JUNIPER NETWORKS

Junos® OS

DDoS Protection Configuration Guide

Release
13.1

Published: 2013-02-12

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

Junos® OS DDoS Protection Configuration Guide
Release 13.1

Revision History
February 2013—R1 Junos OS 13.1

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.

Abbreviated Table of Contents

Table of Contents

Part 4 Indexes

List of Figures

PART 1

Distributed Denial-of-Service (DDoS) Protection

CHAPTER 1

DDoS Overview

Distributed Denial-of-Service (DDoS) Protection Overview

A denial-of-service attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Distributed denial-of-service attacks involve an attack from multiple sources, enabling a much greater amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions to the router's control plane. This results in an excessive processing load that disrupts normal network operations.

Junos OS DDoS protection enables the router to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. A single point of DDoS protection management enables network administrators to customize profiles for their network control traffic. Protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases.

To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the router, Routing Engine, and line cards. You can also control logging of policer events.

The policers at the MPC or FPC5 are the first line of protection. Control traffic is dropped when it exceeds any configured policer values or, for unconfigured policers, the default policer values. Each violation generates a notification to alert operators about a possible attack. The violation is counted, the time that the violation starts is noted, and the time of the last observed violation is noted. When the traffic rate drops below the bandwidth violation threshold, a recovery timer determines when the traffic flow is consider to have returned to normal. If no further violation occurs before the timer expires, the violation state is cleared and a notification is generated.

Policer states and statistics from each line card are relayed to the Routing Engine and aggregated. The policer states are maintained during a switchover. Although line card statistics and violation counts are preserved during a switchover, Routing Engine policer statistics are not.

NOTE: DDoS protection is supported only on MX Series routers that have only MPCs installed and T4000 routers that have only FPC5s installed. If the router has other line cards in addition to MPCs or FPC5s, respectively, the CLI accepts the configuration but the other line cards are not protected and so the router is not protected.

Policer Types and Packet Priorities

DDoS protection includes two types of policers:

- An *aggregate policer* is applied to the complete set of packet types that belong to a protocol group. For example, you can configure an aggregate policer that applies to all PPPoE control packet types or to all DHCPv4 control packet types. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for aggregate policers. An aggregate policer is available for all protocol groups. Aggregate policers are supported by all protocol groups.
- An *individual policer*, also referred to as a *packet-type policer*, is allocated for each control packet type within a protocol group. For example, you can configure a policer for one or more types of PPPoE control packets. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for packet-type policers. Individual policers are not available for all protocol groups. See protocols for a list of protocol groups that have individual policers.

A control packet is policed first by its individual policer (if supported) and then by its aggregate policer. A packet dropped by the individual policer never reaches the aggregate policer. A packet that passes the individual policer can subsequently be dropped by the aggregate policer.

Each packet type within a protocol group has a default, configurable priority: low, medium, or high. Each control packet competes with other packets for the bandwidth within the limit imposed by its aggregate policer based on the priority configured for each packet type in the protocol group.

The priority mechanism is absolute. High-priority traffic gets bandwidth in preference to medium- and low-priority traffic. Medium-priority traffic gets bandwidth in preference to low-priority traffic. Low-priority traffic can use only the bandwidth left by high- and medium-priority traffic. If higher-priority traffic takes all of the bandwidth, then all the lower-priority traffic is dropped.

Example of Policer Priority Behavior

For example, consider how you might configure packet types within the PPPoE protocol group. Ignoring other PPPoE packet types for this example, suppose you configure individual policers for PADI and PADT packets, as well as a PPPoE aggregate policer for all those packets. PADT packets are more important than PADI packets, because PADT packets enable the PPPoE application to release resources to accept new connections. Therefore, you might assign high priority to the PADT packets and low priority to the PADI packets.

The aggregate policer imposes a total bandwidth limit for the protocol group. PADT packets passed by their individual policer have access to that bandwidth before PADI packets passed by their individual policer, because the PADT packets have a higher priority. If so many PADT packets are passed that they use all the available bandwidth, then all the PADI packets are dropped, because there is no bandwidth remaining at the aggregate policer.

Policer Hierarchy

DDoS policers are organized to match the hierarchical flow of protocol control traffic. Control traffic arriving from all ports of a line card converges on the card's Packet Forwarding Engine. Control traffic from all line cards on the router converges on the Routing Engine. Similarly, the DDoS policers are placed hierarchically along the control paths so that excess packets are dropped as early as possible on the path. This design preserves system resources by removing excess, malicious traffic so that the Routing Engine receives only the amount of traffic that it can process. To implement this design, five DDoS policers are present: One at the chipset, two at the line card, and two at the Routing Engine. Figure 1 on page 5 shows the policer process for PPPoE traffic. Figure 2 on page 6 shows the policer process for DHCPv4 traffic. (The same process applies to DHCPv6 traffic.)

Figure 1: Policer Hierarchy for PPPoE Packets

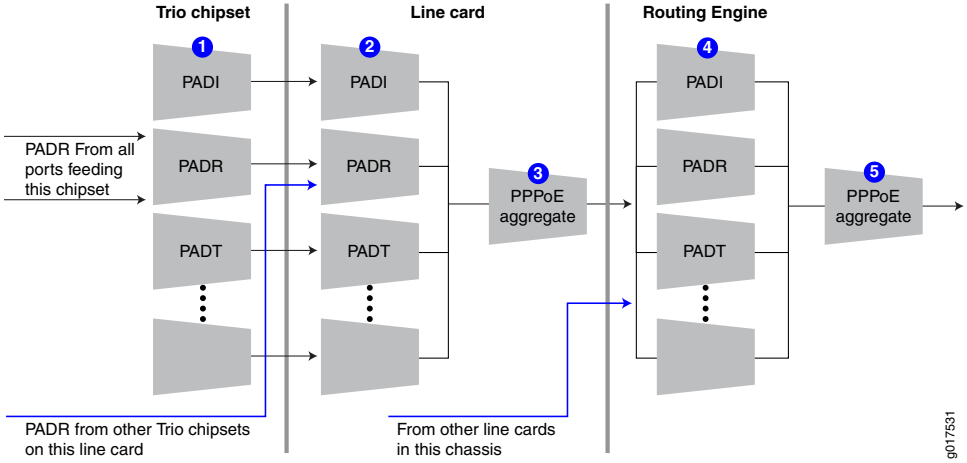
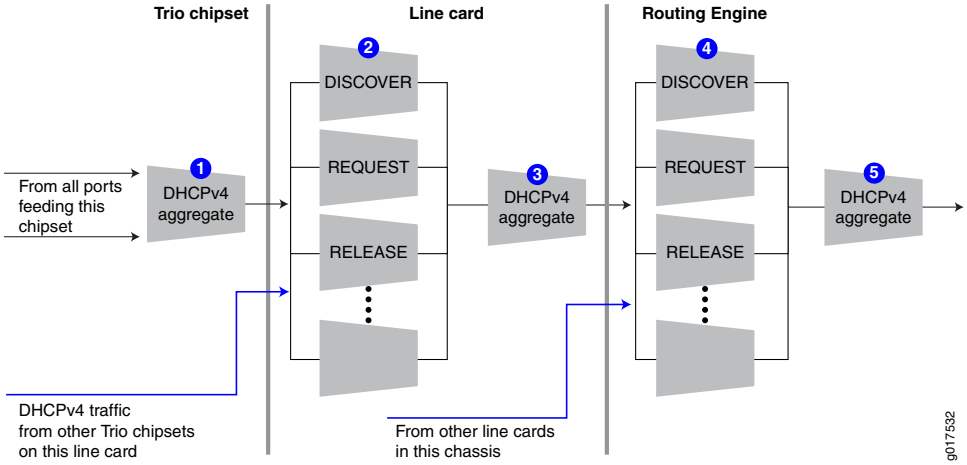


Figure 2: Policer Hierarchy for DHCPv4 Packets



Control packets arrive at the chipset on the MPC or FPC5 for processing and forwarding. The first policer (1) is either an individual policer (Figure 1 on page 5) or an aggregate policer (Figure 2 on page 6).

- The first policer is an individual policer for protocol groups that support individual policers, with two exceptions. For DHCPv4 and DHCPv6 traffic, the first policer is an aggregate policer.
- The first policer is an aggregate policer for protocol groups that support only aggregate policers.

Traffic that passes the first policer is monitored by one or both of the line card policers. If the card has more than one chipset, traffic from all chipsets converges on the line card policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the line card individual policer (2) and then the line card aggregate policer (3). Traffic that passes the individual policer can be dropped by the aggregate policer. Although DHCPv4 and DHCPv6 traffic was monitored by an aggregate policer at the chipset, at the line card it is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the line card aggregate policer monitors the traffic.

Traffic that passes the line card policers is monitored by one or both of the Routing Engine policers. Traffic from all MPCs or FPC5s converges on the Routing Engine policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the Routing Engine individual policer (4) and then the Routing Engine aggregate policer (5). Traffic that passes the individual policer can be dropped by the aggregate policer. As it was at the line card level, DHCPv4 and DHCPv6 traffic at the Routing Engine is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the aggregate policer monitors the traffic.

The result of this design is that traffic for protocol groups that support only aggregate policers is evaluated by three policers. Among other groups, this includes ANCP, dynamic VLAN, FTP, and IGMP traffic. Traffic for protocol groups that support both aggregate and individual policers is evaluated by all five policers. Among other groups, this includes DHCPv4, MLP, PPP, PPPoE, and virtual chassis traffic.

Figure 1 on page 5 shows how DDoS protection polices PPPoE control packets:

1. PADR packets, for example, are evaluated at the first policer on the chipset to determine whether they are within the bandwidth limits. PADR packets that exceed the limit are dropped.
2. All PADR packets that pass the policer on all chipsets on the MPC or FPC5 are next evaluated by the line card individual policer. PADR packets that exceed the limit are dropped.
3. All PADR packets that pass the line card individual policer proceed to the line card aggregate policer. PADR packets that exceed the limit are dropped.
4. All PADR packets that are passed by the line card aggregate policers on all MPCs or FPC5s on the router proceed to the Routing Engine individual policer. PADR packets that exceed the limit are dropped.
5. Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic.

By default, all three individual policers (chipset, line card, and Routing Engine) have the same bandwidth limit for a given packet type. This design enables all the control traffic from a chipset and line card to reach the Routing engine, as long as there is no competing traffic of the same type from other chipsets or line cards. When competing traffic is present, excess packets are dropped at the convergence points. That is, they are dropped at the line card for all competing chipsets and at the Routing Engine for all competing line cards.

