive | main);
            pre-shared-key (ascii-text key | hexadecimal key);
            proposal-set (basic | compatible | standard |suiteb-gcm-128 | suiteb-gcm-256);
            proposals [proposal-name];
            reauth-frequency number;
         }
         proposal proposal-name {
            authentication-algorithm (md5 | sha-256 | sha-384| sha1);
            authentication-method (dsa-signatures | ecdsa-signatures-256 | ecdsa-signatures-384
               | pre-shared-keys | rsa-signatures);
            description description;
            dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);
            encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
            lifetime-seconds seconds;
         }
         respond-bad-spi <max-responses>;
         traceoptions {
            file {
               filename;
               files number;
               match regular-expression;
               size maximum-file-size;
               (world-readable | no-world-readable);
            }
            flag flag;
            no-remote-trace;
            rate-limit messages-per-second;
         }
      }
```

Hierarchy Level	[edit security]
Release Information	Statement modified in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 11.1. The **inet6** option added in Junos OS Release 11.1.
Description	Define Internet Key Exchange (IKE) configuration.
Options	The remaining statements are explained separately. See CLI Explorer.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• *IPsec VPN Overview* • ALG Overview on page 3 • *Understanding Logical Systems for SRX Series Services Gateways*

inactive-media-timeout (Security MGCP)

Supported Platforms	SRX Series, vSRX
Syntax	inactive-media-timeout *value-in-seconds*;
Hierarchy Level	[edit security alg mgcp]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.
Options	*value-in-seconds*—Maximum amount of time that the pinholes remain open.
	Range: 10 through 2550 seconds
	Default: 120 seconds
Required Privilege Level	security—To view this statement in the configuration.
	security-control—To add this statement to the configuration.
Related Documentation	• mgcp on page 354

inactive-media-timeout (Security SCCP)

Supported Platforms	SRX Series, vSRX
Syntax	inactive-media-timeout *value-in-seconds*;
Hierarchy Level	[edit security alg sccp]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.
Options	*value-in-seconds*—Maximum amount of time that the pinholes remain open.
	Range: 10 through 600 seconds
	Default: 120 seconds
Required Privilege Level	security—To view this statement in the configuration.
	security-control—To add this statement to the configuration.
Related Documentation	• sccp on page 370

inactive-media-timeout (Security SIP)

Supported Platforms	SRX Series, vSRX
Syntax	inactive-media-timeout *value-in-seconds*;
Hierarchy Level	[edit security alg sip]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the maximum amount of time that the temporary openings in the firewall (pinholes) remain open for media if no activity is detected.
Options	*value-in-seconds*—Maximum amount of time that the pinholes remain open. **Range:** 0 through 2550 seconds **Default:** 120 seconds
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• sip (Security) on page 373

map-entry-timeout

Supported Platforms	SRX Series, vSRX
Syntax	map-entry-timeout *map-entry-timeout*;
Hierarchy Level	[edit security alg msrpc] [edit security alg sunrpc]
Release Information	Statement introduced in Junos OS Release 12.3X48-D10.
Description	Configure the mapping entry timeout value. When the incoming traffic hits the mapping entry, the timeout value has been reset to configured value. The mapping entry is removed from the table when the timeout value expires. The lifetime of the mapping entry is global and applies to all entries in the table.
Options	*map-entry-timeout*—Specify the Microsoft remote procedure call Application Layer Gateway (MS-RPC ALG) or Sun RPC ALG mapping entry timeout value in hours. **Range:** 1 through 72 hours. **Default:** 32 hours.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• msrpc on page 355 • sunrpc on page 379

maximum-call-duration (Security)

Supported Platforms	SRX Series, vSRX

Syntax

maximum-call-duration *value-in-minutes*;

Hierarchy Level

[edit security alg mgcp],
[edit security alg sip]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the time at which the SIP call ends. The media session is released after the call has ended.

Options

value-in-minutes—Maximum amount of time at which the call ends and releases the media sessions.

Range: 3 through 720 minutes

Default: 720 minutes

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- mgcp on page 354
- sip (Security) on page 373

maximum-message-length

Supported Platforms	SRX Series, vSRX

Syntax

maximum-message-length *number*;

Hierarchy Level

[edit security alg dns]

Release Information

Statement introduced in Junos OS Release 10.1.

Description

Specify the maximum DNS message length.

Options

number—Maximum length in bytes of a single DNS message.

Range: 512 through 8192 bytes.

Default: 512 bytes.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- dns on page 335

media-source-port-any

Supported Platforms	SRX Series, vSRX
Syntax	media-source-port-any;
Hierarchy Level	[edit security alg h323]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Allow media traffic from any port number. By default, this feature is disabled, which allows a temporary opening in the firewall (pinhole) for media traffic to be opened.
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• h323 on page 344

message-flood (Security H323)

Supported Platforms	SRX Series

Syntax	message-flood {
	  gatekeeper {
	    threshold *rate*;
	  }
	}

Hierarchy Level	[edit security alg h323 application-screen]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Limit the rate per second at which remote access server (RAS) requests to the gatekeeper are processed. Messages exceeding the threshold are dropped. This feature is disabled by default.
Options	**gatekeeper threshold *rate***—Maximum number of RAS connection requests per second allowed per gateway. **Range:** 1 through 65,535 **Default:** 1000
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• h323 on page 344

mgcp

Supported Platforms	SRX Series, vSRX

Syntax

```
mgcp {
    application-screen {
        connection-flood {
            threshold rate;
        }
        message-flood {
            threshold rate;
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    disable;
    dscp-rewrite {
        code-point string;
    }
    inactive-media-timeout value-in-seconds;
    maximum-call-duration value-in-minutes;
    traceoptions {
        flag flag <extensive>;
    }
    transaction-timeout value-in-seconds;
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Junos OS Release 9.2.

Description Specify the Media Gateway Control Protocol (MGCP) ALG on the device. MGCP is a text-based Application Layer protocol that can be used for call setup and call control.

Options disable—Disable the MGCP ALG. By default, the MGCP ALG is enabled.

> *i* NOTE: By default, the MGCP ALG is disabled for SRX Series devices.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding the MGCP ALG on page 183

msrpc

Supported Platforms   SRX Series, vSRX

Syntax
```
msrpc {
    disable;
    map-entry-timeout map-entry-timeout;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 9.0.

Description   Specify the Microsoft remote procedure call Application Layer Gateway (MS-RPC ALG) on the device.

Options
- **disable**—Disable the MS-RPC ALG. By default, the MS-RPC ALG is enabled.

- **map-entry-timeout** *map-entry-timeout*—Specify the MS-RPC ALG mapping entry timeout value in hours.

  Range: 1 through 72 hours.

  Default: 32 hours.

- **traceoptions**—Configure MS-RPC ALG tracing options.

  - **flag**—Trace operation to perform.

    - **all**—Trace all events.

    - *extensive*—Display extensive amount of data.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding Microsoft RPC ALGs on page 67

nat

Supported Platforms   SRX Series, vSRX

Syntax
```
nat {
    destination {
        pool pool-name {
            address ip-address {
                (port port-number | to ip-address);
            }
            description text;
            routing-instance routing-instance-name;
        }
        rule-set rule-set-name {
            description text;
            from {
                interface [interface-name];
                routing-instance [routing-instance-name];
                zone [zone-name];
            }
            rule rule-name {
                description text;
                match {
                    (destination-address <ip-address> | destination-address-name <address-name>);
                    destination-port port-number;
                    protocol [protocol-name-or-number];
                    source-address [ip-address];
                    source-address-name [address-name];
                }
                then {
                    destination-nat (off | pool pool-name);
                }
            }
        }
    }
    proxy-arp {
        interface interface-name {
            address ip-address {
                to ip-address;
            }
        }
    }
    proxy-ndp {
        interface interface-name {
            address ip-address {
                to ip-address;
            }
        }
    }
    source {
        address-persistent;
        interface {
            port-overloading {
                off;
            }
```

```
                              }
                              pool pool-name {
                                 address ip-address {
                                    to ip-address;
                                 }
                                 description text;
                                 host-address-base ip-address;
                                 overflow-pool (interface | pool-name);
                                 port {
                                    (no-translation | port-overloading-factor number | range port-low <to port-high>);
                                 }
                                 routing-instance routing-instance-name;
                              }
                              pool-default-port-range lower-port-range to upper-port-range;
                              pool-utilization-alarm {
                                 clear-threshold value;
                                 raise-threshold value;
                              }
                              port-randomization {
                                 disable;
                              }
                              port-round-robin {
                                 disable;
                              }
                              rule-set rule-set-name {
                                 description text;
                                 from {
                                    interface [interface-name];
                                    routing-instance [routing-instance-name];
                                    zone [zone-name];
                                 }
                                 rule rule-name {
                                    description text;
                                    match {
                                       (destination-address <ip-address> | destination-address-name <address-name>);
                                       destination-port port-number;
                                       protocol [protocol-name-or-number];
                                       source-address [ip-address];
                                       source-address-name [address-name];
                                    }
                                    then {
                                       source-nat {
                                          interface {
                                             persistent-nat {
                                                address-mapping;
                                                inactivity-timeout seconds;
                                                max-session-number value;
                                                permit (any-remote-host | target-host | target-host-port);
                                             }
                                          }
                                          off;
                                          pool {
                                             persistent-nat {
                                                address-mapping;
                                                inactivity-timeout seconds;
                                                max-session-number number;
```

```
                                permit (any-remote-host | target-host | target-host-port);
                            }
                            pool-name;
                        }
                    }
                }
            }
            to {
                interface [interface-name];
                routing-instance [routing-instance-name];
                zone [zone-name];
            }
        }
    }
    static {
        rule-set rule-set-name {
            description text;
            from {
                interface [interface-name];
                routing-instance [routing-instance-name];
                zone [zone-name];
            }
            rule rule-name {
                description text;
                match {
                    (destination-address ip-address | destination-address-name address-name);
                }
                then {
                    static-nat {
                        inet {
                            routing-instance (default | routing-instance-name);
                        }
                        prefix {
                            address-prefix;
                            routing-instance (default | routing-instance-name);
                        }
                        prefix-name {
                            address-prefix-name;
                            routing-instance (default | routing-instance-name);
                        }
                    }
                }
            }
        }
    }
}
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
}
```

```
        }
```

Hierarchy Level [edit security]

Release Information Statement modified in Junos OS Release 9.6. The **description** option added in Junos OS Release 12.1.

Description Configure Network Address Translation (NAT) for SRX Series devices.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Introduction to NAT*
- *Understanding Logical System Network Address Translation*

nat-pat-address

Supported Platforms	SRX5400, SRX5600, SRX5800, vSRX

Syntax

```
nat-pat-address {
    maximum amount;
    reserved amount;
}
```

Hierarchy Level   [edit system security-profile *security-profile-name*]

Release Information   Statement introduced in Junos OS Release 11.2.

Description   Specify the number of NAT with port address translation (PAT) configurations that user logical system administrators and master logical system administrators can configure for their logical systems if the security profile is bound to the logical systems.

The master administrator:

- uses security profiles to provision logical systems with resources.

- binds security profiles to user logical systems and the master logical system.

- can configure more than one security profile, specifying different amounts of resource allocations in various profiles.

Only the master administrator can create security profiles and bind them to logical systems.

Options
- maximum *amount*—A maximum allowed quota. If a logical system requires more of a resource than its reserved amount allows it can utilize resources configured for the global maximum amount if they are available—that is, if they are not allocated to other logical systems. The maximum allowed quota specifies the portion of the free global resources that the logical system can use. The maximum allowed quota does not guarantee that the amount specified for the resource in the security profile is available. Logical systems compete for global resources.

- reserved *amount*—A reserved quota that guarantees that the resource amount specified is always available to the logical system.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Understanding Logical System Network Address Translation*

- *Introduction to NAT*

oversize-message-drop

Supported Platforms   SRX Series, vSRX

Syntax   oversize-message-drop;

Hierarchy Level   [edit security alg dns]

Release Information   Statement introduced in Junos OS Release 12.1X46-D55.

Description   Enable or disable oversize message drop.

When you enable the **oversize-message-drop** command, Domain Name System (DNS) packets that exceed the threshold (range from 512 through 8192) are dropped.

When you disable the **oversize-message-drop** command, DNS Application Layer Gateway (ALG) will only record and forward the oversized DNS packets.

Options   **oversize-message-drop**—Drop the oversized DNS packets for which the packet length exceed the threshold value (range from 512 through 8192).

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- dns on page 335

policy (Security Policies)

Supported Platforms   SRX Series, vSRX

Syntax

```
policy policy-name {
    description description;
    match {
        application {
            [application];
            any;
        }
        destination-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
        }
        source-address {
            [address];
            any;
            any-ipv4;
            any-ipv6;
        }
        source-identity {
            [role-name];
            any;
            authenticated-user;
            unauthenticated-user;
            unknown-user;
        }
    }
    scheduler-name scheduler-name;
    then {
        count {
            alarm {
                per-minute-threshold number;
                per-second-threshold number;
            }
        }
        deny;
        log {
            session-close;
            session-init;
        }
        permit {
            application-services {
                application-firewall {
                    rule-set rule-set-name;
                }
                application-traffic-control {
                    rule-set rule-set-name;
                }
                gprs-gtp-profile profile-name;
                gprs-sctp-profile profile-name;
                idp;
```

```
                        redirect-wx | reverse-redirect-wx;
                        ssl-proxy {
                           profile-name profile-name;
                        }
                        uac-policy {
                           captive-portal captive-portal;
                        }
                        utm-policy policy-name;
                     }
                     destination-address {
                        drop-translated;
                        drop-untranslated;
                     }
                     firewall-authentication {
                        pass-through {
                           access-profile profile-name;
                           client-match user-or-group-name;
                           web-redirect;
                        }
                        user-firewall {
                           access-profile profile-name;
                           domain domain-name
                           ssl-termination-profile profile-name;
                        }
                        web-authentication {
                           client-match user-or-group-name;
                        }
                     }
                     services-offload;
                     tcp-options {
                        initial-tcp-mss mss-value;
                        reverse-tcp-mss mss-value;
                        sequence-check-required;
                        syn-check-required;
                     }
                     tunnel {
                        ipsec-group-vpn group-vpn;
                        ipsec-vpn vpn-name;
                        pair-policy pair-policy;
                     }
                  }
                  reject;
               }
            }
         }
```

Hierarchy Level [edit security policies from-zone *zone-name* to-zone *zone-name*]

Release Information Statement introduced in Junos OS Release 8.5. The **services-offload** option added in Junos OS Release 11.4. Statement updated with the **source-identity** option and the **description** option added in Junos OS Release 12.1. Support for the **user-firewall** option added in Junos OS Release 12.1X45-D10. Support for the **initial-tcp-mss** and **reverse-tcp-mss** options added in Junos OS Release 12.3X48-D20.

Description Define a security policy.

Options   *policy-name*—Name of the security policy.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related   • *Configuring SSL Proxy*
Documentation
• *Security Policies Overview*

pptp

Supported Platforms   SRX Series, vSRX

Syntax
```
pptp {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify the Point-to-Point Tunneling Protocol (PPTP) ALG on the device.

