Junos Network Secure

Published: 2013-08-29

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

Junos Network Secure

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- M Series
- T Series
- MX Series
- J Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the**configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

PART 1

Overview

CHAPTER 1

Junos Network Secure

Junos Network Secure Overview

Routers use firewalls to track and control the flow of traffic. The following platforms employ a type of firewall called a *stateful firewall*.

- MultiServices Dense Port Concentrators (MS-DPCs)
- MS-100, MS-400, and MS-500 MultiServices PICs
- MultiServices Modular Port Concentrators (MS-MPCs), and Multiservices Modular Interface Cards (MS-MICs)

The stateful firewall capabilities provided by the Junos OS are collectively known as *Junos Network Secure*.

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

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

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.

NOTE: **MS-MPC and MS-MIC interface cards do not currently support IPv6 traffic for Junos Network Secure Stateful Firewall.**

For more information, see "Configuring Stateful Firewall Rules" on page 9.

Stateful Firewall Support for Application Protocols

By inspecting the application protocol data, the Junos Network Secure stateful 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.

Stateful Firewall Anomaly Checking

The stateful firewall recognizes the following events as anomalies and sends them to the IDS software for processing:

- IP anomalies:
  - IP version is not correct.
  - IP header length field is too small.
  - IP header length is set larger than the entire packet.
  - Bad header checksum.
  - IP total length field is shorter than header length.
  - Packet has incorrect IP options.

- Internet Control Message Protocol (ICMP) packet length error.
- Time-to-live (TTL) equals 0.

- IP address anomalies:
  - IP packet source is a broadcast or multicast.
  - Land attack (source IP equals destination IP).
- IP fragmentation anomalies:
  - IP fragment overlap.
  - IP fragment missed.
  - IP fragment length error.
  - IP packet length is more than 64 kilobytes (KB).
  - Tiny fragment attack.
- TCP anomalies:
  - TCP port 0.
  - TCP sequence number 0 and flags 0.
  - TCP sequence number 0 and FIN/PSH/RST flags set.
  - TCP flags with wrong combination (TCP FIN/RST or SYN/(URG|FIN|RST).
  - Bad TCP checksum.
- UDP anomalies:
  - UDP source or destination port 0.
  - UDP header length check failed.
  - Bad UDP checksum.
- Anomalies found through stateful TCP or UDP checks:
  - SYN followed by SYN-ACK packets without ACK from initiator.
  - SYN followed by RST packets.
  - SYN without SYN-ACK.
  - Non-SYN first flow packet.
  - ICMP unreachable errors for SYN packets.
  - ICMP unreachable errors for UDP packets.
- Packets dropped according to stateful firewall rules.

If you employ stateful anomaly detection in conjunction with stateless detection, IDS can provide early warning for a wide range of attacks, including these:

- TCP or UDP network probes and port scanning

- SYN flood attacks
- IP fragmentation-based attacks such as teardrop, bonk, and boink

PART 2

Configuration

CHAPTER 2

Junos Network Secure Configuration Tasks

Configuring Stateful Firewall Rules

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

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

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 | 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>;
```

```
}
```

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 *Routing Policy Feature Guide for Routing Devices*. 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" on page 15.

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.
- IP creates a unidirectional flow.

You can also include application protocol definitions 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 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);
    allow-ip-options [ values ];
    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 IP Option Handling

You can optionally configure the firewall to inspect IP header information by including the **allow-ip-options** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* then]** hierarchy level. When you configure this statement, all packets that match the criteria specified in the **from** statement are subjected to additional matching criteria. A packet is accepted only when all of its IP option types are configured as values in the **allow-ip-options** statement. If you do not configure **allow-ip-options**, only packets without IP header options are accepted.

The additional IP header option inspection applies only to the **accept** and **reject** stateful firewall actions. This configuration has no effect on the **discard** action. When the IP header inspection fails, reject frames are not sent; in this case, the **reject** action has the same effect as **discard**.

If an IP option packet is accepted by the stateful firewall, Network Address Translation (NAT) and intrusion detection service (IDS) are applied in the same way as to packets without IP option headers. The IP option configuration appears only in the stateful firewall rules; NAT applies to packets with or without IP options.

When a packet is dropped because it fails the IP option inspection, this exception event generates both IDS event and system log messages. The event type depends on the first IP option field rejected.

Table 3 on page 12 lists the possible values for the **allow-ip-options** statement. You can include a range or set of numeric values, or one or more of the predefined IP option settings. You can enter either the option name or its numeric equivalent. For more information, refer to http://www.iana.org/assignments/ip-parameters.

Table 3: IP Option Values

IP Option Name	Numeric Value	Comment
any	**0**	Any IP option
ip-security	**130**	–
ip-stream	**136**	–

Table 3: IP Option Values *(continued)*

IP Option Name	Numeric Value	Comment
loose-source-route	131	–
route-record	7	–
router-alert	148	–
strict-source-route	137	–
timestamp	68	–

Configuring Stateful Firewall Rule Sets

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.

CHAPTER 3

Junos Network Secure Example

Examples: Configuring Stateful Firewall Rules

The following example show 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.

Related Documentation

- *Example: BOOTP and Broadcast Addresses*
- *Example: Dynamic Source NAT as a Next-Hop Service*
- *Example: Virtual Routing and Forwarding (VRF) and Service Configuration*
- *Example: Service Interfaces Configuration*
- Example: Configuring Layer 3 Services and the Services SDK on Two PICs on page 18

Example: Configuring Layer 3 Services and the Services SDK on Two PICs

You can configure the Layer 3 service package and the Services SDK on two PICs. For this example, you must configure an FTP or HTTP client and a server. In this configuration, the client side of the router interface is ge-1/2/2.1 and the server side of the router interface is ge-1/1/0.48. This configuration enables Network Address Translation (NAT) with stateful firewall (SFW) on the uKernel PIC and application identification (APPID), application-aware access list (AACL), and intrusion detection and prevention (IDP) on the Services SDK PIC for FTP or HTTP traffic.

NOTE: **The Services SDK does not support NAT yet. When NAT is required, you can configure the Layer 3 service package to deploy NAT along with the Services SDK such as APPID, AACL, or IDP.**

To deploy the Layer 3 service package and the Services SDK on two PICs:

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

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

2. In the hierarchy level, configure the conditions for the stateful firewall rule **r1**.

   ```
   [edit services stateful-firewall]
   user@host# set rule rule-name match-direction input-output term term from
     applications application-name
   user@host# set rule rule-name match-direction input-output term term then accept
     syslog
   ```

In this example, the stateful firewall term is **ALLOWED-SERVICES**. Enclose the application names—junos-ftp, junos-http, and junos-icmp-ping—in parentheses for *application-name*.

```
[edit services stateful-firewall]
user@host# set rule r1 match-direction input-output term ALLOWED-SERVICES from
  applications [ junos-ftp junos-http junos-icmp-ping ]
user@host# set rule r1 match-direction input-output term ALLOWED-SERVICES then
  accept syslog
```

3. Configure the conditions for the stateful firewall rule **r2**.

```
[edit services stateful-firewall]
user@host# set rule rule-name match-direction input-output term term then discard
user@host# set rule rule-name match-direction input-output term term then syslog
```

In this example, the stateful firewall term is **term1**.

```
[edit services stateful-firewall]
user@host# set rule r2 match-direction input-output term term1 then discard
user@host# set rule r2 match-direction input-output term term1 then syslog
```

4. Go to the following hierarchy level and verify the configuration:

```
[edit services stateful-firewall]
user@host# show
rule r1 {
    match-direction input-output;
    term ALLOWED-SERVICES {
        from {
            applications [ junos-ftp junos-http junos-icmp-ping ];
        }
        then {
            accept;
            syslog;
        }
    }
}
rule r2 {
    match-direction input-output;
    term term1 {
        then {
            discard;
            syslog;
        }
    }
}
```

5. Go to the following hierarchy level:

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

6. In the hierarchy level, configure the NAT pool.

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

In this example, the NAT pool is **OUTBOUND-SERVICES** and the IP address is **10.48.0.2/32**.

```
[edit services natl]
user@host# set pool OUTBOUND-SERVICES address 10.48.0.2/32
user@host# set pool OUTBOUND-SERVICES port automatic
```

7. Configure the NAT rule.

```
[edit services nat]
user@host# set rule rule-name match-direction output term term from applications
  application-name
user@host# set rule rule-name match-direction output term term then translated
  source-pool source-pool translation-type source dynamic
```

In this example, the NAT rule is **SET-MSR-ADDR**, the NAT term is **TRANSLATE-SOURCE-ADDR**, and the source pool is **OUTBOUND-SERVICES**. Enclose the application names—junos-ftp, junos-http, and junos-icmp-ping—in parentheses for *application-name*.

