

Stateful Firewall for JSF



Published: 2011-05-06

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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

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

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Stateful Firewall for JSF
Copyright © 2011, Juniper Networks, Inc.
All rights reserved.

Revision History
May 2011—R1 Stateful Firewall for JSF 11.2

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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés 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

Part 1	Overview	
Chapter 1	Stateful Firewall	3
	Stateful Firewall Overview for JSF	3
	Stateful Firewall Support for Application Protocols	4
Part 2	Configuration	
Chapter 2	Configuration Tasks	7
	Configuring Stateful Firewall Rules for JSF	7
	Configuring Match Direction for Stateful Firewall Rules	8
	Configuring Match Conditions in Stateful Firewall Rules	8
	Configuring Actions in Stateful Firewall Rules	9
	Configuring Stateful Firewall Rule Sets for JSF	10
	Configuring Juniper Service Framework – Stateful Firewall, Rules, and Services Set	10
	Configuring the JSF Stateful Firewall Package	10
	Configuring the Stateful Firewall Rule	12
	Configuring the Services Set for Stateful Firewall	13
Chapter 3	Example	17
	Examples: Configuring Stateful Firewall Rules for JSF	17
Chapter 4	Configuration Statements	21
	allow-ip-options	21
	applications	22
	application-sets	22
	destination-address	23
	destination-address-range	23
	destination-prefix-list	24
	from	25
	match-direction	25
	rule	26
	rule-set	27
	services	27
	source-address	28
	source-address-range	28
	source-prefix-list	29
	syslog	29
	term	30
	then	31

Part 3	Administration	
Chapter 5	Stateful Firewall Operational Mode Commands	35
	clear services stateful-firewall flows	36
	clear services stateful-firewall statistics	38
	show services stateful-firewall flows	39
	show services stateful-firewall statistics	44
Part 4	Troubleshooting	
Chapter 6	Knowledge Base	51
Part 5	Index	
	Index	55

List of Tables

Part 3

Administration

Chapter 5

Stateful Firewall Operational Mode Commands 35

Table 1: clear services stateful-firewall flows Output Fields 37

Table 2: show services stateful-firewall flows Output Fields 41

Table 3: show services stateful-firewall statistics Output Fields 44

PART 1

Overview

- Stateful Firewall on page 3

CHAPTER 1

Stateful Firewall

- Stateful Firewall Overview for JSF on page 3

Stateful Firewall Overview for JSF

Routers use firewalls to track and control the flow of traffic. Adaptive Services and MultiServices PICs employ a type of firewall called a *stateful firewall*. Contrasted with a *stateless* firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts.

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

Stateful firewalls group relevant *flows* into *conversations*. A flow is identified by the following five properties:

- Source address
- Source port
- Destination address
- Destination port
- Protocol



NOTE: The protocols that are not supported on top of TCP/UDP can have the source port and destination port mapped to other fields.

A typical Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) conversation consists of two flows: the initiation flow and the responder flow. However, some conversations, such as an FTP conversation, might consist of two control flows and many data flows.

Firewall rules govern whether the conversation is allowed to be established. If a conversation is allowed, all flows within the conversation are permitted, including flows that are created during the life cycle of the conversation.

You configure stateful firewalls using a powerful rule-driven conversation handling path. A *rule* consists of direction, source address, source port, destination address, destination port, IP protocol value, and application protocol or service. In addition to the specific values you configure, you can assign the value **any** to rule objects, addresses, or ports, which allows them to match any input value. Finally, you can optionally negate the rule objects, which negates the result of the type-specific match.

Firewall rules are directional. For each new conversation, the router software checks the initiation flow matching the direction specified by the rule.

Firewall rules are ordered. The software checks the rules in the order in which you include them in the configuration. The first time the firewall discovers a match, the router implements the action specified by that rule. Rules still unchecked are ignored.

For more information, see “Configuring Stateful Firewall Rules for JSF” on page 7.

Stateful Firewall Support for Application Protocols

By inspecting the application protocol data, the AS or MultiServices PIC firewall can intelligently enforce security policies and allow only the minimal required packet traffic to flow through the firewall.

The firewall rules are configured in relation to an interface. By default, the stateful firewall allows all sessions initiated from the hosts behind the interface to pass through the router.

PART 2

Configuration

- Configuration Tasks on page 7
- Example on page 17
- Configuration Statements on page 21

CHAPTER 2

Configuration Tasks

- Configuring Stateful Firewall Rules for JSF on page 7
- Configuring Stateful Firewall Rule Sets for JSF on page 10
- Configuring Juniper Service Framework – Stateful Firewall, Rules, and Services Set on page 10

Configuring Stateful Firewall Rules for JSF

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

```
[edit services stateful-firewall]
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address address <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address address <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      (accept | discard | reject);
      allow-ip-options [ values ];
      syslog;
    }
  }
}
```

Each stateful firewall rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded. The **from** statement is optional in stateful firewall rules.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software. The **then** statement is mandatory in stateful firewall rules.

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

- Configuring Match Direction for Stateful Firewall Rules on page 8
- Configuring Match Conditions in Stateful Firewall Rules on page 8
- Configuring Actions in Stateful Firewall Rules on page 9

Configuring Match Direction for Stateful Firewall Rules

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

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

If you configure **match-direction input-output**, sessions initiated from both directions might match this rule.

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.

On the PIC, a flow lookup is performed. If no flow is found, rule processing is performed. Rules in this service set are considered in sequence until a match is found. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered. Most packets result in the creation of bidirectional flows.

