JUNIPER NETWORKS

Network Address Translation for JSF

Published: 2011-02-06
Part Number: , Revision

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

Network Address Translation for JSF

Revision History
8 October 2010—Network Address Translation for JSF

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html .

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

List of Figures

List of Tables

PART 1

Overview

CHAPTER 1

Network Address Translation

Network Address Translation Overview for JSF

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 Juniper Networks Junos OS supports NAT on IPv4.

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

You can configure NAT using traditional NAT as described in the following section:

IPv4 to IPv4 Traditional NAT

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

The AS and MultiServices PIC interfaces support three types of NAT processing:

- Static-source translation hides a private network without using NAPT. It features one-to-one mapping between the original address and the translated address and mapping is configured statically.
- Static-destination translation makes selected private servers accessible. It features one-to-one mapping between the translated address and the destination address and mapping is configured statically.
- Dynamic-source translation includes two options, dynamic address-only source translation and NAPT.
  - For the address-only option, 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 using this mapping.
  - In 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.

You can implement NAT to hide one or many hosts on a private network behind a pool of public IP addresses. The pool can be as small as one IP address, or it can be a set of contiguous IP addresses. You can specify a port range to restrict port translation when NAT is configured in dynamic-source mode.

Private address to public address binding can be either static or dynamic. In the basic NAT mode, a NAT rule can force a private IP address to be always bound to a public address; in the NAPT mode, a NAT rule can force a paired private address and private TCP or UDP port to be mapped to a public IP and public TCP or UDP port. However, when the address binding is not statically forced by the NAT rules, NAT can dynamically pick an available address or address and TCP or UDP port pairing when a new session starts. You can specify multiple prefixes and address ranges in a dynamic or static source NAT pool.

You can configure NAT rules without configuring a pool by directly specifying the address prefix to be translated within the rule. And, within the rule, you can assign particular addresses that you do not want to be translated.

Like most traditional NAT implementations, the Junos implementation of NAT supports sessions initiated from the private side only. Sessions initiated from the public side are supported only when you configure static destination address binding.

You are not required to configure a stateful firewall rule to allow NAT to drop traffic. By default, NAT traffic is allowed unless it is explicitly configured to be dropped. If only NAT is configured in a service set, all traffic is accepted.

For more information about configuring NAT rules, see “Configuring NAT Rules” on page 9.

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

You can use the **pool** statement to define the addresses (or prefixes), address ranges, and ports used for network address translation. To configure the information, 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 {
   }
}
```

To configure pools for traditional NAT, specify either a destination pool or a source pool.

With 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.

With static destination NAT, you can also 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 will not be 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.

For constraints on specific translation types, see “Configuring Actions in NAT Rules” on page 12.

With source static NAT, the prefixes and address ranges cannot overlap between separate pools.

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.

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.

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, the Junos OS allocates NAT ports sequentially. To change the way ports are allocated, you can use the **preserve-parity** command, which will allocate even ports for packets with even destination ports and odd ports for packets with odd destination ports, or the **preserve-range** command, which will allocate ports within a range from 0 to 1023 assuming the original packet contains a destination port in the reserved range. This behavior is applicable for control sessions and not the data sessions.

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

You must configure a specific address, a prefix, or the address-range boundaries:

- 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. For more information, see the configuration examples.
- 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 or IPv6 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, it 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 Adaptive Services (AS) or Multiservices PIC.

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-list list-name <except>;
    }
    then {
      no-translation;
      translated {
        destination-pool nat-pool-name;
        destination-prefix prefix;
        source-pool nat-pool-name;
        source-prefix prefix;
        translation-type {
          source (static | dynamic);
          destination (static | dynamic);
        }
      }
      syslog;
    }
  }
}
```

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 10
- Configuring Match Conditions in NAT Rules on page 11
- Configuring Actions in NAT Rules on page 12

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 AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

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 AS or 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. For more information on inside and outside interfaces, see Configuring Service Sets to be Applied to Services Interfaces.

On the AS or 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. For an example, see Examples: Configuring Stateful Firewall Rules.

You can include application protocol definitions that you have configured at the **[edit applications]** hierarchy level; for more information, see Configuring Application Protocol Properties:

- 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 destination-prefix;
        source-pool nat-pool-name;
        source-prefix source-prefix;
        translation-type {
            source (static | dynamic);
            destination static;
        }
    }
}
```

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

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 7.

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

The **translation-type** statement specifies what type of network address translation is used for source or destination traffic. Choices are **source dynamic**, **source static**, or **destination static**. For more information, see Network Address Translation Overview.

- **destination static**—Implement address translation for destination traffic 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.

- **source dynamic**—There are two types of source dynamic translation: network address port translation (NAPT) and address-only translation. You must specify a **source-pool** name. The referenced pool must include either a **port** configuration (for NAPT) or an **address** configuration (for address-only translation).

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

  The **source dynamic** address-only option supports translating up to 16,777,216 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.

- **source static**—Implement address translation for source traffic 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.

For traditional NAT, you can configure either **translation-type destination** or **translation-type source**, but not both. To configure twice NAT, you specify both a **translation-type destination** and a **translation-type source**.

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*.

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 and IPv6 networks, and also on traffic transiting between the two. 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 14
2. Configuring the NAT Rule and NAT Pool on page 16
3. Configuring the Services Set for NAT on page 19

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 1280 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider
  object-cache-size 1280
```

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 1280;
                    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 transaction type** ***transaction type***

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

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

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 {
                        source dynamic;
                    }
                }
            }
        }
    }
}
```

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-interface service-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;
            }
        }
    }
```

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 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 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.

