Stateful Firewall for JSF

Release
12.1

Published: 2012-03-22

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

Stateful Firewall for JSF

Revision History
March 2012—R1 Stateful Firewall for JSF 12.1

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

END USER LICENSE AGREEMENT

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

Table of Contents

Part 1 Overview

Chapter 1 Stateful Firewall . . . 3

Stateful Firewall Overview for JSF . . . 3
Stateful Firewall Support for Application Protocols . . . 4

Part 2 Configuration

Chapter 2 Configuration Tasks . . . 7

Configuring Stateful Firewall Rules for JSF . . . 7
Configuring Match Direction for Stateful Firewall Rules . . . 8
Configuring Match Conditions in Stateful Firewall Rules . . . 8
Configuring Actions in Stateful Firewall Rules . . . 9
Configuring Stateful Firewall Rule Sets for JSF . . . 10
Configuring Juniper Service Framework – Stateful Firewall, Rules, and Services Set . . . 10
Configuring the JSF Stateful Firewall Package . . . 10
Configuring the Stateful Firewall Rule . . . 12
Configuring the Services Set for Stateful Firewall . . . 13

Chapter 3 Example . . . 17

Examples: Configuring Stateful Firewall Rules for JSF . . . 17

Chapter 4 Configuration Statements . . . 21

allow-ip-options . . . 21
applications . . . 22
application-sets . . . 22
destination-address . . . 23
destination-address-range . . . 23
destination-prefix-list . . . 24
from . . . 25
match-direction . . . 25
rule . . . 26
rule-set . . . 27
services . . . 27
source-address . . . 28
source-address-range . . . 28
source-prefix-list . . . 29
syslog . . . 29
term . . . 30
then . . . 31

Part 3 Administration

Chapter 5 Stateful Firewall Operational Mode Commands 35

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

Part 4 Troubleshooting

Chapter 6 Knowledge Base 41

Part 5 Index

Index 45

List of Tables

Part 3 Administration

Chapter 5 Stateful Firewall Operational Mode Commands 35

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

PART 1

Overview

- Stateful Firewall on page 3

CHAPTER 1

Stateful Firewall

- Stateful Firewall Overview for JSF on page 3

Stateful Firewall Overview for JSF

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

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

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

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

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

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

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

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

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

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

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

Stateful Firewall Support for Application Protocols

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

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

PART 2

Configuration

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

CHAPTER 2

Configuration Tasks

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

Configuring Stateful Firewall Rules for JSF

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

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

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

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

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

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

Configuring Match Direction for Stateful Firewall Rules

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

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

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

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.

With a next-hop service set, packet direction is determined by the interface used to route the packet to the AS or Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output.

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

Configuring Match Conditions in Stateful Firewall Rules

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

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

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

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

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

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

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

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

NOTE: If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions.

Configuring Actions in Stateful Firewall Rules

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

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

You must include one of the following three possible actions:

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

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

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

Configuring Stateful Firewall Rule Sets for JSF

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

```
[edit services stateful-firewall]
rule-set rule-set-name {
  rule rule-name;
}
```

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

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

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

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

Configuring the JSF Stateful Firewall Package

To configure the JSF services:

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

   ```
   user@host# edit chassis
   ```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In this example, the size of the object cache is 1280 MB.

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

6. Configure the size of the policy database in MB.

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

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

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

7. Configure the package.

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

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

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

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

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

In this example **syslog** is set to **daemon any** and **external any**:

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

9. Verify the configuration.

```
[edit chassis]
user@host# show chassis
fpc 1 {
    pic 0 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 7;
                    object-cache-size 1280;
                    policy-db-size 64;
                    package jservices-nat;
                    syslog {
                        daemon any;
                        external any;
                    }
                }
            }
        }
    }
}
```

Configuring the Stateful Firewall Rule

To configure the stateful firewall rule:

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

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

2. Configure the Stateful Firewall rule.

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

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

```
[edit services]
```

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

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

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

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

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

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

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

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

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

5. Verify the configuration.

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

Configuring the Services Set for Stateful Firewall

To configure the services set for stateful firewall:

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

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

2. Configure the services set.

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

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

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

3. Configure the services set message rate limit.

```
[edit services service-set sfw-ss]
```

```
user@host# edit syslog syslog
```

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

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

4. Configure the host attributes.

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

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

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

5. Configure the services with services attributes.

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

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

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

6. Configure the services set with SFW rules.

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

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

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

7. Configure the interface.

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

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

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

8. Configure the service interface.

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

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

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

9. Verify the configuration.

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



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

CHAPTER 3

Example

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

Examples: Configuring Stateful Firewall Rules for JSF

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

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

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

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

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

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

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

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

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

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

This is equivalent to the following configuration:

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

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

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

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

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

CHAPTER 4

Configuration Statements

allow-ip-options

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

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

Release Information Statement introduced in Junos OS Release 10.4.