```
[edit services nat]
user@host# set rule SET-MSR-ADDR match-direction output term
  TRANSLATE-SOURCE-ADDR from applications [ junos-ftp junos-http
  junos-icmp-ping ]
user@host# set rule SET-MSR-ADDR match-direction output term
  TRANSLATE-SOURCE-ADDR then translated source-pool OUTBOUND-SERVICES
  translation-type source dynamic
```

8. Go to the following hierarchy level and verify the configuration:

```
[edit services nat]
user@host# show
pool OUTBOUND-SERVICES {
    address 11.48.0.2/32;
    port {
        automatic;
    }
}
rule SET-MSR-ADDR {
    match-direction output;
    term TRANSLATE-SOURCE-ADDR {
        from {
            applications [ junos-ftp junos-http junos-icmp-ping ];
        }
        then {
            translated {
                source-pool OUTBOUND-SERVICES;
                translation-type {
                    source dynamic;
                }
            }
        }
    }
}
```

9. Go to the following hierarchy level:

```
[edit security]
user@host# edit idp
```

10. In the hierarchy level, configure the IDP policy.


```
[edit security idp]
user@host# set idp-policy policy-name rulebase-ips rule rule-name match application
  default attacks predefined-attacks attack-name
user@host# set idp-policy policy-name rulebase-ips rule rule-name match application
  default attacks predefined-attack-groups attack-group--name
user@host# set idp-policy policy-name rulebase-ips rule rule-name then action
  no-action
user@host# set idp-policy policy-name rulebase-ips rule rule-name then notification
  log-attacks alert
```

In this example, the IDP policy is **test1**, the rule is **r1**, the predefined attack is **FTP:USER:ROOT**, and the predefined attack group is **"Recommended Attacks"**.

```
[edit security idp]
user@host# set idp-policy test1 rulebase-ips rule r1 match application default attacks
  predefined-attacks FTP:USER:ROOT
user@host# set idp-policy test1 rulebase-ips rule r1 match application default attacks
  predefined-attack-groups [ "Recommended Attacks" ]
user@host# set idp-policy test1 rulebase-ips rule r1 then action no-action
user@host# set idp-policy test1 rulebase-ips rule r1 then notification log-attacks alert
```

11. Configure the trace options for IDP services.

```
[edit security idp]
user@host# set traceoptions file filename
user@host# set traceoptions flag all
user@host# set traceoptions level all
```

In this example, the log file name is **idp-demo.log**.

```
[edit security idp]
user@host# set traceoptions file idp-demo.log
user@host# set traceoptions flag all
user@host# set traceoptions level all
```

12. Go to the following hierarchy level and verify the configuration:

```
[edit security idp]
user@host# show
idp-policy test1 {
    rulebase-ips {
        rule r1 {
            match {
                application default;
                attacks {
                    predefined-attacks FTP:USER:ROOT;
                    predefined-attack-groups "Recommended Attacks";
                }
            }
            then {
                action {
                    no-action;
                }
                notification {
                    log-attacks {
                        alert;
                    }
                }
            }
        }
    }
```

```
}
traceoptions {
    file idp-demo.log;
    flag all;
    level all;
}
```

13. Go to the following hierarchy level:

    [edit services]
    user@host# edit aacl

14. In the hierarchy level, configure the AACL rules.

    [edit services aacl]
    user@host# set rule *rule-name* match-direction input-output term *term* from application-group-any
    user@host# set rule *rule-name* match-direction input-output term *term* then count application accept

    In this example, the AACL rule is **app-aware** and the term is **t1**.

    [edit services aacl]
    user@host# set rule app-aware match-direction input-output term t1 from application-group-any
    user@host# set rule app-aware match-direction input-output term t1 then count application accept

15. Go to the following hierarchy level and verify the configuration:

```
[edit services aacl]
user@host# show
rule app-aware {
            match-direction input-output;
            term t1 {
                from {
                    application-group-any;
                }
                then {
                    count application;
                    accept;
                }
            }
        }
```

16. Go to the following hierarchy level:

    [edit services]
    user@host# edit service-set App-Aware-Set

17. Configure the APPID profile.

    [edit services service-set App-Aware-Set]
    user@host# set application-identification-profile *application-identification-profile*

    In this example, the APPID profile is **dummy-profile**.

    [edit services service-set App-Aware-Set]
    user@host# set application-identification-profile dummy-profile

18. Configure the IDP profile.

    [edit services service-set App-Aware-Set]


```
user@host# set idp-profile idp-profile
```

In this example, the IDP profile is **test1**.

```
[edit services service-set App-Aware-Set]
user@host# set idp-profile test1
```

19. Configure the policy decision statistics profile.

```
[edit services service-set App-Aware-Set]
user@host# set policy-decision-statistics-profile profile-name
```

In this example, the policy decision statistics profile is **lpdf-stats**.

```
[edit services service-set App-Aware-Set]
user@host# set policy-decision-statistics-profile lpdf-stats
```

20. Configure the AACL rules.

```
[edit services service-set App-Aware-Set]
user@host# set aacl-rules rule-name
```

In this example, the AACL rule name is **app-aware**.

```
[edit services service-set App-Aware-Set]
user@host# set aacl-rules app-aware
```

21. Configure two stateful firewall rules.

```
[edit services service-set App-Aware-Set]
user@host# set stateful-firewall-rules rule-name
user@host# set stateful-firewall-rules rule-name
```

In this example, the first rule is **r1** and the second rule is **r2**.

```
[edit services service-set App-Aware-Set]
user@host# set stateful-firewall-rules r1
user@host# set stateful-firewall-rules r2
```

22. In the hierarchy level, configure the service set to bypass traffic on service PIC failure.

```
[edit services service-set App-Aware-Set]
user@host# set service-set-options bypass-traffic-on-pic-failure
```

23. Configure interface-specific service set options.

```
[edit services service-set App-Aware-Set]
user@host# set interface-service service-interface service-interface
```

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

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

24. Go to the following hierarchy level and verify the configuration:

```
[edit services service-set App-Aware-Set]
user@host# show
application-identification-profile dummy-profile;
idp-profile test1;
policy-decision-statistics-profile {
    lpdf-stats;
}
aacl-rules app-aware;
```

```
stateful-firewall-rules r1;
stateful-firewall-rules r2;
service-set-options {
    bypass-traffic-on-pic-failure;
}
interface-service {
    service-interface ms-0/1/0;
}
```

25. Go to the following hierarchy level:

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

26. In the hierarchy level, configure optional notification parameters for the services interface. Note that it is required only for debugging.

    [edit services NAT-SFW-SET]
    user@host# **set syslog host *host-name* services any**

    In this example, the host to notify is **local**.

    [edit services NAT-SFW-SET]
    user@host# **set services-options syslog host local services any**

27. Configure two stateful firewall rules.

    [edit services NAT-SFW-SET]
    user@host# **set stateful-firewall-rules *rule-name***
    user@host# **set stateful-firewall-rules *rule-name***

    In this example, the first rule is **r1** and the second rule is **r2**.

    [edit services NAT-SFW-SET]
    user@host# **set stateful-firewall-rules r1**
    user@host# **set stateful-firewall-rules r2**

28. Configure NAT rules.

    [edit services NAT-SFW-SET]
    user@host# **set nat-rules *rule-name***

    In this example, the NAT rule is **SET-MSR-ADDR**.

    [edit services NAT-SFW-SET]
    user@host# **set nat-rules SET-MSR-ADDR**

29. Configure interface-specific service set options.

    [edit services NAT-SFW-SET]
    user@host# **set interface-service service-interface *service-interface***

    In this example, the services interface is **sp-3/1/0**.

    [edit services NAT-SFW-SET]
    user@host# **set interface-service service-interface sp-3/1/0**

30. Go to the following hierarchy level and verify the configuration:

```
[edit services service-set NAT-SFW-SET]
user@host# show
syslog {
    host local {
        services any;
```