Configuring Match Conditions in Stateful Firewall Rules

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

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

The source address and destination address can be either IPv4 or IPv6. You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the [Junos OS Routing Policy Configuration Guide](#). You can use the wildcard value **any-unicast**, which denotes matching all unicast addresses.

Alternatively, you can specify a list of source or destination prefixes by configuring the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or the **source-prefix-list** statement in the stateful firewall rule. For an example, see “Examples: Configuring Stateful Firewall Rules for JSF” on page 17.

If you omit the **from** term, the stateful firewall accepts all traffic and the default protocol handlers take effect:

- User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) create a bidirectional flow with a predicted reverse flow.

You can also include application protocol definitions 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 stateful-firewall rule rule-name term term-name from]** hierarchy level.
- To apply one or more sets of application protocol definitions you have defined, include the **application-sets** statement at the **[edit services stateful-firewall 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.

Configuring Actions in Stateful Firewall Rules

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

```
[edit services stateful-firewall rule rule-name term term-name]
then {
  (accept | discard | reject);
  syslog;
}
```

You must include one of the following three possible actions:

- **accept**—The packet is accepted and sent on to its destination.
- **discard**—The packet is not accepted and is not processed further.

- **reject**—The packet is not accepted and a rejection message is returned; UDP sends an ICMP unreachable code and TCP sends RST. Rejected packets can be logged or sampled.

You can optionally configure the firewall to record information in the system logging facility by including the **syslog** statement at the **[edit services stateful-firewall rule rule-name term term-name then]** hierarchy level. This statement overrides any **syslog** setting included in the service set or interface default configuration.

Configuring Stateful Firewall Rule Sets for JSF

The **rule-set** statement defines a collection of stateful firewall 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 stateful-firewall]** hierarchy level with a **rule** statement for each rule:

```
[edit services stateful-firewall]
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, the packet is dropped by default.

Configuring Juniper Service Framework – Stateful Firewall, Rules, and Services Set

Routers use firewalls to track and control the flow of traffic. Adaptive Services and Multiservices PICs employ a type of firewall called a stateful firewall. To use JSF to run Stateful Firewall, you must configure the `jservices-sfw` package at the hierarchy level. In addition, you must configure SFW rules and a services set with a Multiservice interface. This section includes the following tasks:

1. Configuring the JSF Stateful Firewall Package on page 10
2. Configuring the Stateful Firewall Rule on page 12
3. Configuring the Services Set for Stateful Firewall on page 13

Configuring the JSF Stateful Firewall Package

To configure the JSF services:

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 MB. Only values in increments of 128 MB are allowed and the maximum value of object cache can be 1280 MB. To configure the size of the cache:

```
[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 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 **syslog** 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 Stateful Firewall Rule

To configure the stateful firewall rule:

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

```
user@host# edit services
```

2. Configure the Stateful Firewall rule.

```
[edit services]
user@host# set stateful-firewall rule rule
```

In this example, the SFW rule is **rule1 match-direction input-output**.

```
[edit services]
```

```
user@host# set stateful-firewall rule rule1 match-direction input-output
```

3. Configure the rule input conditions for a rule to define the stateful firewall term.

```
[edit services]
user@host# set stateful-firewall rule rule
```

In this example, the rule input conditions are **rule1 term term1 from applications junos-tftp** and **rule1 term term1 from applications junos-rsh**

```
[edit services]
user@host# set stateful-firewall rule rule1 term term1 from applications junos-tftp
user@host# set stateful-firewall rule rule1 term term1 from applications junos-rsh
```

4. Configure the rule for the stateful firewall term actions.

```
[edit services]
user@host# set stateful-firewall rule rule
```

In this example, the rule is **rule1 term term1 then accept**.

```
[edit services]
user@host# set stateful-firewall rule rule1 term term1 then accept
```

5. Verify the configuration.

```
[edit services]
stateful-firewall {
  rule rule1 {
    match-direction input-output;
    term term1 {
      from {
        applications [ junos-tftp junos-rsh ];
      }
      then {
        accept;
      }
    }
  }
}
```

Configuring the Services Set for Stateful Firewall

To configure the services set for stateful firewall:

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

```
user@host# edit services
```

2. Configure the services set.

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

In this example, the services set with a rule is **sfw-ss**.

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

3. Configure the services set message rate limit.

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

4. Configure the host attributes.

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

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

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

5. Configure the services with services attributes.

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

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

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

6. Configure the services set with SFW rules.

```
[edit services service-set sfw-ss]
user@host# edit stateful-firewall-rules stateful-firewall-rules
```

In this example, the SFW rule is **rule1**.

```
[edit services service-set sfw-ss]
user@host# edit stateful-firewall-rules rule1
```

7. Configure the interface.

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

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

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

8. Configure the service interface.

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

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

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

9. Verify the configuration.

```
[edit services]
user@host# show services
service-set sfw-ss {
    syslog {
```

```
        host local {  
            services any;  
        }  
    }  
    stateful-firewall-rules rule1;  
    interface-service {  
        service-interface ms-1/0/0;  
    }  
}
```


