



CHAPTER 11

Identifying and Preventing Distributed-Denial-Of-Service Attacks

This module describes the ability of the SCE platform to identify and prevent DDoS attacks, and the various procedures for configuring and monitoring the Attack Filter Module.

- [Attack Filtering and Attack Detection, page 11-1](#)
- [Configuring Attack Detectors, page 11-6](#)
- [Subscriber Notifications, page 11-17](#)
- [Preventing and Forcing Attack Detection, page 11-18](#)
- [Monitoring Attack Filtering, page 11-20](#)

Attack Filtering and Attack Detection

- [Attack Filtering, page 11-1](#)
- [Specific Attack Filtering, page 11-2](#)
- [Attack Detection, page 11-3](#)
- [Attack Detection Thresholds, page 11-4](#)
- [Attack Handling, page 11-4](#)
- [Hardware Filtering, page 11-5](#)

Attack Filtering

The SCE platform includes extensive capabilities for identifying DDoS attacks, and protecting against them.

Attack filtering is performed using specific-IP attack detectors. A specific-IP attack detector tracks the rate of flows (total open and total suspected) in the SCE platform for each combination of IP address (or pair of IP addresses), protocol (TCP/UDP/ICMP/Other), destination port (for TCP/UDP), interface and direction. When the rates satisfy user-configured criteria, it is considered an attack, and a configured action can take place (report/block, notify subscriber, send SNMP trap).

This mechanism is enabled by default, and can be disabled and enabled for each attack type independently.

There are 32 different attack types:

- **1** — TCP flows from a specific IP address on the subscriber side, regardless of destination port
- **2** — TCP flows to a specific IP address on the subscriber side, regardless of destination port
- **3-4** — Same as 1 and 2, but for the opposite direction (subscriber network)
- **5** — TCP flows from a specific IP address on the subscriber side to a specific IP address on the network side
- **6** — Same as 5, but for the opposite direction (from the network side to the subscriber side)
- **7-12** — Same as 1-6 but with a specific destination port common to all flows of the attack (1-6 are port-less attack types, 7-12 are port-based attack types)
- **13-24** — Same as 1-12 but for UDP instead of TCP
- **25-28** — Same as 1-4 but for ICMP instead of TCP
- **29-32** — Same as 1-4 but for Other protocols instead of TCP

Specific Attack Filtering

When the specific IP attack filter is enabled for a certain attack type, two rates are measured per defined entity:

- Rate of new flows
- Rate of suspected flows (In general, suspected flows are flows for which the SCOS did not see proper establishment (TCP) or saw only a single packet (all other protocols)).

Separate rate meters are maintained both for each IP address separately (single side) and for IP address pairs (the source and destination of a given flow), so when a specific IP is attacking a specific IP, this pair of IP addresses defines a single incident (dual-sided).

Based on these two metrics, a specific-IP attack is declared if either of the following conditions is present:

- The new flows rate exceeds a certain threshold
- The suspected flows rate exceeds a configured threshold and the ratio of suspected flows rate to total new flow rate exceeds a configured threshold.

When the rates stop satisfying this criterion, the end of that attack is declared.



Note

Specific attack filtering is configured in two steps:

- Enabling specific IP filtering for the particular attack type.
- Configuring an attack detector for the relevant attack type. Each attack detector specifies the thresholds that define an attack and the action to be taken when an attack is detected.

In addition to specific attack detectors, a default detector exists that can be configured with user-defined thresholds and action, or system defaults may be retained.

In addition, the user can manually override the configured attack detectors to either force or prevent attack filtering in a particular situation.

Specific IP filtering for selected attack types is enabled with the following parameters. These parameters control which of the 32 attack types are being filtered for:

- **Protocol** — TCP, UDP, ICMP, or Other
- **Attack direction** — The direction of the attack may be identified by only one IP address or by two IP addresses:
 - **single side** — The attack is identified by either the source IP address or the destination address only.

The filter definition may specify the specific side, or may include any single side attack, regardless of side (both).

- **dual side** (TCP and UDP protocols only) — The attack is identified by both the source and destination IP addresses. In other words, when a specific IP attacks a specific IP, this is detected as one incident rather than as two separate incidents.
- **Destination port** (TCP and UDP protocols only) — Defines whether specific IP detection is enabled or disabled for port-based or port-less detections. Enable port-based detection for TCP/UDP attacks that have a fixed destination port or ports.

The list of destination ports for port-based detection is configured separately. (See [Specific Attack Detectors, page 11-12](#).)

Attack Detection

Specific IP detections are identified with the following parameters:

- Specific IP address (or two IP addresses for dual-sided detections)
- Protocol — TCP, UDP, ICMP or Other
- Port — For TCP/UDP attacks that have a fixed destination port
- Side — Interface (Subscriber/Network) from which attack packets are sent
- Attack-direction — If a single IP address is specified, the IP address is an attack-source or an attack-destination address.

The system can identify a maximum of 1000 independent, simultaneous attacks.