```
    }
}
stateful-firewall-rules r1;
stateful-firewall-rules r2;
interface-service {
    service-interface sp-3/1/0;
}
```

31. Go to the following hierarchy level:

    user@host# edit interfaces

32. In the hierarchy level, configure the interface.

    [edit interfaces]
    user@host# set *interface*

    In this example, the interface is **ge-1/2/2.1**.

    [edit interfaces]
    user@host# set ge-1/2/2.1

33. Go to the following hierarchy level:

    [edit interfaces]
    user@host# edit ge-1/2/2.1

34. In the hierarchy level, configure the service set for received packets.

    [edit interfaces ge-1/2/2 unit 1]
    user@host# set family inet service input service-set *service-set-name*

    In this example, the input service set is **App-Aware-Set**.

    [edit interfaces ge-1/2/2 unit 1]
    user@host# set family inet service input service-set App-Aware-Set

35. Configure the service set for transmitted packets.

    [edit interfaces ge-1/2/2 unit 1]
    user@host# set family inet service output service-set *service-set-name*

    In this example, the output service set is **App-Aware-Set**.

    [edit interfaces ge-1/2/2 unit 1]
    user@host# set family inet service output service-set App-Aware-Set

36. Go to the following hierarchy level:

    [edit interfaces ge-1/2/2 unit 1]
    user@host# edit family inet

37. In the hierarchy level, configure the interface address.

    [edit interfaces ge-1/2/2 unit 1 family inet]
    user@host# set address *source*

    In this example, the interface address is **10.10.9.10/30**.

    [edit interfaces]
    user@host# set address 10.10.9.10/30

38. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces ge-1/2/2 unit 1]
user@host# show
family inet {
    service {
        input {
            service-set App-Aware-Set;
        }
        output {
            service-set App-Aware-Set;
        }
    }
    address 10.10.9.10/30;
}
```

39. Go to the following hierarchy level:

    user@host# edit interfaces

40. In the hierarchy level, configure the interface.

    [edit interfaces]
    user@host# set *interface*

    In this example, the interface is **ge-1/1/0.48**.

    [edit interfaces]
    user@host# set ge-1/1/0.48

41. Go to the following hierarchy level:

    [edit interfaces]
    user@host# edit ge-1/1/0.48

42. In the hierarchy level, configure the service set for received packets.

    [edit interfaces ge-1/1/0 unit 48]
    user@host# set family inet service input service-set *service-set-name*

    In this example, the service set is **NAT-SFW-SET**.

    [edit interfaces ge-1/1/0 unit 48]
    user@host# set family inet service input service-set NAT-SFW-SET

43. Configure the service set for transmitted packets.

    [edit interfaces ge-1/1/0 unit 48]
    user@host# set family inet service output service-set *service-set-name*

    In this example, the service set is **NAT-SFW-SET**.

    [edit interfaces ge-1/1/0 unit 48]
    user@host# set family inet service output service-set NAT-SFW-SET

44. Go to the following hierarchy level:

    [edit interfaces ge-1/1/0 unit 48]
    user@host# edit family inet

45. Configure the interface address.

    [edit interfaces ge-1/1/0 unit 48 family inet]
    user@host# set address *source*

In this example, the interface address is **10.48.0.1/31**.

```
[edit interfaces ge-1/1/0 unit 48 family inet]
user@host# set address 10.48.0.1/31
```

46. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces ge-1/1/0 unit 48]
user@host# show
family inet {
    service {
        input {
            service-set NAT-SFW-SET;
            }
        output {
            service-set NAT-SFW-SET;
        }
    }
    address 10.48.0.1/31;
}
```

47. Go to the following hierarchy level:

```
user@host# edit interfaces
```

48. In the hierarchy level, configure the interface.

```
[edit interfaces]
set interface
```

In this example, the interface is **ms-0/1/0.0**.

```
[edit interfaces]
user@host# set ms-0/1/0.0
```

49. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit ms-0/1/0.0
```

50. In the hierarchy level, configure the protocol family.

```
[edit interfaces ms-0/1/0 unit 0]
user@host# set family inet
```

51. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces ms-0/1/0]
user@host# show
unit 0 {
    family inet;
}
```

52. Go to the following hierarchy level:

```
user@host# edit interfaces
```

53. In the hierarchy level, configure the interface.

```
[edit interfaces]
set interface
```

In this example, the interface is **sp-3/1/0.0**.

```
[edit interfaces]
```

```
user@host# set sp-3/1/0.0
```

54. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit sp-3/1/0
```

55. In the hierarchy level, configure optional notification parameters for the services interface. Note that it is required only for debugging.

```
[edit interfaces sp-3/1/0]
user@host# set services-options syslog host host-name services any
```

In this example, the host to notify is **local**.

```
[edit interfaces sp-3/1/0]
user@host# set services-options syslog host local services any
```

56. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit sp-3/1/0.0
```

57. In the hierarchy level, configure the protocol family.

```
[edit interfaces sp-3/1/0 unit 0]
user@host# set family inet
```

58. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces sp-3/1/0]
user@host# show
services-options {
    syslog {
        host local {
            services any;
        }
    }
}
unit 0 {
    family inet;
}
```

59. Go to the following hierarchy level:

```
[edit chassis]
```

60. In the hierarchy level, configure the redundancy settings.

```
[edit chassis]
user@host# set no-service-pic-restart-on-failover
user@host# set redundancy graceful-switchover
```

61. Configure the FPC and PIC.

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

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

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

62. 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
```

63. 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
```

64. Configure the size of the object cache in megabytes. Only values in increments of 128 MB are allowed and the maximum value of object cache can be 1280 MB. On MS-100, the value is 512 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
```

65. Configure the size of the policy database in megabytes.

```
[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
```

66. Configure the packages.

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

In this example, the first package is **jservices-appid**, the second package is **jservices-aacl**, the third package is **jservices-llpdf**, the fourth package is **jservices-idp**, and the fifth package is **jservices-sfw**. jservices-sfw is available only in Junos OS Release 10.1 and later.

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

```
user@host# set adaptive-services service-package extension-provider package
  jservices-aacl
user@host# set adaptive-services service-package extension-provider package
  jservices-llpdf
user@host# set adaptive-services service-package extension-provider package
  jservices-idp
user@host# set adaptive-services service-package extension-provider package
  jservices-sfw
```

67. Configure the IP network services.

```
[edit chassis]
user@host# set network-services ip
```

68. Go to the following hierarchy level and verify the configuration:

```
[edit chassis]
user@host# show chassis
no-service-pic-restart-on-failover;
filter-memory-enhanced;
redundancy {
    graceful-switchover;
}
fpc 0 {
    pic 1 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 7;
                    object-cache-size 1280;
                    policy-db-size 64;
                    package jservices-appid;
                    package jservices-aacl;
                    package jservices-llpdf;
                    package jservices-idp;
                    package jservices-sfw;
                }
            }
        }
    }
}
network-services ip;
```

CHAPTER 4

Junos Network Secure Configuration Statements

allow-ip-options

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

Hierarchy Level [edit services (stateful-firewall) stateful-firewall rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

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 Actions in Stateful Firewall Rules" on page 11.

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

application-sets

Syntax applications-sets *set-name*;

Hierarchy Level [edit services (stateful-firewall) stateful-firewall 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 Stateful Firewall Rules" on page 10.

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 (stateful-firewall) stateful-firewall rule *rule-name* term *term-name* from]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define one or more applications to which the stateful firewall services apply.

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

Usage Guidelines See "Configuring Match Conditions in Stateful Firewall Rules" on page 10.

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 (stateful-firewall) stateful-firewall 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 IPv6 addresses in Junos OS Release 8.5.

Description Specify the destination address for rule matching.

Options

address—Destination IPv4 or IPv6 address or prefix value. Using a value of 0::0/0 with IPv6 is not allowed for M-Series and MX-Series routers.

any-unicast—Match all unicast packets.

except—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.

Usage Guidelines See "Configuring Match Conditions in Stateful Firewall Rules" on page 10.

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 (stateful-firewall) stateful-firewall 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 IPv6 addresses in Junos OS Release 8.5.

Description Specify the destination address range for rule matching.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exclude the specified address range from rule matching.

Usage Guidelines See "Configuring Match Conditions in Stateful Firewall Rules" on page 10.

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 (stateful-firewall) stateful-firewall 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 Stateful Firewall Rules" on page 10.

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

Related Documentation

- *Routing Policy Feature Guide for Routing Devices*

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>;
  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>;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify input conditions for a stateful firewall term.

Options For information on match conditions, see the description of firewall filter match conditions in the *Routing Policy Feature Guide for Routing Devices*.

The remaining statements are explained separately.

Usage Guidelines See "Configuring Stateful Firewall 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 | input-output);

Hierarchy Level [edit services stateful-firewall 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 the input side of the interface.

output—Apply the rule match on the output side of the interface.

input-output—Apply the rule match bidirectionally.

Usage Guidelines See "Configuring Stateful Firewall 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

Syntax