CHAPTER 3

Example

- Examples: Configuring Stateful Firewall Rules for JSF on page 17

Examples: Configuring Stateful Firewall Rules for JSF

The following example shows a stateful firewall configuration containing two rules, one for input matching on a specified application set and the other for output matching on a specified source address:

```
[edit services]
stateful-firewall {
  rule Rule1 {
    match-direction input;
    term 1 {
      from {
        application-sets Applications;
      }
      then {
        accept;
      }
    }
    term accept {
      then {
        accept;
      }
    }
  }
}
rule Rule2 {
  match-direction output;
  term Local {
    from {
      source-address {
        10.1.3.2/32;
      }
    }
    then {
      accept;
    }
  }
}
```

The following example has a single rule with two terms. The first term rejects all traffic in **my-application-group** that originates from the specified source address, and provides a detailed system log record of the rejected packets. The second term accepts Hypertext Transfer Protocol (HTTP) traffic from anyone to the specified destination address.

```
[edit services stateful-firewall]
rule my-firewall-rule {
  match-direction input-output;
  term term1 {
    from {
      source-address 10.1.3.2/32;
      application-sets my-application-group;
    }
    then {
      reject;
      syslog;
    }
  }
  term term2 {
    from {
      destination-address 10.2.3.2/32;
      applications http;
    }
    then {
      accept;
    }
  }
}
```

The following example shows use of source and destination prefix lists. This requires two separate configuration items.

You configure the prefix list at the **[edit policy-options]** hierarchy level:

```
[edit]
policy-options {
  prefix-list p1 {
    1.1.1.1/32;
    2.2.2.0/24;
  }
  prefix-list p2 {
    3.3.3.3/32;
    4.4.4.0/24;
  }
}
```

You reference the configured prefix list in the stateful firewall rule:

```
[edit]
services {
  stateful-firewall {
    rule r1 {
      match-direction input;
      term t1 {
        from {
          source-prefix-list {
```

```

        p1;
    }
    destination-prefix-list {
        p2;
    }
}
then {
    accept;
}
}
}
}
}
}
}
}

```

This is equivalent to the following configuration:

```

[edit]
services {
    stateful-firewall {
        rule r1 {
            match-direction input;
            term t1 {
                from {
                    source-address {
                        1.1.1.1/32;
                        2.2.2.0/24;
                    }
                    destination-address {
                        3.3.3.3/32;
                        4.4.4.0/24;
                    }
                }
            }
            then {
                accept;
            }
        }
    }
}
}
}
}
}
}
}

```

You can use the **except** qualifier with the prefix lists, as in the following example. In this case, the **except** qualifier applies to all prefixes included in prefix list **p2**.

```

[edit]
services {
    stateful-firewall {
        rule r1 {
            match-direction input;
            term t1 {
                from {
                    source-prefix-list {
                        p1;
                    }
                    destination-prefix-list {
                        p2 except;
                    }
                }
            }
        }
    }
}
}
}
}
}
}
}

```

```
    }  
    then {  
        accept;  
    }  
}  
}  
}
```

For additional examples that combine stateful firewall configuration with other services and with virtual private network (VPN) routing and forwarding (VRF) tables, see the configuration examples.

CHAPTER 4

Configuration Statements

allow-ip-options

Syntax `allow-ip-options [values];`

Hierarchy Level `[edit services stateful-firewall rule rule-name term term-name then]`

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure how the stateful firewall handles IP header information. This statement is optional.

Options *value*—Can be a set or range of numeric values, or one or more of the following predefined option types. You can enter either the option name or its numeric equivalent.

Option Name	Numeric Value
any	0
ip-security	130
ip-stream	8
loose-source-route	3
route-record	7
router-alert	148
strict-source-route	9
timestamp	4

Usage Guidelines See “Configuring Stateful Firewall Rules for JSF” on page 7.

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

applications

Syntax	<code>applications [<i>application-names</i>];</code>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Define one or more applications to which the stateful firewall services apply.
Options	<i>application-name</i> —Name of the target application.
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” 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	<code>applications-sets <i>set-name</i>;</code>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Define one or more target application sets.
Options	<i>set-name</i> —Name of the target application set.
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-address

Syntax	<code>destination-address (<i>address</i> any-unicast) <except>;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the destination address for rule matching.
Options	<p><i>address</i>—Destination IPv4 or IPv6 address or prefix value.</p> <p><i>any-unicast</i>—Match all unicast packets.</p> <p><i>except</i>—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

destination-address-range

Syntax	<code>destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the destination address range for rule matching.
Options	<p><i>minimum-value</i>—Lower boundary for the IPv4 or IPv6 address range.</p> <p><i>maximum-value</i>—Upper boundary for the IPv4 or IPv6 address range.</p> <p><i>except</i>—(Optional) Exclude the specified address range from rule matching.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

destination-prefix-list

Syntax	<code>destination-prefix-list <i>list-name</i> <except>;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
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	<p><i>list-name</i>—Destination prefix list.</p> <p>except—(Optional) Exclude the specified prefix list from rule matching.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Junos OS Routing Policy Configuration Guide

from

Syntax	<pre> from { application-sets <i>set-name</i>; applications [<i>application-names</i>]; destination-address <i>address</i> <except>; destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>; destination-prefix-list <i>list-name</i> <except>; source-address <i>address</i> <except>; source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>; source-prefix-list <i>list-name</i> <except>; } </pre>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify input conditions for a stateful firewall term.
Options	<p>For information on match conditions, see the description of firewall filter match conditions in the Junos OS Routing Policy Configuration Guide.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

match-direction

Syntax	match-direction (input output input-output);
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the direction in which the rule match is applied.
Options	<p>input—Apply the rule match on the input side of the interface.</p> <p>output—Apply the rule match on the output side of the interface.</p> <p>input-output—Apply the rule match bidirectionally.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