Once an attack is identified, the system can be instructed to perform any of the following actions:

- **Report** — By default, the attack beginning and end are always reported.
- **Block** — The system will block all attack traffic for the duration of the attack. (The traffic is from or to the attack IP address, depending on whether the IP address is an attack-source or attack-destination)
- **Notify** — Subscriber notification. When the IP address identified is mapped to a particular subscriber context, the system can be configured to notify the subscriber of the fact that he is under an attack (or a machine in his network is generating such an attack), using HTTP Redirect.
- **Alarm** — The system will generate an SNMP trap each time an attack starts and stops.

Attack detection and handling are user-configurable. The remainder of this chapter explains how to configure and monitor attack detection.

Attack Detection Thresholds

There are three thresholds that are used to define an attack. These thresholds are based on meters that are maintained by the SCE platform for each IP address or pair of addresses, protocol, interface and attack-direction.

- **open flow rate** — A flow for which some traffic was seen. Any packet seen for a new flow is enough to declare this flow an open flow.

The rate is measured in new flows per second.

- **suspected flow rate** — A suspected flow is one that was opened, but did not become an established flow.

The rate is measured in new flows per second.

- **suspected flow ratio** — The ratio of the suspected flow rate to the open flow rate.

As explained above, a specific-IP attack is declared if either of the following conditions is present:

- The open flows rate exceeds the threshold
- The suspected flows rate exceeds the threshold and the suspected flows ratio exceeds the threshold.

The values for each attack type will have a separate configured default value.

In general, for a given protocol, the suspected flows rate threshold should be lower for a port-based detection than for a port-less detection. This is because flows with a given IP address and a common destination port are metered twice:

- By themselves — to detect a port-based attack
- Together with flows with the same IP address and different destination ports — to detect a port-less attack

If a port-based attack occurs, and the rate of flows is above both thresholds (port-based thresholds and the port-less thresholds), it is desirable for the port-based attack to be detected before the port-less attack. Similarly, this threshold should be lower for dual-IP detections than for single-IP detections.

The user may define values for these thresholds that override the preset defaults. It is also possible to configure specific thresholds for certain IP addresses and ports (using access lists and port lists). This enables the user to set different detection criteria for different types of network entities, such as a server farm, DNS server, or large enterprise customer.

Attack Handling

Attack handling can be configured as follows

- **Configuring the action:**
 - Report — Attack packets are processed as usual, and the occurrence of the attack is reported.
 - Block — Attack packets are dropped by the SCE platform, and therefore do not reach their destination.

Regardless of which action is configured, two reports are generated for every attack: one when the start of an attack is detected, and one when the end of an attack is detected.

- **Configuring subscriber-notification (notify):**
 - Enabled — If the subscriber IP address is detected to be attacked or attacking, the subscriber is notified about the attack.
 - Disabled — The subscriber is not notified about the attack.

- **Configuring sending an SNMP trap (alarm):**
 - Enabled — An SNMP trap is sent when attack begins and ends.
The SNMP trap contains the following information fields:
 - A specific IP address or
 - **Protocol** (TCP, UDP, ICMP or Other)
 - **Interface** (User/Network) behind which the detected IP address is found. This is referred to below as the attack ‘side’
 - **Attack direction** (whether the IP address is the attack source or the attack destination).
 - **Type of threshold breached** (open- flows / ddos- suspected- flows) [‘attack- start’ traps only]
 - **Threshold value breached** [‘attack- start’ traps only]
 - **Action taken** (report, block) indicating what was the action taken by the SCE platform in response to the detection
 - **Amount of attack flows blocked/ reported** providing the total number of flows detected during the attack [‘attack- stop’ traps only]
 - Disabled — No SNMP trap is sent

Subscriber Notification

When an attack is identified, if the IP address is detected on the subscriber side and is mapped to a subscriber, the system notifies the application about the attack. This enables the application to notify the subscriber about the attack on-line by redirecting HTTP requests of this subscriber to a server that will notify it of the attack.

In addition, when blocking TCP traffic, the system can be configured not to block a specified port to make this redirection possible. This port is then considered to be un-blockable.



Note

Subscriber-notification can only function if supported by the Service Control Application currently loaded to the SCE platform, and the application is configured to activate this capability. To verify whether the application you are using supports attack subscriber notification, and for details about enabling attack subscriber notification in the application, please refer to the documentation of the relevant Service Control Application.

Hardware Filtering

The SCE platform has two ways of handling an attack: by software or by hardware. Normally, attacks are handled by software. This enables the SCE platform to accurately measure the attack flows and to instantly detect that an attack has ended.

However, very strong attacks cannot be handled successfully by the software. If the software cannot adequately handle an attack, the resulting high CPU load will harm the service provided by the SCE platform (normal traffic classification and control). An attack that threatens to overwhelm the software will, therefore, be automatically filtered by the hardware.