```
rule rule-name {
  match-direction (input | output | 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 {
      (accept | discard | reject);
      syslog;
    }
  }
}
```

Hierarchy Level

[edit services stateful-firewall],
[edit services stateful-firewall 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 constitute this rule.

The remaining statements are explained separately.

Usage Guidelines

See "Configuring Stateful Firewall 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 stateful-firewall]

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 Stateful Firewall Rule Sets" on page 13.

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

services (stateful-firewall)

Syntax services stateful-firewall { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 10.4.

Description Define the service rules to be applied to traffic.

Options **stateful-firewall**—Identifies the stateful firewall set of rules statements.

Usage Guidelines See *Junos Network Secure*.

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 stateful-firewall 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 IPv6 addresses in Junos OS Release 8.5.

Description Source address for rule matching.

Options
address—Source IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.

Usage Guidelines See "Configuring Match Conditions in Stateful Firewall Rules" on page 10.

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 stateful-firewall 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 IPv6 addresses in Junos OS Release 8.5.

Description Source address range for rule matching.

Options
minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.

Usage Guidelines See "Configuring Match Conditions in Stateful Firewall Rules" on page 10.

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 stateful-firewall 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 Stateful Firewall Rules" on page 10.

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

Related Documentation
- *Routing Policy Feature Guide for Routing Devices*

syslog

Syntax syslog;

Hierarchy Level [edit services stateful-firewall 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. This setting overrides any **syslog** statement setting included in the service set or interface default configuration.

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

Related Documentation
- Configuring Actions in Stateful Firewall Rules on page 11

term

Syntax

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

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

Release Information Statement introduced before Junos OS Release 7.4.

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" 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 {
  (accept | discard | reject);
  syslog;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

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

accept—Accept the traffic and send it on to its destination.

discard—Do not accept traffic or process it further.

reject—Do not accept the traffic and return a rejection message. Rejected traffic can be logged or sampled.

The remaining statement is explained separately.

Usage Guidelines See "Configuring Actions in Stateful Firewall 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

- *Routing Policy Feature Guide for Routing Devices*

PART 3

Administration

CHAPTER 5

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 before Junos OS Release 7.4.

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 **rsp*number***. 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 63

List of Sample Output clear services stateful-firewall flows on page 47

Output Fields Table 4 on page 47 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 4: 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 sip-call

Syntax clear services stateful-firewall sip-call
<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 7.4.

Description Clear Session Initiation Protocol (SIP) call information in stateful firewall flows.

Options **none**—Clear stateful firewall statistics for all interfaces and all service sets.

application-protocol—(Optional) Clear information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol

- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

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

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

interface ***interface-name***—(Optional) Clear information for a particular adaptive services interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***. On J Series routers, the ***interface-name*** is **sp-*pim*/0/*port***.

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

- **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
- **ipv6**—IPv6 within IP
- **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 information for a particular service set.

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

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

Required Privilege Level view

Related Documentation

- show services stateful-firewall sip-call on page 69

List of Sample Output

clear services stateful-firewall sip-call on page 50

Output Fields

Table 5 on page 50 lists the output fields for the **clear services stateful-firewall sip-call** command. Output fields are listed in the approximate order in which they appear.

Table 5: clear services stateful-firewall sip-call 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.
SIP calls removed	Number of SIP calls removed.

Sample Output

clear services stateful-firewall sip-call

```
user@host> clear services stateful-firewall sip-call
Interface   Service set                                SIP calls removed
sp-0/3/0    test_sip_777                                             1
```

clear services stateful-firewall sip-register

Syntax clear services stateful-firewall sip-register
<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 7.4.

Description Clear Session Initiation Protocol (SIP) register information in stateful firewall flows.

Options **application-protocol**—(Optional) Clear information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet

- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

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

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

interface ***interface***—(Optional) Clear information about a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-***fpc/pic/port* or **rsp***number*. On the J Series routers, the ***interface-name*** is **sp-***pim*/0/*port*.

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

- **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
- **ipv6**—IPv6 within IP
- **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 information for a particular service set.

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

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

Required Privilege Level view

Related Documentation

- show services stateful-firewall sip-register on page 74

List of Sample Output clear services stateful-firewall sip-register on page 53

Output Fields Table 6 on page 53 lists the output fields for the **clear services stateful-firewall sip-register** command. Output fields are listed in the approximate order in which they appear.

Table 6: clear services stateful-firewall sip-register 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.
SIP registration removed	Number of SIP registers removed.

Sample Output

clear services stateful-firewall sip-register

```
user@host> clear services stateful-firewall sip-register
Interface   Service set                          SIP registration removed
sp-0/3/0    test_sip_777                                              1
```

clear services stateful-firewall statistics

Syntax clear services stateful-firewall statistics
<interface *interface-name*>
<service-set *service-set*>

Release Information Command introduced before Junos OS Release 7.4.

Description Clear stateful firewall statistics.

Options **none**—Clear stateful firewall statistics for all interfaces and all service sets.

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

service-set *service-set*—(Optional) Clear stateful firewall statistics for the specified service set.

Required Privilege Level view

Related Documentation
- show services stateful-firewall statistics on page 78

List of Sample Output clear services stateful-firewall statistics on page 54

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 conversations

Syntax

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

Release Information

Command introduced before Junos OS Release 7.4.
pgcp option introduced in Junos OS Release 8.4.

Description

Display information about stateful firewall conversations.

Options

none—Display standard information about all stateful firewall conversations.

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

application-protocol *protocol*—(Optional) Display information about one of the following application protocols:

- **bootp**—Bootstrap protocol
- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **exec**—Exec
- **ftp**—File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol

- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

destination-port ***destination-port***—(Optional) Display information for a particular destination port. The range of values is 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, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***. On J Series routers, the ***interface-name*** is **sp-*pim*/0/*port***.

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

pgcp —(Optional) Display information about stateful firewall conversations for Packet Gateway Control Protocol (PGCP) flows.

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 the specific service set.

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

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

Required Privilege Level view

List of Sample Output show services stateful-firewall conversations on page 58
show services stateful-firewall conversations destination-port on page 58

Output Fields Table 7 on page 57 lists the output fields for the **show services stateful-firewall conversations** command. Output fields are listed in the approximate order in which they appear.

Table 7: show services stateful-firewall conversations Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set. Individual empty service sets are not displayed, but if no service set has any flows, a flow table header is printed for each service set.
Conversation	Information about a group of related flows. • **ALG Protocol**—Application-level gateway protocol. • **Number of initiators**—Number of flows that initiated a session. • **Number of responders**—Number of flows that responded in a session.
Flow or Flow Prot	Protocol used for this flow.
Source	Source prefix of the flow, in the format ***source-prefix-port***.
Destination	Destination prefix of the flow.
State	Status of the flow: • **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**).
Source NAT	Original and translated source IPv4 or IPv6 addresses are displayed if Network Address Translation (NAT) is configured on this particular flow or conversation.
Frm Count	Number of frames in the flow.
Destin NAT	Original and translated destination IPv4 or IPv6 addresses are displayed if NAT is configured on this particular flow or conversation.

Table 7: show services stateful-firewall conversations Output Fields *(continued)*

Field Name	Field Description
Byte count	Number of bytes forwarded in the flow.
TCP established	Whether a TCP connection was established: **Yes** or **No**.
TCP window size	Negotiated TCP connection window size, in bytes.
TCP acknowledge	TCP acknowledgment sequence number.
TCP tickle	Whether TCP inquiry mode is on (**enabled** or **disabled**) and the time remaining to send the next inquiry, in seconds.
Master flow	Flow that initiated the conversation.
TImeout	Lifetime of the flow, in seconds.

Sample Output

show services stateful-firewall conversations

```
user@host> show services stateful-firewall conversations
Interface: sp-1/3/0, Service set: green
Conversation: ALG Protocol: any, Number of initiators: 1,
Number of responders: 1

Flow
Prot     Source                Dest              State      Dir   Frm count
TCP      10.58.255.50:33005->   10.58.255.178:23   Forward    I      13
  Source NAT     10.58.255.50:33005->    10.59.16.100:4000
  Destin NAT     10.58.255.178:23  ->         0.0.0.0:4000
Byte count:          918
TCP established, TCP window size: 65535, TCP acknowledge: 2502627025
TCP tickle enabled, 0 seconds,
Master flow, Timeout: 30 seconds
TCP     10.58.255.178:23   ->    10.59.16.100:4000 Forward    0        8
```

show services stateful-firewall conversations destination-port