Options   • **disable**—Disable the PPTP ALG. By default, the PPTP ALG is enabled.

• **traceoptions**—Configure PPTP ALG tracing options.

  • **flag**—Trace operation to perform.

    • **all**—Trace all events.

    • *extensive*—Display extensive amount of data.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related   • *Building Blocks Feature Guide for Security Devices*
Documentation

protect

Supported Platforms	SRX Series, vSRX

Syntax

```
protect {
    deny {
        all {
            timeout value-in-seconds;
        }
        destination-ip address;
        timeout value-in-seconds;
    }
}
```

Hierarchy Level   [edit security alg sip application-screen]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure options to protect servers against INVITE attacks.

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related   • sip (Security) on page 373
Documentation

protocols (Security Zones Interfaces)

Supported Platforms SRX Series, vSRX

Syntax
```
protocols protocol-name {
    except;
}
```

Hierarchy Level [edit security zones security-zone zone-name interfaces interface-name host-inbound-traffic]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the types of routing protocol traffic that can reach the device on a per-interface basis.

Options • *protocol-name* —Protocol for which traffic is allowed. The following protocols are supported:

- **all**—Enable traffic from all possible protocols available.

- **bfd**—Enable incoming Bidirectional Forwarding Detection (BFD) Protocol traffic.

- **bgp**—Enable incoming BGP traffic.

- **dvmrp**—Enable incoming Distance Vector Multicast Routing Protocol (DVMRP) traffic.

- **igmp**—Enable incoming Internet Group Management Protocol (IGMP) traffic.

- **ldp**—Enable incoming Label Distribution Protocol (LDP) traffic (UDP and TCP port 646).

- **msdp**—Enable incoming Multicast Source Discovery Protocol (MSDP) traffic.

- **nhrp**—Enable incoming Next Hop Resolution Protocol (NHRP) traffic.

- **ospf**—Enable incoming OSPF traffic.

- **ospf3**—Enable incoming OSPF version 3 traffic.

- **pgm**—Enable incoming Pragmatic General Multicast (PGM) protocol traffic (IP protocol number 113).

- **pim**—Enable incoming Protocol Independent Multicast (PIM) traffic.

- **rip**—Enable incoming RIP traffic.

- **ripng**—Enable incoming RIP next generation traffic.

- **router-discovery**—Enable incoming router discovery traffic.

- **rsvp**—Enable incoming Resource Resolution Protocol (RSVP) traffic (IP protocol number 46).

- **sap**— Enable incoming Session Announcement Protocol (SAP) traffic. SAP always listens on **224.2.127.254:9875**.

- **vrrp**—Enable incoming Virtual Router Redundancy Protocol (VRRP) traffic.

except—(Optional) except can only be used if all has been defined.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related   • *Security Zones and Interfaces Overview*
Documentation
                      • *Understanding Functional Zones*

retain-hold-resource

Supported Platforms   SRX Series, vSRX

Syntax   retain-hold-resource;

Hierarchy Level   [edit security alg sip]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Enable the device to not free media resources for a Session Initiation Protocol (SIP)
                      Application Layer Gateway (ALG), even when a media stream is placed on hold. By
                      default, media stream resources are released when the media stream is held.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

Related   • sip (Security) on page 373
Documentation

rsh

Supported Platforms	SRX Series, vSRX

Syntax

```
rsh {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the remote shell (RSH) ALG on the device.

Options
- **disable**—Disable the RSH ALG. By default, the RSH ALG is disabled.

- **traceoptions**—Configure RSH ALG tracing options.

  - **flag**—Trace operation to perform.

    - **all**—Trace all events.

    - *extensive*—Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding the RSH ALG on page 75

rtsp

Supported Platforms   SRX Series, vSRX

Syntax
```
rtsp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify the Real-Time Streaming Protocol (RTSP) ALG on the device.

Options
- **disable**—Disable the RTSP ALG. By default, the RTSP ALG is enabled.

- **traceoptions**—Configure RTSP ALG tracing options.

  - **flag**—Trace operation to perform.

    - **all**—Trace all events.

    - *extensive*—Display extensive amount of data.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding the RTSP ALG on page 89

sccp

Supported Platforms   SRX Series, vSRX

Syntax
```
sccp {
    application-screen {
        call-flood {
            threshold rate;
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    disable;
    dscp-rewrite {
        code-point string;
    }
    inactive-media-timeout value-in-seconds;
    traceoptions {
        flag flag <extensive>;
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify the Skinny Client Control Protocol (SCCP) ALG on the device.

Options   **disable**—Disable the SCCP ALG. By default, the SCCP ALG is enabled.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation   • Understanding SCCP ALGs on page 217

security-zone

Supported Platforms   SRX Series, vSRX

Syntax

```
security-zone zone-name {
    address-book {
        address address-name {
            ip-prefix {
                description text;
            }
            description text;
            dns-name domain-name {
                ipv4-only;
                ipv6-only;
            }
            range-address lower-limit to upper-limit;
            wildcard-address ipv4-address/wildcard-mask;
        }
        address-set address-set-name {
            address address-name;
            address-set address-set-name;
            description text;
        }
    }
    advance-policy-based-routing;
    application-tracking;
    description text;
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
    interfaces interface-name {
        host-inbound-traffic {
            protocols protocol-name {
                except;
            }
            system-services service-name {
                except;
            }
        }
    }
    screen screen-name;
    tcp-rst;
}
```

Hierarchy Level   [edit security zones]

Release Information   Statement introduced in Junos OS Release 8.5. Support for wildcard addresses added in Junos OS Release 11.1. The **description** option added in Junos OS Release 12.1.

Description   Define a security zone, which allows you to divide the network into different segments and apply different security options to each segment.

Options   *zone-name* —Name of the security zone.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Security Zones and Interfaces Overview*
- *Example: Configuring Application Firewall Rule Sets Within a Security Policy*

sip (Security)

Supported Platforms   SRX Series, vSRX

Syntax
```
sip {
    application-screen {
        protect {
            deny {
                all {
                    timeout value-in-seconds;
                }
                destination-ip address;
                timeout value-in-seconds;
            }
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    c-timeout value-in-minutes;
    disable;
    dscp-rewrite {
        code-point string;
    }
    inactive-media-timeout value-in-seconds;
    maximum-call-duration value-in-minutes;
    retain-hold-resource;
    t1-interval value-in-milliseconds;
    t4-interval value-in-seconds;
    traceoptions {
        flag flag <detail | extensive | terse>;
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement modified in Junos OS Release 9.2.

Description   Specify the Session Initiation Protocol (SIP) ALG on the device.

> **NOTE:** IPv6 is supported on the SIP ALG along with Network Address Translation Protocol Translation (NAT-PT) mode and NAT64 address translation.
>
> The type of the <destination-ip-address> is changed from IPv4 address to IP prefix to support all kinds of IP addresses, and correspondingly a prefix is supported to allow multiple IP addresses.

Options   disable—Disable the SIP ALG. Use the **set security alg** *alg-name* **disable** CLI command to disable the SIP ALG.

The remaining statements are explained separately. See CLI Explorer.

> NOTE: By default, the SIP ALG is disabled for SRX5600 and SRX5800 devices. Use the CLI command **delete security alg** *alg-name* **disable** to enable the SIP ALG.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding the SIP ALG on page 241

source-address (Security Destination NAT)

Supported Platforms   SRX Series, vSRX

Syntax   source-address [*ip-address*];

Hierarchy Level   [edit security nat destination rule-set *rule-set-name* rule *rule-name* match]

Release Information   Statement modified in Junos OS Release 9.6.

Description   Specify source address to match the rule. You can configure multiple addresses or subnets.

Options   *ip-address* —Source address or a subnet.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

source-address (Security Policies)

Supported Platforms   SRX Series, vSRX

Syntax

```
source-address {
    [address];
    any;
    any-ipv4;
    any-ipv6;
}
```

Hierarchy Level   [edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* match]

[edit security policies global policy *policy-name* match]

Release Information   Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in Junos OS Release 10.2. Support for IPv6 addresses in active/active chassis cluster configurations (in addition to the existing support of active/passive chassis cluster configurations) added in Junos OS Release 10.4. Support for wildcard addresses added in Junos OS Release 11.1.

Description   Define the matching criteria. You can specify one or more IP addresses, address sets, or wildcard addresses. You can specify wildcards **any**, **any-ipv4**, or **any-ipv6**.

Options   *address*—IP addresses, address sets, or wildcard addresses (represented as A.B.C.D/wildcard-mask). You can configure multiple addresses or address prefixes separated by spaces and enclosed in square brackets.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *Security Policies Overview*
- *Understanding Security Policy Rules*
- *Understanding Security Policy Elements*

source-nat

Supported Platforms   SRX Series, vSRX

Syntax
```
source-nat {
    interface {
        persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number value;
            permit (any-remote-host | target-host | target-host-port);
        }
    }
    off;
    pool <pool-name>;
        persistent-nat {
            address-mapping;
            inactivity-timeout seconds;
            max-session-number number;
            permit (any-remote-host | target-host | target-host-port);
    }
    rule-session-count-alarm (clear-threshold value | raise-threshold value);
}
```

Hierarchy Level   [edit security nat source rule-set rule-set-name rule rule-name then]

Release Information   Statement modified in Junos OS Release 9.6. Statement modified in Junos OS Release 12.1X45-D10.

Description   Specify the action of the source NAT rule.

Options   • **off**—Do not perform the source NAT operation.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege   security — To view this statement in the configuration.
Level   security-control— To add this statement to the configuration.

sql

Supported Platforms   SRX Series, vSRX

Syntax
```
sql {
  disable;
  traceoptions {
    flag {
      all <extensive>;
    }
  }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify the Oracle SQL ALG on the device.

Options
- **disable**—Disable the SQL ALG. By default, the SQL ALG is enabled.

- **traceoptions**—Configure SQL ALG tracing options.

  - **flag**—Trace operation to perform.

    - **all**—Trace all events.

    - *extensive*—Display extensive amount of data.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding the SQLNET ALG on page 103

static-nat

Supported Platforms SRX Series, vSRX

Syntax
```
static-nat {
    inet {
        routing-instance (default | routing-instance-name);
    }
    nptv6-prefix {
        address-prefix;
            routing-instance routing-instance-name;
    nptv6-prefix-name {
        address-prefix-name;
            routing-instance routing-instance-name;
    [
    prefix {
        address-prefix;
        routing-instance (default | routing-instance-name);
    }
    prefix-name {
        address-prefix-name;
        routing-instance (default | routing-instance-name);
    }
    rule-session-count-alarm (clear threshold value | raise threshold value);
}
```

Hierarchy Level   [edit security nat static rule-set rule-set-name rule rule-name then]

Release Information Statement modified in Junos OS Release 9.6. Statement modified in Junos OS Release
12.1X45-D10. Statement modified in Junos OS Release 12.3X48-D25.

Description   Specify the translated address of the static NAT rule.

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege   security—To view this statement in the configuration.
Level   security-control—To add this statement to the configuration.

sunrpc

Supported Platforms   SRX Series, vSRX

Syntax
```
sunrpc {
    disable;
    map-entry-timeout map-entry-timeout;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 9.0.

Description   Specify the Sun Microsystems remote procedure call (RPC) ALG on the device.

Options
- disable—Disable the Sun RPC ALG. By default, the Sun RPC ALG is enabled.

- map-entry-timeout *map-entry-timeout*—Specify the Sun RPC ALG mapping entry timeout value in hours.

  Range: 1 through 72 hours.

  Default: 32 hours.

- traceoptions—Configure the Sun RPC ALG tracing options.

  - flag—Trace operation to perform.

    - all—Trace all events.

    - *extensive*—Display extensive amount of data.

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding Sun RPC ALGs on page 62

system-services (Security Zones Host Inbound Traffic)

Supported Platforms	SRX Series, vSRX

Syntax

```
system-services {
    (service-name | all <service-name except>);
}
```

Hierarchy Level [edit security zones security-zone *zone-name* host-inbound-traffic]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the types of incoming system service traffic that can reach the device for all interfaces in a zone. You can do this in one of several ways:

- You can enable traffic from each system service individually.

- You can enable traffic from all system services.

- You can enable traffic from all but some system services.

Options
- *service-name* —System-service for which traffic is allowed. The following system services are supported:

  - **all**—Enable traffic from the defined system services available on the Routing Engine (RE). Use the *except* option to disallow specific system services.

  - **any-service**—Enable all system services on entire port range including the system services that are not defined.

  - **bootp**—Enable traffic destined to BOOTP and DHCP relay agents.

  - **dhcp**—Enable incoming DHCP requests.

  - **dhcpv6**—Enable incoming DHCP requests for IPv6.

  - **dns**—Enable incoming DNS services.

  - **finger**—Enable incoming finger traffic.

  - **ftp**—Enable incoming FTP traffic.

  - **http**—Enable incoming J-Web or clear-text Web authentication traffic.

