

Chapter 6

Stateful Firewall Services Configuration Guidelines

To configure stateful firewall services, you include statements at the [edit services] hierarchy level of the configuration:

```
[edit services]
stateful-firewall {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      from {
        applications [ application-names ];
        application-sets [ set-names ];
        destination-address address;
        source-address address;
      }
      then {
        (accept | discard | reject);
        allow-ip-option [ values ];
        syslog;
      }
    }
  }
  rule-set rule-set-name {
    [ rule rule-names ];
  }
}
```

This chapter contains the following sections:

Configuring Stateful Firewall Properties on page 63

Examples: Configuring Stateful Firewall Properties on page 67

Configuring Stateful Firewall Properties

This section describes the following tasks for configuring stateful firewalls:

Configuring the Stateful Firewall Rule Set on page 64

Configuring Stateful Firewall Rule Content on page 64

Configuring the Stateful Firewall Rule Set

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:

```
[edit services stateful-firewall]
rule-set rule-set-name {
  rule rule-name1;
  rule rule-name2;
  rule rule-name3;
  ...
}
```

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 Stateful Firewall Rule Content

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 {
      applications [ application-names ];
      application-sets [ set-names ];
      destination-address address;
      source-address address;
    }
    then {
      (accept | discard | reject);
      allow-ip-option [ 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.

then statement—Specifies the actions and action modifiers to be performed by the router software.

In addition, 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, bidirectional rule creation is allowed.

The following sections describe stateful firewall rule content in more detail:

Configuring Stateful Firewall Match Conditions on page 65

Configuring Stateful Firewall Actions on page 66

Configuring Stateful Firewall Match Conditions

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 {
    applications [ application-names ];
    application-sets [ set-names ];
    destination-address address;
    source-address address;
}
```

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 Policy Framework Configuration Guide*. For destination addresses only, you can use the wildcard value any-unicast, which denotes matching all unicast addresses.

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 “Applications Configuration Guidelines” on page 43.

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 Stateful Firewall Actions

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-option [ 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-option` 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-option` statement. If you do not configure `allow-ip-option`, 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 services (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, as long as the packet is accepted by the stateful firewall.

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 8 lists the possible allow-ip-option values. 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.

Table 8: IP Option Values

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

Examples: Configuring Stateful Firewall Properties

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 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 12.2.3.2;
      applications http;
    }
    then {
      accept;
    }
  }
}

```

For additional examples that combine stateful firewall configuration with other services and with VPN routing and forwarding (VRF) tables, see “Examples: Services Interfaces Configuration” on page 31.