```
user@host> show services stateful-firewall conversations destination-port 21
Interface: sp-0/3/0, Service set: svc_set_trust

Interface: sp-0/3/0, Service set: svc_set_untrust
Conversation: ALG protocol: ftp
  Number of initiators: 1, Number of responders: 1
Flow                                              State    Dir       Frm count
TCP         10.50.10.2:2143  ->     10.50.20.2:21    Watch    O              0
TCP         10.50.20.2:21    ->     10.50.10.2:2143  Watch    I              0
TCP         10.50.20.2:21    ->     10.50.10.2:2143  Watch    I              0
```

show services stateful-firewall flow-analysis

Syntax show services stateful-firewall flow-analysis
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 10.4R1.

Description Display stateful firewall flow statistics.

Options **none**—Display standard information about all stateful firewall flow statistics.

interface *interface-name*—(Optional) Display information about a particular interface. .

Required Privilege Level view

List of Sample Output
show services stateful-firewall flow-analysis on page 60
show services stateful-firewall flow-analysis interface sp-3/0/0 on page 61

Output Fields Table 8 on page 59 lists the output fields for the **show services stateful-firewall flow-analysis** command. Output fields are listed in the approximate order in which they appear.

Table 8: show services stateful-firewall flow-analysis Output Fields

Field Name	Field Description
Total Flows Active	Total active flows in the MS-PIC including TCP, UDP, ICMP and Softwires.
Total TCP Flows Active	Total active TCP flows in the MS-PIC.
Total UDP Flows Active	Total active UDP flows in the MS-PIC.
Total Other Flows Active	Total other active flows in the MS-PIC including ICMP and softwires.
Total Predicted Flows Active	Predicted flows are created only by the ALG traffic using the L3/L4 information available.
Created Flows per Second	Flow setup rate at the time of running the command.
Deleted Flows per Second	Flow deletion rate at the time of running the command.
Peak Total Flows Active	The highest number of active flows since the last PIC restart or since the last time flow statistics are flushed.
Peak Total TCP Flows Active	The highest number of active TCP flows since the last PIC restart or since the last time flow stats are flushed.
Peak Total UDP Flows Active	The highest number of active UDP flows since the last PIC restart or since the last time flow statistics are flushed.

Table 8: show services stateful-firewall flow-analysis Output Fields *(continued)*

Field Name	Field Description
Peak Total Other Flows Active	The highest number of other active flows since the last PIC restart or since the last time flow statistics are flushed.
Peak Created Flows per Second	The maximum flow setup rate observed since the last PIC restart or since the last time flow statistics are flushed.
Peak Deleted Flows per Second	The maximum flow deletion rate observed since the last PIC restart or from the last time flow statistics are flushed.
Average HTTP Flow Lifetime(ms)	Average HTTP Flow Lifetime in millisecond.
Packets received	The total number of packets received by the MS-PIC.
Packets transmitted	The total number of packets transmitted by the MS-PIC.
Slow path forward	The number of packets forwarded in the slow path (i.e. after the successful rule match and flow creation).
Slow path discard	The number of packets discarded before the flow creation.
Flow Rate Data: Number of Samples	The number of samples used to calculate the flow rate, since the last PIC restart or since the last time flow statistics are flushed.
Flow Rate Distribution(sec) Flow Operation :Creation Flow Operation :Deletion	Histogram of the samples used for flow rate calculation.
Flow Lifetime Distribution(sec):	Histogram of the samples used to calculate the flow life time in sec.

Sample Output

show services stateful-firewall flow-analysis

```
user@host> show services stateful-firewall flow-analysis
Services PIC Name: sp-3/0/0
 Flow Analysis Statistics:
      Total Flows Active               :40
      Total TCP Flows Active           :0
      Total UDP Flows Active           :40
      Total Other Flows Active         :0
      Total Predicted Flows Active     :0
      Created Flows per Second         :0
      Deleted Flows per Second         :0
      Peak Total Flows Active          :40
      Peak Total TCP Flows Active      :0
      Peak Total UDP Flows Active      :40
      Peak Total Other Flows Active    :0
      Peak Created Flows per Second    :20
```

```
     Peak Deleted Flows per Second    :20
     Average HTTP Flow Lifetime(ms)   :0
     Packets received                 :48682539117
     Packets transmitted              :48682502703
     Slow path forward                :6550
     Slow path discard                :0
 Flow Rate Data:
     Number of Samples: 19720
 Flow Rate Distribution(sec)
 Flow Operation :Creation
     300000+           :0
     250000  - 300000   :0
     200000  - 250000   :0
     160000  - 200000   :0
     150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :19720
 Flow Operation :Deletion
     300000+           :0
     250000  - 300000   :0
     200000  - 250000   :0
     160000  - 200000   :0
     150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :19720
 Flow Lifetime Distribution(sec):
                TCP               UDP               HTTP
  240+          :0                0                 0
  120 - 240     :0                0
   60 - 120     :0                0
   30 - 60      :0                0
   15 - 30      :0                6530
    5 - 15      :0                0
    1 - 5       :0                0
    0 - 1       :0                6530
```

Sample Output

show services stateful-firewall flow-analysis interface sp-3/0/0

```
user@host> show services stateful-firewall flow-analysis interface sp-3/0/0
Services PIC Name: sp-3/0/0
 Flow Analysis Statistics:
     Total Flows Active               :40
     Total TCP Flows Active           :0
     Total UDP Flows Active           :40
     Total Other Flows Active         :0
     Total Predicted Flows Active     :0
     Created Flows per Second         :0
     Deleted Flows per Second         :0
     Peak Total Flows Active          :40
```

```
     Peak Total TCP Flows Active      :0
     Peak Total UDP Flows Active      :40
     Peak Total Other Flows Active    :0
     Peak Created Flows per Second    :20
     Peak Deleted Flows per Second    :20
     Average HTTP Flow Lifetime(ms)   :0
     Packets received                 :54696856768
     Packets transmitted              :54696815873
     Slow path forward                :7350
     Slow path discard                :0
Flow Rate Data:
     Number of Samples: 22139
Flow Rate Distribution(sec)
Flow Operation :Creation
     300000+            :0
     250000  - 300000   :0
     200000  - 250000   :0
     160000  - 200000   :0
     150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :22139
Flow Operation :Deletion
     300000+            :0
     250000  - 300000   :0
     200000  - 250000   :0
     160000  - 200000   :0
     150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :22139
Flow Lifetime Distribution(sec):
               TCP                UDP              HTTP
 240+         :0                 0                0
 120 - 240    :0                 0
  60 - 120    :0                 0
  30 - 60     :0                 0
  15 - 30     :0                 7330
   5 - 15     :0                 0
   1 - 5      :0                 0
   0 - 1      :0                 7330
```

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 before Junos OS Release 7.4.
pgcp option introduced in Junos OS Release 8.4.
application-protocol option introduced in Junos OS Release 10.4.

Description

Display stateful firewall flow table entries. When the interface is used for softwire processing, the type of softwire 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 **rsp*number***. 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 46

List of Sample Output
show services stateful-firewall flows on page 66
show services stateful-firewall flows (For Softwire Flows) on page 66
show services stateful-firewall flows brief on page 67
show services stateful-firewall flows extensive on page 67
show services stateful-firewall flows count on page 67
show services stateful-firewall flows destination port on page 67
show services stateful-firewall flows source port on page 67
show services stateful-firewall flows (Twice NAT) on page 67

Output Fields Table 9 on page 65 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 9: 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.

Table 9: show services stateful-firewall flows Output Fields *(continued)*

Field Name	Field Description
Source	Source prefix of the flow in the format ***source-prefix:port***. For ICMP flows, port information is not displayed.
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.
State	Status of the flow: • **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 Softwire Flows)

When a service set includes softwire processing, the following output format is used for the softwire flows:

```
user@host> show services stateful-firewall flows
Interface: sp-0/1/0, Service set: dslite-svc-set2
Flow                                                 State    Dir       Frm count
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
    Softwire          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
    Softwire          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
    Softwire          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
    Softwire          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
    Softwire          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
    Softwire           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 stateful-firewall flows extensive

```
user@host> show services stateful-firewall flows extensive
Interface: ms-0/3/0, Service set: ss_nat
Flow                                                  State     Dir       Frm
count
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    O
   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 stateful-firewall flows count

```
user@host> show services stateful-firewall flows count
Interface             Service set                                 Flow Count

ms-1/3/0              green                                              2
```

show services stateful-firewall flows destination port

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

show services stateful-firewall flows source port

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

show services stateful-firewall flows (Twice NAT)

```
user@router> show services stateful-firewall flows
```

```
Flow                                                 State    Dir       Frm count
UDP          40.0.0.8:23439 ->     80.0.0.1:16485   Watch    I            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    O            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 sip-call

Syntax show services stateful-firewall sip-call
<brief | extensive | terse>
<application-protocol *protocol*>
<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 7.4.