rule

Syntax	<pre>rule <i>rule-name</i> { match-direction (input output input-output); term <i>term-name</i> { from { application-sets <i>set-name</i>; applications [<i>application-names</i>]; destination-address <i>address</i> <except>; destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>; destination-prefix-list <i>list-name</i> <except>; source-address <i>address</i> <except>; source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>; source-prefix-list <i>list-name</i> <except>; } then { (accept discard reject); syslog; } } }</pre>
Hierarchy Level	[edit services stateful-firewall], [edit services stateful-firewall rule-set <i>rule-set-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the rule the router uses when applying this service.
Options	<i>rule-name</i> —Identifier for the collection of terms that constitute this rule. The remaining statements are explained separately.
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

rule-set

Syntax	<code>rule-set <i>rule-set-name</i> { [rule <i>rule-names</i>]; }</code>
Hierarchy Level	[edit services stateful-firewall]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the rule set the router uses when applying this service.
Options	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
Usage Guidelines	See “Configuring Stateful Firewall Rule Sets for JSF” on page 10.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

services

Syntax	<code>services stateful-firewall { ... }</code>
Hierarchy Level	[edit]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Define the service rules to be applied to traffic.
Options	<i>stateful-firewall</i> —Identifies the stateful firewall set of rules statements.
Usage Guidelines	See “Stateful Firewall Overview for JSF” on page 3.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-address

Syntax	<code>source-address (<i>address</i> any-unicast) <except>;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Source address for rule matching.
Options	<i>address</i> —Source IPv4 or IPv6 address or prefix value. <i>any-unicast</i> —Any unicast packet. <i>except</i> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.

source-address-range

Syntax	<code>source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Source address range for rule matching.
Options	<i>minimum-value</i> —Lower boundary for the IPv4 or IPv6 address range. <i>maximum-value</i> —Upper boundary for the IPv4 or IPv6 address range. <i>except</i> —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.

source-prefix-list

Syntax	<code>source-prefix-list <i>list-name</i> <except>;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
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	<p><i>list-name</i>—Destination prefix list.</p> <p>except—(Optional) Exclude the specified prefix list from rule matching.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Junos OS Routing Policy Configuration Guide

syslog

Syntax	<code>syslog;</code>
Hierarchy Level	<code>[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i> then]</code>
Release Information	Statement introduced in Junos OS Release 10.4.
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. This setting overrides any syslog statement setting included in the service set or interface default configuration.
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

term

Syntax `term term-name {
 from {
 application-sets set-name;
 applications [application-names];
 destination-address address <except>;
 destination-address-range low minimum-value high maximum-value <except>;
 destination-prefix-list list-name <except>;
 source-address address <except>;
 source-address-range low minimum-value high maximum-value <except>;
 source-prefix-list list-name <except>;
 }
 then {
 (accept | discard | reject);
 syslog;
 }
 }`

Hierarchy Level [edit services stateful-firewall rule *rule-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Define the stateful firewall term properties.

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

The remaining statements are explained separately.

Usage Guidelines See “Configuring Stateful Firewall Rules for JSF” on page 7.

Required Privilege interface—To view this statement in the configuration.

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

then

Syntax	<pre> then { (accept discard reject); syslog; } </pre>
Hierarchy Level	[edit services stateful-firewall rule <i>rule-name</i> term <i>term-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Define the stateful firewall term actions. You can configure the router to accept, discard, or reject the targeted traffic. The other actions are optional.
Options	<p>accept—Accept the traffic and send it on to its destination.</p> <p>discard—Do not accept traffic or process it further.</p> <p>reject—Do not accept the traffic and return a rejection message. Rejected traffic can be logged or sampled.</p> <p>The remaining statement is explained separately.</p>
Usage Guidelines	See “Configuring Stateful Firewall Rules for JSF” on page 7.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Junos OS Routing Policy Configuration Guide

PART 3

Administration

- [Stateful Firewall Operational Mode Commands on page 35](#)

CHAPTER 5

Stateful Firewall Operational Mode Commands

clear services stateful-firewall flows

Syntax clear services stateful-firewall flows
<application-protocol *protocol*>
<destination-port *destination-port*>
<destination-prefix *destination-prefix*>
<interface *interface-name*>
<protocol *protocol*>
<service-set *service-set*>
<source-port *source-port*>
<source-prefix *source-prefix*>

Release Information Command introduced in Junos OS Release 10.4.

Description Clear stateful firewall flows.

Options none—Clear all stateful firewall flows.

destination-port *destination-port*—(Optional) Clear stateful firewall flows for a particular destination port. The range of values is 0 to 65535.

destination-prefix *destination-prefix*—(Optional) Clear stateful firewall flows for a particular destination prefix.

interface *interface-name*—(Optional) Clear stateful firewall flows for a particular interface. On M Series and T Series routers, the *interface-name* can be *ms-fpc/pic/port* or *rspnumber*. On J Series routers, the *interface-name* is *ms-pim/0/port*.

protocol—(Optional) Clear stateful firewall flows for one of the following IP types:

- *number*—Numeric protocol value from 0 to 255.
- *ah*—IPsec Authentication Header protocol
- *egp*—An exterior gateway protocol
- *esp*—IPsec Encapsulating Security Payload protocol
- *gre*—A generic routing encapsulation protocol
- *icmp*—Internet Control Message Protocol
- *igmp*—Internet Group Management Protocol
- *ipip*—IP-over-IP Encapsulation Protocol
- *ospf*—Open Shortest Path First protocol
- *pim*—Protocol Independent Multicast protocol
- *rsvp*—Resource Reservation Protocol
- *sctp*—Stream Control Protocol
- *tcp*—Transmission Control Protocol
- *udp*—User Datagram Protocol

`service-set service-set`—(Optional) Clear stateful firewall flows for a particular service set.