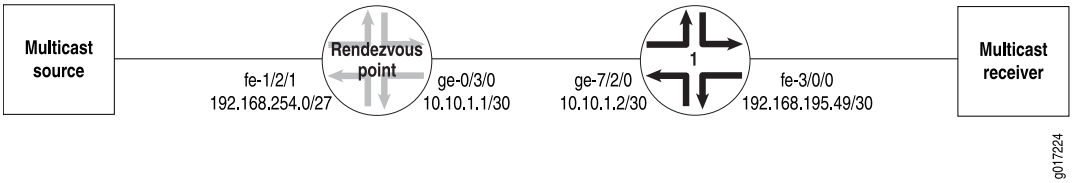
```
[edit services nat]
pool my-pool {
  address-range low 10.10.10.1 high 10.10.10.16;
  port-automatic;
}
rule src-nat {
  match-direction input;
  term t0 {
    from {
      source-address 192.168.20.24/32;
    }
    then {
      no-translation;
    }
  }
```

```
    term t1 {
      then {
        translated {
          translation-type source dynamic;
          source-pool my-pool;
        }
      }
    }
}
```

Example: Configuring NAT for Multicast Traffic

Figure 1 on page 25 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 25
- Router 1 Configuration on page 28

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;
}
```

CHAPTER 4

Configuration Statements

address

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 7.

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 7.

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

application-sets

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 Match Conditions 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.

applications

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 Match Conditions 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.

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 Match Conditions 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.

destination-address-range

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 Match Conditions 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.

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 Actions in NAT Rules” on page 12.

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 Actions in NAT Rules" on page 12.

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

destination-prefix-list

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 Match Conditions 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.

Related Documentation

- *Junos OS Policy Framework Configuration Guide*

from

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>;
  source-address 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 9.

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

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 9.

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 Actions in NAT Rules" on page 12.

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-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.

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 7.

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 7.

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

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>;
      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 {
          source (dynamic | static);
          destination (dynamic | static);
        }
        use-dns-map-for-destination-translation;
      }
      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.

Options

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

Usage Guidelines

See “Configuring NAT Rules” on page 9.

Required Privilege Level

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

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 14.

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.

Usage Guidelines
See Network Address Translation.

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 Match Conditions 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.

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 Match Conditions 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.

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 Actions in NAT Rules” on page 12.

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 Actions in NAT Rules” on page 12.

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 Match Conditions 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.

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 Adaptive Services or Multiservices PIC is passed to the kernel for logging in the **/var/log** directory.

Usage Guidelines See "Configuring Actions in NAT Rules" on page 12.

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>;
    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;
      source-pool nat-pool-name;
      source-prefix source-prefix;
      translation-type {
        source (dynamic | static);
        destination (dynamic | static);
      }
      use-dns-map-for-destination-translation;
    }
    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.

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

Usage Guidelines See “Configuring NAT Rules” on page 9.

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;
    source-pool nat-pool-name;
    source-prefix source-prefix;
    translation-type {
      source (dynamic | static);
      destination (dynamic | static);
    }
    use-dns-map-for-destination-translation;
  }
  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.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring NAT Rules” on page 9.

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 {
    source (dynamic | static);
    destination (dynamic | static);
  }
  use-dns-map-for-destination-translation
}
```

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.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring Actions in NAT Rules” on page 12.

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

translation-type (Traditional NAT)

Syntax translation-type (destination *type* | source *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 *type*—You can specify **source dynamic**, **source static**, or **destination static**.

Usage Guidelines See “Configuring Actions in NAT Rules” on page 12.

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*

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 53
show services nat pool detail on page 53

Output Fields
Table 1 on page 52 lists the output fields for the **show services nat pool** command. Output fields are listed in the approximate order in which they appear.

Table 1: show services nat pool Output Fields

Field Name	Field Description	Level of Output
Interface	Name of an adaptive services 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: **dynamic** or **static**.	All levels
Address or **Address range**	IPv4 address range of the pool.	All levels

Table 1: 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**

show services nat pool brief

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

show services nat pool detail

```
user@host> show services nat pool detail
Interface: sp-1/2/0, Service set: nat-2-internet-rsp0
   NAT pool: src-nat-pool-pl01, Translation type: dynamic
      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

Troubleshooting

CHAPTER 6

Knowledge Base

PART 5

Index

Index

T