When the hardware is used to filter the attack, the software has no knowledge of the attack packets, and therefore the following side effects occur:

- The number of attack flows is greatly under-estimated by the software. This means that the total amount of flows in the attack reported by the CLI (`show interface linecard attack-filter current-attacks`) is considerably lower than the actual amount.
- Similarly, the reported attack flow rate (also reported by the CLI) is also considerably lower than the actual rate. Usually a rate of 0 is measured by the software.
- There is considerable delay in detecting the end of the attack. The delay in detecting the end of attack is limited by two upper bounds.
 - The first upper bound depends on the configured action, as follows:
 - Report — a delay of no more than 8 minutes
 - Block — a delay of no more than 64 minutes
 - A second upper bound for the delay is one minute more than actual duration of the attack (for example, maximum delay for detecting the end of an attack lasting three minutes is four minutes).
- The following examples illustrate the interaction of these two upper bounds:
 - For an attack lasting two minutes, the maximum delay in detecting the end will be three minutes, regardless of configured action
 - For an attack lasting two hours whose configured action is 'report', the maximum delay in detecting the end will be eight minutes
 - For an attack lasting two hours whose configured action is 'block', the maximum delay in detecting the end will be 64 minutes

Hardware attack filtering is an automatic process and is not user-configurable. However, due to the effects of hardware attack filtering on attack reporting, it is important to be aware of when hardware processing has been activated, and so monitoring of hardware filtering is essential. There are two ways to do this (see [Monitoring Attack Filtering, page 11-20](#)):

- Check the "*HW-filter*" field in the **show interface linecard attack-filter current-attacks** command.
- Check the "*HW-filter*" field in the attack log file.

Configuring Attack Detectors

- [Enabling Specific-IP Detection, page 11-8](#)
- [Configuring the Default Attack Detector, page 11-10](#)
- [Specific Attack Detectors, page 11-12](#)
- [Sample Attack Detector Configuration, page 11-16](#)

The Cisco attack detection mechanism is controlled by defining and configuring special entities called Attack Detectors.

There is one attack detector called 'default', which is always enabled, and 99 attack detectors (numbered 1-99), which are disabled by default. Each detector (both the default and detectors 1-99) can be configured with a separate action and threshold values for all 32 possible attack types.

When detectors 1-99 are disabled, the default attack detector configuration determines the thresholds used for detecting an attack, and the action taken by the SCE platform when an attack is detected. For each attack type, a different set of thresholds and action can be set. In addition, subscriber-notification and SNMP traps (alarm) can be enabled or disabled in the same granularity.

The default attack detector should be configured with values that reflect the desired SCE platform behavior for the majority of the traffic flows flowing through it. However, it is not feasible to use the same set of values for all the traffic that traverses through the SCE platform, since there might be some network entities for which the characteristics of their normal traffic should be considered as an attack when coming from most other network elements. Here are two common examples:

- A DNS server is expected to be the target of many short DNS queries. These queries are typically UDP flows, each flow consisting of two packets: The request and the response. Normally, the SCE platform considers all UDP flows that are opened to the DNS server as DDoS-suspected flows, since these flows include less than 3 packets. A DNS server might serve hundreds of DNS requests per second at peak times, and so the system should be configured with a suitable threshold for DDoS-suspected flows for protocol = UDP and direction = attack-destination. A threshold value of 1000 flows/second would probably be suitable for the DNS server. However, this threshold would be unsuitable for almost all other network elements, since, for them, being the destination of such large rate of UDP flows would be considered an attack. Therefore setting a threshold of 1000 for all traffic is not a good solution.
- The subscriber side of the SCE platform might contain many residential subscribers, each having several computers connected through an Internet connection, and each computer having a different IP address. In addition, there might be a few business subscribers, each using a NAT that hides hundreds of computers behind a single IP address. Clearly, the traffic seen for an IP address of a business subscriber contains significantly more flows than the traffic of an IP address belonging to a residential subscriber. The same threshold cannot be adequate in both cases.

To let the SCE platform treat such special cases differently, the user can configure non-default attack detectors in the range of 1-99. Like the default attack detector, non-default attack detectors can be configured with different sets of values of action and thresholds for every attack type. However, to be effective, a non-default attack detector must be enabled and must be assigned an ACL (access control list). The action and thresholds configured for such attack detector are effective only for IP addresses permitted by the ACL. Non-default attack-detectors can be assigned a label for describing their purpose, such as 'DNS servers' or 'Server farm'.

Non-default attack detectors are effective only for attack types that have been specifically configured. This eliminates the need to duplicate the default attack detector configuration into the configuration non-default attack detectors, and is best illustrated with an example: Suppose an HTTP server on the subscriber side of the SCE platform is getting many requests, which requires the use of a non-default attack detector for configuring high threshold values for incoming TCP flow rates. Assume attack detector number 4 is used for this purpose; hence it is enabled, and assigned an ACL which permits the IP address of the HTTP server. Also suppose that it is desirable to protect subscribers from UDP attacks, hence the default attack detector is configured to block UDP attacks coming from the network (The default configuration is only to report attacks, not block them). If the HTTP server is attacked by a UDP attack from the network, the configuration of the default attack detector will hold for this HTTP server as well, since attack detector number 4 was not configured for UDP attacks.

For each of the non-default attack detectors, for each of the 32 attack types, there are four configurable settings:

- Threshold
- Action
- Subscriber-notification
- Alarm

Each of these four settings can be either configured (with a value or set of values) or not configured. The default state is for all them is not configured.