`source-port source-port`—(Optional) Clear stateful firewall flows for a particular source port. The range of values is from 0 through 65535.

`source-prefix source-prefix`—(Optional) Clear stateful firewall flows for a particular source prefix.

Required Privilege Level

view

Related Documentation

- [show services stateful-firewall flows on page 39](#)

List of Sample Output

[clear services stateful-firewall flows on page 37](#)

Output Fields

Table 1 on page 37 lists the output fields for the **clear services stateful-firewall flows** command. Output fields are listed in the approximate order in which they appear.

Table 1: clear services stateful-firewall flows Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of the service set from which flows are being cleared.
Conv removed	Number of conversations removed.

Sample Output

```
clear services stateful-firewall flows user@host> clear services stateful-firewall flows
Interface      Service set      Conv removed
ms-0/3/0       svc_set_trust    0
ms-0/3/0       svc_set_untrust  0
```

clear services stateful-firewall statistics

Syntax	clear services stateful-firewall statistics <interface <i>interface-name</i> > <service-set <i>service-set</i> >
Release Information	Command introduced in Junos OS Release 10.4.
Description	Clear stateful firewall statistics.
Options	<p>none—Clear stateful firewall statistics for all interfaces and all service sets.</p> <p>interface <i>interface-name</i>—(Optional) Clear stateful firewall statistics for the specified interface. On M Series and T Series routers, the <i>interface-name</i> can be <i>ms-fpc/pic/port</i> or <i>rspnumber</i>. On J Series routers, the <i>interface-name</i> is <i>ms-pim/0/port</i>.</p> <p>service-set <i>service-set</i>—(Optional) Clear stateful firewall statistics for the specified service set.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show services stateful-firewall statistics on page 44
List of Sample Output	clear services stateful-firewall statistics on page 38
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services stateful-firewall statistics	user@host> clear services stateful-firewall statistics
---	--

show services stateful-firewall flows

Syntax show services stateful-firewall flows
 <brief | extensive | summary | terse>
 <application-protocol *protocol*>
 <count>
 <destination-port *destination-port*>
 <destination-prefix *destination-prefix*>
 <interface *interface-name*>
 <limit *number*>
 <protocol *protocol*>
 <service-set *service-set*>
 <source-port *source-port*>
 <source-prefix *source-prefix*>

Release Information Command introduced in Junos OS Release 10.4.

Description Display stateful firewall flow table entries. When the interface is used for software processing, the type of software concentrator (**DS-LITE** or **6rd**) is shown, and frame counts are provided.

Options none—Display standard information about all stateful firewall flows.

brief | extensive | summary | terse—(Optional) Display the specified level of output.

application-protocol *application-protocol*—(Optional) Display information about one of the following application-level gateway (ALG) protocol types:

- **bootp**—Bootstrap protocol
- **dce-rpc**—Distributed Computing Environment (DCE) remote procedure call (RPC) protocol



NOTE: Use this option to select Microsoft Remote Procedure Call (MSRPC).

- **dce-rpc-portmap**—Distributed Computing Environment (DCE) remote procedure call (RPC) portmap protocol
- **dns**—Domain Name Service protocol
- **exec**—Remote execution protocol
- **ftp**—File Transfer Protocol
- **h323**—H.323 protocol
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **ip**—Internet protocol
- **netbios**—NetBIOS protocol

- **netshow**—Netshow protocol
- **pptp** —Point-to-Point Tunneling Protocol
- **realaudio**—RealAudio protocol
- **rpc**—Remote Procedure Call protocol



NOTE: Use this option to select Sun Microsystems Remote Procedure Call protocol (SunRPC).

- **rpc-portmap**—Remote Procedure Call portmap protocol
- **rtsp**—Real-Time Streaming Protocol
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **talk**—Talk protocol
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

count—(Optional) Display a count of the matching entries.

destination-port *destination-port*—(Optional) Display information for a particular destination port. The range of values is from 0 to 65535.

destination-prefix *destination-prefix*—(Optional) Display information for a particular destination prefix.

interface *interface-name*—(Optional) Display information about a particular interface. On M Series and T Series routers, *interface-name* can be **ms-fpc/pic/port** or **rspnumber**. On J Series routers, *interface-name* is **ms-pim/0/port**.

limit *number*—(Optional) Maximum number of entries to display.

protocol *protocol*—(Optional) Display information about one of the following IP types:

- **number**—Numeric protocol value from 0 to 255
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol

- **ipip**—IP-within-IP Encapsulation Protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*—(Optional) Display information for a particular service set.

source-port *source-port*—(Optional) Display information for a particular source port. The range of values is from 0 to 65535.

source-prefix *source-prefix*—(Optional) Display information for a particular source prefix.