Description Display stateful firewall Session Initiation Protocol (SIP) call information.

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

brief—(Optional) Display brief SIP call information.

extensive—(Optional) Display detailed SIP call information.

terse—(Optional) Display terse SIP call information.

application-protocol—(Optional) Display information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol

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

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 adaptive services interface. On M Series and T Series routers, ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***. On J Series routers, ***interface-name*** is **sp-*pim*/0/*port***.

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

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

- **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
- **ipv6**—IPv6 within IP
- **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 sip-call on page 48

List of Sample Output show services stateful-firewall sip-call extensive on page 72

Output Fields Table 10 on page 71 lists the output fields for the **show services stateful-firewall sip-call** command. Output fields are listed in the approximate order in which they appear.

Table 10: show services stateful-firewall sip-call Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
From	Initiator address.
To	Responder address.
Call ID	SIP call identification string.
Number of initiator flows	Number of **control**, **contact**, or **media** initiator flows.
Number of responder flows	Number of **control**, **contact**, or **media** responder flows.
protocol	Protocol used for this flow.
source-prefix	Source prefix of the flow in the format ***source-prefix* : *port***.
destination-prefix	Destination prefix of the flow.
state	Status of the flow: • **Drop**—Drop all packets in the flow without a response. • **Forward**—Forward the packet in the flow without examining it. • **Reject**—Drop all packets in the flow with a response. • **Unknown**—Unknown status. • **Watch**—Inspect packets in the flow.
direction	Direction of the flow: input (**I**), output (**O**), or unknown (**U**).

Table 10: show services stateful-firewall sip-call Output Fields *(continued)*

Field Name	Field Description
frame-count	Number of frames in the flow.
Byte count	Number of bytes forwarded in the flow.
Flow role	Role of the flow that is under evaluation: **Initiator**, **Master**, **Responder**, or **Unknown**.
Timeout	Lifetime of the flow, in seconds.

Sample Output

show services stateful-firewall sip-call extensive

```
user@host> show services stateful-firewall sip-call extensive
Interface: sp-0/3/0, Service set: test_sip_777

From: : 6507771234@10.200.100.1:0;000ff73ac89900021bb231dc-3ef68435
To: : 4085551234@10.200.100.1:0;0011bb65c2a30007777bd0fc-5748b749
Call ID: : 000ff73a-c8990004-0741adac-3e027c7e@10.20.70.2
Number of control initiator flows: : 1, Number of control responder flows:
: 1
UDP         10.20.70.2:50354 ->   10.200.100.1:5060  Watch    I
2
  Byte count: 1112
  Flow role: Master, Timeout: 30
UDP       10.200.100.1:5060  ->  10.20.170.111:50354 Watch    O
0
  Byte count: 0
  Flow role: Responder, Timeout: 30
UDP           0.0.0.0:0     ->  10.20.170.111:5060  Watch    O
7
  Byte count: 2749
  Flow role: Responder, Timeout: 30
Number of contact initiator flows: 1, Number of contact responder flows: 1
UDP           0.0.0.0:0     ->   10.20.140.11:5060  Watch    I
1
  Byte count: 409
  Flow role: Master, Timeout: 30
UDP       10.20.140.11:31864 ->  10.20.170.111:18808 Forward  O
622
  Byte count: 124400
  Flow role: Master, Timeout: 30
UDP           0.0.0.0:0     ->  10.20.170.111:18809 Forward  O
0
  Byte count: 0
  Flow role: Initiator, Timeout: 30
Number of media initiator flows: 4, Number of media responder flows: 0
UDP         10.20.70.2:18808 ->   10.20.140.11:31864 Forward  I
628
  Byte count: 125600
  Flow role: Initiator, Timeout: 30
UDP           0.0.0.0:0     ->   10.20.140.11:31865 Forward  I
0
  Byte count: 0
```

```
  Flow role: Initiator, Timeout: 30
0              0.0.0.0:0     ->        0.0.0.0:0     Unknown  U
0
  Byte count: 0
  Flow role: Unknown, Timeout: 0
0              0.0.0.0:0     ->        0.0.0.0:0     Unknown  U
Interface: sp-0/3/0, Service set: test_sip_888
```

show services stateful-firewall sip-register

Syntax show services stateful-firewall sip-register
<brief | extensive | terse>
<application-protocol *protocol*>
<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 7.4.

Description Display stateful firewall Session Initiation Protocol (SIP) register information.

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

brief—(Optional) Display brief SIP register information.

extensive—(Optional) Display detailed SIP register information.

terse—(Optional) Display terse SIP register information.

application-protocol—(Optional) Display information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol

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

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

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

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

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

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

- **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
- **ipv6**—IPv6 within IP
- **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 sip-register on page 51

List of Sample Output show services stateful-firewall sip-register extensive on page 76

Output Fields Table 11 on page 76 lists the output fields for the **show services stateful-firewall sip-register** command. Output fields are listed in the approximate order in which they appear.

Table 11: show services stateful-firewall sip-register Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
SIP Register	Register information header.
Protocol	Protocol used for this flow.
Registered IP	Register IP address.
Port	Register port number.
Expiration timeout	Configured lifetime, in seconds.
Timeout remaining	Lifetime remaining, in seconds.
From	Initiator address.
To	Responder address.
Call ID	SIP call identification string.

Sample Output

show services stateful-firewall sip-register extensive

```
user@host> show services stateful-firewall sip-register extensive
Interface: sp-0/3/0, Service set: test_sip_777

SIP Register: Protocol: UDP, Registered IP: 10.20.170.111, Port: 5060, Acked
    Expiration timeout: 36000, Timeout remaining: 35544
    From: : 6507771234@10.200.100.1:0;
    To: : 6507771234@10.200.100.1:0;
```

```
    Call ID: : 000ff73a-c8990002-23b1d942-2ba1f91f@10.20.70.2

Interface: sp-0/3/0, Service set: test_sip_888

SIP Register: Protocol: UDP, Registered IP: 10.20.170.112, Port: 5060, Acked
    Expiration timeout: 36000, Timeout remaining: 35549
    From: : 8881234@10.200.100.1:0;
    To: : 8881234@10.200.100.1:0;
    Call ID: : 00112096-81fc0002-23b38905-7cb41f62@10.20.71.2
```

show services stateful-firewall statistics

Syntax

show services stateful-firewall statistics
<application-protocol *protocol*>
<brief | detail | extensive | summary>
<interface *interface-name*>
<service-set *service-set*>

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display stateful firewall statistics.

Options

none—Display standard information about all stateful firewall statistics.

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

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

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

Required Privilege Level

view

Related Documentation

- clear services stateful-firewall statistics on page 54

List of Sample Output

show services stateful-firewall statistics extensive on page 85

Output Fields

Table 12 on page 78 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 12: 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: • **Rule Accepts**—New flows accepted. • **Rule Discards**—New flows discarded. • **Rule Rejects**—New flows rejected.
Existing flow types packet counters	Rule match counters for existing flows: • **Accepts**—Match existing forward or watch flow. • **Drop**—Match existing discard flow. • **Rejects**—Match existing reject flow.

Table 12: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
Hairpinning Counters	Hairpinning counters: • **Slow Path Hairpinned Packets**—Slow path packets that were hairpinned back to the internal network. • **Fast Path Hairpinned Packets**—Fast path packets that were hairpinned back to the internal network.
Drops	Drop counters: • **IP option**—Packets dropped in IP options processing. • **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. • **Sessions dropped due to subscriber flow limit**—Sessions dropped because the subscriber's flow limit was exceeded.
Errors	Total errors, categorized by protocol: • **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 packets**—Total non-IPv4 errors. • **ALG**—Total application-level gateway (ALG) errors

Table 12: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
IP Errors	IPv4 errors: • **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. • **Illegal IP protocol number (0 or 255)**—IP protocol is 0 or 255. • **Land attack**—IP source address is the same as the destination address. • **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. • **IP fragment limit exceeded: 0**—Fragments that exceeded the limit. • **Unknown: 0**—Unknown fragments.