Example of Policer Bandwidth Limit Behavior

For example, suppose you set the policer bandwidth for PADI packets to 1000 packets per second. This value applies to the individual PADI policers at the chipset, the line card, and the Routing Engine. If only the card in slot 5 is receiving PADI packets, then up to 1000 PADI pps can reach the Routing Engine (if the PPPoE aggregate policer is not exceeded). However, suppose the card in slot 9 is also receiving PADI packets at 1000 pps and that its PPPoE aggregate policer is not exceeded. The traffic passes the individual and aggregate policers at both line cards and proceeds to the Routing Engine. At the Routing Engine, the combined bandwidth is 2000 pps. Because the PADI policer at the Routing Engine allows only 1000 PADI pps to pass, it drops the excess 1000 packets. It continues to drop the excess packets for as long as the bandwidth is exceeded.

You can apply a scaling factor for both the bandwidth limit and the burst limit at the line card. This enables you to fine-tune the traffic limits for each slot. For example, suppose the individual policer sets the PADI packet bandwidth to 1000 pps and the burst size to 50,000 packets. You can reduce the traffic limit for PADI packets on any line card by

specifying the slot number and scaling factor. A bandwidth scaling factor of 20 for slot 5 reduces the traffic in this example to 20 percent of 1000 pps, or 200 pps for the line card in that slot. Similarly, a burst scaling factor of 50 for that slot reduces the burst size by 50 percent to 25,000 packets. By default, scaling factors are set to 100 so traffic can pass through at 100 percent of the rate limit.

Related Documentation

- Configuring Protection Against DDoS Attacks on page 9
- DDoS Protection Flow Detection Overview on page 31

CHAPTER 2

Configuring DDoS Protection

Configuring Protection Against DDoS Attacks

DDoS protection is enabled by default for all supported protocol groups and packet types. Default values are present for bandwidth, bandwidth scale, burst, burst scale, priority, and recover time. You can change the DDoS configuration for individual packet types within a protocol group or for the aggregate policer for the protocol group. DDoS logging is enabled by default, but you can disable it globally for all DDoS events or for individual packet types within a protocol group. You can also fine-tune monitoring of DDoS events by configuring tracing operations.

You can disable DDoS protection at the Routing Engine and for all line cards either globally or for individual packet types within a protocol group.

NOTE: DDoS protection is supported only on MX Series routers that have only MPCs installed and T4000 routers that have only FPC5s installed. If the router has other line cards in addition to MPCs or FPC5s, respectively, the CLI accepts the configuration but the other line cards are not protected and so the router is not protected.

To configure DDoS protection:

1. (Optional) Configure global DDoS settings.

   See "Disabling DDoS Protection Policers and Logging Globally" on page 10.

2. (Optional) Configure DDoS settings for individual packet types.

   See "Configuring DDoS Protection Policers for Individual Packet Types" on page 11.

3. (Optional) Configure tracing for DDoS operations.

   See "Tracing DDoS Protection Operations" on page 14.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 3
- Example: Configuring DDoS Protection on page 19

Disabling DDoS Protection Policers and Logging Globally

DDoS policers are enabled by default for all supported protocol groups and packet types. Policers are established at the level of the individual line card and the Routing Engine. You can disable the line card policers globally for all MPCs or FPC5s. You can also disable the Routing Engine policer. When you disable either of these policers, the policers at that level for all protocol groups and packet types are disabled.

DDoS logging is also enabled by default. You can disable all DDoS event logging (including flow detection event logging) for all protocol groups and packet types across the router.

NOTE: The global configuration for disabling policers and logging overrides any local configuration for packet types.

To configure global DDoS settings:

1. (Optional) Disable line card policers.

   ```
   [edit system ddos-protection global]
   user@host# set disable-fpc
   ```

2. (Optional) Disable Routing Engine policers.

   ```
   [edit system ddos-protection global]
   user@host# set disable-routing-engine
   ```

3. (Optional) Disable event logging.

```
[edit system ddos-protection global]
user@host# set disable-logging
```

Related Documentation

- Configuring Protection Against DDoS Attacks on page 9

Configuring DDoS Protection Policers for Individual Packet Types

DDoS policers are applied to control packet traffic. You configure the maximum allowed traffic rate, maximum burst size, traffic priority, and how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack. You can also scale the bandwidth and burst values for individual line cards so that the policers at this level trigger at lower thresholds than the overall protocol or packet thresholds.

You can configure an aggregate policer for any protocol group. The aggregate policer applies to the combination of all types of control packet traffic for that group. When you configure an aggregate policer for certain protocol groups, you can optionally bypass that policer for one or more particular packet types in that group. For those same groups, you can configure policers for individual packet types instead of configuring an aggregate policer.

DDoS protection is enabled by default. Although all policers have default parameter values, these values might not accurately reflect the control traffic pattern of your network.

BEST PRACTICE: We recommend that you model your network to determine the best values for your situation. Before you configure policers for your network, you can quickly view the default values for all packet types from operational mode by issuing the **show ddos-protection protocols parameters brief** command. You can also use the command to specify a single protocol group of interest; for example, issue the **show ddos-protection protocols dhcpv4 parameters brief** command.

You can disable a packet type's policer at either the Routing Engine, at a specified line card, or for all line cards. You can also disable logging of all DDoS events for individual packet types within a protocol group.

To configure individual, packet-level DDoS settings:

1. Specify the protocol group.

   ```
   [edit system ddos-protection protocols]
   user@host# edit protocol-group
   ```

   For example, to specify the DHCPv4 protocol group:

   ```
   [edit system ddos-protection protocols]
   user@host# edit dhcpv4
   ```

2. Specify the packet type or the combination of all packet types in the group.

   ```
   [edit system ddos-protection protocols protocol-group]
   user@host# set packet-type
   ```

or

```
[edit system ddos-protection protocols protocol-group]
user@host# set aggregate
```

For example, to specify the DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4]
user@host# edit release
```

3. (Optional) Configure the maximum traffic rate the policer allows for the packet type.

   ```
   [edit system ddos-protection protocols protocol-group packet-type]
   user@host# set bandwidth packets-per-second
   ```

   For example, to set a bandwidth of 600 packets per second for DHCPv4 release packets:

   ```
   [edit system ddos-protection protocols dhcpv4 release]
   user@host# set bandwidth 600
   ```

4. (Optional) Configure the maximum number of packets of the packet type that the policer allows in a burst of traffic.

   ```
   [edit system ddos-protection protocols protocol-group packet-type]
   user@host# set burst size
   ```

   For example, to set a maximum of 5000 DHCPv4 release packets:

   ```
   [edit system ddos-protection protocols dhcpv4 release]
   user@host# set burst 5000
   ```

5. (Optional) Set the traffic priority.

   ```
   [edit system ddos-protection protocols protocol-group packet-type]
   user@host# set priority level
   ```

   For example, to specify a medium priority for DHCPv4 release packets:

   ```
   [edit system ddos-protection protocols dhcpv4 release]
   user@host# set priority medium
   ```

6. (Optional) Configure how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack.

   ```
   [edit system ddos-protection protocols protocol-group packet-type]
   user@host# set recover-time seconds
   ```

   For example, to specify that 600 seconds must have passed since the last violation of the DHCPv4 release packet policer:

   ```
   [edit system ddos-protection protocols dhcpv4 release]
   user@host# set recover-time 600
   ```

7. (Optional) Bypass the aggregate policer configuration. This is relevant only when an aggregate policer is configured for the protocol group.

   ```
   [edit system ddos-protection protocols protocol-group packet-type]
   user@host# set bypass-aggregate
   ```

   For example, to bypass the aggregate policer for DHCPv4 renew packets:

   ```
   [edit system ddos-protection protocols dhcpv4 renew]
   user@host# set bypass-aggregate
   ```

8. (Optional) Disable line card policers for the packet type on all line cards.

   [edit system ddos-protection protocols *protocol-group packet-type*]
   user@host# set disable-fpc

   NOTE: When you disable line card policers globally at the **[edit system ddos-protection global]** hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

   For example, to disable the line card policer for DHCPv4 bootp packets:

   [edit system ddos-protection protocols dhcpv4 bootp]
   user@host# set disable-fpc

9. (Optional) Disable DDoS event logging for only this packet type.

   [edit system ddos-protection protocols *protocol-group packet-type*]
   user@host# set disable-logging

   NOTE: Events disabled for the packet are associated with policer violations; logging of flow detection culprit flow events is not affected by this statement.

   NOTE: When you disable DDoS event logging globally at the **[edit system ddos-protection global]** hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

   For example, to disable DDoS event logging line card policer for DHCPv4 discover packets:

   [edit system ddos-protection protocols dhcpv4 discover]
   user@host# set disable-logging

10. (Optional) Disable the Routing Engine policer for only this packet type.

    [edit system ddos-protection protocols *protocol-group packet-type*]
    user@host# set disable-routing-engine

    NOTE: When you disable the Routing Engine policer globally at the **[edit system ddos-protection global]** hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

    For example, to disable the Routing Engine policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set disable-routing-engine
```

11. (Optional) Configure packet-level settings for the packet type on a single line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type]
    user@host# edit fpc slot-number
    ```

    For example, to access DHCPv4 discover packet settings on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover]
    user@host# edit fpc 3
    ```

12. (Optional) Scale the policer bandwidth for the packet type on the line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type fpc slot-number]
    user@host# set bandwidth-scale percentage
    ```

    For example, to scale the bandwidth to 80 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover fpc 3]
    user@host# edit bandwidth-scale 80
    ```

13. (Optional) Scale the policer burst size for the packet type on the line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type fpc slot-number]
    user@host# set burst-scale percentage
    ```

    For example, to scale the maximum bandwidth to 75 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover fpc 3]
    user@host# edit burst-scale 75
    ```

14. (Optional) Disable the line card policer for the packet type on a particular line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type fpc slot-number]
    user@host# set disable-fpc
    ```

    For example, to disable the line card policer for DHCPv4 discover packets on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover fpc 3]
    user@host# edit disable-fpc
    ```

Related Documentation

- Configuring Protection Against DDoS Attacks on page 9
- For a list of supported protocol groups and packet types, see protocols on page 68.
- Example: Configuring DDoS Protection on page 19

Tracing DDoS Protection Operations

The Junos OS trace feature tracks DDoS protection operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **ddosd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

   You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure all aspects of DDoS tracing operations:

1. (Optional) Configure a trace log filename.

   See "Configuring the DDoS Protection Trace Log Filename" on page 16.
2. (Optional) Configure the number and size of trace logs.

   See "Configuring the Number and Size of DDoS Protection Log Files" on page 16.
3. (Optional) Configure user access to trace logs.

   See "Configuring Access to the DDoS Protection Log File" on page 16.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.

   See "Configuring a Regular Expression for DDoS Protection Messages to Be Logged" on page 17.
5. (Optional) Configure flags to specify which events are logged.

   See "Configuring the DDoS Protection Tracing Flags" on page 17.
6. (Optional) Configure a severity level for messages to specify which event messages are logged.

   See "Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged" on page 18.