  - **https**—Enable incoming J-Web or Web authentication traffic over Secure Sockets Layer (SSL).

  - **ident-reset**—Enable the access that has been blocked by an unacknowledged identification request.

  - **ike**—Enable Internet Key Exchange traffic.

  - **lsping**—Enable label switched path ping service.

  - **netconf**—Enable incoming NETCONF service.

  - **ntp**—Enable incoming Network Time Protocol (NTP) traffic.

  - **ping**—Allow the device to respond to ICMP echo requests.

- **r2cp**—Enable incoming Radio Router Control Protocol traffic.

- **reverse-ssh**—Reverse SSH traffic.

- **reverse-telnet**—Reverse Telnet traffic.

- **rlogin**—Enable incoming **rlogin** (remote login) traffic.

- **rpm**—Enable incoming Real-time performance monitoring (RPM) traffic.

- **rsh**—Enable incoming Remote Shell (**rsh**) traffic.

- **snmp**—Enable incoming SNMP traffic (UDP port 161).

- **snmp-trap**—Enable incoming SNMP traps (UDP port 162).

- **ssh**—Enable incoming SSH traffic.

- **telnet**—Enable incoming Telnet traffic.

- **tftp**—Enable TFTP services.

- **traceroute**—Enable incoming traceroute traffic (UDP port 33434).

- **xnm-clear-text**—Enable incoming Junos XML protocol traffic for all specified interfaces.

- **xnm-ssl**— Enable incoming Junos XML protocol-over-SSL traffic for all specified interfaces.

- **except**—(Optional) Enable specific incoming system service traffic but only when the *all* option has been defined . For example, to enable all but FTP and HTTP system service traffic:

  set security zones security-zone trust host-inbound-traffic system-services all
  set security zones security-zone trust host-inbound-traffic system-services ftp except
  set security zones security-zone trust host-inbound-traffic system-services http except

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- *Security Zones and Interfaces Overview*

- *Supported System Services for Host Inbound Traffic*

t1-interval

Supported Platforms	SRX Series, vSRX
Syntax	t1-interval *value-in-milliseconds*;
Hierarchy Level	[edit security alg sip]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the maximum round-trip time (RTT) (in milliseconds) allowed for Session Initiation Protocol (SIP) transactions.
Options	*value-in-milliseconds*—Maximum round-trip time (RTT) allowed measured in milliseconds. **Range:** 500 through 5000 milliseconds **Default:** 500 milliseconds
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• sip (Security) on page 373

t4-interval

Supported Platforms	SRX Series, vSRX
Syntax	t4-interval *value-in-seconds*;
Hierarchy Level	[edit security alg sip]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the maximum length of time (in seconds) that the network can take to clear messages between client and server Session Initiation Protocol (SIP) transactions.
Options	*value-in-seconds*—Maximum number of seconds that the network can take to clear messages between client and server transactions. **Range:** 5 through 10 seconds **Default:** 5 seconds
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• sip (Security) on page 373

talk

Supported Platforms SRX Series, vSRX

Syntax
```
talk {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the TALK program ALG on the device.

Options
- **disable**—Disable the TALK program ALG. By default, the TALK program ALG is enabled.

- **traceoptions**—Configure TALK program ALG tracing options.

  - **flag**—Trace operation to perform.

    - **all**—Trace all events.

    - *extensive*—Display extensive amount of data.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- Understanding the TALK ALG on page 117

term (Applications)

Supported Platforms   SRX Series, vSRX

Syntax
```
term term-name {
    alg application;
    destination-port port-identifier;
    icmp-code value;
    icmp-type value;
    icmp6-code value;
    icmp6-type value;
    inactivity-timeout (seconds | never);
    protocol number;
    rpc-program-number number;
    source-port port-number;
    uuid hex-value;
}
```

Hierarchy Level   [edit applications application application-name]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Define individual application protocols.

Options   The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level   system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *Security Policy Applications Overview*

tftp (Security ALG)

Supported Platforms SRX Series, vSRX

Syntax
```
tftp {
    disable;
    traceoptions {
        flag {
            all <extensive>;
        }
    }
}
```

Hierarchy Level [edit security alg]

Release Information Statement modified in Junos OS Release 9.2.

Description Configure the Trivial File Transfer Protocol (TFTP) ALG on the device.

Options • **disable**—Disable the TFTP ALG. By default, the TFTP ALG is enabled.

> **NOTE:** By default, the TFTP ALG is disabled for SRX Series devices.

• **traceoptions**—Configure TFTP ALG tracing options.

    • **flag**—Trace operation to perform.

        • **all**—Trace all events.

        • *extensive*—Display extensive amount of data.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related • Understanding the TFTP ALG on page 131
Documentation

traceoptions (Security ALG)

Supported Platforms   SRX Series, vSRX

Syntax
```
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    level (brief | detail | extensive | verbose);
    no-remote-trace;
}
```

Hierarchy Level   [edit security alg]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure ALG tracing options.

Options   • **file**—Configure the trace file options.

- *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.

- **files** *number*—Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed to *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

   If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

   Range: 2 through 1000 files

   Default: 10 files

- **match** *regular-expression*—Refine the output to include lines that contain the regular expression.

- **size** *maximum-file-size*—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the **trace-file** again reaches its maximum size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

   If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

   Syntax: *x* **K** to specify KB, *x* **m** to specify MB, or *x* **g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **level**—Set the level of debugging the output option.

  - **brief**—Match brief messages

  - **detail**—Match detail messages.

  - **extensive**—Match extensive messages.

  - **verbose**—Match verbose messages.

- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege Level   trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation   - alg on page 312

traceoptions (Security H323 ALG)

Supported Platforms   SRX Series

Syntax
```
traceoptions {
    flag flag <detail | extensive | terse>;
}
```

Hierarchy Level   [edit security alg h323]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure H.323 tracing options.

Options
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

    - **all**—Trace with all flags enabled.

    - **chassis-cluster**—Trace chassis cluster information.

    - **h225-asn1**—Trace H.225 ASN.1 processing activity.

    - **h245**—Trace H.245 processing activity.

    - **h245-asn1**—Trace H.245 ASN.1 processing activity.

    - **q931**—Trace Q.931 processing activity.

    - **ras**—Trace remote access server (RAS) processing activity.

    - **ras-asn1**—Trace RAS ASN.1 processing activity.

- **detail**—Display moderate amount of data in trace.

- **extensive**—Display extensive amount of data in trace.

- **terse**—Display minimum amount of data in trace.

Required Privilege Level   trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- h323 on page 344

traceoptions (Security MGCP ALG)

Supported Platforms   SRX Series, vSRX

Syntax
```
traceoptions {
    flag flag <extensive>;
}
```

Hierarchy Level   [edit security alg mgcp]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure Media Gateway Control Protocol (MGCP) tracing options.

Options   • **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

   • **all**—Trace with all flags enabled.

   • **call**—Trace call processing activity.

   • **chassis-cluster**—Trace chassis cluster information.

   • **decode**—Trace decoder operations activity.

   • **error**—Trace processing errors activity.

   • **nat**—Trace Network Address Translation (NAT) processing activity.

   • **packet**—Trace MGCP protocol packet processing activity.

   • **rm**—Trace MGCP Resource Management (Resmgr) functions activity.

Required Privilege Level   trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation   • mgcp on page 354

traceoptions (Security SCCP ALG)

Supported Platforms   SRX Series, vSRX

Syntax
```
traceoptions {
    flag flag <extensive>;
}
```

Hierarchy Level   [edit security alg sccp]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Configure Skinny Client Control Protocol (SCCP) tracing options.

Options
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

  - **all**—Trace with all flags enabled.

  - **call**—Trace call processing activity.

  - **chassis-cluster**—Trace chassis cluster information.

  - **cli**—Trace CLI configuration activity and command changes.

  - **decode**—Trace decoder operations activity.

  - **error**—Trace processing errors activity.

  - **init**—Enable tracing for SCCP initialization errors

  - **nat**—Enable tracing for SCCP NAT processing

  - **rm**——Trace SCCP Resource Management (Resmgr) functions activity.

Required Privilege Level   trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- sccp on page 370

traceoptions (Security SIP ALG)

Supported Platforms SRX Series, vSRX

Syntax
```
traceoptions {
    flag flag <detail | extensive | terse>;
}
```

Hierarchy Level [edit security alg sip]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure Session Initiation Protocol (SIP) tracing options.

Options
- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

  - **all**—Trace with all flags enabled.

  - **call**—Trace call processing activity.

  - **chassis-cluster**—Trace chassis cluster information.

  - **nat**—Trace SIP Network Address Translation (NAT) processing activity.

  - **parser**—Trace SIP parser operations.

  - **rm**—Trace SIP Resource Management (Resmgr) functions activity.

- detail—Display moderate amount of data in trace.

- extensive—Display extensive amount of data in trace.

- terse—Display minimum amount of data in trace.

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation
- sip (Security) on page 373

traceoptions (System Services DNS)

Supported Platforms   SRX Series, vSRX

Syntax
```
traceoptions {
    category {
        category-type;
    }
    file;
}
```

Hierarchy Level   [edit system services dns]

Release Information   Statement introduced in Junos OS Release 10.2.

Description   Defines tracing options for DNS services.

Options   **category**—Specifies the logging category. See Table 15 on page 393 for the different logging categories and their descriptions.

    file—Trace file information.

Table 15: Category Names

Category Name	Description
client	Processing of client requests
config	Configuration file parsing and processing
database	Messages relating to the databases
default	Categories for which there is no specific configuration
delegation-only	Delegation only
dispatch	Dispatching of incoming packets to the server
dnssec	DNSSEC and TSIG protocol processing
edns-disabled	Log query using plain DNS
general	General information
lame-servers	Lame servers
network	Network options
notify	NOTIFY protocol
queries	DNS query resolver
resolver	DNS resolution security
security	Approval and denial of requests
unmatched	Unable to determine the class for messages named
update	Dynamic updates
update-security	Approval and denial of update requests
xfer-in	Zone transfers that the server is receiving xfer-out
xfer-out	Zone transfers that the server is sending

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- *DNS Overview*

transaction-timeout

Supported Platforms	SRX Series, vSRX
Syntax	transaction-timeout *value-in-seconds*;
Hierarchy Level	[edit security alg mgcp]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Timeout value for Media Gateway Control Protocol (MGCP) transactions. If the timeout value exceeds transaction will be removed by MGCP transactions ager out processing.
Options	*value-in-seconds*—Timeout value. **Range:** 3 through 50 seconds **Default:** 30 seconds
Required Privilege Level	security—To view this statement in the configuration. security-control—To add this statement to the configuration.
Related Documentation	• mgcp on page 354

unknown-message (Security H323 ALG)

Supported Platforms   SRX Series

Syntax
```
unknown-message {
    permit-nat-applied;
    permit-routed;
}
```

Hierarchy Level   [edit security alg h323 application-screen]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify how unidentified H.323 messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown H.323 (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options
- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.

- **permit-routed**—Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- h323 on page 344

unknown-message (Security MGCP ALG)

Supported Platforms   SRX Series, vSRX

Syntax

```
unknown-message {
    permit-nat-applied;
    permit-routed;
}
```

Hierarchy Level   [edit security alg mgcp application-screen]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify how unidentified Media Gateway Control Protocol (MGCP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown MGCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options
- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.

- **permit-routed**— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- mgcp on page 354

unknown-message (Security SCCP ALG)

Supported Platforms   SRX Series, vSRX

Syntax
```
unknown-message {
    permit-nat-applied;
    permit-routed;
}
```

Hierarchy Level   [edit security alg sccp application-screen]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify how unidentified Skinny Client Control Protocol (SCCP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SCCP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options
- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.

- **permit-routed**— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- sccp on page 370

unknown-message (Security SIP ALG)

Supported Platforms   SRX Series, vSRX

Syntax

```
unknown-message {
    permit-nat-applied;
    permit-routed;
}
```

Hierarchy Level   [edit security alg sip application-screen]

Release Information   Statement introduced in Junos OS Release 8.5.

Description   Specify how unidentified Session Initiation Protocol (SIP) messages are handled by the device. The default is to drop unknown (unsupported) messages. Permitting unknown messages can compromise security and is not recommended. However, in a secure test or production environment, this statement can be useful for resolving interoperability issues with disparate vendor equipment. By permitting unknown SIP (unsupported) messages, you can get your network operational and later analyze your VoIP traffic to determine why some messages were being dropped.

This statement applies only to received packets identified as supported VoIP packets. If a packet cannot be identified, it is always dropped. If a packet is identified as a supported protocol, the message is forwarded without processing.

Options
- **permit-nat-applied**—Specify that unknown messages be allowed to pass if the session is in NAT mode.

- **permit-routed**— Specify that unknown messages be allowed to pass if the session is in Route mode. (Sessions in Transparent mode are treated as Route mode.)

Required Privilege Level   security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- sip (Security) on page 373

CHAPTER 20

Operational Commands

- clear security alg h323 counters
- clear security alg ike-esp-nat
- clear security alg sccp calls
- clear security alg sccp counters
- clear security alg sip calls
- clear security alg sip counters
- clear security flow session application
- show chassis cluster data-plane statistics
- show chassis cluster statistics
- show security alg h323 counters
- show security alg ike-esp-nat summary
- show security alg msrpc
- show security alg sccp calls
- show security alg sccp counters
- show security alg sip calls
- show security alg sip counters
- show security alg sip rate
- show security alg status
- show security flow gate
- show security flow session
- show security flow session application
- show security flow session resource-manager
- show security idp policy-templates
- show security resource-manager group active
- show security resource-manager resource active
- show security resource-manager summary
- show security zones
- show security zones type

clear security alg h323 counters

Supported Platforms	SRX Series
Syntax	clear security alg h323 counters <node (*node-id* | all | local | primary)>
Release Information	Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.
Description	Clear information about H.323 Application Layer Gateway (ALG) counters.

Options	• none—Clear H.323 ALG counters.
	
	• **node**—(Optional) For chassis cluster configurations, clear H.323 counters on a specific node (device) in the cluster.
	
	   • *node-id* —Identification number of the node. It can be 0 or 1.
	
	   • **all** —Clear all nodes.
	
	   • **local** —Clear the local node.
	
	   • **primary**—Clear the primary node.

Required Privilege Level	clear
Related Documentation	• h323 on page 344 • show security alg h323 counters on page 414
List of Sample Output	clear security alg h323 counters on page 400

Sample Output

clear security alg h323 counters