For each attack type, the set of enabled attack detectors, together with the default attack detector, forms a database used to determine the threshold and action to take when an attack is detected. When the platform detects a possible attack, it uses the following algorithm to determine the thresholds for attack detection.

- Enabled attack detectors are scanned from low to high numbers.
- If the IP address is permitted by the ACL specified by the attack detector, and a threshold is configured for this attack type, then the threshold values specified by this attack detector are used. If not, the scan continues to the next attack detector.
- If no attack detector matches the IP address/protocol combination, then the values of the default attack detector are used.

The same logic is applied when determining the values to use for the remaining settings: action, subscriber-notification and alarm. The value that is used is the one specified by the lowest-numbered enabled attack detector that has a configured value for the attack type. If none exists, the configuration of the default attack detector is used.

Use the following commands to configure and enable attack detection:

- **[no] attack-filter protocol *protocol* attack-direction *direction***
- **attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side* action *action* [open-flows *number* suspected-flows-rate *number* suspected-flows-ratio *number*]**
- **attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side* (notify-subscriber|don't-notify-subscriber)**
- **attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side* (alarm|no-alarm)**
- **default attack-detector (default| *number*) protocol *protocol* attack-direction *direction* side *side***
- **default attack-detector default**
- **default attack-detector *number***
- **default attack-detector (all-numbered|all)**
- **attack-detector *number* access-list *comment***
- **attack-detector *number* (TCP-dest-ports|UDP-dest-ports) (all|(port1 [port2 ...]))**
- **[no] attack-filter subscriber-notification ports *port1***

Enabling Specific-IP Detection

- [Options, page 11-9](#)
- [How to Enable Specific-IP Detection, page 11-9](#)
- [How to Enable Specific-IP Detection for the TCP Protocol Only for all Attack Directions, page 11-9](#)
- [How to Enable Specific-IP Detection for the TCP Protocol for Port-based Detections Only for Dual-sided Attacks, page 11-9](#)
- [How to Disable Specific-IP Detection for Protocols Other than TCP, UDP, and ICMP for all Attack Directions, page 11-10](#)
- [How to Disable Specific-IP Detection for ICMP for Single-sided Attacks Defined by the Source IP, page 11-10](#)

By default, specific-IP detection is enabled for all attack types. You can configure specific IP detection to be enabled or disabled for a specific, defined situation only, depending on the following options:

- For a selected protocol only.
- For TCP and UDP protocols, for only port-based or only port-less detections.
- For a selected attack direction, either for all protocols or for a selected protocol.

Options

The following options are available:

- **protocol** — The specific protocol for which specific IP detection is to be enabled or disabled.
 - Default — all protocols (no protocol specified)
- **attack direction** — Defines whether specific IP detection is enabled or disabled for single sided or dual sided attacks.
 - Default — all directions
- **destination port** (TCP and UDP protocols only) — Defines whether specific IP detection is enabled or disabled for port-based or port-less detections.
 - Default — both port-based or port-less
- Use the **no** form of the command to disable the configured specific-IP detection.

How to Enable Specific-IP Detection

-
- Step 1** From the SCE(config if)# prompt, type **attack-filter [protocol (((TCP|UDP) [dest-port (specific|not-specific|both)])|ICMP|other)] [attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all)]** and press **Enter**.
-

How to Enable Specific-IP Detection for the TCP Protocol Only for all Attack Directions

-
- Step 1** From the SCE(config if)# prompt, type **attack-filter protocol TCP** and press **Enter**.
-

How to Enable Specific-IP Detection for the TCP Protocol for Port-based Detections Only for Dual-sided Attacks

-
- Step 1** From the SCE(config if)# prompt, type **attack-filter protocol TCP dest-port specific attack-direction dual-sided** and press **Enter**.
-

How to Disable Specific-IP Detection for Protocols Other than TCP, UDP, and ICMP for all Attack Directions

-
- Step 1** From the SCE(config if)# prompt, type **no attack-filter protocol other** and press **Enter**.
-

How to Disable Specific-IP Detection for ICMP for Single-sided Attacks Defined by the Source IP

-
- Step 1** From the SCE(config if)# prompt, type **no attack-filter protocol ICMP attack-direction single-side-source** and press **Enter**.
-

Configuring the Default Attack Detector

- [Options, page 11-10](#)
- [How to Define the Default Action and Optionally the Default Thresholds, page 11-11](#)
- [How to Reinstate the System Defaults for a Selected Set of Attack Types, page 11-12](#)
- [How to Reinstate the System Defaults for All Attack Types, page 11-12](#)

Use these commands to configure the values for the default attack detector for the following parameters:

- Attack handling action
- Thresholds
- Subscriber notification
- Sending an SNMP trap

If a specific attack detector is defined for a particular attack type, it will override the configured default attack detector.

Options

The following options are available:

- **attack-detector** — The attack detector being configured; in this case, the default attack detector.
- **protocol** — Defines the protocol to which the default attack detector applies.
- **attack-direction** — Defines whether the default attack detector applies to single sided or dual sided attacks.
- **destination port** {TCP and UDP protocols only} — Defines whether the default attack detector applies to port-based or port-less detections.
- **side** — Defines whether the default attack detector applies to attacks originating at the subscriber or network side.
- **action** — Default action:
 - **report** (default) — Report beginning and end of the attack by writing to the attack-log.
 - **block** — Block all further flows that are part of this attack, the SCE platform drops the packets.