Related Documentation

- Example: Configuring DDoS Protection on page 19

Configuring the DDoS Protection Trace Log Filename

By default, the name of the file that records trace output for DDoS protection is **ddosd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_logfile_1
```

Related Documentation

- Tracing DDoS Protection Operations on page 14

Configuring the Number and Size of DDoS Protection Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 files 20 size 2097152
```

Related Documentation

- Tracing DDoS Protection Operations on page 14

Configuring Access to the DDoS Protection Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1 _logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1 _logfile_1 no-world-readable
```

Related Documentation

- Tracing DDoS Protection Operations on page 14

Configuring a Regular Expression for DDoS Protection Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1 _logfile_1 match regex
```

Related Documentation

- Tracing DDoS Protection Operations on page 14

Configuring the DDoS Protection Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system ddos-protection traceoptions]
user@host# set flag flag
```

Related Documentation

- Tracing DDoS Protection Operations on page 14

Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages . By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

  [edit system ddos-protection traceoptions]
  user@host# **set level** ***severity***

Related Documentation

- Tracing DDoS Protection Operations on page 14

Verifying and Managing DDoS Protection

Purpose View or clear information about DDoS configurations, states, and statistics.

Action

- To display the DDoS policer configuration, violation state, and statistics for all packet types in all protocol groups:

  user@host> **show ddos-protection protocols**

  If you issue the command before you make any configuration changes, the default policer values are displayed.

- To display the DDoS policer configuration, violation state, and statistics for a particular packet type in a particular protocol group:

  user@host> **show ddos-protection protocols** ***protocol-group packet-type***

- To display only the number of DDoS policer violations for all protocol groups:

  user@host> **show ddos-protection protocols violations**

- To display a table of the DDoS configuration for all packet types in all protocol groups:

  user@host> **show ddos-protection protocols parameters brief**

- To display a complete list of packet statistics and DDoS violation statistics for all packet types in all protocol groups:

  user@host> **show ddos-protection protocols statistics detail**

- To display global DDoS violation statistics:

  user@host> **show ddos-protection statistics**

- To display the DDoS version number:

  user@host> **show ddos-protection version**

- To clear DDoS statistics for all packet types in all protocol groups:

  user@host> **clear ddos-protection protocols statistics**

- To clear DDoS statistics for all packet types in a particular protocol group:

  user@host> **clear ddos-protection protocols *protocol-group* statistics**

- To clear DDoS statistics for a particular packet type in a particular protocol group:

  user@host> **clear ddos-protection protocols *protocol-group* statistics*packet-type***

- To clear DDoS violation states for all packet types in all protocol groups:

  user@host> **clear ddos-protection protocols states**

- To clear DDoS violation states for all packet types in a particular protocol group:

  user@host> **clear ddos-protection protocols *protocol-group* states**

- To clear DDoS violation states for a particular packet type in a particular protocol group:

  user@host> **clear ddos-protection protocols *protocol-group* states*packet-type***

Related Documentation

- Verifying and Managing Flow Detection on page 44
- Junos OS Operational Mode Commands

Example: Configuring DDoS Protection

This example shows how to configure DDoS protection that enables the router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.

Requirements

DDoS protection requires the following hardware and software:

- MX Series 3D Universal Edge Routers that have only MPCs installed or T4000 Core Routers that have only FPC5s installed.

  NOTE: If the router has other cards in addition to MPCs or FPC5s, the CLI accepts the configuration but the other cards are not protected and therefore the router is not protected.

- Junos OS Release 11.2 or later

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Distributed denial-of-service attacks use multiple sources to flood a network or router with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and attempts exhaust the system resources to deny valid users access to the network or server.

This example describes how to configure rate-limiting policers that identify excess control traffic and drop the packets before the router is adversely affected. Sample tasks include configuring policers for particular control packet types within a protocol group, configuring an aggregate policer for a protocol group and bypassing that policer for a particular control packet type, and specifying trace options for DDoS operations.

This example does not show all possible configuration choices.

Configuration

CLI Quick Configuration

To quickly configure DDoS protection for protocol groups and particular control packet types, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit system
set ddos-protection protocols dhcpv4 aggregate bandwidth 669
set ddos-protection protocols dhcpv4 aggregate burst 6000
set ddos-protection protocols dhcpv4 discover bandwidth 100
set ddos-protection protocols dhcpv4 discover recover-time 200
set ddos-protection protocols dhcpv4 discover burst 300
set ddos-protection protocols dhcpv4 offer priority medium
set ddos-protection protocols dhcpv4 offer bypass-aggregate
set ddos-protection protocols dhcpv4 offer fpc 1 bandwidth-scale 80
set ddos-protection protocols dhcpv4 offer fpc 1 burst-scale 75
set ddos-protection protocols pppoe aggregate bandwidth 800
set ddos-protection traceoptions file ddos-trace size 10m
set ddos-protection traceoptions flag all
top
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure DDoS protection:

1. Specify a protocol group.

   ```
   [edit system ddos-protection protocols]
   user@host# edit dhcpv4
   ```

2. Configure the maximum traffic rate for the DHCPv4 aggregate policer; that is, for the combination of all DHCPv4 packets.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set aggregate bandwidth 669
   ```

3. Configure the maximum burst rate for the DHCPv4 aggregate policer.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set aggregate burst 6000
```

4. Configure the maximum traffic rate for the DHCPv4 policer for discover packets.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set discover bandwidth 100
```

5. Decrease the recover time for violations of the DHCPv4 discover policer.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set discover recover-time 200
```

6. Configure the maximum burst rate for the DHCPv4 discover policer.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set discover burst 300
```

7. Increase the priority for DHCPv4 offer packets.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set offer priority medium
```

8. Prevent offer packets from being included in the aggregate bandwidth; that is, offer packets do not contribute towards the combined DHCPv4 traffic to determine whether the aggregate bandwidth is exceeded. However, the offer packets are still included in traffic rate statistics.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set offer bypass-aggregate
```

9. Reduce the bandwidth and burst size allowed before violation is declared for the DHCPv4 offer policer on the MPC or FPC5 in slot 1.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set offer fpc 1 bandwidth-scale 80
user@host# set offer fpc 1 burst-scale 75
```

10. Configure the maximum traffic rate for the PPPoE aggregate policer, that is, for the combination of all PPPoE packets.

```
[edit system ddos-protection protocols dhcpv4]
user@host# up
[edit system ddos-protection protocols]
user@host# set pppoe aggregate bandwidth 800
```

11. Configure tracing for all DDoS protocol processing events.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos-log
user@host# set file size 10m
user@host# set flag all
```

Results From configuration mode, confirm your configuration by entering the **show ddos-protection** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit system]
user@host# show ddos-protection
```

```
traceoptions {
  file ddos-trace size 10m;
  flag all;
}
  protocols {
    pppoe {
      aggregate {
        bandwidth 800;
      }
    }
    dhcpv4 {
      aggregate {
        bandwidth 669;
        burst 6000;
      }
      discover {
        bandwidth 100;
        burst 300;
        recover-time 200;
      }
      offer {
        priority medium;
        fpc 1 {
          bandwidth-scale 80;
          burst-scale 75;
        }
        bypass-aggregate;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the DDoS protection configuration is working properly, perform these tasks:

- Verifying the DHCPv4 DDoS Protection Configuration and Operation on page 22
- Verifying the PPPoE DDoS Configuration on page 25

Verifying the DHCPv4 DDoS Protection Configuration and Operation

Purpose Verify that the DHCPv4 aggregate and protocol policer values have changed from the default. With DHCPv4 and PPPoE traffic flowing, verify that the policers are working correctly. You can enter commands to display the individual policers you are interested in, as shown here, or you can enter the **show ddos-protection protocols dhcpv4** command to display this information for all DHCPv4 packet types.

Action From operational mode, enter the **show ddos-protection protocols dhcpv4 aggregate** command.

```
user@host> show ddos-protection protocols dhcpv4 aggregate
```

```
Protocol Group: DHCPv4

  Packet type: aggregate (aggregate for all DHCPv4 traffic)
    Aggregate policer configuration:
      Bandwidth:        669 pps
      Burst:            6000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
    System-wide information:
      Aggregate bandwidth is no longer being violated
        No. of FPCs currently receiving excess traffic: 0
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-03-10 06:27:47 PST
        Violation last seen at:      2011-03-10 06:28:57 PST
        Duration of violation: 00:01:10 Number of violations: 1
      Received:  71064              Arrival rate:     0 pps
      Dropped:   23115              Max arrival rate: 1000 pps
    Routing Engine information:
      Bandwidth: 669 pps, Burst: 6000 packets, enabled
      Aggregate policer is never violated
      Received:  36130              Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 671 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled
      Aggregate policer is no longer being violated
        Violation first detected at: 2011-03-10 06:27:48 PST
        Violation last seen at:      2011-03-10 06:28:58 PST
        Duration of violation: 00:01:10 Number of violations: 1
      Received:  71064              Arrival rate:     0 pps
      Dropped:   34934              Max arrival rate: 1000 pps
        Dropped by individual policers: 11819
        Dropped by aggregate policer: 23115
```

From operational mode, enter the **show ddos-protection protocols dhcpv4 discover** command.

```
user@host> show ddos-protection protocols dhcpv4 discover
Protocol Group: DHCPv4

  Packet type: discover (DHCPv4 DHCPDISCOVER)
    Individual policer configuration:
      Bandwidth:        100 pps
      Burst:            300 packets
      Priority:         low
      Recover time:     200 seconds
      Enabled:          Yes
      Bypass aggregate: No
    System-wide information:
      Bandwidth is no longer being violated
        No. of FPCs currently receiving excess traffic: 0
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-03-10 06:28:34 PST
        Violation last seen at:      2011-03-10 06:28:55 PST
        Duration of violation: 00:00:21 Number of violations: 1
      Received:  47949              Arrival rate:     0 pps
      Dropped:   11819              Max arrival rate: 671 pps
    Routing Engine information:
      Bandwidth: 100 pps, Burst: 300 packets, enabled
      Policer is never violated
```

```
    Received:  36130              Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Bandwidth: 100% (100 pps), Burst: 100% (300 packets), enabled
    Policer is no longer being violated
      Violation first detected at: 2011-03-10 06:28:35 PST
      Violation last seen at:      2011-03-10 06:28:55 PST
      Duration of violation: 00:00:20 Number of violations: 1
    Received:  47949              Arrival rate:     0 pps
    Dropped:   11819              Max arrival rate: 671 pps
      Dropped by this policer: 11819
      Dropped by aggregate policer: 0
```

From operational mode, enter the **show ddos-protection protocols dhcpv4 offer** command.

```
user@host> show ddos-protection protocols dhcpv4 offer
Protocol Group: DHCPv4

  Packet type: offer (DHCPv4 DHCPOFFER)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: Yes
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 80% (800 pps), Burst: 75% (750 packets), enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
```

Meaning The output of these commands lists the policer configuration and traffic statistics for the DHCPv4 aggregate, discover, and offer policers respectively.

