JUNIPER NETWORKS

Network Address Translation for JSF

Published: 2012-07-02

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

Network Address Translation for JSF

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

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:

- M Series
- T Series
- MX Series
- J 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 the *Junos OS CLI User Guide*.

Documentation Conventions

Table 1 on page xiii 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.

Table 2 on page xiii 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**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration 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)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify 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.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web 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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC 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: https://www.juniper.net/alerts/

- 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

CHAPTER 1

Network Address Translation

Network Address Translation Overview for JSF

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks.

NAT is supported on Junos Services Framework (JSF). JSF is a unified framework for the integration of services on Junos OS-based platforms.

NOTE: **Junos operating system (Junos OS) supports NAT on IPv4 and IPv6 networks. However, JSF does not support NAT on IPv6 networks. Therefore, ensure that IPv4 networks are used for configuring NAT on JSF.**

For more information about NAT, refer to the following topics:

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAPT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

Translation Types

The Multiservices PIC interfaces support the following types of translation:

- Static-source translation—Allows you to hide a private network without using NAPT (Network Address Port Translation). It features one-to-one mapping between the original address and the translated address, and mapping is configured statically. For more information, see "Basic NAT" on page 5.
- Dynamic-source translation—Includes two options: dynamic address-only source translation and Network Address Port Translation (NAPT).
  - Dynamic address-only source translation—A NAT address is picked up dynamically from a source NAT pool and the mapping from the original source address to the translated address is maintained as long as there is at least one active flow that uses this mapping. For more information, see "Dynamic NAT" on page 6.
  - NAPT—Both the original source address and the source port are translated. The translated address and port are picked up from the corresponding NAT pool. For more information, see "NAPT" on page 6.
- Static destination translation—Allows you to make selected private servers accessible. It features one-to-one mapping between the translated address and the destination address, and mapping is configured statically. For more information, see "Static Destination NAT" on page 6.

Junos OS supports NAT functionality described in the following RFCs and Internet drafts:

- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 4787, *NAT Behavioral Requirements for Unicast UDP*
- RFC 5382, *NAT Behavioral Requirements for TCP*
- RFC 5508, *NAT Behavioral Requirements for ICMP*

Related Documentation

- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAPT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

IPv4 to IPv4 Traditional NAT

Basic Network Address Translation or Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation or NAPT is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. Together, these two operations, referred

to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.

Traditional NAT, specified in RFC 3022, *Traditional IP Network Address Translator*, is fully supported by Junos OS. In addition, network address port translation (NAPT) is supported for source addresses.

Basic NAT

With Basic NAT, a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, Basic NAT translates source IP addresses and related fields such as IP, TCP, UDP, and ICMP header checksums. For inbound packets, the destination IP address and the checksums listed above are translated.

NAPT

Use Network Address Port Translation (NAPT) to enable the components of the private network to share a single external address. NAPT translates the transport identifier (for example, TCP port number, UDP port number, or ICMP query ID) of the private network into a single external address. NAPT can be combined with Basic NAT to use a pool of external addresses in conjunction with port translation.

For packets outbound from the private network, NAPT translates the source IP address, source transport identifier (TCP/UDP port or ICMP query ID), and related fields, such as IP, TCP, UDP, and ICMP header checksums. For inbound packets, the destination IP address, the destination transport identifier, and the IP and transport header checksums are translated.

Related Documentation

- Translation Types on page 4
- Dynamic NAT on page 6
- Static Destination NAT on page 6

Basic NAT

With Basic NAT, a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, the Basic NAT translates source IP address and related fields such as IP, TCP, UDP and ICMP header checksums. For inbound packets, the destination IP address and the checksums as listed above are translated.

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- NAPT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

NAPT

Network address port translation (NAPT) is a mechanism that allows a private network to share a single external address. NAPT translates the transport identifier (for example, the TCP and UDP port numbers or the ICMP query ID) of the private network into a single external address. NAPT can be combined with Basic NAT to use a pool of external addresses in conjunction with port translation.

For packets outbound from the private network, NAPT translates the source IP address, source transport identifier (TCP/UDP port or ICMP query ID) and related fields, such as IP, TCP, UDP and ICMP header checksums. For inbound packets, the destination IP address, destination transport identifier and the IP and transport header checksums are translated.

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- Dynamic NAT on page 6
- Static Destination NAT on page 6

Dynamic NAT

Dynamic NAT is a mechanism with which a private IP address (source) is mapped to a public IP address drawing from a pool of registered (public) IP addresses. NAT addresses from the pool are assigned dynamically. Assigning addresses dynamically also allows a few public IP addresses to be used by several private hosts in contrast with an equal-sized pool required by source static NAT.

For more information about dynamic address translation, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAPT on page 6
- Static Destination NAT on page 6

Static Destination NAT

Static destination NAT translates the destination address for external traffic to an address specified in a destination pool. The destination pool contains one address and no port configuration.

For more information about static address translation, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAPT on page 6
- Dynamic NAT on page 6

PART 2

Configuration

CHAPTER 2

Configuration Tasks

Configuring Addresses and Ports for Use in NAT Rules

For information about configuring translated addresses, see the following sections:

Configuring Pools of Addresses and Ports

To configure pools for NAT, you need to specify a destination pool or a source pool. You use the **pool** statement to define the addresses that constitute the pool. You can define the pool by specifying addresses (or prefixes), address ranges, and ports that need to be used for network address translation.

To configure a NAT pool, include the **pool** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
pool nat-pool-name {
   address ip-prefix</prefix-length>;
   address-range low minimum-value high maximum-value;
   port (automatic | range low minimum-value high maximum-value)
      preserve-parity
      preserve-range {
   }
}
```

The **address** statement specifies the addresses that constitute the pool. Using this statement, you define the pool by specifying the IP address and IP address prefix.

The **address-range** statement also specifies the addresses that constitute the pool. Using this statement, you define the pool by specifying an address range. In an address range, the **low** value must be a lower number than the **high** value. When multiple address ranges and prefixes are configured, the prefixes are depleted first, followed by the address ranges.

The **port** statement specifies port assignment for the translated addresses. To configure automatic assignment of ports, include the **port automatic** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level. To configure a specific range of port numbers, include the **port range low *minimum-value* high *maximum-value*** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level. By default, Junos OS allocates NAT ports sequentially. To change the way ports are allocated, you can use the **preserve-parity** command, which allocates even ports for packets with even destination ports and odd ports for packets with odd destination ports, or the **preserve-range** command, which allocates ports within a range from 0 through 1023 assuming the original packet contains a destination port in the reserved range. This behavior is applicable to control sessions and not data sessions.

Pool Configuration Constraints for NAT

You must consider the following constraints when configuring a pool for NAT:

- For static source NAT and dynamic source NAT, you can specify multiple IPv4 addresses (or prefixes) and IPv4 address ranges. Up to 32 prefixes or address ranges (or a combination) can be supported within a single pool.
- For static source NAT, the prefixes and address ranges cannot overlap between separate pools.
- For static destination NAT, you can specify multiple address prefixes and address ranges in a single term. Multiple destination NAT terms can share a destination NAT pool. However, the netmask or range for the **from** address must be smaller or equal to the netmask or range for the destination pool address. If you define the pool to be larger than required, some addresses are not used. For example, if you define the pool size as 100 addresses and the rule specifies only 80 addresses, the last 20 addresses in the pool are not used.
- When you specify a port for dynamic source NAT, address ranges are limited to a maximum of 65,000 addresses, for a total of (65,000 x 65,535) or 4,259,775,000 flows. A dynamic NAT pool with no address port translation supports up to 65,535 addresses. There is no limit on the pool size for static source NAT.
- With Network Address Port Translation (NAPT), you can configure up to 32 address ranges with up to 65,536 addresses each.

For constraints on specific translation types, see "Configuring Actions in NAT Rules" on page 17.

Specifying Destination and Source Prefixes

You can directly specify the destination or source prefix used in network address translation without configuring a pool.

To configure the information, include the **rule** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
rule rule-name {
  term term-name {
    then {
      translated {
        destination-prefix prefix;
      }
    }
  }
}
```

Requirements for NAT Addresses

When configuring NAT addresses, keep in mind the following requirements:

- The following addresses, while valid in **inet.0**, cannot be used for NAT translation:
  - **0.0.0.0/32**
  - **127.0.0.0/8** (loopback)
  - **128.0.0.0/16** (martian)
  - **191.255.0.0/16** (martian)
  - **192.0.0.0/24** (martian)
  - **223.255.255.0/24** (martian)
  - **224.0.0.0/4** (multicast)
  - **240.0.0.0/4** (reserved)
  - **255.255.255.255** (broadcast)
- You can specify one or more IPv4 address prefixes in the **pool** statement and in the **from** clause of the NAT rule term. This enables you to configure source translation from a private subnet to a public subnet without defining a rule term for each address in the subnet. Destination translation cannot be configured by this method.
- When you configure static source NAT, the **address** prefix size you configure at the **[edit services nat pool *pool-name*]** hierarchy level must be larger than the **source-address** prefix range configured at the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy level. The **source-address** prefix range must also map to a single subnet or range of IPv4 addresses in the **pool** statement. Any pool addresses that are not used by the **source-address** prefix range are left unused; pools cannot be shared.