Required Privilege Level view

Related Documentation • [clear services stateful-firewall flows on page 36](#)

List of Sample Output [show services stateful-firewall flows on page 42](#)
[show services stateful-firewall flows \(For Software Flows\) on page 42](#)
[show services stateful-firewall flows brief on page 42](#)
[show services stateful-firewall flows extensive on page 43](#)
[show services stateful-firewall flows count on page 43](#)
[show services stateful-firewall flows destination port on page 43](#)
[show services stateful-firewall flows source port on page 43](#)
[show services stateful-firewall flows \(Twice NAT\) on page 43](#)

Output Fields Table 2 on page 41 lists the output fields for the **show services stateful-firewall flows** command. Output fields are listed in the approximate order in which they appear.

Table 2: show services stateful-firewall flows Output Fields

Field Name	Field Description
Interface	Name of the interface.
Service set	Name of a service set. Individual empty service sets are not displayed. If no service set has any flows, a flow table header is displayed for each service set.
Flow Count	Number of flows in a session.
Flow or Flow Prot	Protocol used for this flow.
Source	Source prefix of the flow in the format <i>source-prefix:port</i> . For ICMP flows, port information is not displayed.
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.

Table 2: show services stateful-firewall flows Output Fields (*continued*)

Field Name	Field Description
State	Status of the flow: <ul style="list-style-type: none"> • Drop—Drop all packets in the flow without response. • Forward—Forward the packet in the flow without looking at it. • Reject—Drop all packets in the flow with response. • Watch—Inspect packets in the flow.
Dir	Direction of the flow: input (I) or output (O).
Frm count	Number of frames in the flow.

Sample Output

show services stateful-firewall flows user@host> **show services stateful-firewall flows**
Interface: ms-1/3/0, Service set: green

```
Flow
Prot      Source                Dest                State      Dir      Frm count
TCP       10.58.255.178:23    -> 10.59.16.100:4000 Forward    O
TCP       10.58.255.50:33005-> 10.58.255.178:23 Forward    I          1
Source NAT 10.58.255.50:33005-> 10.59.16.100:4000
Destin NAT 10.58.255.178:23    -> 0.0.0.0:4000
```

show services stateful-firewall flows (For Software Flows) When a service set includes software processing, the following output format is used for the software flows:

```
user@host> show services stateful-firewall flows
Interface: sp-0/1/0, Service set: dslite-svc-set2
Flow
TCP       200.200.200.2:80    -> 44.44.44.1:1025 Forward    O          219942
NAT dest  44.44.44.1:1025    -> 20.20.1.4:1025
Software  2001::2            -> 1001::1
TCP       20.20.1.2:1025     -> 200.200.200.2:80 Forward    I          110244
NAT source 20.20.1.2:1025    -> 44.44.44.1:1024
Software  2001::2            -> 1001::1
TCP       200.200.200.2:80    -> 44.44.44.1:1024 Forward    O          219140
NAT dest  44.44.44.1:1024    -> 20.20.1.2:1025
Software  2001::2            -> 1001::1
DS-LITE   2001::2            -> 1001::1 Forward    I          988729
TCP       200.200.200.2:80    -> 44.44.44.1:1026 Forward    O          218906
NAT dest  44.44.44.1:1026    -> 20.20.1.3:1025
Software  2001::2            -> 1001::1
TCP       20.20.1.3:1025     -> 200.200.200.2:80 Forward    I          110303
NAT source 20.20.1.3:1025    -> 44.44.44.1:1026
Software  2001::2            -> 1001::1
TCP       20.20.1.4:1025     -> 200.200.200.2:80 Forward    I          110944
NAT source 20.20.1.4:1025    -> 44.44.44.1:1025
Software  2001::2            -> 1001::1
```

show services stateful-firewall flows brief The output for the **show services stateful-firewall flows brief** command is identical to that for the **show services stateful-firewall flows** command. For sample output, see **show services stateful-firewall flows**.

```

show services      user@host> show services stateful-firewall flows extensive
stateful-firewall flows
extensive          Interface: ms-0/3/0, Service set: ss_nat
Flow count          State      Dir      Frm
TCP                 16.1.0.1:2330 ->      16.49.0.1:21    Forward  I
8
  NAT source        16.1.0.1:2330 ->      16.41.0.1:2330
  NAT dest          16.49.0.1:21 ->      16.99.0.1:21
Byte count: 455, TCP established, TCP window size: 57344
TCP acknowledge: 3251737524, TCP tickle enabled, tcp_tickle: 0
Flow role: Master, Timeout: 720
TCP                 16.99.0.1:21 ->      16.41.0.1:2330    Forward  0
5
  NAT source        16.99.0.1:21 ->      16.49.0.1:21
  NAT dest          16.41.0.1:2330 ->      16.1.0.1:2330
Byte count: 480, TCP established, TCP window size: 57344
TCP acknowledge: 463128048, TCP tickle enabled, tcp_tickle: 0
Flow role: Responder, Timeout: 720

show services      user@host> show services stateful-firewall flows count
stateful-firewall flows
count              Interface      Service set      Flow Count
ms-1/3/0              green              2

show services      user@router> show services stateful-firewall flows destination-port 21
stateful-firewall flows
destination port  Interface: ms-0/3/0, Service set: svc_set_trust
Flow
Interface: ms-0/3/0, Service set: svc_set_untrust
Flow
TCP                 10.50.10.2:2143 ->      10.50.20.2:21    Watch    0      Frm count 0

show services      user@router> show services stateful-firewall flows source-port 2143
stateful-firewall flows
source port       Interface: ms-0/3/0, Service set: svc_set_trust
Flow
Interface: ms-0/3/0, Service set: svc_set_untrust
Flow
TCP                 10.50.10.2:2143 ->      10.50.20.2:21    Watch    0      Frm count 0

show services      user@router> show services stateful-firewall flows
stateful-firewall flows
(Twice NAT)       Flow
UDP                 40.0.0.8:23439 ->      80.0.0.1:16485    Watch    I      Frm count 20
  NAT source        40.0.0.8:23439 ->      172.16.1.10:1028
  NAT dest          80.0.0.1:16485 ->      192.16.1.10:22415
UDP                 192.16.1.10:22415 ->      172.16.1.10:1028    Watch    0      20
  NAT source        192.16.1.10:22415 ->      80.0.0.1:16485
  NAT dest          172.16.1.10:1028 ->      40.0.0.8:23439