The **Aggregate policer configuration** section in the first output example and **Individual policer configuration** sections in the second and third output examples list the configured values for bandwidth, burst, priority, recover time, and bypass-aggregate.

The **System-wide information** section shows the total of all DHCPv4 traffic statistics and violations for the policer recorded across all line cards and at the Routing Engine. The **Routing engine information** section shows the traffic statistics and violations for the policer recorded at the Routing Engine. The **FPC slot 1 information** section shows the traffic statistics and violations for the policer recorded only at the line card in slot 1.

The output for the aggregate policer in this example shows the following information:

- The **System-wide information** section shows that 71,064 DHCPv4 packets of all types were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 23,115 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 71,064 DHCPv4 packets, but its aggregate policer experienced a violation and dropped the 23,115 packets shown in the other section. The line card individual policers dropped an additional 11,819 packets.
- The **Routing Engine information** section shows that the remaining 36,130 packets all reached the Routing Engine and that its aggregate policer dropped no additional packets.

  The difference between the number of DHCPv4 packets received and dropped at the line card [71,064 - (23,115 + 11,819)] matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1received any DHCPv4 packets.

The output for the DHCPv4 discover packet policer in this example shows the following information:

- The **System-wide information** section shows that 47,949 DHCPv4 discover packets were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 11,819 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 47,949 DHCPv4 discover packets, but its individual policer experienced a violation and dropped the 11,819 packets shown in the other section.
- The **Routing Engine information** section shows that only 36,130 DHCPv4 discover packets reached the Routing Engine and that it dropped no additional packets.

  The difference between the number of DHCPv4 discover packets received and dropped at the line card (47,949 - 11,819) matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1received any DHCPv4 discover packets.

The output for the DHCPv4 offer packet policer in this example shows the following information:

- This individual policer has never been violated at any location.
- No DHCPv4 offer packets have been received at any location.

Verifying the PPPoE DDoS Configuration

Purpose Verify that the PPPoE policer values have changed from the default.

Action From operational mode, enter the **show ddos-protection protocols pppoe parameters brief** command.

```
user@host> show ddos-protection protocols pppoe parameters brief
Number of policers modified: 1
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
pppoe       aggregate   800*      2000   medium   300       yes     --     no
pppoe       padi        500       500    low      300       yes     no     no
pppoe       pado        0         0      low      300       yes     no     no
pppoe       padr        500       500    medium   300       yes     no     no
pppoe       pads        0         0      low      300       yes     no     no
pppoe       padt        1000      1000   high     300       yes     no     no
pppoe       padm        0         0      low      300       yes     no     no
pppoe       padn        0         0      low      300       yes     no     no
```

From operational mode, enter the **show ddos-protection protocols pppoe padi** command, and enter the command for **padr** as well.

```
user@host> show ddos-protection protocols pppoe padi
Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    System-wide information:
      Bandwidth for this packet type is being violated!
        Number of slots currently receiving excess traffic: 1
        Number of slots that have received excess traffic:  1
        Violation first detected at: 2011-03-09 11:26:33 PST
        Violation last seen at:      2011-03-10 12:03:44 PST
        Duration of violation: 1d 00:37 Number of violations: 1
      Received:  704832908           Arrival rate:     8000 pps
      Dropped:   660788548           Max arrival rate: 8008 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  39950330            Arrival rate:     298 pps
      Dropped:   0                   Max arrival rate: 503 pps
        Dropped by aggregate policer: 0
    FPC slot 3 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Policer is currently being violated!
        Violation first detected at: 2011-03-09 11:26:35 PST
        Violation last seen at:      2011-03-10 12:03:44 PST
        Duration of violation: 1d 00:37 Number of violations: 1
      Received:  704832908           Arrival rate:     8000 pps
      Dropped:   664882578           Max arrival rate: 8008 pps
        Dropped by this policer: 660788548
        Dropped by aggregate policer: 4094030

user@host> show ddos-protection protocols pppoe padr
Protocol Group: PPPoE

  Packet type: padr (PPPoE PADR)
    Individual policer configuration:
```



```
  Bandwidth:        500 pps
  Burst:            500 packets
  Priority:         medium
  Recover time:     300 seconds
  Enabled:          Yes
  Bypass aggregate: No
System-wide information:
  Bandwidth for this packet type is being violated!
    Number of slots currently receiving excess traffic: 1
    Number of slots that have received excess traffic:  1
    Violation first detected at: 2011-03-10 06:21:17 PST
    Violation last seen at:      2011-03-10 12:04:14 PST
    Duration of violation: 05:42:57 Number of violations: 1
  Received:  494663595           Arrival rate:     24038 pps
  Dropped:   484375900           Max arrival rate: 24062 pps
Routing Engine information:
  Bandwidth: 500 pps, Burst: 500 packets, enabled
  Policer is never violated
  Received:  10287695            Arrival rate:     500 pps
  Dropped:   0                   Max arrival rate: 502 pps
    Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
  Policer is currently being violated!
    Violation first detected at: 2011-03-10 06:21:18 PST
    Violation last seen at:      2011-03-10 12:04:14 PST
    Duration of violation: 05:42:56 Number of violations: 1
  Received:  494663595           Arrival rate:     24038 pps
  Dropped:   484375900           Max arrival rate: 24062 pps
    Dropped by this policer: 484375900
    Dropped by aggregate policer: 0
```

Meaning The output from the **show ddos-protection protocols pppoe parameters brief** command lists the current configuration for each of the individual PPPoE packet policers and the PPPoE aggregate policer. A change from a default value is indicated by an asterisk next to the modified value. The only change made to PPPoE policers in the configuration steps was to the aggregate policer bandwidth; this change is confirmed in the output. Besides the configuration values, the command output also reports whether a policer has been disabled, whether it bypasses the aggregate policer (meaning that the traffic for that packet type is not included for evaluation by the aggregate policer), and whether the policer has been modified for one or more line cards.

The output of the **show ddos-protection protocols pppoe padi** command in this example shows the following information:

- The **System-wide information** section shows that 704,832,908 PPPoE PADI packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the aggregate policer at the line card dropped 660,788,548 of the PADI packets.
- The **FPC slot 3 information** section shows that this line card received all 704,832,908 PADI packets. Its individual policer dropped 660,788,548 of those packets and its aggregate policer dropped the other 4,094,030 packets. The violation is ongoing and has lasted more than a day.
- The **Routing Engine information** section shows that only 39,950,330 PADI packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of PADI packets received and dropped at the line card [704,832,908 - (660,788,548 + 4,094030)] matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 3 received any PADI packets.

The output of the **show ddos-protection protocols pppoe padr** command in this example shows the following information:

- The **System-wide information** section shows that 494,663,595 PPPoE PADR packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the policer at the line card dropped 484,375,900 of the PADR packets.
- The **FPC slot 1 information** section shows that this line card received all 494,663,595 PADR packets. Its individual policer dropped 484,375,900 of those packets. The violation is ongoing and has lasted more than five hours.
- The **Routing Engine information** section shows that only 10,287,695 PADR packets reached the Routing Engine and that it dropped no additional packets.

  The difference between the number of PADR packets received and dropped at the line card (494,663,595 - 484,375,900) matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any PADR packets.

NOTE: This scenario is unrealistic in showing all PADI packets received on one line card and all PADR packets on a different line card. The intent of the scenario is to illustrate how policer violations are reported for individual line cards.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 3
- Configuring Protection Against DDoS Attacks on page 9

PART 2

Flow Detection

CHAPTER 3

Flow Detection Overview

DDoS Protection Flow Detection Overview

Flow detection is an enhancement to DDoS protection that supplements the DDoS policer hierarchies; it is part of a complete DDOS protection solution. Flow detection uses a limited amount of hardware resources to monitor the arrival rate of host-bound flows of control traffic. Flow detection is much more scalable than a solution based on filter policers. Filter policers track all flows, which consumes a considerable amount of resources. In contrast, flow detection only tracks flows it identifies as suspicious, using far fewer resources to do so.

The flow detection application has two interrelated components, detection and tracking. Detection is the process where flows suspected of being improper are identified and subsequently controlled. Tracking is the process where flows are tracked to determine whether they are truly hostile and when these flows recover to within acceptable limits.

Flow Detection and Control

Flow detection is disabled by default. When you enable it at the **[edit system ddos-protection global]** hierarchy level, the application begins monitoring control traffic flows when a DDoS protection policer is violated for all protocol groups and packet types. Other than event report rates, all other characteristics of flow detection are configurable only at the level of individual packet types.

Control flows are aggregated at three levels. The *subscriber level* is the finest grained of the three and consists of flows for individual subscriber sessions. The *logical interface level* aggregates multiple subscriber flows, so it is coarser grained and does not provide discrimination into individual subscriber flows. The *physical interface level* aggregates multiple logical interface flows, so it provides the coarsest view of traffic flows.

You can turn flow detection off or on at any of these levels. You can also configure whether it is automatically triggered by the violation of a DDoS protection policer or is always on—meaning that it always monitors flows, even when no policer is being violated. Flow

detection begins at the finest-grained level that has detection configured to **on** or **automatic**.

When a flow arrives, flow detection checks whether the flow is already listed in a table of *suspicious* flows. A suspicious flow is one that exceeds the bandwidth allowed by default or configuration. If the flow is not in the table and the aggregation level flow detection mode is **on**, then flow detection lists the flow in the table. If the flow is not in the table and the flow detection mode is **automatic**, flow detection checks whether this flow is suspicious.

If the flow is suspicious, then it goes in the flow table. If the flow is not suspicious, then it is processed the same way at the next coarser aggregation level that has flow detection set to **on**. If none of the higher levels have detection on, then the flow continues to the DDoS protection packet policer for action, where it can be passed or dropped.

When the initial check finds the flow in the table, then the flow is dropped, policed, or kept, depending on the control mode setting for that aggregation level. All packets in dropped flows are dropped. In policed flows, packets are dropped until the flow is within the acceptable bandwidth for the aggregation level. Kept flows are passed along to the next aggregation level for processing.

Flow Tracking

The flow detection application tracks flows that have been listed in the suspicious flow table. It periodically checks each entry in the table to determine whether the listed flow is still suspicious (violating the bandwidth). If a suspicious flow has continuously violated the bandwidth since it was inserted in the table for a period greater than the configurable flow detection period, then it is considered to be a *culprit* flow rather than merely suspicious. However, if the bandwidth has been violated for less than the detection period, the violation is treated as a false positive. Flow detection considers the flow to be safe and stops tracking it (deletes it from the table).

You can enable a timeout feature that suppresses culprit flows for a configurable timeout period, during which the flow is kept in the flow table. (Suppression is the default behavior, but the flow detection action can be changed by the flow level control configuration.) If the check of listed flows finds one for which the timeout is enabled and the timeout period has expired, then the flow has timed out and it is removed from the flow table.