- **Thresholds:**
 - **open-flows-rate** — Default threshold for rate of open flows. **suspected-flows-rate** — Default threshold for rate of suspected DDoS flows.
 - **suspected-flows-ratio** — Default threshold for ratio of suspected flow rate to open flow rate.
- Use the appropriate keyword to enable or disable subscriber notification by default:
 - **notify-subscriber** — Enable subscriber notification.
 - **don't-notify-subscriber** — Disable subscriber notification.
- Use the appropriate keyword to enable or disable sending an SNMP trap by default:
 - **alarm** — Enable sending an SNMP trap.
 - **no-alarm** — Disable sending an SNMP trap.

How to Define the Default Action and Optionally the Default Thresholds

Defaults

The default values for the default attack detector are:

- Action — Report
- Thresholds — Varies according to the attack type
- Subscriber notification — Disabled
- Sending an SNMP trap — Disabled

Step 1 From the SCE(config if)# prompt, type **attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) [action (report|block)] [open-flows-rate *number* suspected-flows-rate *rate* suspected-flows-ratio *ratio*]** and press **Enter**.

Configures the default attack detector for the defined attack type.

Step 2 From the SCE(config if)# prompt, type **attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) (notify-subscriber|don't-notify-subscriber)** and press **Enter**.

Enables or disables subscriber notification by default for the defined attack type.

The attack type must be defined the same as in Step 1.

Step 3 From the SCE(config if)# prompt, type **attack-detector default protocol (((TCP|UDP) [dest-port (specific|not- specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) (alarm|no-alarm)** and press **Enter**.

Enables or disables sending an SNMP trap by default for the defined attack type.

The attack type must be defined the same as in Step 1.

How to Reinstate the System Defaults for a Selected Set of Attack Types

Use the following command to delete user-defined default values for action, thresholds, subscriber notification, and sending an SNMP trap for a selected set of attack types, and reinstate the system defaults.

-
- Step 1** From the SCE(config if)# prompt, type **default attack-detector default protocol (((TCP|UDP) [dest-port (specific|not-specific|both)])|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both)** and press **Enter**.

Reinstates the system defaults for the defined attack types.

How to Reinstate the System Defaults for All Attack Types

-
- Step 1** From the SCE(config if)# prompt, type **default attack-detector default** and press **Enter**.

Reinstates the system defaults for the defined attack types.

Specific Attack Detectors

Use these commands to define thresholds, actions, subscriber notification setting, and sending an SNMP trap for a specific attack detector for selected set of attack types.

- [Options, page 11-13](#)
- [How to Enable a Specific Attack Detector and Assign it an ACL, page 11-14](#)
- [How to Define the Action and Optionally the Thresholds for a Specific Attack Detector, page 11-14](#)
- [How to Define the Subscriber Notification Setting for a Specific Attack Detector, page 11-14](#)
- [How to Define the SNMP Trap Setting for a Specific Attack Detector, page 11-14](#)
- [How to Define the List of Destination Ports for TCP or UDP Protocols for a Specific Attack Detector, page 11-15](#)
- [How to Delete User-Defined Values, page 11-15](#)
- [How to Disable a Specific Attack Detector, page 11-15](#)
- [How to Disable All Non-default Attack Detectors, page 11-15](#)
- [How to Disable All Attack Detectors, page 11-16](#)

Options

A specific attack detector may be configured for each possible combination of protocol, attack direction, and side. The SCE platform supports a maximum of 100 attack detectors. Each attack detector is identified by a number (1-100). Each detector can be either disabled (default) or enabled. An enabled attack detector must be configured with the following parameters:

- **access-list** — The number of the Access-Control List (ACL) associated with the specified attack detector. The ACL identifies the IP addresses selected by this detector. (See Access Control Lists.)
 - For dual-ip detections, the destination IP address is used for matching with the ACL.
 - Use the "none" keyword to indicate that all IP addresses are permitted by this attack-detector.

This option is useful when using the command to define a port list, and the desired configuration should be set for all IP addresses.

- **comment** — For documentation purposes.

In addition, an enabled attack detector may contain the following settings:

- **TCP-port-list/UDP-port-list** — Destination port list for the specified protocol. TCP and UDP protocols may be configured for specified ports only. This is the list of specified destination ports per protocol.

Up to 15 different TCP port numbers and 15 different UDP port numbers can be specified.

Configuring a TCP/UDP port list for a given attack detector affects only attack types that have the same protocol (TCP/UDP) and are port-based (i.e. detect a specific destination port). Settings for other attack types are not affected by the configured port list(s).

The following settings are configurable for each attack type in each attack detector. Each setting can either be in a 'not configured' state (which is the default), or be configured with a specific value.