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

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

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

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

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

applications

Syntax applications [*application-names*];

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

Release Information Statement introduced in Junos OS Release 10.4.

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

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

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

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

application-sets

Syntax applications-sets *set-name*;

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

Release Information Statement introduced in Junos OS Release 10.4.

Description Define one or more arget application sets.

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

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

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

destination-address

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

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

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the destination address for rule matching.

Options

address—Destination IPv4 or IPv6 address or prefix value.

any-unicast—Match all unicast packets.

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

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

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

destination-address-range

Syntax destination-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 10.4.

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 Stateful Firewall Rules for JSF" on page 7.

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

destination-prefix-list

Syntax destination-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 10.4.

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

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

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

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

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

Related Documentation

- *Junos OS Policy Framework Configuration Guide*

from

Syntax

```
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>;
}
```

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

Release Information Statement introduced in Junos OS Release 10.4.

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 *Junos OS Policy Framework Configuration Guide*.

The remaining statements are explained separately.

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

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

match-direction

Syntax match-direction (input | output | input-output);

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

Release Information Statement introduced in Junos OS Release 10.4.

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 for JSF" on page 7.

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

rule

Syntax

```
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);
      syslog;
    }
  }
}
```

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

Release Information Statement introduced in Junos OS Release 10.4.

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 for JSF" on page 7.

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

rule-set

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

Hierarchy Level [edit services stateful-firewall]

Release Information Statement introduced in Junos OS Release 10.4.

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

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

Usage Guidelines See "Configuring Stateful Firewall Rule Sets for JSF" on page 10.

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

services

Syntax services stateful-firewall { ... }

Hierarchy Level [edit]

Release Information 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 "Stateful Firewall Overview for JSF" on page 3.

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

source-address

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

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

Release Information Statement introduced in Junos OS Release 10.4.

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 Stateful Firewall Rules for JSF" on page 7.

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

source-address-range

Syntax 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 10.4.

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 Stateful Firewall Rules for JSF" on page 7.

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

source-prefix-list

Syntax 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 10.4.

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

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

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

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

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

Related Documentation
- *Junos OS Policy Framework Configuration Guide*

syslog

Syntax syslog;

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

Release Information Statement introduced in Junos OS Release 10.4.

Description Enable system logging. The system log information from the Adaptive Services or Multiservices PIC is passed to the kernel for logging in the **/var/log** directory. This setting overrides any **syslog** statement setting included in the service set or interface default configuration.

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

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

term

Syntax

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

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

Release Information Statement introduced in Junos OS Release 10.4.

Description Define the stateful firewall term properties.

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

The remaining statements are explained separately.

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

Required Privilege 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 in Junos OS Release 10.4.

Description Define the stateful firewall term actions. You can configure the router to accept, discard, or reject the targeted traffic. The other actions are optional.

Options

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 Stateful Firewall Rules for JSF" on page 7.

Required Privilege Level

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

Related Documentation

- *Junos OS Policy Framework Configuration Guide*

PART 3

Administration

- Stateful Firewall Operational Mode Commands on page 35

CHAPTER 5

Stateful Firewall Operational Mode Commands

clear services stateful-firewall flows

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

Release Information Command introduced in Junos OS Release 10.4.

Description Clear stateful firewall flows.

Options **none**—Clear all stateful firewall flows.

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

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

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

List of Sample Output clear services stateful-firewall flows on page 37

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

Table 1: clear services stateful-firewall flows Output Fields

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

Sample Output

clear services stateful-firewall flows

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

clear services stateful-firewall statistics

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

Release Information Command introduced in Junos OS Release 10.4.

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

List of Sample Output clear services stateful-firewall statistics on page 38

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services stateful-firewall statistics

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

PART 4

Troubleshooting

- Knowledge Base on page 41

CHAPTER 6

Knowledge Base

PART 5

Index

- Index on page 45

Index

A

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

C

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

D

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

F

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

M

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

R

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

S

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

T

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