NOTE: When you include a NAT configuration that changes IP addresses, the configuration might affect forwarding path features elsewhere in your router configuration, such as source class usage (SCU), destination class usage (DCU), filter-based forwarding, or other features that target specific IP addresses or prefixes.

NAT configuration might also affect routing protocols operation, because the protocol peering, neighbor, and interface addresses can be altered when routing protocols packets transit the Multiservices PIC.

Related Documentation

- Network Address Translation Overview for JSF on page 3
- Example: Configuring Dynamic Address-only Source Translation on page 37
- Example: Configuring Dynamic Source Translation (NAPT) on page 38
- Example: Configuring Static Source Translation on page 39
- Example: Configuring Dynamic and Static Source Translation on page 40
- Example: Configuring Static Source Translation with Multiple Prefixes and Address Ranges on page 41
- Example: Configuring NAT Rules Without Defining a Pool on page 41

Configuring NAT Rules

To configure a NAT rule, include the **rule *rule-name*** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-listlist-name <except>;
    }
    then {
      no-translation;
      translated {
        destination-pool nat-pool-name;
        destination-prefix prefix;
        source-pool nat-pool-name;
        source-prefix prefix;
        translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
      }
```

```
        syslog;
      }
    }
  }
```

Each rule must include a **match-direction** statement that specifies the direction in which the match is applied.

In addition, each NAT rule consists of a set of terms, similar to a firewall filter. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections explain how to configure the components of NAT rules:

- Configuring Match Direction for NAT Rules on page 15
- Configuring Match Conditions in NAT Rules on page 15
- Configuring Actions in NAT Rules on page 17

Configuring Match Direction for NAT Rules

Each rule must include a **match-direction** statement that specifies the direction in which the match is applied. To configure where the match is applied, include the **match-direction** statement at the **[edit services nat rule *rule-name*]** hierarchy level:

```
[edit services nat rule rule-name]
match-direction (input | output);
```

The match direction is used with respect to the traffic flow through the Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it. The criteria for determining packet direction is as follows:

- With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.
- With a next-hop service set, packet direction is determined by the interface used to route the packet to the Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output..
- On the Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered.

Configuring Match Conditions in NAT Rules

To configure NAT match conditions, include the **from** statement at the **[edit services nat rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services nat rule rule-name term term-name]
from {
  application-sets set-name;
  applications [ application-names ];
  destination-address (address | any-unicast) <except>;
  destination-address-range low minimum-value high maximum-value <except>;
  destination-prefix-list list-name <except>;
  source-address (address | any-unicast) <except>;
  source-address-range low minimum-value high maximum-value <except>;
  source-prefix-list list-name <except>;
}
```

To configure traditional NAT, you can use the destination address, a range of destination addresses, the source address, or a range of source addresses as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Junos OS Policy Framework Configuration Guide*.

Alternatively, you can specify a list of source or destination prefixes by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or **source-prefix-list** statement in the NAT rule.

NOTE: If you configure a service set with a destination NAT rule, the address configured in the from condition must be translated. If the service set is deleted from the interface and you want traffic destined to the address to be forwarded without translation, you must explicitly deactivate either the service set or the NAT rule within the service set.

You can include application protocol definitions that you have configured at the **[edit applications]** hierarchy level:

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy level.
- To apply one or more sets of application protocol definitions that you have defined, include the **application-sets** statement at the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy level.

NOTE: If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions. When matched rules include more than one ALG, the more specific ALG takes effect; for example, if the stateful firewall rule includes TCP and the NAT rule includes FTP, the NAT rule takes precedence.

You can configure ALGs for ICMP and trace route under stateful firewall and NAT.

By default, NAT can restore IP, TCP, and UDP headers embedded in the payload of ICMP error messages. You can include the **protocol tcp** and **protocol udp** statements with the **application** statement for NAT configurations.

Configuring Actions in NAT Rules

To configure NAT actions, include the **then** statement at the **[edit services nat rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services nat rule rule-name term term-name]
then {
  >no-translation;
  syslog;
  translated {
    destination-pool nat-pool-name;
    destination-prefix prefix;
    source-pool nat-pool-name;
    source-prefix prefix;
    translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
  }
}
```

The **no-translation** statement allows you to specify addresses that you want to be excluded from NAT.

The **syslog** statement enables you to record an alert in the system logging facility.

The **destination-pool**, **destination-prefix**, **source-pool**, and **source-prefix** statements specify addressing information that you define by including the **pool** statement at the **[edit services nat]** hierarchy level; for more information, see "Configuring Addresses and Ports for Use in NAT Rules" on page 11.

The **translation-type** statement specifies the type of network address translation used for source or destination traffic. Choices are **basic-nat44**, **dynamic-nat44**, **napt44**, or **dnat-44**, which are explained in the following list. For more information, see "Network Address Translation Overview for JSF" on page 3.

NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in IPv4 networks. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in IPv6 networks. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not mentioned here.

- **basic-nat44**—Implement static translation of source IP addresses without port mapping. You must configure the **from destination-address** statement in the match condition for the rule. The size of the address range specified in the statement must be the same or smaller than the destination pool. You must specify either a **destination-pool** or a **destination-prefix**. The referenced pool can contain multiple addresses but no **port** configuration.

  NOTE: In an interface service set, all packets destined for the **destination-address** specified in the match condition are automatically routed to the services PIC, even if no service set is associated with the interface.

- **dynamic-nat44**—Implement dynamic translation of source IP addresses without port mapping. You must specify a **source-pool** name. The referenced pool must include an **address** configuration (for address-only translation).

  The **dynamic-nat44** option supports translating up to 64,000 addresses to a smaller size pool. The requests from the source address range are assigned to the addresses in the pool until the pool is used up, and any additional requests are rejected. A NAT address assigned to a host is used for all concurrent sessions from that host. The address is released to the pool only after all the sessions for that host expire. This feature enables the router to share a few public IP addresses between several private hosts. Since all the private hosts might not simultaneously create sessions, they can share a few public IP addresses.

- **napt44**—Implement dynamic address translation for destination traffic with port mapping. You must specify a **source-pool** name. The referenced pool must include a port configuration (for NAPT). The **napt44** option supports translating up to 32 addresses to a smaller size pool.

  If you specify **port automatic** or a port range, NAPT is used. If a port is not defined, the port value defaults to 1.

- **dnat-44**—Implement static translation of destination IP addresses without port mapping. The size of the pool address space must be greater than or equal to the source address space. You must specify a **source-pool** name. The referenced pool can contain multiple addresses, ranges, or prefixes, as long as the number of NAT addresses in the pool is larger than the number of source addresses in the **from** statement. You must include exactly one **source-address** value at the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy level; if it is a prefix, the size must be less than or equal

to the pool prefix size. Any addresses in the pool that are not matched in the **source-address** value remain unused, because a pool cannot be shared among multiple terms or rules.

NOTE: When configuring NAT, if any traffic is destined for the following addresses and does not match a NAT flow or NAT rule, the traffic is dropped:

- Addresses specified in the **from destination-address** statement, when you are using destination translation
- Addresses specified in the source NAT pool when you are using source translation

For more information on NAT methods, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

Related Documentation

- Network Address Translation Overview for JSF on page 3
- Configuring Addresses and Ports for Use in NAT Rules on page 11
- Configuring NAT Rule Sets on page 19

Configuring NAT Rule Sets

The **rule-set** statement defines a collection of NAT rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services nat]** hierarchy level with a **rule** statement for each rule:

```
rule-set rule-set-name {
  rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, no NAT action is performed on the packet. If a packet is destined to a NAT pool address, it is dropped.