If the timeout has not yet expired or if the timeout feature is not enabled, then the application performs a recovery check. If the time since the flow last violated the bandwidth is longer than the configurable recovery period, the flow has recovered and is removed from the flow table. If the time since last violation is less than the recovery period, the flow is kept in the flow table.

Notifications

By default, flow detection automatically generates system logs for a variety of events that occur during flow detection. The logs are referred to as *reports* in the flow detection CLI. All protocol groups and packet types are covered by default, but you can disable automatic logging for individual packet types. You can also configure the rate at which reports are sent, but this applies globally to all packet types.

Each report belongs to one of the following two types:

- Flow reports—These reports are generated by events associated with the identification and tracking of culprit flows. Each report includes identifying information for the flow that experienced the event. This information is used to accurately maintain the flow table; flows are deleted or retained in the table based on the information in the report. Table 1 on page 33 describes the event that triggers each flow report.

Table 1: Triggering Event for Flow Detection Reports

Name	Description
DDOS_SCFD_FLOW_FOUND	A suspicious flow is detected.
DDOS_SCFD_FLOW_TIMEOUT	The timeout period expires for a culprit flow. Flow detection stops suppressing (or monitoring) the flow.
DDOS_SCFD_FLOW_RETURN_NORMAL	A culprit flow returns to within the bandwidth limit.
DDOS_SCFD_FLOW_CLEARED	A culprit flow is cleared manually with a **clear** command or automatically as the result of suspicious flow monitoring shifting to a different aggregation level.
DDOS_SCFD_FLOW_AGGREGATED	Control flows are aggregated to a coarser level. This event happens when the flow table nears capacity or when the flow cannot be found at a particular flow level and the next coarser level has to be searched.
DDOS_SCFD_FLOW_DEAGGREGATED	Control flows are deaggregated to a finer level. This event happens when the flow table is not very full or when flow control is effective and the total arrival rate for the flow at the policer for the packet type is below its bandwidth for a fixed, internal period.

- Bandwidth violation reports—These reports are generated by events associated with the discovery of suspicious flows. Each report includes identifying information for the flow that experienced the event. This information is used to track the suspicious flow and identify flows that are placed in the flow table. Table 2 on page 33 describes the event that triggers each violation report.

Table 2: Triggering Event for Bandwidth Violation Reports

Name	Description
DDOS_PROTOCOL_VIOLATION_SET	The incoming traffic for a violated control protocol returned to normal.
DDOS_PROTOCOL_VIOLATION_CLEAR	The incoming traffic for a control protocol exceeded the configured bandwidth.

A report is sent only when triggered by an event; that is, there are no null or empty reports. Because the reports are made periodically, the only events of interest are ones that occur during the interval since the last report.

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

CHAPTER 4

Configuring Flow Detection

Configuring Flow Detection for DDoS Protection

Flow detection monitors the flows of control traffic for violation of the bandwidth allowed for each flow and manages traffic identified as a culprit flow. Suppression of the traffic is the default management option. Flow detection is typically implemented as part of an overall DDoS protection strategy, but it is also useful for troubleshooting and understanding traffic flow in new configurations. Flow detection is disabled by default.

Before you begin, ensure you have configured DDoS protection appropriately for you network. See "Configuring Protection Against DDoS Attacks" on page 9 for detailed information about DDoS protection.

To configure flow detection:

1. Enable flow detection globally for all protocol groups and packet types.

   See "Enabling Flow Detection for All Protocol Groups and Packet Types" on page 37.

2. (Optional) Set the rate at which culprit flow events are reported for all line cards, protocol groups, and packet types.

   See "Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types" on page 37.

3. Set the rate at which bandwidth violations are reported for all line cards, protocol groups, and packet types.

   See "Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types" on page 37.

4. (Optional) Configure how long a suspicious flow must be in violation of flow bandwidth before being declared a culprit flow.

   See "Configuring the Detection Period for Suspicious Flows" on page 38.

5. (Optional) Configure how long a culprit flow must drop to within its allowed bandwidth before being declared normal.

   See "Configuring the Recovery Period for a Culprit Flow" on page 38.

6. (Optional) Enable and configure how long a culprit flow is suppressed or monitored.

   See "Configuring the Timeout Period for a Culprit Flow" on page 39.

7. (Optional) Configure when flow detection monitors flows.

   See "Configuring Flow Detection for Individual Protocol Groups or Packets" on page 40.

8. (Optional) Configure when flow detection operates at each flow aggregation level (subscriber, logical interface, and physical interface).

   See "Configuring How Flow Detection Operates at Each Flow Aggregation Level" on page 40.

9. Configure the maximum bandwidth for packet flows at each flow aggregation level (subscriber, logical interface, and physical interface).

   See "Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level" on page 42.

10. (Optional) Configure how traffic is controlled at each flow aggregation level (subscriber, logical interface, and physical interface) for flows that violate their bandwidth.

    See "Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level" on page 42.

11. (Optional) Disable automatic logging of suspicious flows.

    See "Disabling Automatic Logging of Culprit Flow Events for a Packet Type" on page 43.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 3
- DDoS Protection Flow Detection Overview on page 31

Enabling Flow Detection for All Protocol Groups and Packet Types

By default, flow detection is disabled for all protocol groups and packet types. You must enable flow detection globally by including the **flow-detection** statement. If you subsequently disable flow detection for individual packet types, you cannot use this global statement to override all such individual configurations; you must re-enable detection at the packet configuration level.

To enable flow detection globally:

- Set flow detection.

```
[edit system ddos-protection global]
user@host# set flow-detection
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35
- Configuring Protection Against DDoS Attacks on page 9

Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types

When flow detection confirms that a suspicious flow it is tracking on a line card is indeed a culprit flow, it sends a report to the Routing Engine. Flow detection also reports each culprit flow that subsequently recovers to within the allowed bandwidth or is cleared. You can include the **flow-report-rate** statement to limit how many flows per second on each line card can be reported. Culprit flow events are reported for all protocol groups and packet types by default. When too many flows are reported, congestion can occur on the host path to the Routing Engine flow.

To globally configure the maximum report rate for culprit flows:

- Set the reporting rate.

```
[edit system ddos-protection global]
user@host# set flow-report-rate rate
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35
- Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43

Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types

By default, flow detection reports to the Routing Engine all violations of bandwidth at the FPC for all protocol groups and packet types. You can include the **violation-report-rate** statement to limit how many violations per second flow detection reports from the line

cards, thus reducing the load on the router. We recommend that you configure a report rate that is suitable for your network rather than rely on the default value.

To globally configure the maximum bandwidth violation reporting rate:

- Set the reporting rate.

  ```
  [edit system ddos-protection global]
  user@host# set violation-report-rate rate
  ```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

Configuring the Detection Period for Suspicious Flows

DDoS protection flow detection considers a monitored flow to be a suspicious flow whenever the flow exceeds its allowed bandwidth, based on a crude test that eliminates obviously good flows from consideration. A closer examination of a suspicious flow requires the flow to remain in violation of the bandwidth for a period of time before flow detection considers it to be a culprit flow against which it must take action. You can include the **flow-detect-time** statement to configure the duration of this detection period or you can rely on the default period of three seconds.

BEST PRACTICE: **We recommend that you use the default value for the detection period.**

To specify how long a flow must be in violation before flow detection declares it to be a culprit flow:

- Set the detection period.

  ```
  [edit system ddos-protection protocols protocol-group packet-type]
  user@host# set flow-detect-time seconds
  ```

  For example, include the following statement to require the DHCPv4 discover packet flow to be in violation of its allowed bandwidth for 30 seconds before it is considered to be a culprit flow:

  ```
  [edit system ddos-protection protocols dhcpv4 discover]
  user@host# set flow-detect-time 30
  ```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

Configuring the Recovery Period for a Culprit Flow

After DDoS protection flow detection has identified a suspicious flow as a culprit flow, it has to determine when that flow no longer represents a threat to the router. When the traffic flow rate drops back to within the allowed bandwidth, the rate must remain within the bandwidth for a recovery period. Only then does flow detection consider the flow to be normal and stop the traffic handling action enacted against the culprit flow. You can

include the **flow-recover-time** statement to configure the duration of this recovery period or you can rely on the default period of 60 seconds.

To specify how long a flow must be within its allowed bandwidth after a violation before flow detection declares it to be a normal flow:

- Set the recovery period.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** flow-recover-time ***seconds***

  For example, include the following statement to require the DHCPv4 discover packet flow to be in recovery for five minutes (300 seconds):

  [edit system ddos-protection protocols dhcpv4 discover]
  user@host# **set** flow-recover-time **300**

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

Configuring the Timeout Period for a Culprit Flow

When DDoS protection flow detection identifies a suspicious flow as a culprit flow, by default it suppresses traffic for that flow for as long as the traffic flow exceeds the bandwidth limit. Suppression stops and the flow is removed from the flow table when the time since the last violation by the flow is greater than the recovery period.

Alternatively, you can include the **timeout-active-flows** statement to enable flow detection to suppress a culprit flow for a configurable timeout period. When the timeout period expires, suppression stops and the flow is removed from the flow table. You can either include the **flow-timeout-time** statement to configure the duration of the timeout period or rely on the default timeout of 300 seconds.

To enable flow detection to suppress a culprit flow for a timeout period:

1. Enable the timeout.

   [edit system ddos-protection protocols *protocol-group packet-type*]
   user@host# **set** timeout-active-flows

2. Specify the timeout period.

   [edit system ddos-protection protocols *protocol-group packet-type*]
   user@host# **set**flow-timeout-time ***seconds***

For example, include the following statements to suppress the DHCPv4 discover packet flow for 10 minutes (600 seconds):

[edit system ddos-protection protocols dhcpv4 discover]
user@host# **set** timeout-active-flows
user@host# **set**flow-timeout-time **600**

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

Configuring Flow Detection for Individual Protocol Groups or Packets

By default, flow detection is disabled for all protocol groups and packet types. After you have turned on flow detection globally, you can include the **flow-detection-mode** statement to configure flow detection to operate differently for individual packet types. By default, flow detection operates in automatic mode for all packet types, meaning that it monitors control traffic for suspicious flows only after a DDoS policer has been violated. You can also configure flow detection either to never monitor flows or to always monitor flows.

NOTE: **The flow detection mode at the packet level must be either automatic or on for flow detection to operate at individual flow aggregation levels.**

To configure how flow detection operates:

- Disable suspicious flow detection for a packet type.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** flow-detection-mode **off**

- Set flow detection to operate automatically when a policer is violated.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** flow-detection-mode **automatic**

- Specify that flow detection is always on for a packet type.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** flow-detection-mode **on**

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40

Configuring How Flow Detection Operates at Each Flow Aggregation Level

When flow detection is turned on, traffic flows are monitored by default for all protocol groups and packet types. When a policer violation occurs, each suspicious flow is examined to determine whether it is the culprit flow that caused the violation. You can include the **flow-level-detection** statement to configure how flow detection works at each flow aggregation level for a packet type: subscriber, logical interface, or physical interface.