```
user@host> clear security alg h323 counters
```

clear security alg ike-esp-nat

Supported Platforms	SRX Series, vSRX
Syntax	clear security alg ike-esp-nat
Release Information	Command introduced in Junos OS Release 10.2.
Description	Clear state information about Application Layer Gateway (ALG) for IKE and ESP.
Required Privilege Level	clear
Related Documentation	• show security alg ike-esp-nat summary on page 416
List of Sample Output	clear security alg ike-esp-nat on page 401

Sample Output

clear security alg ike-esp-nat

```
user@host> clear security alg ike-esp-nat
10 active IKE-ESP alg state cleared
```

clear security alg sccp calls

Supported Platforms	SRX Series, vSRX
Syntax	clear security alg sccp calls <node (*node-id* | all | local | primary)>
Release Information	Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.
Description	Clear Skinny Client Protocol (SCCP) Application Layer Gateway (ALG) call information.

Options

- none—Clear all SCCP ALG calls.

- **node**—(Optional) For chassis cluster configurations, clear SCCP calls on a specific node (device) in the cluster.

  - *node-id* —Identification number of the node. It can be 0 or 1.

  - **all** —Clear all nodes.

  - **local** —Clear the local node.

  - **primary**—Clear the primary node.

Required Privilege Level	clear
Related Documentation	• sccp on page 370 • show security alg sccp calls on page 419
Output Fields	This command produces no output.

clear security alg sccp counters

Supported Platforms	SRX Series, vSRX
Syntax	clear security alg sccp counters <node (*node-id* | all | local | primary)>
Release Information	Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.
Description	Clear Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) counters.

Options

- none—Clear all SCCP ALG counters.

- **node**—(Optional) For chassis cluster configurations, clear SCCP counters on a specific node (device) in the cluster.

  - *node-id* —Identification number of the node. It can be 0 or 1.

  - **all** —Clear all nodes.

  - **local** —Clear the local node.

  - **primary**—Clear the primary node.

Required Privilege Level	clear
Related Documentation	• sccp on page 370
	• show security alg sccp counters on page 421
List of Sample Output	clear security alg sccp counters on page 403

Sample Output

clear security alg sccp counters

```
user@host> clear security alg sccp counters
```

clear security alg sip calls

Supported Platforms	SRX Series, vSRX
Syntax	clear security alg sip calls <node (*node-id* | all | local | primary)>
Release Information	Command modified in Junos OS Release 9.2; **node** options added in Junos OS Release 9.0.
Description	Clear Session Initiation Protocol (SIP) Application Layer Gateway (ALG) call information.
Options	• none—Clear all SIP ALG calls.
	• node—(Optional) For chassis cluster configuration, clear SIP calls on a specific node (device) in the cluster.
	• *node-id* —Identification number of the node. It can be 0 or 1.
	• all —Clear all nodes.
	• local —Clear the local node.
	• primary—Clear the primary node.
Required Privilege Level	clear
Related Documentation	• sip (Security) on page 373
	• show security alg sip calls on page 423
List of Sample Output	clear security alg sip calls on page 404

Sample Output

clear security alg sip calls

```
user@host> clear security alg sip calls
```

clear security alg sip counters

Supported Platforms   SRX Series, vSRX

Syntax   clear security alg sip counters
<node (*node-id* | all | local | primary)>

Release Information   Command modified in Junos OS Release 9,2; **node** options added in Junos OS Release 9.0.

Description   Clear Session Initiation Protocol (SIP) Application Layer Gateway (ALG) counters.

Options   • none—Clear all SIP ALG counters.

• **node**—(Optional) For chassis cluster configurations, clear SIP counters on a specific node (device) in the cluster.

   • *node-id* —Identification number of the node. It can be 0 or 1.

   • **all** —Clear all nodes.

   • **local** —Clear the local node.

   • **primary**—Clear the primary node.

Required Privilege Level   clear

Related Documentation   • sip (Security) on page 373

• show security alg sip counters on page 425

List of Sample Output   clear security alg sip counters on page 405

Sample Output

clear security alg sip counters

```
user@host>  clear security alg sip counters
```

clear security flow session application

Supported Platforms SRX Series, vSRX

Syntax clear security flow session application
application-name
<node (*node-id* | all | local | primary)>

Release Information Command introduced in Junos OS Release 8.5. The **node** options added in Junos OS Release 9.0.

Description Clear currently active sessions for application types or application sets.

Options
- *application-name* —Name of the specified application type or application set.

  - **dns**—Domain Name System

  - **ftp**—File Transfer Protocol

  - **ignore**—Ignore application type

  - **mgcp-ca**—Media Gateway Control Protocol with Call Agent

  - **mgcp-ua**—MGCP with User Agent

  - **ms-rpc**—Microsoft RPC

  - **pptp**—Point-to-Point Tunneling Protocol

  - **q931**—ISDN connection control protocol

  - **ras**—RAS

  - **realaudio**—RealAudio

  - **rsh**—UNIX remote shell services

  - **rtsp**—Real-Time Streaming Protocol

  - **sccp**—Skinny Client Control Protocol

  - **sip**—Session Initiation Protocol

  - **sqlnet-v2**—Oracle SQLNET

  - **sun-rpc**—Sun Microsystems RPC

  - **talk**—TALK program

  - **tftp**—Trivial File Transfer Protocol

- **node**—(Optional) For chassis cluster configurations, clear sessions for applications on a specific node (device) in the cluster.

  - *node-id* —Identification number of the node. It can be 0 or 1.

  - **all** —Clear all nodes.

- **local** —Clear the local node.

- **primary**—Clear the primary node.

Required Privilege Level   clear

Related Documentation

- show security flow session application on page 443

List of Sample Output   clear security flow session application dns on page 407
clear security flow session application dns node 0 on page 407

Output Fields   When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security flow session application dns

```
user@host> clear security flow session application dns
node0:
--------------------------------------------------------------------------
0 active sessions cleared
node1:
--------------------------------------------------------------------------
0 active sessions cleared
```

Sample Output

clear security flow session application dns node 0

```
user@host> clear security flow session application dns node 0
node0:
--------------------------------------------------------------------------
0 active sessions cleared
```

show chassis cluster data-plane statistics

Supported Platforms	SRX Series, vSRX
Syntax	show chassis cluster data-plane statistics
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display information about chassis cluster data plane statistics.
Required Privilege Level	view
Related Documentation	• *clear chassis cluster data-plane statistics*
List of Sample Output	show chassis cluster data-plane statistics on page 409
Output Fields	Table 16 on page 408 lists the output fields for the **show chassis cluster data-plane statistics** command. Output fields are listed in the approximate order in which they appear.

Table 16: show chassis cluster data-plane statistics Output Fields

Field Name	Field Description
Services Synchronized	• **Service name**—Name of the service.
	• **Rtos sent**—Number of runtime objects (RTOs) sent.
	• **Rtos received**—Number of RTOs received.
	• **Translation context**—Messages synchronizing Network Address Translation (NAT) translation context.
	• **Incoming NAT**—Messages synchronizing incoming Network Address Translation (NAT) service.
	• **Resource manager**—Messages synchronizing resource manager groups and resources.
	• **Session create**—Messages synchronizing session creation.
	• **Session close**—Messages synchronizing session close.
	• **Session change**—Messages synchronizing session change.
	• **Gate create**—Messages synchronizing creation of pinholes (temporary openings in the firewall).
	• **Session ageout refresh request**—Messages synchronizing request session after age-out.
	• **Session ageout refresh reply**—Messages synchronizing reply session after age-out.
	• **IPsec VPN**—Messages synchronizing VPN session.
	• **Firewall user authentication**—Messages synchronizing firewall user authentication session.
	• **MGCP ALG**—Messages synchronizing MGCP ALG sessions.
	• **H323 ALG**—Messages synchronizing H.323 ALG sessions.
	• **SIP ALG**—Messages synchronizing SIP ALG sessions.
	• **SCCP ALG**—Messages synchronizing SCCP ALG sessions.
	• **PPTP ALG**—Messages synchronizing PPTP ALG sessions.
	• **RTSP ALG**—Messages synchronizing RTSP ALG sessions.

Sample Output

show chassis cluster data-plane statistics

```
user@host> show chassis cluster data-plane statistics
Services Synchronized:
    Service name                        RTOs sent     RTOs received
    Translation context                 0             0
    Incoming NAT                        0             0
    Resource manager                    0             0
    Session create                      0             0
    Session close                       0             0
    Session change                      0             0
    Gate create                         0             0
    Session ageout refresh requests     0             0
    Session ageout refresh replies      0             0
    IPsec VPN                           0             0
    Firewall user authentication        0             0
    MGCP ALG                            0             0
    H323 ALG                            0             0
    SIP ALG                             0             0
    SCCP ALG                            0             0
    PPTP ALG                            0             0
    RTSP ALG                            0             0
```

show chassis cluster statistics

Supported Platforms	SRX Series, vSRX
Syntax	show chassis cluster statistics
Release Information	Command modified in Junos OS Release 9.0. Output changed to support dual control ports in Junos OS Release 10.0.
Description	Display information about chassis cluster services and interfaces.
Required Privilege Level	view
Related Documentation	• *clear chassis cluster statistics*
List of Sample Output	show chassis cluster statistics on page 411 show chassis cluster statistics (SRX5000 line devices) on page 412 show chassis cluster statistics (SRX5000 line devices) on page 413
Output Fields	Table 17 on page 410 lists the output fields for the **show chassis cluster statistics** command. Output fields are listed in the approximate order in which they appear.

Table 17: show chassis cluster statistics Output Fields

Field Name	Field Description
Control link statistics	Statistics of the control link used by chassis cluster traffic. Statistics for **Control link 1** are displayed when you use dual control links (SRX5000 lines only). Note that the output for the SRX5000 lines will always show **Control link 0** and **Control link 1** statistics, even though only one control link is active or working. • **Heartbeat packets sent**—Number of heartbeat messages sent on the control link. • **Heartbeat packets received**—Number of heartbeat messages received on the control link. • **Heartbeat packet errors**—Number of heartbeat packets received with errors on the control link.
Fabric link statistics	Statistics of the fabric link used by chassis cluster traffic. Statistics for **Child Link 1** are displayed when you use dual fabric links. • **Probes sent**—Number of probes sent on the fabric link. • **Probes received**—Number of probes received on the fabric link.

Table 17: show chassis cluster statistics Output Fields *(continued)*

Field Name	Field Description
Services Synchronized	- **Service name**—Name of the service. - **Rtos sent**—Number of runtime objects (RTOs) sent. - **Rtos received**—Number of RTOs received. - **Translation context**—Messages synchronizing Network Address Translation (NAT) translation context. - **Incoming NAT**—Messages synchronizing incoming Network Address Translation (NAT) service. - **Resource manager**—Messages synchronizing resource manager groups and resources. - **Session create**—Messages synchronizing session creation. - **Session close**—Messages synchronizing session close. - **Session change**—Messages synchronizing session change. - **Gate create**—Messages synchronizing creation of pinholes (temporary openings in the firewall). - **Session ageout refresh request**—Messages synchronizing request session after age-out. - **Session ageout refresh reply**—Messages synchronizing reply session after age-out. - **IPsec VPN**—Messages synchronizing VPN session. - **Firewall user authentication**—Messages synchronizing firewall user authentication session. - **MGCP ALG**—Messages synchronizing MGCP ALG sessions. - **H323 ALG**—Messages synchronizing H.323 ALG sessions. - **SIP ALG**—Messages synchronizing SIP ALG sessions. - **SCCP ALG**—Messages synchronizing SCCP ALG sessions. - **PPTP ALG**—Messages synchronizing PPTP ALG sessions. - **RTSP ALG**—Messages synchronizing RTSP ALG sessions. - **MAC address learning**—Messages synchronizing MAC address learning.

Sample Output

show chassis cluster statistics

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 798
        Heartbeat packets received: 784
        Heartbeat packets errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 793
        Probes received: 0
Services Synchronized:
    Service name                        RTOs sent    RTOs received
    Translation context                 0            0
    Incoming NAT                        0            0
    Resource manager                    0            0
    Session create                      0            0
    Session close                       0            0
    Session change                      0            0
    Gate create                         0            0
```

Session ageout refresh requests	0	0
Session ageout refresh replies	0	0
IPsec VPN	0	0
Firewall user authentication	0	0
MGCP ALG	0	0
H323 ALG	0	0
SIP ALG	0	0
SCCP ALG	0	0
PPTP ALG	0	0
RTSP ALG	0	0
MAC address learning	0	0

Sample Output

show chassis cluster statistics (SRX5000 line devices)

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 258689
        Heartbeat packets received: 258684
        Heartbeat packets errors: 0
    Control link 1:
        Heartbeat packets sent: 258689
        Heartbeat packets received: 258684
        Heartbeat packets errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 258681
        Probes received: 258681
    Child link 1
        Probes sent: 258501
        Probes received: 258501
Services Synchronized:
    Service name                        RTOs sent     RTOs received
    Translation context                 0             0
    Incoming NAT                        0             0
    Resource manager                    0             0
    Session create                      1             0
    Session close                       1             0
    Session change                      0             0
    Gate create                         0             0
    Session ageout refresh requests     0             0
    Session ageout refresh replies      0             0
    IPSec VPN                           0             0
    Firewall user authentication        0             0
    MGCP ALG                            0             0
    H323 ALG                            0             0
    SIP ALG                             0             0
    SCCP ALG                            0             0
    PPTP ALG                            0             0
    RPC ALG                             0             0
    RTSP ALG                            0             0
    RAS ALG                             0             0
    MAC address learning                0             0
    GPRS GTP                            0             0
```

Sample Output

show chassis cluster statistics (SRX5000 line devices)