Table 12: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
TCP Errors	

Table 12: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
	TCP protocol errors: • **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 and flags combinations** — 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 a SYN message**—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 (TCP 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. • **TCP reconstructor sequence number error**—This counter is incremented in the following cases: The TCP seqno is 0 and all the TCP flags are also 0. The TCP seqno is 0 and FIN/PSH/URG TCP flags are set. • **TCP reconstructor retransmissions**—This counter is incremented for the retransmitted packets during connection 3-way handshake. • **TCP partially opened connection timeout (SYN)**—This counter is incremented when the SYN Defender is enabled and the 3-way handshake is not completed within the SYN DEFENDER TIMEOUT. The connection will be closed and resources will be released by sending RST to the responder. • **TCP partially opened connection timeout (SYN-ACK)**—This counter is incremented when the SYN Defender is enabled and the 3-way handshake is not completed within the SYN DEFENDER TIMEOUT. The connection will be closed and resources will be released by sending RST to the responder. • **TCP partially closed connection reuse**—Not supported. • **TCP 3-way error - client sent SYN+ACK**—A SYN/ACK should be sent by the server on receiving a SYN. This counter is incremented when the first message received from the initiator is SYN+ACK. • **TCP 3-way error - server sent ACK**—ACK should be sent by the client on receiving a SYN/ACK from the server. This counter is incremented when the ACK is received from the Server instead of from the Client. • **TCP 3-way error - SYN seq number retransmission mismatch**—This counter is incremented when the SYN is received again with a different sequence number from the first SYN sequence number. • **TCP 3-way error - RST seq number mismatch**—A reset could be received from either side. The server could send a RST on receiving a SYN or the client could send a RST on receiving SYN/ACK. This counter is incremented when the

Table 12: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
	RST is received either from the client or server with a non-matching sequence number. • **TCP 3-way error - FIN received**—This counter is incremented when the FIN is received during the 3-way handshake. • **TCP 3-way error - invalid flags (PSH, URG, ECE, CWR)**—This counter is incremented when any of the PSH, URG, ECE, or CWR flags were received during the 3-way handshake. • **TCP 3-way error - SYN recvd but no client flows**—This counter is incremented when SYN is received but not from the connection initiator. The counter is not incremented in the case of simultaneous open, when the SYN is received in both the directions. • **TCP 3-way error - first packet SYN+ACK**—The first packet received was SYN+ACK instead of SYN. • **TCP 3-way error - first packet FIN+ACK**—The first packet received was FIN+ACK instead of SYN. • **TCP 3-way error - first packet FIN**—The first packet received was FIN instead of SYN. • **TCP 3-way error - first packet RST**—The first packet received was RST instead of SYN. • **TCP 3-way error - first packet ACK**—The first packet received was ACK instead of SYN. • **TCP 3-way error - first packet invalid flags (PSH, URG, ECE, CWR)**—The first packet received had invalid flags. • **TCP Close error - no final ACK**—This counter is incremented when ACK is not received after the FINs are received from both directions. • **TCP Resumed Flow**—Plain ACKs create flows if rule match permits, and these are classified as TCP Resumed Flows. This counter is incremented in the case of a TCP Resumed Flow.
UDP Errors	UDP protocol errors: • **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	ICMP protocol errors: • **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. • **Duplicate ping sequence number**—Received ping packet has a duplicate sequence number. • **Mismatched ping sequence number**—Received ping packet has a mismatched sequence number. • **No matching flow**—No matching existing flow was found for the ICMP error.

Table 12: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
ALG errors	Accumulation of all the application-level gateway protocol (ALG) drops counted separately in the ALG context: • **BOOTP**—Bootstrap protocol errors • **DCE-RPC**—Distributed Computing Environment-Remote Procedure Call protocols errors • **DCE-RPC portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service errors • **DNS**—Domain Name System protocol errors • **Exec**—Exec errors • **FTP**—File Transfer Protocol errors • **H323**—H.323 standards errors • **ICMP**—Internet Control Message Protocol errors • **IIOP**—Internet Inter-ORB Protocol errors • **Login**—Login errors • **NetBIOS**—NetBIOS errors • **Netshow**—NetShow errors • **Real Audio**—RealAudio errors • **RPC**—Remote Procedure Call protocol errors • **RPC portmap**—Remote Procedure Call protocol portmap service errors • **RTSP**—Real-Time Streaming Protocol errors • **Shell**—Shell errors • **SIP**—Session Initiation Protocol errors • **SNMP**—Simple Network Management Protocol errors • **SQLNet**—SQLNet errors • **TFTP**—Trivial File Transfer Protocol errors • **Traceroute**—Traceroute errors
Drop Flows	• **Maximum Ingress Drop flows allowed**-–Maximum number of ingress flow drops allowed. • **Maximum Egress Drop flows allowed**-–Maximum number of egress flow drops allowed. • **Current Ingress Drop flows**-–Current number of ingress flow drops. • **Current Egress Drop flows**-–Current number of egress flow drops. • **Ingress Drop Flow limit drops count**-–Number of ingress flow drops due to maximum number of ingress flow drops being exceeded. • **Egress Drop Flow limit drops count**-–Number of egress flow drops due to maximum number of egress flow drops being exceeded.

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:
      Rule Accepts: 907, Rule Discards: 0, Rule Rejects: 0
    Existing flow types packet counters:
      Accepts: 3535, Drop: 0, Rejects: 0
    Haripinning counters:
      Slow Path Hairpinned Packets: 0, Fast Path Hairpinned Packets: 0
    Drops:
      IP option: 0, TCP SYN defense: 0
      NAT ports exhausted: 0, Sessions dropped due to subscriber flow limit: 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, Illegal IP protocol number (0 or 255): 0
      Land attack: 0
      Non-IPv4 packets: 0, Bad checksum: 0
      Illegal IP fragment length: 0
      IP fragment overlap: 0
      IP fragment reassembly timeout: 0
      IP fragment limit exceeded:0
      Unknown: 0
    TCP errors:
      TCP header length inconsistencies: 0
      Source or destination port number is zero: 0
      Illegal sequence number and flags combination: 0
      SYN attack (multiple SYN messages seen for the same flow): 0
      First packet not a SYN message: 0
      TCP port scan (TCP handshake, RST seen from server for SYN): 0
      Bad SYN cookie response: 0
      TCP reconstructor sequence number error: 0
      TCP reconstructor retransmissions: 0
      TCP partially opened connection timeout (SYN): 0
      TCP partially opened connection timeout (SYN-ACK): 0
      TCP partially closed connection reuse: 0
      TCP 3-way error - client sent SYN+ACK: 0
      TCP 3-way error - server sent ACK: 0
      TCP 3-way error - SYN seq number retransmission mismatch: 0
      TCP 3-way error - RST seq number mismatch: 0
      TCP 3-way error - FIN received: 0
      TCP 3-way error - invalid flags (PSH, URG, ECE, CWR): 0
      TCP 3-way error - SYN recvd but no client flows: 0
      TCP 3-way error - first packet SYN+ACK: 0
      TCP 3-way error - first packet FIN+ACK: 0
      TCP 3-way error - first packet FIN: 0
      TCP 3-way error - first packet RST: 0
      TCP 3-way error - first packet ACK: 0
      TCP 3-way error - first packet invalid flags (PSH, URG, ECE, CWR): 0
      TCP Close error - no final ACK: 0
```

```
      TCP Resumed Flow: 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
      Duplicate ping sequence number: 0
      Mismatched ping  sequence number: 0
      No matching flow: 0
    ALG errors:
      BOOTP: 0, DCE-RPC: 0, DCE-RPC portmap: 0
      DNS: 0, Exec: 0, FTP: 0
      H323: 0, ICMP: 0, IIOP: 0
      Login: 0, NetBIOS: 0, Netshow: 0
      Real Audio: 0, RPC: 0, RPC portmap: 0
      RTSP: 0, Shell: 0, SIP: 0
      SNMP: 0, SQLNet: 0, TFTP: 0
      Traceroute: 0
    Drop Flows:
      Maximum Ingress Drop flows allowed: 20
      Maximum Egress Drop flows allowed: 20
      Current Ingress Drop flows: 0
      Current Egress Drop flows: 0
      Ingress Drop Flow limit drops count: 0
      Egress Drop Flow limit drops count: 0