Configuring Juniper Service Framework – Network Address Translation Package, Rules, and Services Set

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks. The Junos operating system (Junos OS) supports NAT on IPv4 networks. To use Junos Services Framework (JSF) to run NAT, you must configure the jservices-nat package at the

hierarchy level. In addition, you must configure NAT rules and a service set with a Multiservice interface. This topic includes the following tasks:

1. Configuring the JSF NAT Package on page 20
2. Configuring the NAT Rule and NAT Pool on page 22
3. Configuring the Services Set for NAT on page 24

Configuring the JSF NAT Package

To configure the JSF-NAT package:

1. In configuration mode, go to the following hierarchy level:

   user@host# edit chassis

2. In the hierarchy level, configure the FPC and PIC.

   [edit chassis]
   user@host# edit fpc *slot* pic *slot*

   In this example, the FPC is in slot 1 and the PIC is in slot 0:

   [edit chassis]
   user@host# edit fpc 1 pic 0

3. Configure the number of cores dedicated to run control functionality.

   [edit chassis fpc *slot* pic *slot*]
   user@host# set adaptive-services service-package extension-provider control-cores *control-cores*

   In this example, the number of control cores is 1.

   [edit chassis fpc 1 pic 0]
   user@host# set adaptive-services service-package extension-provider control-cores 1

4. Configure the number of processing cores dedicated to data.

   [edit chassis fpc *slot* pic *slot*]
   user@host# set adaptive-services service-package extension-provider data-cores *data-cores*

   In this example, the number of data cores is 7.

   [edit chassis fpc 1 pic 0]
   user@host# set adaptive-services service-package extension-provider data-cores 7

5. Configure the size of the object cache in megabytes (MB). Only values in increments of 128 MB are allowed and the maximum value of the object cache can be 1280 MB.

   [edit chassis fpc *slot* pic *slot*]
   user@host# set adaptive-services service-package extension-provider object-cache-size *object-cache-size*

In this example, the size of the object cache is 512 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider
  object-cache-size 512
```

6. Configure the size of the policy database in megabytes (MB).

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider policy-db-size
  policy-db-size
```

In this example, the size of the policy database is 64 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider policy-db-size
  64
```

7. Configure the package.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider package
  package
```

In this example, the package is **jservices-nat**.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider package
  jservices-nat
```

8. Configure the extension provider system log, to enable PIC system logging to record or view system log messages:

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider syslog syslog
```

In this example, the system log is set to **daemon any** and **external any**:

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider syslog daemon
  any
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider syslog external
  any
```

9. Verify the configuration.

```
[edit chassis]
user@host# show chassis
fpc 1 {
    pic 0 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 7;
                    object-cache-size 512;
                    policy-db-size 64;
                    package jservices-nat;
                    syslog {
                        daemon any;
                        external any;
```

```
                    }
                }
            }
        }
    }
}
```

Configuring the NAT Rule and NAT Pool

To configure the NAT pool and NAT rule:

1. In configuration mode, go to the following hierarchy level:

   user@host# edit services

2. Configure the NAT pool.

   [edit services]
   user@host# set nat pool *pool*

   In this example, the NAT pool is **p1**.

   [edit services]
   user@host# set nat pool p1

3. Configure the NAT pool address.

   [edit services]
   user@host# set nat pool p1 address *address*

   In this example, the NAT pool address is **20.1.1.10/32**.

   [edit services]
   user@host# set nat pool p1 address 20.1.1.10/32;

4. Configure the NAT pool port.

   [edit services]
   user@host# set nat pool p1 port *port*;

   In this example, the NAT pool port is **automatic**.

   [edit services]
   user@host# set nat pool p1 port automatic;

5. Configure the rule.

   [edit services]
   user@host# set nat rule *rule*

   In this example, the rule is **r1**.

   [edit services]
   user@host# set nat rule r1

6. Configure the match direction.

   [edit services]
   user@host# set nat rule r1 match-direction *match-direction*

   In this example, the match direction is **input**.

   [edit services]

```
user@host# set nat rule r1 match-direction input
```

7. Configure the term.

```
[edit services]
user@host# set nat rule r1 term term
```

In this example, the term is **t1**.

```
[edit services]
user@host# set nat rule r1 term t1
```

8. Configure the input conditions for the NAT term.

```
[edit services]
user@host# set nat rule r1 term t1 from from
```

In this example, the input conditions are **applications junos-tftp** and **applications junos-rsh**.

```
[edit services]
user@host# set nat rule r1 term t1 from applications junos-tftp
[edit services]
user@host# set nat rule r1 term t1 from applications junos-rsh
```

9. Configure the NAT term action.

```
[edit services]
user@host# set nat rule r1 term then then
```

In this example, the term action is **translated**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated
```

10. Configure the properties for translated traffic.

```
[edit services]
user@host# set nat rule r1 term then translated translated
```

In this example, the property for the translated traffic is **source-pool p1**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated source-pool p1
```

11. Configure the properties for translated traffic transaction type.

```
[edit services]
user@host# set nat rule r1 term then translated translation-type translation type
```

In this example, the property for the translated traffic is **dynamic-nat44**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated translation-type dynamic-nat44
```

12. Verify the configuration:

```
[edit services]
user@host# show
}
nat {
    pool p1 {
        address 20.1.1.10/32;
        port {
```

```
            automatic;
        }
    }
    rule r1 {
        match-direction input;
        term t1 {
            from {
                applications [ junos-tftp junos-rsh ];
            }
            then {
                translated {
                    source-pool p1;
                    translation-type dynamic-nat44;
                                    }
            }
        }
    }
}
```

Configuring the Services Set for NAT

To configure the services set for NAT:

1. In configuration mode, go to the following hierarchy level:

   user@host# edit services

2. Configure the service set with a rule.

   [edit services]
   user@host# edit service-set *service-set*

   In this example, the service set with rule is **nat-ss**.

   [edit services]
   user@host# edit service-set nat-ss

3. Configure the service set message rate limit.

   [edit services service-set nat ss]
   user@host# edit syslog *syslog*

   In this example, the service set message rate limit is set to **syslog**, which is the maximum number of system log messages per second allowed from this interface.

   [edit services service-set nat-ss]
   user@host# edit syslog

4. Configure the host attributes.

   [edit services service-set nat ss syslog]
   user@host# edit host *host*

   In this example, the host is **host-local**.

   [edit services service-set nat-ss syslog]
   user@host# edit host host-local

5. Configure the services with services attributes.

   [edit services service-set nat-ss syslog host host-local]
   user@host# set services *services*

In this example, the services attributes is **any**.

```
[edit services service-set nat-ss syslog host host-local]
user@host# set services any
```

6. Configure the service set with NAT rules.

```
[edit services service-set nat ss]
user@host# edit nat-rules nat-rules
```

In this example, the NAT rules is **r1**.

```
[edit services service-set nat-ss]
user@host# edit nat-rules r1
```

7. Configure the interface.

```
[edit services service-set nat ss]
user@host# edit interface interface
```

In this example, the interface is **interface-service**.

```
[edit services service-set nat-ss]
user@host# edit interface interface-service
```

8. Configure the service interface.

```
[edit services service-set nat-ss interface-service]
user@host# set service-interfaceservice-interface
```

In this example, the interface is **ms-1/0/0**.

```
[edit services service-set nat-ss interface-service]
user@host# set service-interface ms-1/0/0
```

9. Verify the configuration.

```
[edit services]
user@host# show services
service-set nat-ss {
            syslog {
                host local {
                    services any;
                }
            }
            nat-rules r1;
            interface-service {
                service-interface ms-1/0/0;
            }
        }
    }
```

Configuring Static Source Translation in IPv4 Networks

To configure the translation type as **basic-nat44**, you must configure the NAT pool and rule, service set with service interface, and trace options. This topic includes the following tasks:

1. Configuring the NAT Pool and Rule on page 26
2. Configuring the Service Set for NAT on page 27
3. Configuring Trace Options on page 28

Configuring the NAT Pool and Rule

To configure the NAT pool, rule, and term:

1. In configuration mode, go to the **[edit services nat]** hierarchy level:

   ```
   [edit]
   user@host# edit services nat
   ```

2. Configure the NAT pool with an address.

   ```
   [edit services nat]
   user@host# set pool pool name address address
   ```

   In the following example, the pool name is **src_pool** and the address is **10.10.10.2/32**.