```
user@host> show chassis cluster statistics
Control link statistics:
    Control link 0:
        Heartbeat packets sent: 82371
        Heartbeat packets received: 82321
        Heartbeat packets errors: 0
    Control link 1:
        Heartbeat packets sent: 0
        Heartbeat packets received: 0
        Heartbeat packets errors: 0
Fabric link statistics:
    Child link 0
        Probes sent: 258681
        Probes received: 258681
    Child link 1
        Probes sent: 258501
        Probes received: 258501
Services Synchronized:
    Service name                          RTOs sent    RTOs received
    Translation context                   0            0
    Incoming NAT                          0            0
    Resource manager                      0            0
    Session create                        1            0
    Session close                         1            0
    Session change                        0            0
    Gate create                           0            0
    Session ageout refresh requests       0            0
    Session ageout refresh replies        0            0
    IPSec VPN                             0            0
    Firewall user authentication          0            0
    MGCP ALG                              0            0
    H323 ALG                              0            0
    SIP ALG                               0            0
    SCCP ALG                              0            0
    PPTP ALG                              0            0
    RPC ALG                               0            0
    RTSP ALG                              0            0
    RAS ALG                               0            0
    MAC address learning                  0            0
    GPRS GTP                              0            0
```

show security alg h323 counters

Supported Platforms	SRX Series
Syntax	show security alg h323 counters <node (*node-id* | all | local | primary)>
Release Information	Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.
Description	Display H.323 Application Layer Gateway (ALG) counters information.
Options	• none—Display H.323 ALG counters. information.
	• node—(Optional) For chassis cluster configurations, display H.323 counters on a specific node (device) in the cluster.
	• *node-id* —Identification number of the node. It can be 0 or 1.
	• all—Display information about all nodes.
	• local—Display information about the local node.
	• primary—Display information about the primary node.
Required Privilege Level	view
Related Documentation	• h323 on page 344
	• clear security alg h323 counters on page 400
List of Sample Output	show security alg h323 counters on page 415
Output Fields	Table 18 on page 414 lists the output fields for the **show security alg h323 counters** command. Output fields are listed in the approximate order in which they appear.

Table 18: show security alg h323 counters Output Fields

Field Name	Field Description
Packets received	Number of H.323 ALG packets received.
Packets dropped	Number of H.323 ALG packets dropped.
RAS message received	Number of incoming RAS (Endpoint Registration, Admission, and Status) messages per second per gatekeeper received and processed.
Q.931 message received	Counter for Q.931 message received.
H.245 message received	Counter for H.245 message received.

Table 18: show security alg h323 counters Output Fields *(continued)*

Field Name	Field Description
Number of calls	Total number of H.323 ALG calls.
	NOTE:
	This counter displays the number of call legs and may not display the exact number of voice calls that are active. For instance, for a single active voice call between two endpoints, this counter might display a value of **2**.
Number of active calls	Number of active H.323 ALG calls.
Decoding errors	Number of decoding errors.
Message flood dropped	Error counter for message flood dropped.
NAT errors	H.323 ALG Network Address Translation (NAT) errors.
Resource manager errors	H.323 ALG resource manager errors.

Sample Output

show security alg h323 counters

```
user@host> show security alg h323 counters
H.323 counters summary:
Packets received            :4060
Packets dropped             :24
RAS message received        :3690
Q.931 message received       :202
H.245 message received       :145
Number of calls        :25
Number of active calls       :0
H.323 Error Counters:
Decoding errors             :24
Message flood dropped        :0
NAT errors              :0
Resource manager errors       :0
H.323 Message Counters:
RRQ      : 431   RCF      :  49 ARQ  : 60  ACF       : 33
URQ      : 34    UCF      : 25 DRQ  : 55   DCF       : 44
oth RAS  : 2942  Setup    : 28 Alert     : 9 Connect    : 25
CallPrcd : 18  Info      : 0  RelCmpl  : 39  Facility   : 14
Progress : 0  Empty      : 65  OLC      : 20 OLC-ACK  :   20
oth H245  : 16
```

show security alg ike-esp-nat summary

Supported Platforms	SRX Series, vSRX
Syntax	show security alg ike-esp-nat summary
Release Information	Command introduced in Junos OS Release 10.2.
Description	Display Application Layer Gateway (ALG) for IKE and ESP information summary.
Required Privilege Level	view
Related Documentation	• clear security alg ike-esp-nat on page 401
List of Sample Output	show security alg ike-esp-nat summary on page 416

Sample Output

show security alg ike-esp-nat summary

```
user@host> security alg ike-esp-nat summary
Initiator cookie: d5732d9b4114de1a
Responder cookie: 4776fe31164ef
Session-ID:      13
ALG state :      1
Timeout:         6292
Used IKE cookies: 0
Maximum IKE cookies: 2400
```

show security alg msrpc

Supported Platforms	SRX Series, vSRX
Syntax	show security alg msrpc <object-id-map> <node (*node-id* | all | local | primary)>
Release Information	Command modified in Junos OS Release 10.1.
Description	Display Microsoft (MS) remote procedure call (RPC) Application Layer Gateway (ALG) information.

Options

- none—Display all MS-RPC ID (UUID) to object ID (OID) table information.

- **object-id-map**—(Optional) Display information from the MS-RPC ID (UUID) to object ID (OID) table.

- **node**—(Optional) For chassis cluster configurations, display MS-RPC UUID-to-object-ID mapping information on a specific node (device) in the cluster.

  - *node-id* —Identification number of the node. It can be 0 or 1.

  - **all**—Display information about all nodes.

  - **local**—Display information about the local node.

  - **primary**—Display information about the primary node.

Required Privilege Level	view
Related Documentation	• msrpc on page 355
List of Sample Output	show security alg msrpc object-id-map on page 418
Output Fields	

Table 19 on page 418 lists the output fields for the **show security alg msrpc** command. Output fields are listed in the approximate order in which they appear.

Table 19: show security alg msrpc Output Fields

Field Name	Field Description
UUID	MS-RPC ID.
OID	MS-RPC object ID.

Sample Output

show security alg msrpc object-id-map

```
user@host> show security alg msrpc object-id-map
UUID                                     OID
1be617c0-31a5-11cf-a7d8-00805f48a135     0x80000020
e3514235-4b06-11d1-ab04-00c04fc2dcd2     0x80000002
67df7c70-0f04-11ce-b13f-00aa003bac6c     0x80000014
```

show security alg sccp calls

Supported Platforms SRX Series, vSRX

Syntax show security alg sccp calls
< brief | detail | node (*node-id* | all | local | primary) >

Release Information Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.

Description Display information about Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) calls.

Options
- none | **brief**—Display brief call information.

- **detail**—(Optional) Display detailed call information.

- **node**—(Optional) For chassis cluster configurations, display SCCP calls on a specific node (device) in the cluster.

  - *node-id* —Identification number of the node. It can be 0 or 1.

  - **all**—Display information about all nodes.

  - **local**—Display information about the local node.

  - **primary**—Display information about the primary node.

Required Privilege Level view

Related Documentation
- sccp on page 370

- clear security alg sccp calls on page 402

List of Sample Output show security alg sccp calls on page 420
show security alg sccp calls detail on page 420

Output Fields Table 20 on page 420 lists the output fields for the **show security alg sccp calls** command. Output fields are listed in the approximate order in which they appear.

Table 20: show security alg sccp calls Output Fields

Field Name	Field Description
Client IP address	IP address of the client.
Client zone	Client zone ID.
Call manager	IP address of the call manager.
Resource manager group	Resource manager group ID.

Sample Output

show security alg sccp calls

```
user@host> show security alg sccp calls
Client IP         Zone      Call Manager      Conference ID  RM group
11.0.102.91       7         13.0.99.226       16789504       2047
12.0.102.96       8         13.0.99.226       16789505       2048
```

Sample Output

show security alg sccp calls detail

```
user@host> show security alg sccp calls detail
Client IP address: 11.0.102.91
Client zone: 7
Call Manager IP: 13.0.99.226
Conference ID: 16789504
Resource manager group: 2048
SCCP channel information:
    Media transmit channel address (IP address/Port): 0.0.0.0:0
    Media transmit channel translated address (IP address/Port): 0.0.0.0:0
    Media transmit channel pass-through party ID (PPID): 0
    Media transmit channel resource ID: 0
    Media receive channel address (IP address/Port): 11.0.102.91:20060
    Media receive channel translated address (IP address/Port): 25.0.0.1:1032
    Media receive channel pass-through party ID (PPID): 16934451
    Media receive channel resource ID: 8185
    Multimedia transmit channel address (IP address/Port): 0.0.0.0:0
    Multimedia transmit channel translated address (IP address/Port): 0.0.0.0:0
    Multimedia transmit channel pass-through party ID (PPID): 0
    Multimedia transmit channel resource ID: 0
    Multimedia receive channel address (IP address/Port): 0.0.0.0:0
    Multimedia receive channel translated address (IP address/Port): 0.0.0.0:0
    Multimedia receive channel pass-through party ID (PPID): 0
    Multimedia receive channel resource ID: 0
Total number of calls = 1
```

show security alg sccp counters

Supported Platforms	SRX Series, vSRX
Syntax	show security alg sccp counters <node (*node-id* | all | local | primary)>
Release Information	Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.
Description	Display information about Skinny Client Control Protocol (SCCP) Application Layer Gateway (ALG) counters.

Options	• none—Display all SCCP ALG counters.
	
	• **node**—(Optional) For chassis cluster configurations, display SCCP counters on a specific node (device) in the cluster.
	
	  • *node-id* —Identification number of the node. It can be 0 or 1.
	
	  • **all**—Display information about all nodes.
	
	  • **local**—Display information about the local node.
	
	  • **primary**—Display information about the primary node.

Required Privilege Level	view
Related Documentation	• sccp on page 370 • clear security alg sccp counters on page 403
List of Sample Output	show security alg sccp counters on page 422
Output Fields	Table 21 on page 421 lists the output fields for the **show security alg sccp counters** command. Output fields are listed in the approximate order in which they appear.

Table 21: show security alg sccp counters Output Fields

Field Name	Field Description
Active client sessions	Number of active SCCP ALG client sessions.
Active calls	Number of active SCCP ALG calls.
Total calls	Total number of SCCP ALG calls.
Packets received	Number of SCCP ALG packets received.
PDUs processed	Number of SCCP ALG protocol data units (PDU) processed.
Current call rate	Number of calls per second.

Table 21: show security alg sccp counters Output Fields *(continued)*

Field Name	Field Description
Packets dropped	Number of packets dropped by the SCCP ALG.
Decode errors	Number of decoding errors.
Protocol errors	Number of protocol errors.
Address translation errors	Number of NAT errors.
Policy lookup errors	Number of errors occurring during policy lookups.
Unknown PDUs	Number of unknown protocol data units (PDUs).
Maximum calls exceed	Number of times the maximum number of calls was exceeded.
Maximum call rate exceed	Number of times the maximum call rate was exceeded.
Initialization errors	Number of call initialization errors.
Internal errors	Number of internal errors.
Nonspecific error	Number of nonspecific errors.

Sample Output

show security alg sccp counters

```
user@host> show security alg sccp counters
SCCP call statistics:
   Active client sessions      : 4
   Active calls                : 2
   Total calls                 : 3
   Packets received            : 232
   PDUs processed              : 232
   Current call rate           : 0
Error counters:
   Packets dropped             : 0
   Decode errors               : 0
   Protocol errors             : 0
   Address translation errors  : 0
   Policy lookup errors        : 0
   Unknown PDUs                : 0
   Maximum calls exceeded      : 0
   Maximum call rate exceeded  : 0
   Initialization errors       : 0
   Internal errors             : 0
   Nonspecific error           : 0
```

show security alg sip calls

Supported Platforms	SRX Series, vSRX
Syntax	show security alg sip calls <brief | detail | node (*node-id* | all | local | primary) >
Release Information	Command modified in Junos OS Release 9.2; **node** options added in Junos OS Release 9.0.
Description	Display information about Session Initiation Protocols (SIP) Application Layer Gateway (ALG) calls.

Options	• none | **brief**—Display brief call information.
	
	• **detail**—(Optional) Display detailed information about SIP ALG calls.
	
	• **node**—(Optional) For chassis cluster configurations, display SIP calls on a specific node (device) in the cluster.
	
	   • *node-id*—Identification number of the node. It can be 0 or 1.
	
	   • **all**—Display information about all nodes.
	
	   • **local**—Display information about the local node.
	
	   • **primary**—Display information about the primary node.

Required Privilege Level	view
Related Documentation	• sip (Security) on page 373 • clear security alg sip calls on page 404
List of Sample Output	show security alg sip calls on page 424 show security alg sip calls detail on page 424
Output Fields	Table 22 on page 423 lists the output fields for the **show security alg sip calls** command. Output fields are listed in the approximate order in which they appear.

Table 22: show security alg sip calls Output Fields

Field Name	Field Description
UAS callid	Call Identifier for the SIP ALG user agent server.
State	State of the SIP ALG user agent server.

Sample Output

show security alg sip calls

```
user@host> show security alg sip calls
Total number of calls: 1
      Call ID  : 1-2468@20.0.0.174
    Method   : INVITE
```

Sample Output

show security alg sip calls detail