NOTE: **The flow detection mode at the packet level must be either automatic or on for flow detection to operate at individual flow aggregation levels.**

Flow detection supports three operation modes:

- automatic—When a DDoS protection policer is violated, traffic flows at this flow aggregation level are monitored for suspicious behavior only until flow detection determines that the suspect flow is not at this aggregation level and instead must be at a coarser level of aggregation. Flows at this level are subsequently not searched again until the policer is no longer violated at the coarser level.
- off—Traffic flows are never monitored at this flow aggregation level.
- on—Traffic flows at this flow aggregation level are monitored for suspicious flows even when no DDoS protection policer is currently being violated, if flow detection at the packet level is configured to **on**. Monitoring continues at this level regardless of whether a suspect flow is identified at this level. However, If the packet level mode is **automatic**, then the policer must be in violation for traffic flows to be checked at this level.

Flows are examined first at the finest-grained (lowest bandwidth) flow aggregation level, subscriber. If the suspect flow is not found at the subscriber level, then flows are checked at the logical interface level. Finally, if the suspect is not found there, then flows are checked at the physical interface level; barring some misconfiguration, the culprit flow must be found at this level.

To configure how flow detection operates at each flow aggregation level:

1. (Optional) Specify the detection mode at the subscriber level.

   [edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]
   user@host# set subscriber ***flow-operation-mode***

2. (Optional) Specify the detection mode at the logical interface level.

   [edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]
   user@host# set logical-interface ***flow-operation-mode***

3. (Optional) Specify the detection mode at the physical interface level.

   [edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]
   user@host# set physical-interface ***flow-operation-mode***

For example, include the following statements to configure flow detection to check for suspicious flows at the subscriber level only when the policer is being violated, to never check at the logical interface level, and to always check at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-detection
user@host# set subscriber automatic
user@host# set logical-interface off
user@host# set physical-interface on
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35
- Configuring Flow Detection for Individual Protocol Groups or Packets on page 40

Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level

You can include the **flow-level-bandwidth** statement to configure the maximum acceptable bandwidth for traffic flows for individual packet types. You have to specify the bandwidth behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface. We recommend that you tune the bandwidth values for your entwork rather than rely on the defaults.

To configure the maximum bandwidth for traffic flows each flow aggregation level:

1. (Optional) Configure the bandwidth for flows at the subscriber level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type
     flow-level-bandwidth]
   user@host# set subscriber flow-bandwidth
   ```

2. (Optional) Configure the bandwidth for flows at the logical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type
     flow-level-bandwidth]
   user@host# set logical-interface flow-bandwidth
   ```

3. (Optional) Configure the bandwidth for flows at the physical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type
     flow-level-bandwidth]
   user@host# set physical-interface flow-bandwidth
   ```

For example, to configure the flow bandwidth to 1000 pps at the subscriber level, 5000 pps at the logical interface level, and 30,000 at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-bandwidth
user@host# set subscriber 10
user@host# set logical-interface 100
user@host# set physical-interface 1000
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level

When flow detection is enabled, all traffic in a culprit flow is dropped by default for all protocol groups and packet types and at all flow aggregation levels. You can include the **flow-level-control** statement to configure flow detection to control traffic differently for individual packet types. You have to specify the control behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface.

You can configure flow detection flow control to employ one of the following modes for a packet type:

- Drop all traffic—Configure flow control to drop all traffic when you think the flow that is violating a bandwidth limit is malicious. This behavior is the default at all flow aggregation levels.

- Police traffic—Configure flow control to police a flow that is violating bandwidth, forcing the rate below the bandwidth limit. Flow control acts as a simple policer in this case.
- Keep all traffic—Configure flow control to keep all traffic whether the flow is in violation or below the bandwidth limit. This mode is helpful when you need to debug traffic flow for your network.

Flow control mode enables great flexibility in how you manage control traffic in your network. For example, if you only want to ensure that control flows for a packet type at all aggregation levels are within their limits, you can configure flow control to police the traffic at each level. Or if you want to detect culprit flows and suppress them at one level but only restrain traffic to the allowed bandwidth at another level, you can configure one level to drop all traffic and the other to police traffic.

To configure how flow detection controls traffic in a culprit flow:

1. (Optional) Specify the control mode at the subscriber level.

   [edit system ddos-protection protocols *protocol-group packet-type* scfd flow-level-control]
   user@host# set subscriber ***flow-control-mode***

2. (Optional) Specify the control mode at the logical interface level.

   [edit system ddos-protection protocols *protocol-group packet-type* scfd flow-level-control]
   user@host# set logical-interface ***flow-control-mode***

3. (Optional) Specify the control mode at the physical interface level.

   [edit system ddos-protection protocols *protocol-group packet-type* scfd flow-level-control]
   user@host# set physical-interface ***flow-control-mode***

For example, to configure flow detection to keep all traffic for a physical interface under the configured bandwidth, but detect and suppress culprit flows at the subscriber level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-control
user@host# set subscriber drop
user@host# set physical-interface police
user@host# edit flow-level-detection
user@host# set logical-interface off
```

In this example, you do not care about the logical interface, so flow detection is turned off for that level. Because flow detection is disabled, the state of flow control for that level does not matter.

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

Disabling Automatic Logging of Culprit Flow Events for a Packet Type

By default, flow detection automatically logs policer violation events associated with suspicious flows (violation reports) and culprit flow events (flow reports) for all protocol groups and packet types. You can include the **no-flow-logging** statement to prevent

automatic logging of culprit flow events for individual packet types. Automatic logging of suspicious flow violation events is disabled with the **disable-logging** statement at the **[edit system ddos-protection global** hierarchy level.

To disable automatic culprit flow event logging for a packet type:

- Disable logging.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** no-flow-logging

To disable automatic suspicious flow violation event logging for a packet type:

- Disable logging.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** disable-logging

For example, include the following statement to disable automatic logging for DHCPv4 DISCOVER packet flows:

[edit system ddos-protection protocols dhcpv4 discover]
user@host# **set** no-flow-logging

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35
- Configuring DDoS Protection Policers for Individual Packet Types on page 11

Verifying and Managing Flow Detection

Purpose View or clear information about flow detection as part of a DDoS protection configuration.

Action

- To display configuration information for flow detection:

  user@host> **show ddos-protection protocols flow-detection**

- To display information about culprit flows identified by flow detection, including number of flows detected and tracked, source address of the flow, arriving interface, and rates:

  user@host> **show ddos-protection protocols culprit-flows**

- To clear culprit flows for all packet types in all protocol groups:

  user@host> **clear ddos-protection protocols culprit-flows**

- To clear culprit flows for all packet types in a particular protocol group:

  user@host> **clear ddos-protection protocols *protocol-group* culprit-flows**

Related Documentation

- Verifying and Managing DDoS Protection on page 18
- Junos OS Operational Mode Commands

PART 3

Complete Configuration Statement Hierarchy and Summary of Statements for DDoS Protection and Flow Detection

CHAPTER 5

DDoS Protection and Flow Detection Configuration Hierarchy

[edit system ddos-protection] Hierarchy Level

```
system {
  ddos-protection {
    global {
      disable-fpc;
      disable-logging;
      disable-routing-engine;
      flow-detection;
      flow-report-rate;
      violation-report-rate;
    }
    protocols protocol-group (aggregate | packet-type) {
      bandwidth packets-per-second;
      burst size;
      bypass-aggregate;
      disable-fpc;
      disable-logging;
      disable-routing-engine;
      flow-detection-mode (automatic | off | on);
      flow-detect-time seconds;
      flow-level-bandwidth {
        logical-interface flow-bandwidth;
        physical-interface flow-bandwidth;
        subscriber flow-bandwidth;
      }
      flow-level-control {
        logical-interface flow-control-mode;
        physical-interface flow-control-mode;
        subscriber flow-control-mode;
      }
      flow-level-detection {
        logical-interface flow-operation-mode;
        physical-interface flow-operation-mode;
        subscriber flow-operation-mode;
      }
      flow-recover-time seconds;
```

```
        flow-timeout-time seconds;
        fpc slot-number {
          bandwidth-scale percentage;
          burst-scale percentage;
          disable-fpc;
        }
        no-flow-logging
        priority level;
        recover-time seconds;timeout-active-flows;
      }
      traceoptions{
        file filename <files number> <match regular-expression > <size maximum-file-size>
          <world-readable | no-world-readable>;
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
      }
    }
  }
```

Related Documentation

- Configuring Protection Against DDoS Attacks on page 9
- Configuring Flow Detection for DDoS Protection on page 35

CHAPTER 6

DDoS Protection and Flow Detection Configuration Statements

bandwidth (DDoS)

Syntax bandwidth *packets-per-second*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the DDoS bandwidth rate limit; the maximum traffic rate (packets per second) allowed for the packet type. When the value is exceeded, a violation is declared.

Options ***packets-per-second***—Number of packets per second that are allowed for the packet type.

Range: 1 through 100,000 packets per second

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 11

bandwidth-scale (DDoS)

Syntax bandwidth-scale *percentage*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the percentage by which the DDoS bandwidth rate limit is scaled down for the packet type on the card in the specified slot.

Options *percentage*—Percentage multiplied by the bandwidth rate limit to reduce the number of packets per second allowed for the packet type.

Range: 1 through 100 percent

Default: 100

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

burst (DDoS)

Syntax burst *size*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the DDoS burst limit; the maximum number of packets of the packet type that is allowed in a burst of traffic. When this value is exceeded, a violation is declared.

Options *size*—Number of packets that are allowed in a burst for the packet type.

Range: 1 through 100,000 packets

Default: The default burst value varies by packet type. You can view the default values for all packet types on an unconfigured router by entering the **show ddos-protection protocols parameters brief** command from operational mode.

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 11

burst-scale (DDoS)

Syntax burst-scale *percentage*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the percentage by which the DDoS burst limit is scaled down for the packet type on the specified card.

Options *percentage*—Percentage multiplied by the burst limit to reduce the number of packets allowed in a burst for the packet type.

Range: 1 through 100 percent

Default: 100

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 11

bypass-aggregate (DDoS)

Syntax bypass-aggregate;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Prevent this packet type from being considered by the DDoS aggregate policer. Traffic for the packet type is still included in traffic statistics.