- **action** — action:
 - **report** (default) — Report beginning and end of the attack by writing to the attack-log.
 - **block** — Block all further flows that are part of this attack, the SCE platform drops the packets.
- **Thresholds:**
 - **open-flows-rate** — Default threshold for rate of open flows. **suspected-flows-rate** — Default threshold for rate of suspected DDoS flows.
 - **suspected-flows-ratio** — Default threshold for ratio of suspected flow rate to open flow rate.
- Use the appropriate keyword to enable or disable subscriber notification by default:
 - **notify-subscriber** — Enable subscriber notification.
 - **don't-notify-subscriber** — Disable subscriber notification.
- Use the appropriate keyword to enable or disable sending an SNMP trap by default:
 - **alarm** — Enable sending an SNMP trap.
 - **no-alarm** — Disable sending an SNMP trap.

How to Enable a Specific Attack Detector and Assign it an ACL

- Step 1** From the SCE(config if)# prompt, type **attack-detector** *number* **access-list** (*aclnumber* |none) [**comment** *comment*] and press **Enter**.

Enables the attack detector and assigns it the specified ACL.

How to Define the Action and Optionally the Thresholds for a Specific Attack Detector

- Step 1** From the SCE(config if)# prompt, type **attack-detector** *number* **protocol** (((TCP|UDP) [**dest-port** (specific|not- specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (subscriber|network|both) [**action** (report|block)] [**open-flows-rate** *number* **suspected-flows-rate** *rate* **suspected-flows-ratio** *ratio*] and press **Enter**.

Defines the action of the specified attack detector

How to Define the Subscriber Notification Setting for a Specific Attack Detector

Use the following command to set the subscriber notification setting for a given attack detector and selected set of attack types.

- Step 1** From the SCE(config if)# prompt, type **attack-detector** *number* **protocol** (((TCP|UDP) [**dest-port** (specific|not- specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (subscriber|network|both) (**notify-subscriber**|don't-notify-subscriber) and press **Enter**.

Defines the subscriber notification setting for the specified attack detector

How to Define the SNMP Trap Setting for a Specific Attack Detector

Use the following command to enable or disable sending an SNMP trap for a given attack detector and selected set of attack types.

- Step 1** From the SCE(config if)# prompt, type **attack-detector** *number* **protocol** (((TCP|UDP) [**dest-port** (specific|not- specific|both)])|ICMP|other|all) **attack-direction** (single-side-source|single-side-destination|single-side-both|dual-sided|all) **side** (subscriber|network|both) (**alarm**|no-alarm) and press **Enter**.

Defines the SNMP trap setting for the specified attack detector.

How to Define the List of Destination Ports for TCP or UDP Protocols for a Specific Attack Detector

Use the following command to define the list of destination ports for specific port detections for TCP or UDP protocols.

-
- Step 1** From the SCE(config if)# prompt, type **attack-detector** *number* **TCP-port-list|UDP-port-list** (**all|**(*port1* [, *port2*, *port3*...]) and press **Enter**.
Defines the port list for the specified protocol and attack detector.
-

How to Delete User-Defined Values

Use the following command to remove settings of action, thresholds, subscriber notification, and sending an SNMP trap for a specific attack detector and selected set of attack types.

Removing these settings for a given attack type restores them to the default 'not configured' state, which means that the attack detector does not take part in determining the response for attacks of this attack type.

-
- Step 1** From the SCE(config if)# prompt, type **default attack-detector** *number* **protocol** (((**TCP|UDP**) [**dest-port** (**specific|not-specific|both**)])|**ICMP|other**|**all**) **attack-direction** (**single-side-source|single-side-destination|single-side-both|dual-sided**|**all**) **side** (**subscriber|network|both**) and press **Enter**.
Deletes the configured attack detector settings for the specified attack type.
-

How to Disable a Specific Attack Detector

Use the following command to disable a specific attack detector, configuring it to use the default action, threshold values and subscriber notification for all protocols, attack directions and sides.

-
- Step 1** From the SCE(config if)# prompt, type **default attack-detector** *number* and press **Enter**.
Disables the specified attack detector.
-

How to Disable All Non-default Attack Detectors

Use the following command to disable all non-default attack detectors, configuring them to use the default values.

-
- Step 1** From the SCE(config if)# prompt, type **default attack-detector all-numbered** and press **Enter**.
Disables all non-default attack detectors.
-

How to Disable All Attack Detectors

Use the following command to disable all attack detectors, configuring them to use the default values.

-
- Step 1** From the SCE(config if)# prompt, type **default attack-detector all** and press **Enter**.
Disables all attack detectors.
-

Sample Attack Detector Configuration

The following configuration changes the default user threshold values used for detecting ICMP attacks, and configures an attack-detector with high thresholds for UDP attacks, preventing false detections of two DNS servers (10.1.1.10 and 10.1.1.13) as being attacked.