```
user@host> show security alg sip calls detail
Total number of calls: 1
      Call ID  : 1-2468@20.0.0.174
    Method   : INVITE
    State    : SETUP
    Group ID : 307
```

show security alg sip counters

Supported Platforms	SRX Series, vSRX
Syntax	show security alg sip counters <node (*node-id* | all | local | primary)>
Release Information	Command modified in Junos OS Release 9.2; **node** options added in Junos OS Release 9.0.
Description	Display information about Session Initiation Protocol (SIP) Application Layer Gateway (ALG) counters.

Options
- none—Display all SIP ALG counters.
- **node**—(Optional) For chassis cluster configurations, display SIP counters on a specific node (device) in the cluster.
  - *node-id* —Identification number of the node. It can be 0 or 1.
  - **all**—Display information about all nodes.
  - **local**—Display information about the local node.
  - **primary**—Display information about the primary node.

Required Privilege Level	view
Related Documentation	• sip (Security) on page 373 • clear security alg sip counters on page 405
List of Sample Output	show security alg sip counters on page 427
Output Fields	Table 23 on page 425 lists the output fields for the **show security alg sip counters** command. Output fields are listed in the approximate order in which they appear.

Table 23: show security alg sip counters Output Fields

Field Name	Field Description
INVITE	Number of INVITE requests sent. An INVITE request is sent to invite another user to participate in a session.
CANCEL	Number of CANCEL requests sent. 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
ACK	Number of ACK requests sent. The user from whom the INVITE originated sends an ACK request to confirm reception of the final response to the INVITE request.
BYE	Number of BYE requests sent. A user sends a BYE request to abandon a session. A BYE request from either user automatically terminates the session.

Table 23: show security alg sip counters Output Fields *(continued)*

Field Name	Field Description
RR header exceeded max	Number of times the SIP ALG RR (Record-Route) headers exceeded the maximum limit.
REGISTER	Number of REGISTER requests sent. 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.
OPTIONS	Number of OPTIONS requests sent. An OPTION request is 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.
INFO	Number of INFO requests sent. AN INFO message is used to communicate mid-session signaling information along the signaling path for the call.
MESSAGE	Number of MESSAGE requests sent. 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).
NOTIFY	Number of NOTIFY requests sent. NOTIFY requests are sent to inform subscribers of changes in state to which the subscriber has a subscription.
PRACK	Number of PRACK requests sent. The PRACK request plays the same role as ACK, but for provisional responses.
PUBLISH	Number of PUBLISH requests sent. The PUBLISH request used for publishing event state. PUBLISH is similar to REGISTER in that it allows a user to create, modify, and remove state in another entity which manages this state on behalf of the user.
REFER	Number of REFER requests sent. A REFER request is used to refer the recipient (identified by the Request-URI) to a third party by the contact information provided in the request.
SUBSCRIBE	Number of SUBSCRIBE requests sent. A SUBCRIBE request is used to request current state and state updates from a remote node.
UPDATE	Number of UPDATE requests sent. AN UPDATE request is used to create a temporary opening in the firewall (pinhole) for new or updates Session Description Protocol (SDP) information. The following fields are modified: Via, From, To, Call-ID, Contact, Route, and Record-Route.
BENOTIFY	Number of BENOTIFY requests sent. A BENOTIFY request is used to reduce the unnecessary SIP signaling traffic on application servers. Applications that do not need a response for a NOTIFY request can enhance performance by enabling BENOTIFY.
SERVICE	Number of SERVICE requests sent. The SERVICE method used by a SIP client to request a service of a SIP server. It is a standard SIP message and will be forwarded until it reaches the server or end user which is performing the service.
OTHER	Number of OTHER requests sent.
Total Pkt-in	Number of SIP ALG total packets received.

Table 23: show security alg sip counters Output Fields *(continued)*

Field Name	Field Description
Total Pkt dropped on error	Number of SIP ALG total packets dropped while transmission and retransmission of messages.
Call error	Number of SIP ALG call errors.
IP resolve error	Number of SIP ALG IP address resolution errors.
NAT error	Number of SIP ALG NAT errors.
Resource manager error	Number of SIP ALG resource manager errors.
Contact header exceeded max	Number of times the SIP ALG contact headers exceeded the maximum limit.
Invite Dropped due to call limit	Number of SIP ALG invite dropped due to call limits.
SIP msg not processed by stack	Number of SIP ALG stack errors.
SIP msg not processed by alg	Number of SIP ALG messages not processed by ALGs.
SIP unknown method dropped	Number of SIP ALG unknown method errors.
Decoding error	Number of SIP ALG decoding errors.
Request for disconnected call	Number of SIP ALG calls disconnected.
Request out of state	Number of SIP ALG messages out of state errors.

Sample Output

show security alg sip counters

```
user@host> show security alg sip counters
SIP message counters(T:Transmit, RT:Retransmit):
   Method      T     1xx   2xx   3xx   4xx   5xx   6xx
               RT    RT    RT    RT    RT    RT    RT
      INVITE   4     4     3     0     0     0     0
               0     0     0     0     0     0     0
      CANCEL   0     0     0     0     0     0     0
               0     0     0     0     0     0     0
         ACK   3     0     0     0     0     0     0
               0     0     0     0     0     0     0
         BYE   3     0     3     0     0     0     0
               0     0     0     0     0     0     0
    REGISTER   7     0     7     0     0     0     0
               0     0     0     0     0     0     0
     OPTIONS   0     0     0     0     0     0     0
               0     0     0     0     0     0     0
        INFO   0     0     0     0     0     0     0
               0     0     0     0     0     0     0
     MESSAGE   0     0     0     0     0     0     0
```

	0	0	0	0	0	0	0
NOTIFY	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
PRACK	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
PUBLISH	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
REFER	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
SUBSCRIBE	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
UPDATE	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
BENOTIFY	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
SERVICE	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
OTHER	0	0	0	0	0	0	0
	0	0	0	0	0	0	0

```
SIP Error Counters:
Total Pkt-in                      :34
Total Pkt dropped on error        :0
Call error                        :0
IP resolve error                  :0
NAT error                         :0
Resource manager error            :0
RR header exceeded max            :0
Contact header exceeded max       :0
Call Dropped due to limit              : 0
SIP stack error                            : 0
SIP decode error                        : 0
SIP unknown method error          : 0
RTO message sent                     : 0
RTO message received              : 0
RTO buffer allocation failure        : 0
RTO buffer transmit failure          : 0
RTO send processing error         : 0
RTO receive processing error      : 0
RTO receive invalid length          : 0
RTO receive call process error     : 0
RTO receive call allocation error    : 0
RTO receive call register error      : 0
RTO receive invalid status error    : 0
```

show security alg sip rate

Supported Platforms	SRX Series, vSRX
Syntax	show security alg sip rate <node (*node-id* | all | local | primary)>
Release Information	Command modified in Junos OS Release 9.2; **node** options added in Junos OS Release 9.0.
Description	Display rate information for Session Initiation Protocol (SIP) Application Layer Protocol (ALG) messages.

Options	• none—Display all SIP ALG rate information.
	
	• **node**—(Optional) For chassis cluster configurations, display SIP rate on a specific node (device) in the cluster.
	
	    • *node-id* —Identification number of the node. It can be 0 or 1.
	
	    • **all**—Display information about all nodes.
	
	    • **local**—Display information about the local node.
	
	    • **primary**—Display information about the primary node.

Required Privilege Level	view
Related Documentation	• sip (Security) on page 373
List of Sample Output	show security alg sip rate on page 430
Output Fields	Table 24 on page 429 lists the output fields for the **show security alg sip rate** command. Output fields are listed in the approximate order in which they appear.

Table 24: show security alg sip rate Output Fields

Field Name	Field Description
CPU ticks	SIP ALG CPU ticks per microsecond.
Time taken	Time, in microseconds, that the last SIP ALG message needed to transit the network.
Total time	Total time, in microseconds, during an interval of less than 10 minutes for the specified number of SIP ALG messages to transit the network.
Rate	Number of SIP ALG messages per second transiting the network.

Sample Output

show security alg sip rate

```
user@host> show security alg sip rate
CPU ticks per us is 166
Time taken for the last message is 1103 us
Total time taken for 3124 messages is 6221482 us (in less than 10 minutes)
Rate: 502 messages/second
```

show security alg status

Supported Platforms	SRX Series, vSRX
Syntax	**show security alg status**
Release Information	Command modified in Junos OS Release 9.5.
Description	Display the status (enabled/disabled) of the supported Application Layer Gateway (ALG) transactions.

The following list describes the default status on each of these devices:

- SRX1500, SRX5400, SRX5600, and SRX5800 devices—FTP, TFTP, DNS, MS-RPC, PPTP, SUNRPC, SQL, and TALK ALGs are enabled by default. All other ALGs are disabled.

- SRX300, SRX320, SRX340, and SRX1500 devices—All supported ALGs are enabled by default.

- On all SRX Series devices — The RSH ALG is disabled by default.

Options	none—Display status of all supported ALGs.
Required Privilege Level	view
Related Documentation	• alg on page 312
Output Fields	The following list describes the output fields for the **show security alg status** command. Output fields are listed in the approximate order in which they appear.

- **DNS**—Domain Name Server

- **FTP**—File Transfer Protocol

- **H323**—H.323 protocol

- **MGCP**—Media Gateway Control Protocol

- **MSRPC**—Microsoft remote procedure call

- **PPTP**—Point-to-Point Tunneling Protocol

- **RSH**—UNIX remote shell services

- **RTSP**—Real-Time Streaming Protocol

- **SCCP**—Skinny Client Control Protocol

- **SIP**—Session Initiation Protocol

- **SQL**—Oracle SQL

- **SUNRPC**—Sun Microsystems remote procedure call

- **TALK**—TALK program

- **TFTP**—Trivial File Transfer Protocol

- **IKE-ESP**—Internet Key Exchange and Encapsulating Security Payload

Sample Output

show security alg status

```
user@host> show security alg status
ALG Status :

  DNS       : Enabled

  FTP       : Enabled

  H323      : Disabled

  MGCP      : Disabled

  MSRPC     : Enabled

  PPTP      : Enabled

  RSH       : Disabled

  RTSP      : Disabled

  SCCP      : Disabled

  SIP       : Disabled

  SQL       : Enabled

  SUNRPC    : Enabled

  TALK      : Enabled

  TFTP      : Enabled

  IKE-ESP   : Disabled
```

show security flow gate

Supported Platforms	SRX Series, vSRX
Syntax	show security flow gate [<filter>] [brief | summary}
Release Information	Command introduced in Junos OS Release 8.5; Filter and display options added in Junos OS Release 10.2.
Description	Display information about temporary openings known as pinholes or gates in the security firewall. Pinholes are used by applications that commonly have both control and data sessions and must create openings in the firewall for the data sessions based on information from the parent sessions.
Options	• destination-port—Destination port • destination-prefix—Destination IP prefix or address • protocol—IP protocol number • source-port—Source port • source-prefix—Source IP prefix or address • brief | summary—Display the specified level of output.
Required Privilege Level	view
Related Documentation	• *show security flow gate brief node* • *show security flow gate destination-port* • *show security flow gate destination-prefix* • *show security flow gate protocol* • *show security flow gate summary node*
List of Sample Output	show security flow gate on page 434 show security flow gate brief on page 435 show security flow gate summary on page 436
Output Fields	Table 25 on page 433 lists the output fields for the **show security flow gate** command. Output fields are listed in the approximate order in which they appear.

Table 25: show security flow gate Output Fields

Field Name	Field Description
Hole	Range of flows permitted by the pinhole.

Table 25: show security flow gate Output Fields *(continued)*

Field Name	Field Description
Translated	Tuples used to create the session if it matches the pinhole. • Source address and port • Destination address and port
Protocol	Application protocol, such as UDP or TCP.
Application	Name of the application.
Age	Idle timeout for the pinhole.
Flags	Internal debug flags for the pinhole.
Zone	Incoming zone.
Reference count	Number of resource manager references to the pinhole.
Resource	Resource manager information about the pinhole.
Valid gates	Number of valid gates.
Pending gates	Number of pending gates.
Invalidated gates	Number of invalid gates.
Gates in other states	Number of gates in other states.
Total gates	Number of gates in total.
Maximum gates	Number of maximum gates

Sample Output

show security flow gate

```
user@host> show security flow gate
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.198.51.100.252/64515-64515
Translated: 0.0.0.0/0->10.0.31.161/25415
Protocol: udp
Application: none/0
Age: 101 seconds
Flags: 0xe001
Zone: untrust
Reference count: 1
Resource: 5-1024-8185
Hole: 0.0.0.0-0.0.0.0/0-198.51.100.252/1046-1046
Translated: 198.51.100.252/36039-> 203.0.113.1/5060
Protocol: udp
Application: junos-sip/63
Age: 65535 seconds
```

```
Flags: 0xe200
Zone: untrust
Reference count: 1
Resource: 5-1024-8189
Hole: 0.0.0.0-0.0.0.0/0-0->198.51.100.252-198.51.100.252/24101-24101
Translated: 0.0.0.0/0-> 198.51.100.252/24101
Protocol: udp
Application: none/0
Age: 93 seconds
Flags: 0xe001
Zone: trust
Reference count: 1
Resource: 5-1024-8188
Hole: 0.0.0.0-0.0.0.0/0-0->40.1.1.5-198.51.100.252/24100-24100
Translated: 0.0.0.0/0->198.51.100.252/24100
Protocol: udp
Application: none/0
Age: 93 seconds
Flags: 0xe001
Zone: trust
Reference count: 1
Resource: 5-1024-8191
Hole: 0.0.0.0-0.0.0.0/0-0->198.51.100.252-198.51.100.252/5060-5060
Translated: 0.0.0.0/0->198.51.100.252/5060
Protocol: udp
Application: junos-sip/63
Age: 65535 seconds
Flags: 0xe200
Zone: trust
Reference count: 1
Resource: 5-1024-8190
```

show security flow gate brief

```
root> show security flow gate brief
Flow Gates on FPC4 PIC1:

Hole: 192.0.2.1-192.0.2.1/0->192.0.2.100-192.0.2.100/38143-38143
  Translated: 192.0.2.1->192.0.2.100/38143
  Protocol: tcp
  Application: FTP ALG/79
  Age: 65532 seconds
  Flags: 0x0080
  Zone: trust
  Reference count: 1
  Resource: 1-24576-86016

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

```
Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
```

show security flow gate summary

```
root> show security flow gate summary
Flow Gates on FPC4 PIC1:

Valid gates: 1
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 1
Maximum gates: 131072

Flow Gates on FPC5 PIC0:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072

Flow Gates on FPC5 PIC1:

Valid gates: 0
Pending gates: 0
Invalidated gates: 0
Gates in other states: 0
Total gates: 0
Maximum gates: 131072
```

show security flow session

Supported Platforms	SRX Series, vSRX
Syntax	show security flow session [*filter*] [brief | extensive | summary]
Release Information	Command introduced in Junos OS Release 8.5. Support for filter and view options added in Junos OS Release 10.2. Application firewall, dynamic application, and logical system filters added in Junos OS Release 11.2. Policy ID filter added in Junos OS Release 12.3X48-D10. Support for connection tag added in Junos OS Release 15.1X49-D40.
Description	Display information about all currently active security sessions on the device.

