

Configuring Stateful Firewall Actions

You can configure stateful firewall actions for JUNOS ASP policy rules. Stateful firewall actions specify the action to take on packets that match the classify-traffic condition.

The type of action that you can create depends on the type of policy rule. See Policy Information Model.

Use the following configuration statements to configure stateful firewall actions:

```
policies group name list name rule name stateful-firewall name {  
    description description ;  
}  
policies group name list name rule name stateful-firewall name packet-action  
    reject {  
        message-type message-type ;  
    }  
policies group name list name rule name stateful-firewall name packet-action  
    parameter {  
        action action ;  
    }
```

To configure a stateful firewall action:

1. From configuration mode, enter the stateful firewall action configuration. For example, in this procedure, sfa is the name of the stateful firewall action.

```
user@host# edit policies group junos list sfw rule pr stateful-firewall sfa
```

2. (Optional) Set the action to take on a packet to one of the following:

- Filter.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]  
user@host# set packet-action filter
```

- Forward.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]  
user@host# set packet-action forward
```

- Reject. If you set the action to reject, configure the type of ICMP destination unreachable message sent to the client.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]  
user@host# set packet-action reject message-type message-type
```

- Parameter. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]  
user@host# set packet-action parameter action action
```

3. (Optional) Enter a description for the stateful firewall action.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]
```

```
user@host# set description description
```

4. (Optional) Verify the stateful firewall action configuration.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]  
user@host# show  
packet-action {  
    reject {  
        message-type administratively-prohibited;  
    }  
}  
description "Stateful firewall action";
```