-
- Step 1** From the SCE(config)# prompt, type **interface linecard 0** and press **Enter**.
Enters linecard interface configuration mode
- Step 2** From the SCE(config if)# prompt, type **attack-detector default protocol ICMP attack-direction single-side-source side both action report open-flow-rate 1000 suspected-flows-rate 100 suspected-flows-ratio 10** and press **Enter**.
Configures the default ICMP threshold and action.
- Step 3** From the SCE(config if)# prompt, type **attack-detector 1 access-list 3 comment "DNS servers"** and press **Enter**.
Enables attack detector #1 and assigns ACL #3 to it.
- Step 4** From the SCE(config if)# prompt, type **attack-detector 1 UDP-ports-list 53**
Defines the list of UDP destination ports for attack detector #1 with one port, port 53
- Step 5** From the SCE(config if)# prompt, type **attack-detector 1 protocol UDP dest-port specific attack-direction single-side-destination side both action report open-flow-rate 1000000 suspected-flows-rate 1000000** and press **Enter**.
Defines the thresholds and action for attack detector #1.
- Step 6** From the SCE(config if)# prompt, type **attack-detector 1 protocol UDP dest-port specific attack-direction single-side-destination side subscriber notify-subscriber** and press **Enter**.
Enables subscriber notification for attack detector #1.
- Step 7** From the SCE(config if)# prompt, type **exit** and press **Enter**.
Exits the linecard interface configuration mode.
- Step 8** Configure ACL #3, which has been assigned to the attack detector.
- ```
SCE(config)# access-list 3 permit 10.1.1.10
SCE(config)# access-list 3 permit 10.1.1.13
```
-



# Subscriber Notifications

- [Configuring the Subscriber Notification Port, page 11-17](#)
- [How to Remove the Subscriber Notification Port, page 11-17](#)

Subscriber notification is a capability used- for notifying a subscriber in real-time about current attacks involving IP addresses mapped to that subscriber. Subscriber notification is configured on a per-attack-detector level, as explained above, and must also be enabled and configured by the application loaded to the SCE platform, as explained in the [Cisco Service Control Application for Broadband User Guide](#).

In the current solutions, the SCE Platform notifies the subscriber about the attack by redirecting HTTP flows originating from the subscriber to the service provider's server, that should notify the subscriber that he is under attack. This raises a question regarding TCP attacks originating from the subscriber that are configured with block action. Such attacks cannot normally be notified to the subscriber using HTTP redirection, since all HTTP flows originating from the subscriber are TCP flows, and they are therefore blocked along with all other attack flows. To enable effective use of HTTP redirect, there is a CLI command that prevents blocking of TCP flows originating from the subscriber to a specified TCP port, even when the above scenario occurs.

## Configuring the Subscriber Notification Port

You can define a port to be used as the subscriber notification port. The attack filter will never block TCP traffic from the subscriber side of the SCE platform to this port, leaving it always available for subscriber notification.

### Options

The following option is available:

- **portnumber** — the number of the port to be used as the subscriber notification port

---

**Step 1** From the SCE(config if)# prompt, type **attack-filter subscriber-notification ports portnumber** and press **Enter**.

---

## How to Remove the Subscriber Notification Port

---

**Step 1** From the SCE(config if)# prompt, type **no attack-filter subscriber-notification ports** and press **Enter**.

---

# Preventing and Forcing Attack Detection

- [Options, page 11-18](#)
- [Preventing Attack Filtering, page 11-19](#)
- [Forcing Attack Filtering, page 11-19](#)

After configuring the attack detectors, the SCE platform automatically detects attacks and handles them according to the configuration. However, there are scenarios in which a manual intervention is desired, either for debug purposes, or because it is not trivial to reconfigure the SCE platform attack-detectors properly. For example:

- The SCE platform has detected an attack, but the user knows this to be a false alarm. The proper action that should be taken by the user is to configure the system with higher thresholds (for the whole IP range, or maybe for specific IP addresses or ports). However, this might take time, and, if attack handling is specified as 'Block', the user may wish to stop the block action for this specific attack quickly, leaving the configuration changes for a future time when there is time to plan the needed changes properly.

Use the **dont-filter** command described below for this type of case.

- An ISP is informed that one of his subscribers is being attacked by a UDP attack from the network side. The ISP wants to protect the subscriber from this attack by blocking all UDP traffic to the subscriber, but unfortunately the SCE platform did not recognize the attack. (Alternatively, it could be that the attack was recognized, but the configured action was 'report' and not 'block').

Use the **force-filter** command described below for this type of case.

The user can use the CLI attack filtering commands to do the following:

- Configure a **dont-filter** command to prevent or stop filtering of an attack related to a specified IP address
- Configure a **force-filter** command to force filtering (with a specific action) of an attack related to a specified IP address

Use the following commands to either force or prevent attack filtering:

- [no] attack-filter dont-filter
- [no] attack-filter force-filter

## Options

In addition to the attack detector options described above, the following options are available:

- **ip-address** — the IP address for which to prevent attack filtering.  
If **attack -direction** is dual-sided, an IP address must be configured for both the source (*source-ip-address*) and the destination (*dest-ip-address*) sides.

## Preventing Attack Filtering

Attack filtering can be prevented for a specified IP address and attack type by executing a **dont-filter** CLI command. If filtering is already in process, it will be stopped. When attack filtering has been stopped, it remains stopped until explicitly restored by another CLI command (either **force-filter** or **no dont-filter**).