> NOTE: For the normal flow sessions, the show security flow session command displays bytes counters based on IP header length. However for sessions in Express Path mode, the statistics is collected from IOC2 and IOC3 ASIC hardware engine, and includes full packet length with L2 headers. Because of this, the output displays slightly larger bytes counters for sessions in Express Path mode than the normal flow session.

Options

- *filter*—Filter the display by the specified criteria.

  The following filters reduce the display to those sessions that match the criteria specified by the filter. Refer to the specific **show** command for examples of the filtered output.

  application—Predefined application name

  application-firewall—Application firewall enabled

  application-firewall-rule-set—Application firewall enabled with the specified rule set

  application-traffic-control—Application traffic control session

  application-traffic-control-rule-set—Application traffic control rule set name and rule name

  conn-tag—Session connection tag

  destination-port—Destination port

  destination-prefix—Destination IP prefix or address

  dynamic-application—Dynamic application

  dynamic-application-group—Dynamic application

  encrypted—Encrypted traffic

  extensive—Display detailed output

family—Display session by family

idp—IDP enabled sessions

interface—Name of incoming or outgoing interface

logical-system (all | *logical-system-name*)—Name of a specific logical system or all to display all logical systems

nat—Display sessions with network address translation

policy-id—Display session information based on policy ID; the range is 1 through 4,294,967,295

protocol—IP protocol number

resource-manager—Resource manager

root-logical-system—Display root logical system as default

security-intelligence—Display security intelligence sessions

services-offload—Display services offload sessions

session-identifier—Display session with specified session identifier

source-port—Source port

source-prefix—Source IP prefix

summary—Display output summary

tunnel—Tunnel sessions

- brief | extensive | summary—Display the specified level of output.
- none—Display information about all active sessions.

Required Privilege Level	view

Related Documentation

- *Juniper Networks Devices Processing Overview*
- *clear security flow session all*

List of Sample Output

Output Fields

lists the output fields for the **show security flow session** command. Output fields are listed in the approximate order in which they appear.

Table 26: show security flow session Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. Use this ID to get more information about the session.
Conn Tag	A 32-bit connection tag that uniquely identifies the GPRS tunneling protocol, user plane (GTP-U) and the Stream Control Transmission Protocol (STCP) sessions. The connection tag for GTP-U is the tunnel endpoint identifier (TEID) and for SCTP is the vTag. The connection ID remains 0 if the connection tag is not used by the sessions.
CP Session ID	Number that identifies the central point session. Use this ID to get more information about the central point session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes. The three available flags are: • flag • natflag • natflag2
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Dynamic application	Name of the application.
Application traffic control rule-set	AppQoS rule set for this session.
Rule	AppQoS rule for this session.
Forwarding class	The AppQoS forwarding class name for this session that distinguishes the transmission priority
DSCP code point	Differentiated Services (DiffServ) code point (DSCP) value remarked by the matching rule for this session.

Table 26: show security flow session Output Fields *(continued)*

Field Name	Field Description
Loss priority	One of four priority levels set by the matching rule to control discarding a packet during periods of congestion. A high loss priority means a high probability that the packet could be dropped during a period of congestion.
Rate limiter client to server	The rate-limiter profile assigned to the client-to-server traffic defining a unique combination of **bandwidth-limit** and **burst-size-limit** specifications.
Rate limiter server to client	The rate-limiter profile assigned to the server-to-client traffic defining a unique combination of **bandwidth-limit** and **burst-size-limit** specifications.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Maximum number of sessions permitted.

Sample Output

show security flow session

```
root> show security flow session
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 56, Valid
  In: 203.0.113.1/1000 --> 203.0.113.11/2000;udp, Conn Tag: 0x0, If: reth1.0,
Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.11/2000 --> 203.0.113.1/1000;udp, Conn Tag: 0x0, If: reth0.0,
Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1
```

show security flow session brief

```
root> show security flow session brief
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Policy name: SG/4, State: Active, Timeout: 62, Valid
  In: 203.0.113.11/1000 --> 203.0.113.1/2000;udp, Conn Tag: 0x0, If: reth1.0,
Pkts: 1, Bytes: 86, CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp, Conn Tag: 0x0, If: reth0.0,
Pkts: 0, Bytes: 0, CP Session ID: 10320276

Total sessions: 1
```

show security flow session extensive

```
root> show security flow session extensive
Flow Sessions on FPC0 PIC1:

Session ID: 10115977, Status: Normal, State: Active
Flags: 0x8000040/0x18000000/0x12000003
Policy name: SG/4
Source NAT pool: Null, Application: junos-gprs-gtp-v0-udp/76
Dynamic application: junos:UNKNOWN,
Encryption:  Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 90, Current timeout: 54
Session State: Valid
Start time: 6704, Duration: 35
  In: 203.0.113.11/1000 --> 201.11.0.100/2000;udp,
  Conn Tag: 0x0, Interface: reth1.0,
    Session token: 0x6, Flag: 0x40000021
    Route: 0x86053c2, Gateway: 201.10.0.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 1, Bytes: 86
    CP Session ID: 10320276
  Out: 203.0.113.1/2000 --> 203.0.113.11/1000;udp,
  Conn Tag: 0x0, Interface: reth0.0,
    Session token: 0x7, Flag: 0x50000000
    Route: 0x86143c2, Gateway: 203.0.113.11, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 0, Bytes: 0
    CP Session ID: 10320276
Total sessions: 1
```

show security flow session summary

```
root> show security flow session summary
Flow Sessions on FPC10 PIC1:
Unicast-sessions: 1
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 1
  Valid sessions: 1
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456
```

```
Flow Sessions on FPC10 PIC2:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456

Flow Sessions on FPC10 PIC3:
Unicast-sessions: 0
Multicast-sessions: 0
Services-offload-sessions: 0
Failed-sessions: 0
Sessions-in-use: 0
  Valid sessions: 0
  Pending sessions: 0
  Invalidated sessions: 0
  Sessions in other states: 0
Maximum-sessions: 6291456
```

show security flow session application

Supported Platforms   SRX Series, vSRX

Syntax   show security flow session application
application-name [brief | extensive | summary]

Release Information   Command introduced in Junos OS Release 8.5. Filter and view options added in Junos OS Release 10.2.

Description   Display information about each session of the specified application type.

Options   • *application-name*—Type of application about which to display sessions information. Possible values are:

  • dns—Domain Name System

  • ftp—File Transfer Protocol

  • ignore—Ignore application type

  • mgcp-ca—Media Gateway Control Protocol with Call Agent

  • mgcp-ua—MGCP with User Agent

  • pptp—Point-to-Point Tunneling Protocol

  • q931—ISDN connection control protocol

  • ras—Remote Access Server

  • realaudio—RealAudio

  • rsh—UNIX remote shell services

  • rtsp—Real-Time Streaming Protocol

  • sccp—Skinny Client Control Protocol

  • sip—Session Initiation Protocol

  • sqlnet-v2—Oracle SQLNET

  • talk—TALK program

  • tftp—Trivial File Transfer Protocol

• brief | extensive | summary—Display the specified level of output.

Required Privilege Level   view

Related Documentation   • clear security flow session application on page 406

List of Sample Output   show security flow session application telnet on page 445
show security flow session application telnet brief on page 445
show security flow session application telnet extensive on page 445

Output Fields   lists the output fields for the **show security flow session application** command. Output fields are listed in the approximate order in which they appear.

Table 27: show security flow session application Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Unicast-sessions	Number of unicast sessions.
Multicast-sessions	Number of multicast sessions.
Failed-sessions	Number of failed sessions.

Table 27: show security flow session application Output Fields *(continued)*

Field Name	Field Description
Sessions-in-use	Number of sessions in use. • Valid sessions • Pending sessions • Invalidated sessions • Sessions in other states
Maximum-sessions	Number of maximum sessions.

Sample Output

show security flow session application telnet

```
root> show security flow session application telnet
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 203.0.113.2/32781 --> 192.0.2.5/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 192.0.2.5/23 --> 203.0.113.2/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

show security flow session application telnet brief

```
root> show security flow session application telnet brief
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Policy name: default-policy/2, Timeout: 1796, Valid
  In: 203.0.113.2/32781 --> 192.0.2.5/23;tcp, If: ge-0/0/2.0, Pkts: 10, Bytes:
610
  Out: 192.0.2.5/23 --> 203.0.113.2/32781;tcp, If: ge-0/0/1.0, Pkts: 9, Bytes:
602
Total sessions: 1
```

show security flow session application telnet extensive

```
root> show security flow session application telnet extensive
Flow Sessions on FPC4 PIC1:
Total sessions: 0

Flow Sessions on FPC5 PIC0:
Total sessions: 0
```

```
Flow Sessions on FPC5 PIC1:

Session ID: 210067547, Status: Normal
Flag: 0x40
Policy name: default-policy/2
Source NAT pool: Null, Application: junos-telnet/10
Maximum timeout: 1800, Current timeout: 1788
Session State: Valid
Start time: 670184, Duration: 33
   In: 203.0.113.2/32781 --> 192.0.2.5/23;tcp,
    Interface: ge-0/0/2.0,
    Session token: 0x180, Flag: 0x0x21
    Route: 0x60010, Gateway: 203.0.113.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 10, Bytes: 610
   Out: 192.0.2.5/23 --> 203.0.113.2/32781;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x1c0, Flag: 0x0x20
    Route: 0x70010, Gateway: 192.0.2.100, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 9, Bytes: 602
Total sessions: 1
```

show security flow session application telnet summary

```
root> show security flow session application telnet summary
Flow Sessions on FPC4 PIC1:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC0:

Valid sessions: 0
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 0

Flow Sessions on FPC5 PIC1:

Valid sessions: 1
Pending sessions: 0
Invalidated sessions: 0
Sessions in other states: 0
Total sessions: 1
```

show security flow session resource-manager

Supported Platforms	SRX Series, vSRX
Syntax	show security flow session resource-manager [brief | extensive | summary]
Release Information	Command introduced in Junos OS Release 8.5; Filter and view options introduced in Junos OS Release 10.2.
Description	Display information about sessions created by the resource manager.
Options	none—Display all resource manager sessions. **brief | extensive | summary**—Display the specified level of output.
Required Privilege Level	view
Related Documentation	• *Juniper Networks Devices Processing Overview* • *clear security flow session resource-manager*
List of Sample Output	show security flow session resource-manager on page 448 show security flow session resource-manager brief on page 449 show security flow session resource-manager extensive on page 449 show security flow session resource-manager summary on page 450
Output Fields	Table 28 on page 447 lists the output fields for the **show security flow session resource-manager** command. Output fields are listed in the approximate order in which they appear.

Table 28: show security flow session resource-manager Output Fields

Field Name	Field Description
Session ID	Number that identifies the session. You can use this ID to get additional information about the session.
Policy name	Policy that permitted the traffic.
Timeout	Idle timeout after which the session expires.
Resource information	Information about the session particular to the resource manager, including the name of the ALG, the group ID. and the resource ID.
In	Incoming flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).

Table 28: show security flow session resource-manager Output Fields *(continued)*

Field Name	Field Description
Out	Reverse flow (source and destination IP addresses, application protocol, interface, session token, route, gateway, tunnel, port sequence, FIN sequence, FIN state, packets and bytes).
Total sessions	Total number of sessions.
Status	Session status.
Flag	Internal flag depicting the state of the session, used for debugging purposes.
Policy name	Name and ID of the policy that the first packet of the session matched.
Source NAT pool	The name of the source pool where NAT is used.
Application	Name of the application.
Maximum timeout	Maximum session timeout.
Current timeout	Remaining time for the session unless traffic exists in the session.
Session State	Session state.
Start time	Time when the session was created, offset from the system start time.
Valid sessions	Number of valid sessions.
Pending sessions	Number of pending sessions.
Invalidated sessions	Number of invalidated sessions.
Sessions in other states	Number of sessions in other states.
CP Session ID	Number that identifies the central point session. Use this ID to get more information about the central point session.

Sample Output

show security flow session resource-manager

```
root> show security flow session resource-manager
Flow Sessions on FPC10 PIC1:

Session ID: 410000664, Policy name: p1/4, Timeout: 1734, Valid
Resource information : FTP ALG, 1, 0
  In: 200.0.0.10/41047 --> 60.0.0.2/21;tcp, If: ge-7/1/0.0, Pkts: 13, Bytes: 586,
 CP Session ID: 410001274
  Out: 60.0.0.2/21 --> 200.0.0.10/41047;tcp, If: ge-7/1/1.0, Pkts: 13, Bytes:
803, CP Session ID: 410001274
Total sessions: 1
```

```
                                  Flow Sessions on FPC10 PIC2:
                                  Total sessions: 0

                                  Flow Sessions on FPC10 PIC3:
                                  Total sessions: 0
```

show security flow session resource-manager brief

```
                      root> show security flow session resource-manager brief
                      Flow Sessions on FPC10 PIC1:

                      Session ID: 410000664, Policy name: p1/4, Timeout: 1704, Valid
                      Resource information : FTP ALG, 1, 0
                        In: 200.0.0.10/41047 --> 60.0.0.2/21;tcp, If: ge-7/1/0.0, Pkts: 13, Bytes: 586,
                       CP Session ID: 410001274
                        Out: 60.0.0.2/21 --> 200.0.0.10/41047;tcp, If: ge-7/1/1.0, Pkts: 13, Bytes:
                      803, CP Session ID: 410001274
                      Total sessions: 1