```

show services stateful-firewall statistics

Syntax	<pre>show services stateful-firewall statistics <application-protocol <i>protocol</i>> <brief detail extensive summary> <interface <i>interface-name</i>> <service-set <i>service-set</i>></pre>
Release Information	Command introduced in Junos OS Release 10.4.
Description	Display stateful firewall statistics.
Options	<p>none—Display standard information about all stateful firewall statistics.</p> <p>brief detail extensive summary—(Optional) Display the specified level of output.</p> <p>interface <i>interface-name</i>—(Optional) Display information about a particular interface. On M Series and T Series routers, the <i>interface-name</i> can be <i>ms-fpc/pic/port</i> or <i>rspnumber</i>. On J Series routers, the <i>interface-name</i> is <i>ms-pim/O/port</i>.</p> <p>service-set <i>service-set</i>—(Optional) Display information about a particular service set.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear services stateful-firewall statistics on page 38
List of Sample Output	show services stateful-firewall statistics extensive on page 47
Output Fields	Table 3 on page 44 lists the output fields for the show services stateful-firewall statistics command. Output fields are listed in the approximate order in which they appear.

Table 3: show services stateful-firewall statistics Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
New flows	Rule match counters for new flows: <ul style="list-style-type: none"> Accept—New flows accepted. Discard—New flows discarded. Reject—New flows rejected.
Existing flows	Rule match counters for existing flows: <ul style="list-style-type: none"> Accept—Match existing forward or watch flow. Discard—Match existing discard flow. Reject—Match existing reject flow.

Table 3: show services stateful-firewall statistics Output Fields (*continued*)

Field Name	Field Description
Drops	<p>Drop counters:</p> <ul style="list-style-type: none"> • TCP SYN defense—Packets dropped by SYN defender. • NAT ports exhausted—Hide mode. The router has no available Network Address Translation (NAT) ports for a given address or pool.
Errors	<p>Total errors, categorized by protocol:</p> <ul style="list-style-type: none"> • IP—Total IP version 4 errors. • TCP—Total Transmission Control Protocol (TCP) errors. • UDP—Total User Datagram Protocol (UDP) errors. • ICMP—Total Internet Control Message Protocol (ICMP) errors. • Non-IP—Total non-IPv4 errors.
IP Errors	<p>IPv4 errors:</p> <ul style="list-style-type: none"> • IP packet length inconsistencies—IP packet length does not match the Layer 2 reported length. • Minimum IP header length check failures—Minimum IP header length is 20 bytes. The received packet contains less than 20 bytes. • Reassembled packet exceeds maximum IP length—After fragment reassembly, the reassembled IP packet length exceeds 65,535. • Illegal source address 0—Source address is not a valid address. Invalid addresses are, loopback, broadcast, multicast, and reserved addresses. Source address 0, however, is allowed to support BOOTP and the destination address 0xffffffff. • Illegal destination address 0—Destination address is not a valid address. The address is reserved. • TTL zero errors—Received packet had a time-to-live (TTL) value of 0. • IP protocol number 0 or 255—IP protocol is 0 or 255. • Land attack—IP source address is the same as the destination address. • Smurf attack—Echo request is sent to a directed broadcast address. • Non-IP packets—Packet did not conform to the IP standard. • IP option—Packet dropped because of a nonallowed IP option. • Non-IPv4 packets—Packet was not IPv4. (Only IPv4 is supported.) • Bad checksum—Packet had an invalid IP checksum. • Illegal IP fragment length—Illegal fragment length. All fragments (other than the last fragment) must have a length that is a multiple of 8 bytes. • IP fragment overlap—Fragments have overlapping fragment offsets. • IP fragment reassembly timeout—Some of the fragments for an IP packet were not received in time, and the reassembly handler dropped partial fragments.

Table 3: show services stateful-firewall statistics Output Fields (*continued*)