**If max-drop-flows is not configured, the following is shown**
    Drop Flows:
      Maximum Ingress Drop flows allowed: Default
      Maximum Egress Drop flows allowed: Default
```

show services stateful-firewall statistics application-protocol sip

Syntax show services stateful-firewall application-protocol sip

Release Information Command introduced in Junos OS Release 7.4.

Description Display stateful firewall Session Initiation Protocol (SIP) statistics.

Options This command has no options.

Required Privilege Level view

List of Sample Output show services stateful-firewall statistics application-protocol-sip on page 88

Output Fields Table 13 on page 87 lists the output fields for the **show services stateful-firewall statistics application-protocol-sip** command. Output fields are listed in the approximate order in which they appear.

Table 13: show services stateful-firewall statistics application-protocol-sip Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of the service set flow.
ALG	Name of the application-layer gateway.
Active SIP call count	Number of active SIP calls.
Active SIP registration count	Number of active SIP registrations.
REGISTER	Number of new, invalid, and retransmitted register requests sent to the SIP registrar.
INVITE	Number of new, invalid, and retransmitted invite messages sent by user agent clients.
ReINVITE	Number of new, invalid, and retransmitted reinvite messages sent by user agent clients.
ACK	Number of new, invalid, and retransmitted ACK messages received (in response to a SIP Call Invite message).
BYE	Number of new, invalid, and retransmitted requests to terminate SIP dialogues.
CANCEL	Number of new, invalid, and retransmitted SIP request cancellations.
SUBSCRIBE	Number of new, invalid, and retransmitted SIP requests to subscribe for event notifications.
NOTIFY	Number of new, invalid, and retransmitted event notifications in SIP dialogues.

Table 13: show services stateful-firewall statistics application-protocol-sip Output Fields *(continued)*

Field Name	Field Description
OPTIONS	Number of new, invalid, and retransmitted requests to query SIP capabilities.
INFO	Number of new, invalid, and retransmitted requests carrying application-level information.
UPDATE	Number of new, invalid, and retransmitted SIP dialogue updates.
REFER	Number of new, invalid, and retransmitted requests to the recipient to contact a third party.
Provisional responses	Number of new, invalid, and retransmitted responses from the user agent server to indicate the progress of a SIP transaction.
OK responses to INVITEs	OK responses sent from the user agent clients to user agent servers in response to Invite messages. The server can then return an ACK message.
OK responses to non-INVITES	OK responses to SIP messages other than an Invite message.
Redirection responses	Responses from the user agent server to a user agent client requesting the client to contact a different SIP uniform resource identifier (URI).
Request failure responses	Responses that indicate a definite failure from a particular server. The client must not retry the same request without modification after receiving this response.
Server failure responses	Responses that indicate a server failure.
Global failure responses	Responses that indicate a server has definitive information about a particular user, not just the particular instance indicated in the Request URI.
Invalid responses	Responses that are invalid.
Response (all) retransmits	Retransmissions of all responses.
Parser	Syntax errors, content errors, and unknown methods counted by the message parser.

Sample Output

show services stateful-firewall statistics application-protocol-sip

```
user@host> show services stateful-firewall statistics application-protocol sip
Interface: sp-0/3/0
  Service set: test_sip_777, ALG: SIP
  Active SIP call count: 0, Active SIP registration count: 1
                    New      Invalid    Retransmit
    REGISTER          2
    INVITE            1                          0
    ReINVITE          1
    ACK               1            0             0
    BYE               0            0
```

```
  CANCEL            0            0
  SUBSCRIBE         0            0
  NOTIFY            0            0
  OPTIONS           0            0
  INFO              0            0
  UPDATE            0            0
  REFER             0            0
  Provisional responses (18x): 1, OK responses to INVITEs: 2
  OK responses to non-INVITEs: 2, Redirection (3xx) responses: 0
  Request failure (4xx) responses: 0, Server failure (5xx) responses: 0
  Global failure (6xx) responses: 0, Invalid responses: 0
  Response (all) retransmits: 0
  Parser:
    Syntax errors: 0, Content errors: 0, Unknown methods: 0
Service set: test_sip_888, ALG: SIP
Active SIP call count: 0, Active SIP registration count: 1
                 New      Invalid    Retransmit
  REGISTER         2
  INVITE           0                          0
  ReINVITE         0
  ACK              0            0             0
  BYE              0            0
  CANCEL           0            0
  SUBSCRIBE        0            0
  NOTIFY           0            0
  OPTIONS          0            0
  INFO             0            0
  UPDATE           0            0
  REFER            0            0
  Provisional responses (18x): 0, OK responses to INVITEs: 0
  OK responses to non-INVITEs: 2, Redirection (3xx) responses: 0
  Request failure (4xx) responses: 0, Server failure (5xx) responses: 0
  Global failure (6xx) responses: 0, Invalid responses: 0
  Response (all) retransmits: 0
  Parser:
    Syntax errors: 0, Content errors: 0, Unknown methods: 0
```

show services stateful-firewall subscriber-analysis

Syntax show services stateful-firewall subscriber analysis
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 11.4.

Description Display information about the number of active subscribers on the service physical interface card (PIC).

Options **none**—Display standard information about all active subscribers on the PIC.

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level view

List of Sample Output show services stateful-firewall subscriber analysis on page 91
show services stateful-firewall subscriber-analysis on page 91

Output Fields Table 14 on page 90 lists the output fields for the **show services stateful-firewall subscriber analysis** command. Output fields are listed in the approximate order in which they appear.

Table 14: show services stateful-firewall subscriber-analysis Output Fields

Field Name	Field Description
Services PIC Name	Name of an adaptive services interface.
Total Subscribers Active	Total number of subscribers currently active on the service PIC.
Created Subscribers per Second	Rate at which subscribers are currently being created on the service PIC.
Deleted Subscribers per Second	Rate at which subscribers are currently being deleted on the service PIC.
Peak Total Subscribers Active	Highest number of subscribers that were active during the lifetime of the service PIC.
Peak Created Subscribers per Second	Highest rate at which subscribers were being created during the lifetime of the service PIC.
Peak Deleted Subscribers per Second	Highest rate at which subscribers were being deleted during the lifetime of the service PIC.
Number of Samples	The current sampling period lifetime.
Subscriber Operation: Creation	Number of sampling intervals during which a number of subscribers in the indicated range were created during the current sampling period.
Subscriber Operation: Deletion	Number of sampling intervals during which a number of subscribers in the indicated range were deleted during the current sampling period.

Sample Output

show services stateful-firewall subscriber analysis

```
user@host> show services stateful-firewall subscriber analysis
  Services PIC Name:    sp-2/0/0
Subscriber Analysis Statistics:
  Total Subscribers Active               :100000
  Created Subscribers per Second         :0
  Deleted Subscribers per Second         :0
  Peak Total Subscribers Active          :100000
  Peak Created Subscribers per Second    :2389
  Peak Deleted Subscribers per Second    :0

Subscriber Rate Data:
  Number of Samples: 55

Subscriber Rate Distribution(sec)
Subscriber Operation :Creation

    300000+            :0
    250000  - 300000   :0
    200000  - 250000   :0
    160000  - 200000   :0
    150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
      1000  -  10000   :42
         0  -   1000   :1
Subscriber Operation :Deletion
    300000+            :0
    250000  - 300000   :0
    200000  - 250000   :0
    160000  - 200000   :0
    150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
```

show services stateful-firewall subscriber-analysis

```
user@host> show services stateful-firewall subscriber analysis
  Services PIC Name:    sp-2/0/0

Subscriber Analysis Statistics:

  Total Subscribers Active               :23547
  Created Subscribers per Second         :2389
  Deleted Subscribers per Second         :0
  Peak Total Subscribers Active          :23547
  Peak Created Subscribers per Second    :2389
  Peak Deleted Subscribers per Second    :0

Subscriber Rate Data:
  Number of Samples: 16

 Subscriber Rate Distribution(sec)
```

```
Subscriber Operation :Creation

   300000+            :0
   250000  - 300000   :0
   200000  - 250000   :0
   160000  - 200000   :0
   150000  - 160000   :0
    50000  - 150000   :0
    40000  -  50000   :0
    30000  -  40000   :0
    20000  -  30000   :0
    10000  -  20000   :0
     1000  -  10000   :9
        0  -   1000   :1


Subscriber Operation :Deletion

   300000+            :0
   250000  - 300000   :0
   200000  - 250000   :0
   160000  - 200000   :0
   150000  - 160000   :0
    50000  - 150000   :0
    40000  -  50000   :0
    30000  -  40000   :0
    20000  -  30000   :0
    10000  -  20000   :0
     1000  -  10000   :0
        0  -   1000   :0
```

PART 4

Index

Index

Symbols

A

B

C

D

F

J

M

P

R

S

T