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 11

ddos-protection (DDoS)

Syntax

```
ddos-protection
  global {
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection;
    flow-report-rate;
    violation-report-rate;
  }
  protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    bypass-aggregate;
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection-mode (automatic | off | on);
    flow-detect-time seconds;
    flow-level-bandwidth {
      logical-interface flow-bandwidth;
      physical-interface flow-bandwidth;
      subscriber flow-bandwidth;
    }
    flow-level-control {
      logical-interface flow-control-mode;
      physical-interface flow-control-mode;
      subscriber flow-control-mode;
    }
    flow-level-detection {
      logical-interface flow-operation-mode;
      physical-interface flow-operation-mode;
      subscriber flow-operation-mode;
    }
    flow-recover-time seconds;
    flow-timeout-time seconds;
    fpc slot-number {
      bandwidth-scale percentage;
      burst-scale percentage;
      disable-fpc;
    }
    no-flow-logging
    priority level;
    recover-time seconds;
    timeout-active-flows;
  }
  traceoptions{
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
```

}

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure DDoS policers.

The remaining statements are explained separately.

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

Related Documentation
- Configuring Protection Against DDoS Attacks on page 9
- Configuring Flow Detection for DDoS Protection on page 35

disable-fpc (DDoS)

Syntax disable-fpc;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.
Support at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level introduced in Junos OS Release 12.1.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Disable DDoS policers for debugging purposes on the card in the specified slot for a particular packet type within a protocol group, on all cards for a particular packet type within a protocol group, or globally on all cards and for all packet types in all protocols. This statement does not affect the state of the Routing Engine policers.

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

Related Documentation
- Disabling DDoS Protection Policers and Logging Globally on page 10
- Configuring DDoS Protection Policers for Individual Packet Types on page 11

disable-logging (DDoS)

Syntax disable-logging;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.
Support at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level introduced in Junos OS Release 12.1.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Disable router-wide logging of all DDoS violation and flow detection events globally. Disable only logging of events other than flow detection culprit flow events for a particular packet type within a protocol group. Typically used for debugging purposes.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 10
- Configuring DDoS Protection Policers for Individual Packet Types on page 11
- Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43

disable-routing-engine (DDoS)

Syntax disable-routing-engine;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Disable DDoS Routing Engine policers for debugging purposes for a particular packet type within a protocol group or globally for all packet types in all protocols. This statement does not affect the state of the line card policers.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 10

flow-detection (DDoS Flow Detection)

Syntax flow-detection;

Hierarchy Level [edit system ddos-protection global]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Enable flow detection globally for all protocol groups and packet types.

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

Related Documentation

- Enabling Flow Detection for All Protocol Groups and Packet Types on page 37
- Configuring Flow Detection for DDoS Protection on page 35

flow-detection (DDoS Packet Level)

Syntax

```
flow-detection {
  flow-detect-time detect-period;
  no-flow-logging;
  timeout-active-flows enable-period;
  flow-level-bandwidth {
    logical-interface flow-bandwidth;
    physical-interface flow-bandwidth;
    subscriber flow-bandwidth;
  }
  flow-level-control {
    logical-interface flow-control-mode;
    physical-interface flow-control-mode;
    subscriber flow-control-mode;
  }
  flow-level-detection {
    logical-interface operation-mode;
    physical-interface operation-mode;
    subscriber operation-mode;
  }
  flow-detection-mode (automatic |off | on);
  flow-recover-time recover-period;
  flow-timeout-time timeout-period;
}
```

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure DDoS protection suspicious control flow detection for a packet type.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 35

flow-detection-mode (DDoS Flow Detection)

Syntax flow-detection-mode (automatic | off | on)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure the mode of operation for flow detection for the packet type. The operation mode is effective only when flow detection is enabled.

Default The default mode for all protocol groups and packet types is **automatic**.

Options **automatic**—Detect flows only when the policer is being violated.

off—Disable flow detection.

on—Always monitor and detect flows, even when the policer is not being violated.

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

Related Documentation

- Configuring Flow Detection for Individual Protocol Groups or Packets on page 40
- Configuring Flow Detection for DDoS Protection on page 35

flow-detect-time (DDoS Flow Detection)

Syntax flow-detect-time *seconds*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-detection]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure how much time must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is confirmed to be a culprit flow.

BEST PRACTICE: **We recommend that you use the default value for the detection period.**

Options ***seconds***—Period of excessive bandwidth required for flow to be a culprit flow.

Range: 1 through 60 seconds

Default: Three seconds

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

Related Documentation

- Configuring the Detection Period for Suspicious Flows on page 38
- Configuring Flow Detection for DDoS Protection on page 35

flow-level-bandwidth (DDoS Flow Detection)

Syntax

```
flow-level-bandwidth {
  logical-interface flow-bandwidth;
  physical-interface flow-bandwidth;
  subscriber flow-bandwidth;
}
```

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure allowed flow bandwidth for the packet type at each flow aggregation level.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42
- Configuring Flow Detection for DDoS Protection on page 35

flow-level-control (DDoS Flow Detection)

Syntax

```
flow-level-control {
  logical-interface flow-control-mode;
  physical-interface flow-control-mode;
  subscriber flow-control-mode;
}
```

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Specify how traffic in the detected flow is handled for the packet type at each flow aggregation level.

The remaining statements are explained separately.

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

Related Documentation

- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42
- Configuring Flow Detection for DDoS Protection on page 35

flow-level-detection (DDoS Flow Detection)

Syntax

```
flow-level-detection {
  logical-interface flow-operation-mode;
  physical-interface flow-operation-mode;
  subscriber flow-operation-mode;
}
```

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure the mode of operation for flow detection for the packet type at each flow aggregation level.

The remaining statements are explained separately.

NOTE: Flow detection operates for individual flow aggregation levels only when the flow detection mode at the packet level is configured to either automatic or on.

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

Related Documentation

- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40
- Configuring Flow Detection for DDoS Protection on page 35

flow-recover-time (DDoS Flow Detection)

Syntax flow-recover-time *seconds*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure how much time must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.

Options ***seconds***—Period required for the traffic to recover.
Range: 1 through 3600 seconds
Default: 60 seconds

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

Related Documentation
- Configuring the Recovery Period for a Culprit Flow on page 38
- Configuring Flow Detection for DDoS Protection on page 35

flow-report-rate (DDoS Flow Detection)

Syntax flow-report-rate *report-rate*;

Hierarchy Level [edit system ddos-protection global]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Set the rate at which culprit flow events are reported by system log messages, for all protocol groups and packet types on all line cards.

Options ***report-rate***—Number of flows per second.
Range: 1 through 50,000
Default: 10

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

Related Documentation
- Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types on page 37
- Configuring Flow Detection for DDoS Protection on page 35

flow-timeout-time (DDoS Flow Detection)

Syntax flow-timeout-time *seconds*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure the period of time that a culprit flow is suppressed for the packet type. The timeout period is effective only when timing out has been enabled with the timeout-active-flows statement.

Options ***seconds***—Period that the traffic is suppressed.

Range: 1 through 7200 seconds

Default: 300 seconds

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

Related Documentation

- Configuring the Timeout Period for a Culprit Flow on page 39
- Configuring Flow Detection for DDoS Protection on page 35

fpc (DDoS)

Syntax

```
fpc slot-number;
  bandwidth-scale percentage;
  burst-scale percentage;
  disable-fpc;
}
```

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Modify the DDoS policer for the packet type on the specified card.

Options ***slot-number***—Slot number of the card.

Range: Depends on the router model

The remaining statements are explained separately.

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 11

global (DDoS)

Syntax

```
global {
  disable-fpc;
  disable-logging;
  disable-routing-engine;
  flow-detection;
  flow-report-rate;
  violation-report-rate;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description Modify DDoS policers, event logging, and flow detection globally for all protocols.

The remaining statements are explained separately.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 10

logical-interface (DDoS Flow Detection)

Syntax logical-interface (*flow-bandwidth* | *flow-control-mode* | *flow-detection-mode*)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure flow bandwidth, flow control mode, or flow detection mode for flow detection at the logical interface flow aggregation level for the packet type.

Options ***flow-bandwidth***—Bandwidth for the flow at the logical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth]** hierarchy level.

Default: 200 packets per second

Range: 1 through 30,000 packets per second

flow-control-mode—Mode for how traffic in the detected flow is controlled at the logical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control]** hierarchy level.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

flow-detection-mode—Mode for how flow detection operates at the logical interface level when a policer has been violated. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]** hierarchy level.

- **automatic**—Search flows at the logical interface level only when a DDoS policer is being violated and only when the flow causing the policer violation is not discovered at the finer flow aggregation level, subscriber. When the suspicious flow is not found at this level, then the search moves to a coarser level of flow aggregation (physical interface). Flows at the logical interface level are subsequently not searched again until the policer is no longer violated at the coarser level, and a subsequent violation occurs that cannot be found at the subscriber level.
- **off**—Disable flow detection at the logical interface level so that flows are never searched at this level.
- **on**—Search flows at the logical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40
- Configuring Flow Detection for DDoS Protection on page 35

no-flow-logging (DDoS Flow Detection)

Syntax no-flow-logging;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Disable automatic logging of flow detection culprit flow events (flow reports) for the packet type.

NOTE: You can disable ogging of suspicious flow events (violation reports) with the disable-logging statement at the [edit system ddos-protection global hierarchy level.

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

Related Documentation

- Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43
- Configuring Flow Detection for DDoS Protection on page 35

physical-interface (DDoS Flow Detection)

Syntax physical-interface (*flow-bandwidth* | *flow-control-mode* | *flow-detection-mode*)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure flow bandwidth, flow control mode, or flow detection mode at the physical interface flow aggregation level for the packet type.

Options ***flow-bandwidth***—Bandwidth for the flow at the physical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth]** hierarchy level.

Default: 20,000 packets per second

Range: 1 through 50,000 packets per second

flow-control-mode—Mode for how traffic in the detected flow is controlled at the physical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control]** hierarchy level.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

flow-detection-mode—Mode for how flow detection operates at the physical interface level when a policer has been violated. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]** hierarchy level.

- **automatic**—Search flows at the physical interface level only when a DDoS policer is being violated and only when the policer violation is not discovered at the finer aggregation levels, logical interface or subscriber. Flows at the physical interface level are subsequently not searched again until a subsequent violation occurs that cannot be found at the subscriber or logical interface levels.
- **off**—Disable flow detection at the physical interface level so that flows are never searched at this level.
- **on**—Search flows at the physical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40
- Configuring Flow Detection for DDoS Protection on page 35

priority (DDoS)

Syntax priority *level*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the priority for the packet type within the parent protocol group. In the event of downstream traffic congestion, high priority packets are provided bandwidth before medium priority packets. In turn, medium priority packets are provided bandwidth before low priority packets. Packets are dropped when there is insufficient available bandwidth.

Options ***level***—Priority of the packet type, low, medium, or high.

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 11

protocols (DDoS)

Syntax

```
protocols protocol-group (aggregate | packet-type) {
  bandwidth packets-per-second;
  burst size;
  bypass-aggregate;
  disable-fpc;
  disable-logging;
  disable-routing-engine;
  flow-detection-mode (automatic | off | on);
  flow-detect-time seconds;
  flow-level-bandwidth {
    logical-interface flow-bandwidth;
    physical-interface flow-bandwidth;
    subscriber flow-bandwidth;
  }
  flow-level-control {
    logical-interface flow-control-mode;
    physical-interface flow-control-mode;
    subscriber flow-control-mode;
  }
  flow-level-detection {
    logical-interface flow-operation-mode;
    physical-interface flow-operation-mode;
    subscriber flow-operation-mode;
  }
  flow-recover-time seconds;
  flow-timeout-time seconds;
  fpc slot-number {
    bandwidth-scale percentage;
    burst-scale percentage;
    disable-fpc;
  }
  no-flow-logging
  priority level;
  recover-time seconds;
  timeout-active-flows;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure DDoS policers for all packet types within a protocol group or for a particular packet type within a protocol group.