   ```
   [edit services nat]
   user@host# set pool src_pool address 10.10.10.2/32
   ```

3. Configure the NAT rule and the match direction.

   ```
   [edit services nat]
   user@host# set rule rule-name match-direction match-direction
   ```

   In the following example, the NAT rule name is **rule-basic-nat44** and the match direction is **input**.

   ```
   [edit services nat]
   user@host# set rule rule-basic-nat44 match-direction input
   ```

4. Configure the source address in the **from** statement.

   ```
   [edit services nat]
   user@host# set rule rule-basic-nat44 term term-name from from
   ```

   In the following example, the term name is **t1** and the input condition is **source-address 3.1.1.2/32**.

   ```
   [edit services nat]
   user@host# set rule rule-basic-nat44 term t1 from source-address 3.1.1.2/32
   ```

5. Configure the NAT term action and properties of the translated traffic.

   ```
   [edit services nat]
   user@host# set rule rule-basic-nat44 term t1 then term-action translated-property
   ```

In the following example, the term action is **translated** and the property of the translated traffic is **source-pool src_pool**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated source-pool src_pool
```

6. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated translation-type
  translation-type
```

In the following example, the translation type is **basic-nat44**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated translation-type
  basic-nat44
```

7. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level:

```
[edit services]
user@host# show
nat {
    pool src_pool {
        address 10.10.10.2/32;
    }
    rule rule-basic-nat44 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    3.1.1.2/32;
                }
            }
            then {
                translated {
                    source-pool src_pool;
                    translation-type {
                        basic-nat44;
                    }
                }
            }
        }
    }
}
```

Configuring the Service Set for NAT

To configure the service set for NAT:

1. In configuration mode, go to the **[edit services]** hierarchy level:

```
[edit]
user@host# edit services
```

2. Configure the service set.

```
[edit services]
user@host# edit service-set service-set-name
```

In the following example, the service set name is **s1**.

```
[edit services]
user@host# edit service-set s1
```

3. For the **s1** service set, set the reference to the NAT rules configured at the **[edit services nat]** hierarchy level.

   ```
   [edit services service-set s1]
   user@host# set nat-rules rule-name
   ```

   In the following example, the rule name is **rule-basic-nat44**.

   ```
   [edit services service-set s1]
   user@host# set nat-rules rule-basic-nat44
   ```

4. Configure the service interface.

   ```
   [edit services service-set s1]
   user@host# set interface-service service-interface service-interface-name
   ```

   In the following example, the service interface name is **ms-1/2/0**.

   ```
   [edit services service-set s1]
   user@host# set interface-service service-interface ms-1/2/0
   ```

5. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

   ```
   [edit services]
   user@host# show
   service-set s1 {
       nat-rules rule-basic-nat44;
       interface-service {
           service-interface ms-1/2/0;
       }
   }
   ```

Configuring Trace Options

To configure the trace options at the **[edit services adaptive-services-pics]** hierarchy level:

1. In configuration mode, go to the **[edit services adaptive-services-pics]** hierarchy level:

   ```
   [edit]
   user@host# edit services adaptive-services-pics
   ```

2. Configure the trace options:

   ```
   [edit services adaptive-services-pics]
   user@host# set traceoptions flag tracing parameter
   ```

   In the following example, the tracing parameter is **all**.

   ```
   [edit services adaptive-services-pics]
   user@host# set traceoptions flag all
   ```

3. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

   ```
   [edit services]
   user@host# show
   ```

```
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

Configuring Dynamic Source Address and Port Translation in IPv4 Networks

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. This translation can be configured in both IPv4 and IPv6 networks. This section describes the steps for configuring NAPT in IPv4 networks.

To configure NAPT, you need to configure a rule at the **[edit services nat]** hierarchy level for dynamically translating the source IPv4 addresses.

To configure the NAPT in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level:

   ```
   [edit]
   user@host# edit services
   ```

2. Configure the service set and NAT rule.

   ```
   [edit services]
   user@host# set service-set service-set-name nat-rules rule-name
   ```

   In the following example, the name of the service set is **s1** and the name of the NAT rule is **rule-napt-44**.

   ```
   [edit services]
   user@host# set service-set s1 nat-rules rule-napt-44
   ```

3. Go to the **[interface-service]** hierarchy level of the service set.

   ```
   [edit services]
   user@host# edit service-set s1 interface-service
   ```

4. Configure the service interface.

   ```
   [edit services service-set s1 interface service]
   user@host# set service-interface service-interface-name
   ```

   In the following example, the name of the service interface is **ms-0/1/0**.

   NOTE: If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

   ```
   [edit services service-set s1 interface service]
   user@host# set service-interface ms-0/1/0
   ```

5. Go to the **[edit services nat]** hierarchy level. Issue the command from the top of the services hierarchy, or use the **top** keyword.

   ```
   [edit services service-set s1 interface service]
   ```

```
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the pool is **napt-pool** and the address is **10.10.10.0**.

```
[edit services nat]
user@host# set pool napt-pool address 10.10.10.0
```

7. Configure the port.

```
[edit services nat]
user@host# set pool pool-name port port-type
```

In the following example, the port type is selected as **automatic**.

```
[edit services nat]
user@host# set pool napt-pool port automatic
```

8. Configure the rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction  match-direction
```

In the following example, the name of the rule is **rule-napt-44** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-napt-44 match-direction input
```

9. Configure the term, the action for the translated traffic, and the translation type.

```
[edit services nat]
user@host# set rule rule-name term term-name then translated translated-action
  translation-type translation- type
```

In the following example, the name of the term is **t1**, the action for the translated traffic is **translated**, the name of the source pool is **napt-pool**, and the translation type is **napt-44**.

```
[edit services nat]
user@host# set rule rule-napt-44 match-direction input term t1 then translated
  source-pool napt-pool translation-type napt-44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
```

```
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-napt-44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
nat {
    pool napt-pool {
        address 10.10.10.0/32;
        port {
            automatic;
        }
    }
    rule rule-napt-44 {
        match-direction input;
        term t1 {
            then {
                translated {
                    source-pool napt-pool;
                    translation-type {
                        napt-44;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

Related Documentation

- Example: Configuring Dynamic Source Translation for an IPv4 Network on page 39

Configuring Dynamic Address-Only Source Translation in IPv4 Networks

In IPv4 networks, dynamic address translation (dynamic NAT) is a mechanism to dynamically translate the destination traffic without port mapping. To use dynamic NAT, you must specify a source pool name, which includes an address configuration.

To configure dynamic NAT in IPv4 networks:

1. In configuration mode, navigate to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure the service set and NAT rule.

```
[edit services]
```

```
user@host# set service-set service-set-name nat-rules rule-name
```

In the following example, the name of the service set is **s1**, and the name of the NAT rule is **rule-dynamic-nat44**.

```
[edit services]
user@host# set service-set s1 nat-rules rule-dynamic-nat44
```

3. Go to the **[interface-service]** hierarchy level for the service set.

```
[edit services]
user@host# edit service-set s1 interface-service
```

4. Configure the service interface.

```
[edit services service-set s1 interface-service]
user@host# set service-interface service-interface-name
```

In the following example, the name of the service interface is **ms-0/1/0**.

NOTE: If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface-service]
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the following command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1 interface-service]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the pool is **source-dynamic-pool**, and the address is **10.10.10.0**.

```
[edit services nat]
user@host# set pool source-dynamic-pool address 10.10.10.0
```

7. Configure the rule, match direction, term, and source address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
  source-address address
```

In the following example, the name of the rule is **rule-dynamic-nat44**, the match direction is **input**, the name of the term is **t1**, and the source address is **3.1.1.0**.

```
[edit services nat]
user@host# set rule rule-dynamic-nat44 match-direction input match-direction t1
  from source-address 3.1.1.0
```

8. Go to the **[edit rule rule-dynamic-nat-44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dynamic-nat44 term t1
```

9. Configure the source pool and the translation type.

   ```
   [edit services nat rule rule-dynamic-nat44 term t1]
   user@host# set then translated source-pool src-pool-name translation-type
     translation-type
   ```

   In the following example, the name of the source pool is **source-dynamic-pool** and the translation type is **dynamic-nat44**.