                      Flow Sessions on FPC10 PIC2:
                      Total sessions: 0

                      Flow Sessions on FPC10 PIC3:
                      Total sessions: 0
```

show security flow session resource-manager extensive

```
                      root> show security flow session resource-manager extensive
                      Flow Sessions on FPC10 PIC1:

                      Session ID: 410000664, Status: Normal
                      Flags: 0x42/0x0/0x2010103
                      Policy name: p1/4
                      Source NAT pool: Null, Application: junos-ftp/1
                      Dynamic application: junos:UNKNOWN,
                      Encryption:  Unknown
                      Application traffic control rule-set: INVALID, Rule: INVALID
                      Maximum timeout: 1800, Current timeout: 1682
                      Session State: Valid
                      Start time: 160496, Duration: 153
                      Client: FTP ALG, Group: 1, Resource: 0
                        In: 200.0.0.10/41047 --> 60.0.0.2/21;tcp,
                          Interface: ge-7/1/0.0,
                          Session token: 0x6, Flag: 0xc0002621
                          Route: 0x70010, Gateway: 200.0.0.10, Tunnel: 0
                          Port sequence: 0, FIN sequence: 0,
                          FIN state: 0,
                          Pkts: 13, Bytes: 586
                          CP Session ID: 410001274
                        Out: 60.0.0.2/21 --> 200.0.0.10/41047;tcp,
                          Interface: ge-7/1/1.0,
                          Session token: 0x7, Flag: 0xc0002620
                          Route: 0x80010, Gateway: 60.0.0.2, Tunnel: 0
                          Port sequence: 0, FIN sequence: 0,
                          FIN state: 0,
                          Pkts: 13, Bytes: 803
                          CP Session ID: 410001274
                      Total sessions: 1

                      Flow Sessions on FPC10 PIC2:
```

```
                              Total sessions: 0

                              Flow Sessions on FPC10 PIC3:
                              Total sessions: 0
```

show security flow session resource-manager summary

```
               root> show security flow session resource-manager summary
               Flow Sessions on FPC10 PIC1:

               Valid sessions: 1
               Pending sessions: 0
               Invalidated sessions: 0
               Sessions in other states: 0
               Total sessions: 1

               Flow Sessions on FPC10 PIC2:

               Valid sessions: 0
               Pending sessions: 0
               Invalidated sessions: 0
               Sessions in other states: 0
               Total sessions: 0

               Flow Sessions on FPC10 PIC3:

               Valid sessions: 0
               Pending sessions: 0
               Invalidated sessions: 0
               Sessions in other states: 0
               Total sessions: 0
```

show security idp policy-templates

Supported Platforms	SRX Series, vSRX
Syntax	show security idp policy-templates
Release Information	Command introduced in Junos OS Release 10.1.
Description	Display the list of available policy templates.
Required Privilege Level	view
Related Documentation	• *show security idp active-policy*
Output Fields	user@host> **show security idp policy-templates**

Sample Output

```
DMZ_Services
DNS_Service
File_Server
Getting_Started
IDP_Default
Recommended
Web_Server
```

show security resource-manager group active

Supported Platforms   SRX Series, vSRX

Syntax   show security resource-manager group active
<group-number >
<node (*node-id* | all | local | primary)>

Release Information   Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.

Description   Display security information about active groups created through the resource manager.

Options
- none—Display resource manager group service information for all active groups.

- *group-number* —(Optional) Display resource manager group service information for a specific group identification number.

- **node**—(Optional) For chassis cluster configurations, display active resource manager group service information on a specific node.

  - *node-id* —Identification number of the node. It can be 0 or 1.

  - **all**—Display information about all nodes.

  - **local**—Display information about the local node.

  - **primary**—Display information about the primary node.

Required Privilege Level   view

Related Documentation
- *Juniper Networks Devices Processing Overview*

List of Sample Output
show security resource-manager group active on page 453
show security resource-manager group active 2048 on page 453
show security resource-manager group active node primary on page 453
show security resource-manager group active node all on page 453
show security resource-manager group active 1024 node all on page 453

Output Fields   Table 29 on page 452 lists the output fields for the **show security resource-manager group** command. Output fields are listed in the approximate order in which they appear.

Table 29: show security resource-manager group Output Fields

Field Name	Field Description
Total groups	Total number of groups in the system.
active groups	Number of active groups.
Group ID	Identification number whose group information is displayed.

Sample Output

show security resource-manager group active

```
user@host> show security resource-manager group active
Total groups 32, active groups 0
```

Sample Output

show security resource-manager group active 2048

```
user@host> show security resource-manager group active 2048
Total groups 2048, active groups 1
Group ID 2048: state - Active
        : Virtual System    - root
        : Application        - SIP ALG
        : Group Timeout      - 65535
        : Number of resources - 3
            Resource ID - 8190
            Resource ID - 8188
            Resource ID - 8187
```

Sample Output

show security resource-manager group active node primary

```
user@host> show security resource-manager group active node primary
node0:
--------------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
```

Sample Output

show security resource-manager group active node all

```
user@host> show security resource-manager group active node all
node0:
--------------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
node1:
--------------------------------------------------------------------------------
Group ID 1024: Application - SIP ALG
Total groups 1024, active groups 1
```

Sample Output

show security resource-manager group active 1024 node all

```
user@host> show security resource-manager group active 1024 node all
node0:
--------------------------------------------------------------------------------
Group ID 1024: state - Active
        : Application        - SIP ALG
        : Group Timeout      - 65535
        : Number of resources - 3
            Resource ID - 8192
            Resource ID - 8188
            Resource ID - 8187
```

```
node1:
--------------------------------------------------------------------------
Group ID 1024: state - Active
        : Application        - SIP ALG
        : Group Timeout      - 65535
        : Number of resources - 3
              Resource ID - 8187
              Resource ID - 8186
              Resource ID - 8190
```

show security resource-manager resource active

Supported Platforms	SRX Series, vSRX
Syntax	show security resource-manager resource **active** *<resource-id >* <node (*node-id* | all | local | primary)>
Release Information	Command introduced in Junos OS Release 8.5; **node** options added in Junos OS Release 9.0.
Description	Display security information about active resources created through the resource manager.

Options	• none—Display information for all active resources.
	• *resource-id* —(Optional) Display information for a resource with a specific identification number.
	• **node**—(Optional) For chassis cluster configurations, display active resource manager information on a specific node.
	    • *node-id* —Identification number of the node. It can be 0 or 1.
	    • **all**—Display information about all nodes.
	    • **local**—Display information about the local node.
	    • **primary**—Display information about the primary node.

Required Privilege Level	view
Related Documentation	• *Juniper Networks Devices Processing Overview*
List of Sample Output	show security resource-manager resource active on page 456 show security resource-manager resource active 5 on page 456 show security resource-manager resource active node local on page 456 show security resource-manager resource active node primary on page 456
Output Fields	Table 30 on page 455 lists the output fields for the **show security resource-manager resource** command. Output fields are listed in the approximate order in which they appear.

Table 30: show security resource-manager resource Output Fields

Field Name	Field Description
Total resources	Total number of resources in the system.
active resources	Number of active resources.
Resource ID	Identification number whose resource information is displayed.

Sample Output

show security resource-manager resource active

```
user@host> show security resource-manager resource active
    Resource ID 7: Group ID - 2, Application - JSF_sip

    Resource ID 6: Group ID - 2, Application - JSF_sip

    Resource ID 5: Group ID - 2, Application - JSF_sip

    Resource ID 4: Group ID - 2, Application - JSF_sip

    Resource ID 3: Group ID - 2, Application - JSF_sip

    Resource ID 1: Group ID - 2, Application - JSF_sip

    Resource ID 2: Group ID - 2, Application - JSF_sip
Total Resources 4326, active resources 7
```

Sample Output

show security resource-manager resource active 5

```
user@host> show security resource-manager resource active 5
Resource ID 5: state - Active
    Application        - asl_client
    Parent group       - 2
    Policy             - 5
    From zone          - untrust
    To zone            - trust
    Resource timeout   - 0
    Number of sessions - 0
    Number of Holes    - 1
        Source IP range        - {0.0.0.0, 0.0.0.0}
        Source port range      - {0, 0}
        Destination IP range   - {33.1.0.200, 33.1.0.200}
        Destination port range - {5060, 5060}
        Translated             - {0.0.0.0/0 -> 33.1.0.200/5060}
        Protocol               - 17
        Reference count        - 1
```

Sample Output

show security resource-manager resource active node local

```
user@host> show security resource-manager resource active node local
node0:
--------------------------------------------------------------------------
    Resource ID 8192: Group ID - 1024, Application - SIP ALG
    Resource ID 8188: Group ID - 1024, Application - SIP ALG
    Resource ID 8187: Group ID - 1024, Application - SIP ALG
Total Resources 8192, active resources 3
```

Sample Output

show security resource-manager resource active node primary

```
user@host> show security resource-manager resource active node primary
node0:
--------------------------------------------------------------------------
```

```
                Resource ID 8192: Group ID - 1024, Application - SIP ALG
                Resource ID 8188: Group ID - 1024, Application - SIP ALG
                Resource ID 8187: Group ID - 1024, Application - SIP ALG
          Total Resources 8192, active resources 3
```

show security resource-manager summary

Supported Platforms	SRX Series, vSRX
Syntax	show security resource-manager summary
Release Information	Command introduced in Junos OS Release 11.4.
Description	Display summary information about active resources, clients, groups, and sessions created through the resource manager.
Required Privilege Level	view
Related Documentation	• *Juniper Networks Devices Processing Overview*
List of Sample Output	show security resource-manager summary on page 458
Output Fields	Table 31 on page 458 lists the output fields for the **show security resource-manager summary** command. Output fields are listed in the approximate order in which they appear.

Table 31: show security resource-manager summary Output Fields

Field Name	Field Description
Active resource-manager clients	Number of active resource manager clients.
Active resource-manager groups	Number of active resource manager groups.
Active resource-manager resources	Number of active resource manager resources.
Active resource-manager sessions	Number of active resource manager sessions.

Sample Output

show security resource-manager summary

```
user@host> show security resource-manager summary

Active resource-manager clients   : 15
Active resource-manager groups    : 1
Active resource-manager resources : 1
Active resource-manager sessions  : 0
```

show security zones

Supported Platforms	SRX Series, vSRX
Syntax	show security zones <detail | terse> < *zone-name* >
Release Information	Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.
Description	Display information about security zones.
Options	• none—Display information about all zones. • **detail** | **terse**—(Optional) Display the specified level of output. • *zone-name* —(Optional) Display information about the specified zone.
Required Privilege Level	view
Related Documentation	• *Security Zones and Interfaces Overview* • *Supported System Services for Host Inbound Traffic* • security-zone on page 371
List of Sample Output	show security zones on page 460 show security zones abc on page 460 show security zones abc detail on page 460 show security zones terse on page 461
Output Fields	Table 32 on page 459 lists the output fields for the **show security zones** command. Output fields are listed in the approximate order in which they appear.

Table 32: show security zones Output Fields

Field Name	Field Description
Security zone	Name of the security zone.
Description	Description of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.
Zone	Name of the zone.

Table 32: show security zones Output Fields *(continued)*

Field Name	Field Description
Type	Type of the zone.

Sample Output

show security zones

```
user@host> show security zones
Functional zone: management
   Description: This is the management zone.
   Policy configurable: No
   Interfaces bound: 1
   Interfaces:
     ge-0/0/0.0
Security zone: Host
   Description: This is the host zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     fxp0.0
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
Security zone: def
   Description: This is the def zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/2.0
```

Sample Output

show security zones abc

```
user@host> show security zones abc
Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
     ge-0/0/1.0
```

Sample Output

show security zones abc detail

```
user@host> show security zones abc detail
Security zone: abc
   Description: This is the abc zone.
```

```
                     Send reset for non-SYN session TCP packets: Off
                     Policy configurable: Yes
                     Interfaces bound: 1
                     Interfaces:
                       ge-0/0/1.0
```

Sample Output

show security zones terse

```
        user@host> show security zones terse
        Zone                    Type
        my-internal             Security
        my-external             Security
        dmz                     Security
```

show security zones type

Supported Platforms	SRX Series, vSRX
Syntax	show security zones type (functional | security) <detail | terse>
Release Information	Command introduced in Junos OS Release 8.5. The **Description** output field added in Junos OS Release 12.1.
Description	Display information about security zones of the specified type.
Options	• **functional**—Display functional zones. • **security**—Display security zones. • **detail | terse**—(Optional) Display the specified level of output.
Required Privilege Level	view
Related Documentation	• *Security Zones and Interfaces Overview* • *Supported System Services for Host Inbound Traffic* • security-zone on page 371
List of Sample Output	show security zones type functional on page 463 show security zones type security on page 463 show security zones type security terse on page 463 show security zones type security detail on page 464
Output Fields	Table 33 on page 462 lists the output fields for the **show security zones type** command. Output fields are listed in the approximate order in which they appear.

Table 33: show security zones type Output Fields

Field Name	Field Description
Security zone	Zone name.
Description	Description of the security zone.
Policy configurable	Whether the policy can be configured or not.
Interfaces bound	Number of interfaces in the zone.
Interfaces	List of the interfaces in the zone.
Zone	Name of the zone.

Table 33: show security zones type Output Fields *(continued)*

Field Name	Field Description
Type	Type of the zone.

Sample Output

show security zones type functional

```
user@host> show security zones type functional
Functional zone: management
  Description: management zone
  Policy configurable: No
  Interfaces bound: 0
  Interfaces:
```

Sample Output

show security zones type security

```
user@host> show security zones type security
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

Sample Output

show security zones type security terse

```
user@host> show security zones type security terse
Zone                   Type
trust                  Security
untrust                Security
junos-host             Security
```

Sample Output

show security zones type security detail

```
user@host> show security zones type security detail
Security zone: trust
  Description: trust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/0.0
Security zone: untrust
  Description: untrust zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
  ge-0/0/1.0
Security zone: junos-host
  Description: junos-host zone
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```