Options

aggregate—Configure the policer to monitor all control packets within the protocol group. You can configure an aggregate policer for any protocol group.

packet-type—(Optional) Name of the control packet type to be policed. You can configure a specific policer for only the following packet types and protocol groups:

- **dhcpv4**—The following packet types are available for DHCPv4 traffic:

- **ack**—DHCPACK packets.
- **bad-packets**—DHCPv4 packets with bad formats.
- **bootp**—DHCPBOOTP packets.
- **decline**—DHCPDECLINE packets.
- **discover**—DHCPDISCOVER packets.
- **force-renew**—DHCPFORCERENEW packets.
- **inform**—DHCPINFORM packets.
- **lease-active**—DHCPLEASEACTIVE packets.
- **lease-query**—DHCPLEASEQUERYpackets.
- **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
- **lease-unknown**—DHCPLEASEUNKNOWN packets.
- **nak**—DHCPNAK packets.
- **no-message-type**—DHCP packets that are missing the message type.
- **offer**—DHCPOFFER packets.
- **release**—DHCPRELEASE packets.
- **renew**—DHCPRENEW packets.
- **request**—DHCPREQUEST packets.
- **unclassified**—All unclassified packets in the protocol group.

- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
  - **advertise**—ADVERTISE packets.
  - **confirm**—CONFIRM packets.
  - **decline**—DECLINE packets.
  - **information-request**—INFORMATION-REQUEST packets.
  - **leasequery**—LEASEQUERY packets.
  - **leasequery-data**—LEASEQUERY-DATA packets.
  - **leasequery-done**—LEASEQUERY-DONE packets.
  - **leasequery-reply**—LEASEQUERY-REPLY packets.
  - **rebind**—REBIND packets.
  - **reconfigure**—RECONFIGURE packets.
  - **relay-forward**—RELAY-FORWARD packets.
  - **relay-reply**—RELAY-REPLY packets.
  - **release**—RELEASE packets.
  - **renew**—RENEW packets.
  - **reply**—REPLY packets.
  - **request**—REQUEST packets.
  - **solicit**—SOLICIT packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **frame-relay**—The following packet types are available for Frame Relay traffic:
  - **frf15**—Multilink frame relay FRF.15 packets.
  - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
  - **first-fragment**—First IP fragment.
  - **trail-fragment**—Last IP fragment.
- **ip-options**—The following packet types are available for IP option traffic:
  - **router-alert**—Router alert options packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **ipv4-unclassified**—All unclassified host-bound IPv4 traffic.
- **ipv6-unclassified**—All unclassified host-bound IPv6 traffic.

- **mcast-snoop**—Control traffic for multicast snooping.
  - **igmp**—Snooped IGMP traffic.
  - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
  - **aging-exception**—MLP aging exception packets.
  - **packets**—MLP packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **ipcp**—IP Control Protocol packets.
  - **ipv6cp**—IPv6 Control Protocol packets.
  - **isis**—IS-IS packets.
  - **lcp**—Link Control Protocol packets.
  - **mlppp-lcp**—MLPPP LCP packets.
  - **mplscp**—MPLS Control Protocol packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
  - **padi**—PADI packets.
  - **padm**—PADM packets.
  - **padn**—PADN packets.
  - **pado**—PADO packets.
  - **padr**—PADR packets.
  - **pads**—PADS packets.
  - **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:
  - **accounting**—RADIUS accounting packets.
  - **authorization**—RADIUS authorization packets.
  - **server**—RADIUS server traffic.
  - **unclassified**—All unclassified packets in the protocol group.

- **tcp-flags**—The following TCP-flagged packet types are available:
  - **established**—TCP ACK and RST connection packets.
  - **initial**—TCP SYN and NAK packets.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
  - **control-low**—Low-priority control packets.
  - **control-high**—High-priority control packets.
  - **unclassified**—All unclassified packets in the protocol group.
  - **vc-packets**—All exception packets on the virtual chassis link.
  - **vc-ttl-errors**—Virtual chassis TTL error packets.

protocol-group—Name of the protocol group for which traffic is policed. You can configure a policer for any of the following protocol groups:

- **amtv4**—IPv4 AMT traffic.
- **amtv6**—IPv6 AMT traffic.
- **ancp**—ANCP traffic.
- **ancpv6**—ANCPv6 traffic.
- **arp**—ARP traffic.
- **atm**—ATM traffic.
- **bfd**—BFD traffic.
- **bfdv6**—BFDv6 traffic.
- **bgp**—BGP traffic.
- **bgpv6**—BGPv6 traffic.
- **control**—Control traffic.
- **demux-autosense**—Demux autosensing traffic.
- **dhcpv4**—DHCPv4 traffic.
- **dhcpv6**—DHCPv6 traffic.
- **diameter**—Diameter and Gx-Plus traffic.
- **dns**—DNS traffic.
- **dtcp**—DTCP traffic.
- **dynamic-vlan**—Dynamic VLAN exception traffic.
- **egpv6**—EGPv6 traffic.
- **eoam**—EOAM traffic.
- **esmc**—ESMC traffic.
- **firewall-host**—Firewall send-to-host traffic.
- **frame-relay**—Frame relay traffic.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.
- **inline-ka**—Inline service interfaces keepalive traffic.

- **inline-svcs**—Inline services traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**–IP traffic with IP packet header options.
- **ipv4-unclassified**—Unclassified IPv4 host-bound traffic.
- **ipv6-unclassified**—Unclassified IPv6 host-bound traffic.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **keepalive**—Keepalive traffic.
- **l2pt**—Layer 2 protocol tunneling traffic.
- **l2tp**—L2TP traffic.
- **lacp**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mcast-snoop**—Control traffic for multicast snooping.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic
- **pim**—PIM traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.
- **pppoe**—PPPoE traffic.

- **ptp**—PTP traffic.
- **pvstp**—PVSTP traffic.
- **radius**—RADIUS traffic.
- **redirect**—Traffic that triggers ICMP redirects.
- **reject**—Packets rejected by a next-hop forwarding decision.
- **rip**—RIP traffic.
- **ripv6**—RIPv6 traffic.
- **rsvp**—RSVP traffic.
- **rsvpv6**—RSVPv6 traffic.
- **services**–Service traffic.
- **snmp**—SNMP traffic.
- **snmpv6**—SNMPv6 traffic.
- **ssh**—SSH traffic.
- **sshv6**—SSHv6 traffic.
- **stp**—STP traffic.
- **tacacs**—TACACS traffic.
- **tcp-flags**—Traffic with TCP flags.
- **telnet**—TELNET traffic.
- **telnetv6**—TELNETv6 traffic.
- **ttl**—TTL traffic.
- **tunnel-fragment**—Tunnel fragments traffic.
- **virtual-chassis**—Virtual chassis traffic.
- **vrrp**—VRRP traffic.
- **vrrpv6**—VRRPv6 traffic.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 11

recover-time (DDoS)

Syntax recover-time *seconds*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure how much time must pass since the last detected DDoS violation before the traffic is considered to have recovered from the attack and returned to normal.

Options ***seconds***—Period required for the traffic to recover.

Range: 1 through 3600 seconds

Default: 300

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 11

subscriber (DDoS Flow Detection)

Syntax subscriber (*flow-bandwidth* | *flow-control-mode* | *flow-detection-mode*)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Configure flow bandwidth, flow control mode, or flow detection mode at the subscriber flow aggregation level for the packet type.

Options ***flow-bandwidth***—Specify the bandwidth for the flow at the subscriber level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth]** hierarchy level.

Default: 100 packets per second

Range: 1 through 10,000 packets per second

flow-control-mode—Specify how traffic in the detected flow is controlled at the subscriber level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control]** hierarchy level.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

flow-detection-mode—Specify how flow detection operates at the subscriber level when a DDoS protection policer has been violated. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]** hierarchy level.

- **automatic**—Search flows at the subscriber level only when a DDoS policer is being violated and only until it is established that the flow causing the violation is not at this level. When the suspicious flow is not at this level, then the search moves to a coarser level of flow aggregation (logical interface). Flows at the subscriber level are subsequently not searched again until the policer is no longer violated at the coarser level.
- **off**—Disable flow detection at the subscriber level so that flows are never searched at this level.
- **on**—Search flows at the subscriber level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40
- Configuring Flow Detection for DDoS Protection on page 35

timeout-active-flows (DDoS Flow Detection)

Syntax timeout-active-flows;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Enable culprit flows for the packet type to time out according to the timeout period. The culprit flow is suppressed for the duration of the timeout period. When the period expires, the flow times out and is released from suppression.

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

Related Documentation

- Configuring the Timeout Period for a Culprit Flow on page 39
- Configuring Flow Detection for DDoS Protection on page 35

traceoptions (DDoS)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description Define tracing operations for DDoS protection processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **config**—Trace configuration events.
- **events**—Trace all events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc**—Trace IPC events.
- **memory**—Trace memory management code.
- **protocol**—Trace DDoS protocol processing events.
- **rtsock**—Trace routing socket events.
- **signal**—Trace signal handling events.
- **socket**—Trace socket events.
- **state**—Trace state machine events.
- **timer**—Trace timer events.
- **ui**—Trace user interface events.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions reqcliring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size ***maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** to specify GB

Range: 10,240 through 1,073,741,824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

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

Related Documentation

- Tracing DDoS Protection Operations on page 14

violation-report-rate (DDoS Flow Detection)

Syntax violation-report-rate *report-rate*;

Hierarchy Level [edit system ddos-protection global]

Release Information Statement introduced in Junos OS Release 12.3.

Description (MX Series routers with MPCs only) Limit the rate at which bandwidth violations (violation reports) are reported from an FPC to the Routing Engine, for all protocol groups and packet types on all line cards.

Options *report-rate*—Number of violations per second.

Range: 1 through 50,000

Default: 100

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

Related Documentation

- Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types on page 37
- Configuring Flow Detection for DDoS Protection on page 35

PART 4

Indexes

Index

T

V

Index of Statements and Commands