   ```
   [edit services nat rule rule-dynamic-nat44 term t1]
   user@host# set then translated source-pool  source-dynamic-pool translation-type
     dynamic-nat44
   ```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the following command, the **top** keyword ensures that the command is run from the top of the hierarchy.

    ```
    [edit services nat rule rule-dynamic-nat44 term t1]
    user@host# top edit services adaptive-services-pics
    ```

11. Configure the trace options.

    ```
    [edit services adaptive-services-pics]
    user@host# set traceoptions flag tracing parameter
    ```

    In the following example, the tracing parameter is configured as **all**.

    ```
    [edit services adaptive-services-pics]
    user@host# set traceoptions flag all
    ```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

    ```
    [edit services]
    user@host# show
    service-set s1 {
        nat-rules rule-dynamic-nat44;
        interface-service {
            service-interface ms-0/1/0;
        }
    }
     nat {
        pool source-dynamic-pool {
            address 10.1.1.0/24;
        }
        rule rule-dynamic-nat44 {
            match-direction input;
            term t1 {
                from {
                    source-address {
                        3.1.1.0/24;
                    }
                }
                then {
                    translated {
                        destination-pool source-dynamic-pool;
                        translation-type {
                            dynamic-nat44;
                        }
                    }
                }
            }
    ```

```
    }
}
 adaptive-services-pics {
    traceoptions {
        flag all;
    }
 }
```

Related Documentation

- Example: Configuring Dynamic Address-Only Source Translation in an IPv4 Network on page 38

Configuring Static Destination Address Translation in IPv4 Networks

In IPv4 networks, destination address translation is a mechanism to implement address translation for destination traffic without port mapping. To use destination address translation, the size of the pool address space must be greater than or equal to the destination address space. You must specify a name for the **destination-pool** statement, which can contain multiple addresses, ranges, or prefixes, as long as the number of NAT addresses in the pool is larger than the number of destination addresses in the **from** statement.

To configure destination address translation in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level.

   ```
   [edit]
   user@host# edit services
   ```

2. Configure the service set and the NAT rule.

   ```
   [edit services]
   user@host# set service-set service-set-name nat-rules rule-name
   ```

   In the following example, the name of the service set is **s1** and the name of the NAT rule is **rule-dnat44**.

   ```
   [edit services]
   user@host# set service-set s1 nat-rules rule-dnat44
   ```

3. Go to the **[interface-service]** hierarchy level of the service set.

   ```
   [edit services]
   user@host# edit service-set s1 interface-service
   ```

4. Configure the service interface.

   ```
   [edit services service-set s1 interface-service]
   user@host# set service-interface service-interface-name
   ```

   In the following example, the name of the service interface is **ms-0/1/0**.

   NOTE: If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

   ```
   [edit services service-set s1 interface-service]
   ```

```
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the following command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, **dest-pool** is used as the pool name and **4.1.1.2** as the address.

```
user@host# set pool dest-pool address 4.1.1.2
```

7. Configure the rule, match direction, term, and destination address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
  destination-address  address
```

In the following example, the name of the rule is **rule-dnat44**, the match direction is **input**, the name of the term is **t1**, and the address is **20.20.20.20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from
  destination-address 20.20.20.20
```

8. Go to the **[edit services nat rule rule-dnat44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dnat44 term t1
```

9. Configure the destination pool and the translation type.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool-name translation-type
  translation-type
```

In the following example, the destination pool name is **dest-pool**, and the translation type is **dnat-44**.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool translation-type dnat-44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the following command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat rule rule-dnat44 term t1]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
```

```
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-dnat44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
 nat {
    pool dest-pool {
        address 4.1.1.2/32;
    }
    rule rule-dnat44 {
        match-direction input;
        term t1 {
            from {
                destination-address {
                    20.20.20.20/32;
                }
            }
            then {
                translated {
                    destination-pool dest-pool;
                    translation-type {
                        dnat-44;
                    }
                }
            }
        }
    }
}
  adaptive-services-pics {
    traceoptions {
        flag all;
    }
  }
```

Related Documentation

- Example: Configuring Static Destination Address Translation on page 46

CHAPTER 3

NAT Rules Examples

Example: Configuring Dynamic Address-only Source Translation

The following example configures dynamic address-only source translation:

```
[edit services nat]
pool public {
   address-range low 192.16.2.1 high 192.16.2.32;
}
rule Private-Public {
   match-direction input;
   term Translate {
      then {
         translated {
            source-pool public;
            translation-type source dynamic;
         }
      }
   }
}
```

Example: Configuring Dynamic Address-Only Source Translation in an IPv4 Network

The following example configures the translation type as **dynamic-nat44**.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-dynamic-nat44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
 nat {
    pool source-dynamic-pool {
        address 10.1.1.0/24;
    }
    rule rule-dynamic-nat44 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    3.1.1.0/24;
                }
            }
            then {
                translated {
                    destination-pool source-dynamic-pool;
                    translation-type {
                        dynamic-nat44;
                    }
                }
            }
        }
    }
}
 adaptive-services-pics {
    traceoptions {
        flag all;
    }
  }
```

Example: Configuring Dynamic Source Translation (NAPT)

The following example configures dynamic source (address and port) translation, or NAPT:

```
[edit services nat]
pool public {
   address-range low 192.16.2.1 high 192.16.2.32;
   port automatic;
}
rule Private-Public {
   match-direction input;
   term Translate {
     then {
       translated {
         source-pool public;
```

```
            translation-type source dynamic;
        }
    }
}
}
```

NOTE: The only difference between the configurations for dynamic address-only source translation and NAPT is the inclusion of the **port** statement for NAPT.

Example: Configuring Dynamic Source Translation for an IPv4 Network

The following example configures the translation type as **napt-44**.

```
[edit services]
    user@host# show
    service-set s1 {
    nat-rules rule-napt-44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
nat {
    pool napt-pool {
        address 10.10.10.0/32;
        port {
            automatic;
        }
    }
    rule rule-napt-44 {
        match-direction input;
        term t1 {
            then {
                translated {
                    source-pool napt-pool;
                    translation-type {
                        napt-44;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

Example: Configuring Static Source Translation

The following configuration sets up one-to-one mapping between a private subnet and a public subnet:

```
[edit services nat]
pool mypool {
   address 192.16.1.0/28; # public subnet
}
rule src-nat {
   match-direction input;
   term t1 {
      from {
         source-address 10.150.1.0/28; # private subnet
      }
      then {
         translated {
            source-pool mypool;
            translation-type source static;
         }
      }
   }
}
```

Example: Configuring Dynamic and Static Source Translation

In the following configuration, **term1** configures source address translation for traffic from any private address to any public address. The translation is applied for all services. **term2** performs destination address translation for Hypertext Transfer Protocol (HTTP) traffic from any public address to the server's virtual IP address. The virtual server IP address is translated to an internal IP address.

```
[edit services nat]
rule my-nat-rule {
   match-direction input;
   term my-term1 {
      from {
         source-address private;
         destination-address public;
      }
      then {
         translated {
            source-pool my-pool; # pick address from a pool
            translation-type source dynamic; # dynamic NAT with port translation
         }
      }
   }
   term my-term2 {
      from {
         destination-address 192.168.137.3; # my server's virtual address
         application http;
      }
      then {
         translated {
            destination-pool nat-pool-name;
            translation-type destination static; # static destination NAT
         }
      }
   }
}
```

Example: Configuring Static Source Translation with Multiple Prefixes and Address Ranges

The following configuration creates a static pool with an address prefix and an address range and uses static source NAT translation.

```
[edit services nat]
pool p1 {
   address 30.30.30.252/30;
   address-range low 20.20.20.1 high 20.20.20.2;
}
rule r1 {
   match-direction input;
   term {
      from {
         source-address {
            10.10.10.252/30;
         }
      }
      then {
         translated {
            source-pool p1;
            translation-type source static;
         }
      }
   }
}
```

Example: Configuring NAT Rules Without Defining a Pool

The following configuration performs network address translation using the source prefix **20.20.10.0/24** without defining a pool.

```
[edit services nat]
rule src-nat {
   match-direction input;
   term t1 {
      then {
         translation-type source dynamic;
         source-prefix 20.20.10.0/24;
      }
   }
}
```

