

Configuring Policers to Control Traffic Rates (CLI Procedure)

You can configure policers to rate limit traffic on EX Series switches. After you configure a policer, you can include it in an ingress firewall filter configuration.

When you configure a firewall filter, you can specify a policer action for any term or terms within the filter. All traffic that matches a term that contains a policer action goes through the policer that the term references. Each policer that you configure includes an implicit counter. To get term-specific packet counts, you must configure a new policer for each filter term that requires policing.

The following policer limits apply on the switch:

- A maximum of 512 policers can be configured for port firewall filters.
- A maximum of 512 policers can be configured for VLAN and Layer 3 firewall filters.

If the policer configuration exceeds these limits, the switch returns the following message after the commit operation:

Cannot assign policers: Max policer limit reached

1. Configuring Policers on page 1
2. Specifying Policers in a Firewall Filter Configuration on page 2
3. Applying a Firewall Filter That Is Configured with a Policer on page 2

Configuring Policers

To configure a policer:

1. Specify the name of the policer:

```
[edit firewall]  
user@switch# set policer policer-one
```

The policer name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long.

2. Configure rate limiting for the policer:
 - a. Specify the bandwidth limit in bits per second (bps) to control the traffic rate on an interface:

```
[edit firewall policer policer-one]  
user@switch# set if-exceeding bandwidth-limit 300k
```

The range for the bandwidth limit is 1k through 102.3g bps.

- b. Specify the maximum allowed burst size to control the amount of traffic bursting:

```
[edit firewall policer policer-one]
user@switch# set if-exceeding burst-size-limit 500k
```

To determine the value for the burst-size limit, multiply the bandwidth of the interface on which the filter is applied by the amount of time to allow a burst of traffic at that bandwidth to occur:

burst size = bandwidth * allowable time for burst traffic

The range for the burst-size limit is 1 through 2,147,450,880 bytes.

3. Specify the policer action `discard` to discard packets that exceed the rate limits:

```
[edit firewall policer]
user@switch# set policer-one then discard
```

Discard is the only supported policer action.

Specifying Policers in a Firewall Filter Configuration

To reference a policer, configure a filter term that includes the policer action:

```
[edit firewall family ethernet-switching]
user@switch# set filter limit-hosts term term-one from source-address 192.0.2.16/28
userswitch# set filter limit-hosts term term-one then policer policer-one
```

Applying a Firewall Filter That Is Configured with a Policer

A firewall filter that is configured with one or more policer actions, like any other filter, must be applied to a port, VLAN, or Layer 3 interface. For information about applying firewall filters, see the sections on applying firewall filters in *Configuring Firewall Filters (CLI Procedure)*.



NOTE: You can include policer actions on ingress firewall filters only.

- Related Topics**
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches
 - Configuring Firewall Filters (CLI Procedure)
 - Configuring Firewall Filters (J-Web Procedure)

- Verifying That Policers Are Operational
- Understanding the Use of Policers in Firewall Filters

Published: 2009-07-28