Field Name	Field Description
TCP Errors	<p>TCP protocol errors:</p> <ul style="list-style-type: none"> • TCP header length inconsistencies—Minimum TCP header length is 20 bytes, and the IP packet received does not contain at least 20 bytes. • Source or destination port number is zero—TCP source or destination port is zero. • Illegal sequence number, flags combination—Dropped because of TCP errors, such as an illegal sequence number, which causes an illogical combination of flags to be set. • SYN attack (multiple SYN messages seen for the same flow)—Multiple SYN packets received for the same flow are treated as a SYN attack. The packets might be retransmitted SYN packets and therefore valid, but a large number is cause for concern. • First packet not SYN—First packets for a connection are not SYN packets. These packets might originate from previous connections or from someone performing an ACK/FIN scan. • TCP port scan (Handshake, RST seen from server for SYN)—In the case of a SYN defender, if an RST (reset) packet is received instead of a SYN/ACK message, someone is probably trying to scan the server. This behavior can result in false alarms if the RST packet is not combined with an intrusion detection service (IDS). • Bad SYN cookie response—SYN cookie generates a SYN/ACK message for all incoming SYN packets. If the ACK received for the SYN/ACK message does not match, this counter is incremented.
UDP Errors	<p>UDP protocol errors:</p> <ul style="list-style-type: none"> • IP data length less than minimum UDP header length (8 bytes)—Minimum UDP header length is 8 bytes. The received IP packets contain less than 8 bytes. • Source or destination port is zero—UDP source or destination port is 0. • UDP port scan (ICMP error seen for UDP flow)—ICMP error is received for a UDP flow. This could be a genuine UDP flow, but it is counted as an error.
ICMP Errors	<p>ICMP protocol errors:</p> <ul style="list-style-type: none"> • IP data length less than minimum ICMP header length (8 bytes)—ICMP header length is 8 bytes. This counter is incremented when received IP packets contain less than 8 bytes. • ICMP error length inconsistencies—Minimum length of an ICMP error packet is 48 bytes, and the maximum length is 576 bytes. This counter is incremented when the received ICMP error falls outside this range. • Ping duplicate sequence number—Received ping packet has a duplicate sequence number. • Ping mismatched sequence number—Received ping packet has a mismatched sequence number.

Sample Output

```

show services stateful-firewall statistics extensive
user@host> show services stateful-firewall statistics extensive
Interface: ms-1/3/0
Service set: interface-svc-set
New flows:
  Accept: 907, Discard: 0, Reject: 0
Existing flows:
  Accept: 3535, Discard: 0, Reject: 0
Drops:
  IP option: 0, TCP SYN defense: 0
  NAT ports exhausted: 0
Errors:
  IP: 0, TCP: 0
  UDP: 0, ICMP: 0
  Non-IP packets: 0, ALG: 0
IP errors:
  IP packet length inconsistencies: 0
  Minimum IP header length check failures: 0
  Reassembled packet exceeds maximum IP length: 0
  Illegal source address: 0
  Illegal destination address: 0
  TTL zero errors: 0, IP protocol number 0 or 255: 0
  Land attack: 0, Smurf attack: 0
  Non IP packets: 0, IP option: 0
  Non-IPv4 packets: 0, Bad checksum: 0
  Illegal IP fragment length: 0
  IP fragment overlap: 0
  IP fragment reassembly timeout: 0
TCP errors:
  TCP header length inconsistencies: 0
  Source or destination port number is zero: 0
  Illegal sequence number, flags combination: 0
  SYN attack (multiple SYNs seen for the same flow): 0
  First packet not SYN: 0
  TCP port scan (Handshake, RST seen from server for SYN): 0
  Bad SYN cookie response: 0
UDP errors:
  IP data length less than minimum UDP header length (8 bytes): 0
  Source or destination port is zero: 0
  UDP port scan (ICMP error seen for UDP flow): 0
ICMP errors:
  IP data length less than minimum ICMP header length (8 bytes): 0
  ICMP error length inconsistencies: 0
  Ping duplicate sequence number: 0
  Ping mismatched sequence number: 0
ALG drops:
  BOOTP: 0, DCE-RPC: 0, DCE-RPC portmap: 0
  DNS: 0, Exec: 0, FTP: 0
  ICMP: 0
  Login: 0, Netbios: 0, Netshow: 0
  RPC: 0, RPC portmap: 0
  RTSP: 0, Shell: 0
  SNMP: 0, Sqlnet: 0, TFTP: 0
  Traceroute: 0

```


PART 4

Troubleshooting

- Knowledge Base on page 51

CHAPTER 6

Knowledge Base

PART 5

Index

- Index on page 55

Index

A

allow-ip-options statement.....	21
usage guidelines.....	9
application-sets statement	
stateful firewall.....	22
usage guidelines.....	8
applications statement	
application-level gateways.....	22
stateful firewall.....	22
usage guidelines.....	8

C

clear services stateful-firewall flows	
command.....	36
clear services stateful-firewall statistics	
command.....	38

D

destination-address statement	
stateful firewall.....	23
usage guidelines.....	8
destination-address-range statement	
stateful firewall.....	23
usage guidelines.....	8
destination-prefix-list statement	
stateful firewall.....	24
usage guidelines.....	8

F

from statement	
stateful firewall.....	25
usage guidelines.....	7, 8

M

match-direction statement	
stateful firewall.....	25
usage guidelines.....	8

R

rule statement	
stateful firewall.....	26
usage guidelines.....	7
rule-set statement	
stateful firewall.....	27
usage guidelines.....	10

S

services statement	
stateful firewall.....	27
show services stateful-firewall flows	
command.....	39
show services stateful-firewall statistics	
command.....	44
source-address statement	
stateful firewall.....	28
usage guidelines.....	8
source-address-range statement	
stateful firewall.....	28
usage guidelines.....	8
source-prefix-list statement	
stateful firewall.....	29
usage guidelines.....	8
stateful firewall	
action statements.....	9
applications.....	8
example configuration.....	17
flows	
clearing.....	36
displaying.....	39
match conditions.....	8
rules.....	10
statistics	
clearing.....	38
displaying.....	44
syslog statement	
stateful firewall.....	29
usage guidelines.....	9

T

term statement	
stateful firewall.....	30
usage guidelines.....	7
then statement	
stateful firewall.....	31
usage guidelines.....	7, 9