The following configuration performs network address translation using the destination prefix **20.20.10.0/32** without defining a pool.

```
[edit services nat]
rule src-nat {
   match-direction input;
   term t1 {
      from {
         destination-address 10.10.10.10/32;
         then {
```

```
            translation-type destination static;
            destination-prefix 20.20.10.0/24;
          }
        }
      }
    }
```

Example: Preventing Translation of Specific Addresses

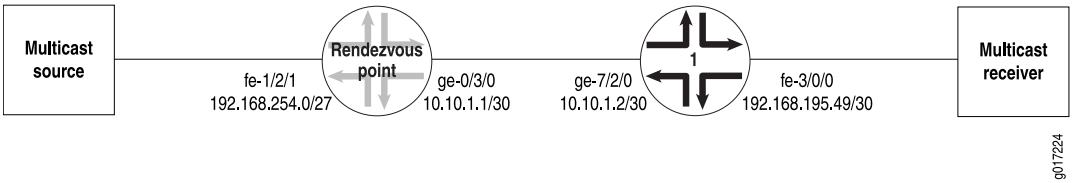
The following configuration specifies that network address translation is not performed on incoming traffic from the source address **192.168.20.24/32**. Dynamic NAT is performed on all other incoming traffic.

```
[edit services nat]
pool my-pool {
  address-range low 10.10.10.1 high 10.10.10.16;
  port-automatic;
}
rule src-nat {
  match-direction input;
  term t0 {
    from {
      source-address 192.168.20.24/32;
    }
    then {
      no-translation;
    }
  }
  term t1 {
    then {
      translated {
        translation-type source dynamic;
        source-pool my-pool;
      }
    }
  }
}
```

Example: Configuring NAT for Multicast Traffic

Figure 1 on page 42 illustrates the network setup for the following configuration, which allows IP multicast traffic to be sent to the Adaptive Services (AS) or MultiServices PIC.

Figure 1: Configuring NAT for Multicast Traffic



- Rendezvous Point Configuration on page 43
- Router 1 Configuration on page 46

Rendezvous Point Configuration

On the rendezvous point (RP), all incoming traffic from the multicast source at **192.168.254.0/27** is sent to the static NAT pool **mcast_pool**, where its source is translated to **20.20.20.0/27**. The service set **nat_ss** is a next-hop service set that allows IP multicast traffic to be sent to the AS or MultiServices PIC. The inside interface on the PIC is **sp-1/1/0.1** and the outside interface is **sp-1/1/0.2**.

```
[edit services]
nat {
    pool mcast_pool {
        address 20.20.20.0/27;
    }
    rule nat_rule_1 {
        match-direction input;
        term 1 {
            from {
                source-address 192.168.254.0/27;
            }
        }
        then {
            translated {
                source-pool mcast_pool;
                translation-type source static;
            }
            syslog;
        }
    }
}
service-set nat_ss {
    allow-multicast;
    nat-rules nat_rule_1;
    next-hop-service {
        inside-service-interface sp-1/1/0.1;
        outside-service-interface sp-1/1/0.2;
    }
}
```

The Gigabit Ethernet interface **ge-0/3/0** carries traffic out of the RP to Router 1. The adaptive services interface **sp-1/1/0** has two logical interfaces: **unit 1** is the inside interface for next-hop services and **unit 2** is the outside interface for next-hop services. Multicast source traffic comes in on the Fast Ethernet interface **fe-1/2/1**, which has the firewall filter **fbf** applied to incoming traffic.

```
[edit interfaces]
ge-0/3/0 {
    unit 0 {
        family inet {
            address 10.10.1.1/30;
        }
    }
}
sp-1/1/0 {
    unit 0 {
```

```
        family inet;
    }
    unit 1 {
        family inet;
        service-domain inside;
    }
    unit 2 {
        family inet;
        service-domain outside;
    }
}
fe-1/2/1 {
    unit 0 {
        family inet {
            filter {
                input fbf;
            }
            address 192.168.254.27/27;
        }
    }
}
```

Multicast packets can only be directed to the AS or MultiServices PIC using a next-hop service set. In the case of NAT, you must also configure a VRF. Therefore, the routing instance **stage** is created as a "dummy" forwarding instance. To direct incoming packets to **stage**, you configure filter-based forwarding through a firewall filter called **fbf**, which is applied to the incoming interface **fe-1/2/1**. A lookup is performed in **stage.inet.0**, which has a multicast static route that is installed with the next hop pointing to the PIC's inside interface. All multicast traffic matching this route is sent to the PIC.

```
[edit firewall]
filter fbf {
    term 1 {
        then {
            routing-instance stage;
        }
    }
}
```

The routing instance **stage** forwards IP multicast traffic to the inside interface **sp-1/1/0.1** on the AS or MultiServices PIC:

```
[edit]
routing-instances stage {
    instance-type forwarding;
    routing-options {
        static {
            route 224.0.0.0/4 next-hop sp-1/1/0.1;
        }
    }
}
```

You enable OSPF and Protocol Independent Multicast (PIM) on the Fast Ethernet and Gigabit Ethernet logical interfaces over which IP multicast traffic enters and leaves the RP. You also enable PIM on the outside interface (**sp-1/1/0.2**) of the next-hop service set.

```
[edit protocols]
ospf {
   area 0.0.0.0 {
      interface fe-1/2/1.0 {
         passive;
      }
      interface lo0.0;
      interface ge-0/3/0.0;
   }
}
pim {
   rp {
      local {
         address 10.255.14.160;
      }
   }
   interface fe-1/2/1.0;
   interface lo0.0;
   interface ge-0/3/0.0;
   interface sp-1/1/0.2;
}
```

As with any filter-based forwarding configuration, in order for the static route in the forwarding instance **stage** to have a reachable next hop, you must configure routing table groups so that all interface routes are copied from **inet.0** to the routing table in the forwarding instance. You configure routing tables **inet.0** and **stage.inet.0** as members of **fbf_rib_group**, so that all interface routes are imported into both tables.

```
[edit routing-options]
interface-routes {
   rib-group inet fbf_rib_group;
}
rib-groups fbf_rib_group {
   import-rib [ inet.0 stage.inet.0 ];
}
multicast {
   rpf-check-policy no_rpf;
}
```

Reverse path forwarding (RPF) checking must be disabled for the multicast group on which source NAT is applied. You can disable RPF checking for specific multicast groups by configuring a policy similar to the one in the example that follows. In this case, the **no_rpf** policy disables RPF check for multicast groups belonging to **224.0.0.0/4**.

```
[edit policy-options]
policy-statement no_rpf {
   term 1 {
      from {
         route-filter 224.0.0.0/4 orlonger;
      }
      then reject;
   }
}
```

Router 1 Configuration

The Internet Group Management Protocol (IGMP), OSPF, and PIM configuration on Router 1 is as follows. Because of IGMP static group configuration, traffic is forwarded out **fe-3/0/0.0** to the multicast receiver without receiving membership reports from host members.

```
[edit protocols]
igmp {
  interface fe-3/0/0.0 {
  }
}
ospf {
  area 0.0.0.0 {
    interface fe-3/0/0.0 {
      passive;
    }
    interface lo0.0;
    interface ge-7/2/0.0;
  }
  pim {
    rp {
      static {
        address 10.255.14.160;
      }
    }
    interface fe-3/0/0.0;
    interface lo0.0;
    interface ge-7/2/0.0;
  }
}
```

The routing option creates a static route to the NAT pool, **mcast_pool**, on the RP.

```
[edit routing-options]
static {
  route 20.20.20.0/27 next-hop 10.10.1.1;
}
```

Example: Configuring Static Destination Address Translation

The following example configures the translation type as **dnat-44**.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-dnat44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
 nat {
    pool dest-pool {
        address 4.1.1.2/32;
    }
    rule rule-dnat44 {
```

```
        match-direction input;
        term t1 {
            from {
                destination-address {
                    20.20.20.20/32;
                }
            }
            then {
                translated {
                    destination-pool dest-pool;
                    translation-type {
                        dnat-44;
                    }
                }
            }
        }
    }
}
  adaptive-services-pics {
    traceoptions {
        flag all;
    }
  }
```

Example: Configuring Dynamic Source Translation for an IPv4 Network

The following example configures the translation type as **napt-44**.

```
[edit services]
    user@host# show
    service-set s1 {
    nat-rules rule-napt-44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
nat {
    pool napt-pool {
        address 10.10.10.0/32;
        port {
            automatic;
        }
    }
    rule rule-napt-44 {
        match-direction input;
        term t1 {
            then {
                translated {
                    source-pool napt-pool;
                    translation-type {
                        napt-44;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
```

```
        }
    }
```

CHAPTER 4

Configuration Statements

address (Services NAT Pool)

Syntax address *ip-prefix</prefix-length>*;

Hierarchy Level [edit services nat pool *nat-pool-name*]

Release Information Statement introduced before Junos OS Release 7.4.
prefix option enhanced to support IPv4 addresses in Junos OS Release 8.5.

Description Specify the NAT pool prefix value.

Options ***prefix***—Specify an IPv4 prefix value.

Usage Guidelines See "Configuring Addresses and Ports for Use in NAT Rules" on page 11.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

address-allocation

Syntax address-allocation round-robin

Hierarchy Level [edit services nat pool *pool-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description When you use round-robin allocation, one port is allocated from each address in a range before repeating the process for each address in the next range. After ports have been allocated for all addresses in the last range, the allocation process wraps around and allocates the next unused port for addresses in the first range.

Usage Guidelines See "Configuring Addresses and Ports for Use in NAT Rules" on page 11.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

address-range

Syntax address-range low *minimum-value* high *maximum-value*;

Hierarchy Level [edit services nat pool *nat-pool-name*]

Release Information Statement introduced before Junos OS Release 7.4.
minimum-value and ***maximum-value*** options enhanced to support IPv4 addresses in Junos OS Release 8.5.

Description Specify the NAT pool address range.

Options ***minimum-value***—Lower boundary for the IPv4 address range.

maximum-value—Upper boundary for the IPv4 address range.

Usage Guidelines See "Configuring Addresses and Ports for Use in NAT Rules" on page 11.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

application-sets (Services NAT)

Syntax applications-sets *set-name*;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define one or more target application sets.

Options ***set-name***—Name of the target application set.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

applications (Services NAT)

Syntax applications [*application-names*];

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define one or more application protocols to which the NAT services apply.

Options ***application-name***—Name of the target application.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

destination-address

Syntax destination-address (*address* | any-unicast) <except>;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.
any-unicast and **except** options introduced in Junos OS Release 7.6.
address option enhanced to support IPv4 and addresses in Junos OS Release 8.5.

Description Specify the destination address for rule matching.

Options ***address***—Destination IPv4 or address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Prevent the specified address, prefix, or unicast packets from being translated.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

destination-address-range (Services NAT)

Syntax destination-address-range low *minimum-value* high *maximum-value* <except>;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and addresses in Junos OS Release 8.5.

Description Specify the destination address range for rule matching.

Options ***minimum-value***—Lower boundary for the IPv4 address range.

maximum-value—Upper boundary for the IPv4 address range.

except—(Optional) Prevent the specified address range from being translated.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

destination-pool

Syntax destination-pool *nat-pool-name*;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then translated]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the destination address pool for translated traffic.

Options ***nat-pool-name***—Destination pool name.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

destination-prefix

Syntax destination-prefix *destination-prefix*;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then translated]

Release Information Statement introduced in Junos OS Release 7.6.
destination-prefix option enhanced to support IPv4 addresses in Junos OS Release 8.5.

Description Specify the destination prefix for translated traffic.

Options ***destination-prefix***—IPv4 destination prefix value.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

destination-prefix-list (Services NAT)

Syntax destination-prefix-list *list-name* <except>;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 8.2.

Description Specify the destination prefix list for rule matching. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level.

Options ***list-name***—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Policy Framework Configuration Guide*

from (Services NAT)

Syntax

```
from {
  application-sets set-name;
  applications [ application-names ];
  destination-address (address | any-unicast) <except>;
  destination-address-range low minimum-value high maximum-value <except>;
  destination-prefix-list list-name <except>;
  source-address (address | any-unicast) <except>;
  source-address-range low minimum-value high maximum-value <except>;
}
```

Hierarchy Level [edit services nat rule *rule-name* term *term-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify input conditions for the NAT term.

Options For information on match conditions, see the description of firewall filter match conditions in the *Junos OS Policy Framework Configuration Guide*.

The remaining statements are explained separately.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

hint

Syntax hint [*hint-strings*];

Hierarchy Level [edit services nat pool *nat-pool-name* pgcp]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure a hint that enables the BGF to choose a NAT pool by direction rather than by virtual interface. The BGF matches the configured hint with a termination hint located in the Direction field of a nonstandard termination ID.

Default When no hint is configured, the BGF can choose any NAT pool associated with the virtual interface.

Options ***hint-string***—Alphanumeric string of up to 3 characters that the BGF uses to match with a termination hint located in the Direction field of a nonstandard termination ID. You can also include underscores (_) and hyphens (-) within the string. To specify a list of hints, use the format: **[hint *xx* hint *yy*]**.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Session Border Control Solutions Guide Using BGF and IMSG*

match-direction

Syntax match-direction (input | output);

Hierarchy Level [edit services nat rule *rule-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the direction in which the rule match is applied.

Options **input**—Apply the rule match on input.

output—Apply the rule match on output.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

no-translation

Syntax no-translation;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then]

Release Information Statement introduced in Junos OS Release 7.6.

Description Specify that traffic is not to be translated.

Options none

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

pool

Syntax

```
pool nat-pool-name {
  address ip-prefix</prefix-length>;
  address-allocation round-robin;
  address-range low minimum-value high maximum-value;
  mapping-timeout seconds;
  pgcp {
    hint [ hint-strings ];
    ports-per-session ports;
    remotely-controlled;
    transport [ transport-protocols ];
  }
  port (automatic | range low minimum-value high maximum-value);
}
```

Hierarchy Level [edit services nat]

Release Information Statement introduced before Junos OS Release 7.4.
pgcp statement added in Junos OS Release 8.4.
remotely-controlled and **ports-per-session** statements added in Junos OS Release 8.5.
hint statement added in Junos OS Release 9.0.
address-allocation statement added in Junos OS Release 11.2.

Description Specify the NAT name and properties.

Options *nat-pool-name*—Identifier for the NAT address pool.

The remaining statements are explained separately.

Usage Guidelines See "Configuring Addresses and Ports for Use in NAT Rules" on page 11.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

port

Syntax port (automatic | range low *minimum-value* high *maximum-value*) {
}

Hierarchy Level [edit services nat pool *nat-pool-name*]

Release Information **port** statement introduced before Junos OS Release 7.4.
random-allocation statement introduced in Junos OS Release 9.3.

Description Specify the NAT pool port or range. You can configure an automatically assigned port or specify a range with minimum and maximum values.

Options **automatic**—Router-assigned port.

minimum-value—Lower boundary for the port range.

maximum-value—Upper boundary for the port range.

Usage Guidelines See "Configuring Addresses and Ports for Use in NAT Rules" on page 11.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

ports-per-session

Syntax ports-per-session *ports*;

Hierarchy Level [edit services nat pool *nat-pool-name* pgcp]

Release Information Statement introduced in Junos OS Release 8.4.

Description Configure the number of ports required to support Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP), Real-Time Streaming Protocol (RTSP), forward error correction (FEC) for voice and video flows on the Multiservices PIC.

Options ***number-of-ports***—Number of ports to enable: 2 or 4 for combined voice and video services.
Default: 2

Required Privilege Level interface—To view this statement in the configuration.
interface–control—To add this statement to the configuration.

Related Documentation
- *Session Border Control Solutions Guide Using BGF and IMSG*

pgcp

Syntax

```
pgcp {
  hint [ hint-strings ];
  ports-per-session ports;
  remotely-controlled;
  transport [ transport-protocols ];
}
```

Hierarchy Level [edit services nat pool *nat-pool-name*]

Release Information Statement introduced in Junos OS Release 8.4.
remotely-controlled and **ports-per-session** statements added in Junos OS Release 8.5.
hint statement added in Junos OS Release 9.0.

Description Specify that the NAT pool is used exclusively by the BGF.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Session Border Control Solutions Guide Using BGF and IMSG*

remotely-controlled

Syntax

```
remotely-controlled;
```

Hierarchy Level [edit services nat pool *nat-pool-name* pgcp]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure the addresses and ports in a NAT pool to be remotely controlled by the gateway controller.

Required Privilege Level interface—To view this statement in the configuration.
interface–control—To add this statement to the configuration.

Related Documentation
- *Session Border Control Solutions Guide Using BGF and IMSG*

rule-set

Syntax
```
rule-set rule-set-name {
    [ rule rule-names ];
}
```

Hierarchy Level [edit services nat]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the rule set the router uses when applying this service.

Options ***rule-set-name***—Identifier for the collection of rules that constitute this rule set.

Usage Guidelines See "Configuring NAT Rule Sets" on page 19.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

services

Syntax services nat { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the service rules to be applied to traffic.

Options **nat**—Identifies the NAT set of rules statements.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

source-address

Syntax source-address (*address* | any-unicast) <except>;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.
any-unicast and **except** options introduced in Junos OS Release 7.6.
address option enhanced to support IPv4 addresses in Junos OS Release 8.5.

Description Specify the source address for rule matching.

Options ***address***—Source IPv4 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Prevent the specified address or unicast packets from being translated.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

source-address-range

Syntax source-address-range low *minimum-value* high *maximum-value* <except>;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 addresses in Junos OS Release 8.5.

Description Specify the source address range for rule matching.

Options ***minimum-value***—Lower boundary for the IPv4 address range.

maximum-value—Upper boundary for the IPv4 address range.

except—(Optional) Prevent the specified address range from being translated.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

source-pool

Syntax source-pool *nat-pool-name*;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then translated]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the source address pool for translated traffic.

Options ***nat-pool-name***—Source pool name.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

source-prefix

Syntax source-prefix *source-prefix*;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then translated]

Release Information Statement introduced in Junos OS Release 7.6.
source-prefix option enhanced to support IPv4 addresses in Junos OS Release 8.5.

Description Specify the source prefix for translated traffic.

Options ***source-prefix***—IPv4 source prefix value.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

source-prefix-list

Syntax source-prefix-list *list-name* <except>;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* from]

Release Information Statement introduced in Junos OS Release 8.2.

Description Specify the source prefix list for rule matching. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level.

Options ***list-name***—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Policy Framework Configuration Guide*

syslog

Syntax syslog;

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable system logging. The system log information from the Multiservices PIC is passed to the kernel for logging in the **/var/log** directory.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

transport

Syntax transport [*transport-protocols*];

Hierarchy Level [edit services nat pool *nat-pool-name* pgcp]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure the BGF to select a NAT pool based on transport protocol type.

Options **[*transport-protocol*]**—One or more transport protocols.

Values: **rtp-avp**, **tcp**, **udp**

Syntax: One or more protocols. If you specify more than one protocol, you must enclose all protocols in brackets.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Session Border Control Solutions Guide Using BGF and IMSG*

rule

Syntax

```
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
    }
    then {
      no-translation;
      translated {
        address-pooling paired;
        destination-pool nat-pool-name;
        destination-prefix destination-prefix;
        dns-alg-pool dns-alg-pool;
        dns-alg-prefix dns-alg-prefix;
        filtering-type endpoint-independent;
        mapping-type endpoint-independent;
        overload-pool overload-pool;
        overload-prefix overload-prefix;
        source-pool nat-pool-name;
        source-prefix source-prefix;
        translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
      }
      syslog;
    }
  }
}
```

Hierarchy Level

[edit services nat],
[edit services nat rule-set *rule-set-name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the rule the router uses when applying this service.

NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options ***rule-name***—Identifier for the collection of terms that comprise this rule.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

term

Syntax

```
term term-name {
  from {
    application-sets set-name;
    applications [ application-names ];
    destination-address (address | any-unicast) <except>;
    destination-address-range low minimum-value high maximum-value <except>;
    destination-prefix-list list-name <except>;
    source-address (address | any-unicast) <except>;
    source-address-range low minimum-value high maximum-value <except>;
  }
  then {
    no-translation;
    translated {
      address-pooling paired;
      destination-pool nat-pool-name;
      destination-prefix destination-prefix;
      dns-alg-pool dns-alg-pool;
      dns-alg-prefix dns-alg-prefix;
      filtering-type endpoint-independent;
      mapping-type endpoint-independent;
      overload-pool overload-pool;
      overload-prefix overload-prefix;
      source-pool nat-pool-name;
      source-prefix source-prefix;
      translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
    }
    syslog;
  }
}
```

Hierarchy Level [edit services nat rule *rule-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the NAT term properties.

NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options ***term-name***—Identifier for the term.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

then

Syntax

```
then {
  no-translation;
  translated {
    address-pooling paired;
    destination-pool nat-pool-name;
    destination-prefix destination-prefix;
    dns-alg-pool dns-alg-pool;
    dns-alg-prefix dns-alg-prefix;
    filtering-type endpoint-independent;
    mapping-type endpoint-independent;
    overload-pool overload-pool;
    overload-prefix overload-prefix;
    source-pool nat-pool-name;
    source-prefix source-prefix;
    translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
  }
  syslog;
}
```

Hierarchy Level [edit services nat rule *rule-name* term *term-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the NAT term actions.

NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

translated

Syntax

```
translated {
  address-pooling paired;
  destination-pool nat-pool-name;
  dns-alg-pool dns-alg-pool;
  dns-alg-prefix dns-alg-prefix;
  filtering-type endpoint-independent;
  mapping-type endpoint-independent;
  source-pool nat-pool-name;
  translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
}
```

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define properties for translated traffic.

NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

translation-type

Syntax translation-type *translation type*

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then translated]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the NAT types for traditional NAT.

Options ***translation type***—You can specify **basic-nat44**, **dynamic-nat44**, **napt44**, or **dnat-44**.

NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the options above.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

PART 3

Administration

CHAPTER 5

Network Address Translation Operational Mode Commands

show services nat pool

Syntax
show services nat pool
<brief | detail>
<*pool-name*>
pgcp <ports-per-session | remotely-controlled>

Release Information
Command introduced before Junos OS Release 7.4.
pgcp option added in Junos OS Release 8.5.

Description
Display information about Network Address Translation (NAT) pools.

Options
none—Display standard information about all NAT pools.

brief | detail—(Optional) Display the specified level of output.

pool-name—(Optional) Display information about the specified NAT pool.

pgcp—(Optional) Display information about a NAT pool that is exclusive to the BGF.

ports-per-session—(Optional) Display the number of ports allocated per session from the NAT pool.

remotely-controlled—(Optional) Display if the NAT pool is explicitly specified by the gateway controller.

Required Privilege Level
view

List of Sample Output
show services nat pool brief on page 75
show services nat pool detail on page 75

Output Fields
Table 3 on page 74 lists the output fields for the **show services nat pool** command. Output fields are listed in the approximate order in which they appear.

Table 3: show services nat pool Output Fields

Field Name	Field Description	Level of Output
Interface	Name of an Multiservices interface.	All levels
Service set	Name of a service set. Individual empty service sets are not displayed, but if none of the service sets has any flows, a flow table header is printed for each service set.	All levels
NAT pool	Name of the Network Address Translation pool.	All levels
Type or **Translation type**	Address translation type: **basic-nat44**, **dynamic-nat44**, **napt44**, or **dnat-44**.	All levels
Address or **Address range**	IPv4 address range of the pool.	All levels

Table 3: show services nat pool Output Fields *(continued)*

Field Name	Field Description	Level of Output
Port or **Port range**	Port range of the pool. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	All levels
Ports used' or **Ports in use**	Number of ports allocated in this pool with this name. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	All levels
Out of port errors	Number of port allocation errors. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	**detail**
Max ports used	Maximum number of ports used. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	**detail**
Addresses in use	Number of addresses in use for dynamic source address NAT pools.	**detail**

Sample Output

show services nat pool brief

```
user@host> show services nat pool brief
Interface: ms-1/3/0, Service set: blue
NAT pool Type    Address                          Port        Ports used
pool1    DNAT-44  100.100.100.100-100.100.100.100
pool2    NAPT-44  200.200.200.200-200.200.200.200
pool3    DYNAMIC NAT44 210.210.210.210-210.210.210.230 65530-65535          0
```

show services nat pool detail

```
user@host> show services nat pool detail
Interface: ms-1/2/0, Service set: nat-2-internet-rsp0
   NAT pool: src-nat-pool-pl01, Translation type: DNAT-44
      Address range: 1.1.1.0-1.1.1.0
      Address range: 2.2.2.2-2.2.2.2
      Port range: 512-65535, Ports in use: 0, Out of port errors: 0, Max ports
used: 0
```

PART 4

Index

Index

T