- [How to Configure a dont-filter Setting for a Specified Situation, page 11-19](#)
- [How to Remove a dont-filter Setting from a Specified Situation, page 11-19](#)
- [How to Remove All dont-filter Settings, page 11-19](#)

### How to Configure a dont-filter Setting for a Specified Situation

- 
- Step 1** From the SCE(config if)# prompt, type **attack-filter dont-filter protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip ip-address)|dual-sided source-ip source-ip-address destination-ip dest-ip-address)) side (subscriber|network|both)** and press **Enter**.
- 

### How to Remove a dont-filter Setting from a Specified Situation

- 
- Step 1** From the SCE(config if)# prompt, type **no attack-filter dont-filter protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip ip-address)|dual-sided source-ip source-ip-address destination-ip dest-ip-address)) side (subscriber|network|both)** and press **Enter**.
- 

### How to Remove All dont-filter Settings

- 
- Step 1** From the SCE(config if)# prompt, type **no attack-filter dont-filter all** and press **Enter**.
- 

## Forcing Attack Filtering

Attack filtering can be forced for a specified IP address/protocol. Forced attack filtering will continue until undone by an explicit CLI command (either **no force-filter** or **dont-filter**).

- [How to Configure a force-filter Setting for a Specified Situation, page 11-20](#)
- [How to Remove a force-filter Setting from a Specified Situation, page 11-20](#)
- [How to Remove All force-filter Settings, page 11-20](#)

## How to Configure a force-filter Setting for a Specified Situation

- 
- Step 1** From the SCE(config if)# prompt, type **attack-filter force-filter action (block|report) protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip ip-address)|dual-sided source-ip source-ip-address destination-ip dest-ip-address)) side (subscriber|network|both)[notify-subscriber]** and press **Enter**.
- 

## How to Remove a force-filter Setting from a Specified Situation

- 
- Step 1** From the SCE(config if)# prompt, type **no attack-filter force-filter protocol (((TCP|UDP) [dest-port (port-number |not-specific))|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) (ip ip-address)|dual-sided source-ip source-ip-address destination-ip dest-ip-address)) side (subscriber|network|both)** and press **Enter**.
- 

## How to Remove All force-filter Settings

- 
- Step 1** From the SCE(config if)# prompt, type **no attack-filter force-filter all** and press **Enter**.
- 

# Monitoring Attack Filtering

- [Monitoring Attack Filtering Using SNMP Traps, page 11-20](#)
- [Monitoring Attack Filtering Using CLI Commands, page 11-22](#)
- [Viewing the Attack Log, page 11-28](#)

There are three options for monitoring attack filtering and detection:

- CLI show commands
- SNMP attack detection traps
- Attack log

## Monitoring Attack Filtering Using SNMP Traps

The system sends a trap at the start of a specific attack detection event, and also when a specific detection event ends, as follows:

- **STARTED\_FILTERING** trap – String with the attack information
- **STOPPED\_FILTERING**
  - String with the attack information
  - String with the reason for stopping

The format of the attack-information string sent when an attack begins is:

- If attack was detected in the traffic:

```
Attack detected: Attack 'IP-info' from 'side' side, protocol 'protocol'. 'rate1' open
flows per second detected, 'rate2' Ddos-suspected flows per second detected. Action
is: 'action'.
```

- If attack was declared as a result of a **force-filter** command:

```
Attack Filter: Forced 'forced-action' 'IP-info' from 'side' side, protocol 'protocol'.
Attack forced using a force-filter command.
```

The format of the attack-information string sent when an attack ends is:

- If attack was detected in the traffic:

```
End-of-attack detected: Attack 'IP-info' from 'side' side, protocol 'protocol'. Action
is: 'action' Duration 'duration' seconds, 'total-flows' 'hw-filter'
```

- If the end of the attack was declared as a result of a **no force-filter** command or a new **don't-filter** command:

```
Attack Filter: Forced to end 'action2' 'IP-info' from 'side' side, protocol
'protocol'. Attack end forced using a 'no force-filter' or a 'don't-filter' command.
```

The format of the reason string sent when an attack begins is:

- If attack end was detected in the traffic:

```
Detected attack end
```

- If the end of the attack was declared as a result of a **no force-filter** command or a new **don't-filter** command:

```
Forced attack end
```

Following are the possible values that may appear in the fields indicated in the information strings ("):

- 'action'
  - Report
  - Block
- 'forced-action' is one of the following values, depending on the configured force-filter action.
  - block of flows
  - report
- 'IP-info' is in one of the following formats, depending on the direction of the attack, and whether one or two IP addresses were detected
  - from IP address A.B.C.D
  - on IP address A.B.C.D
  - from IP address A.B.C.D to IP address A.B.C.D
- 'side'
  - subscriber
  - network

- 'protocol'
  - TCP
  - UDP
  - ICMP
  - other
- 'rate1' and 'rate2' are numbers
- 'duration' is a number.
- 'total-flows' is one of the following strings, depending on the attack action:
  - If 'action' is block: 'number' flows blocked.
  - If 'action' is report: attack comprised of 'number' flows.
- 'hw-filter'
  - If the attack was not filtered by a hardware filter: empty string
  - If the attack was filtered by a hardware filter: HW filters used, actual attack duration is probably smaller than reported above, actual amount of flows handled is probably larger than reported above.

## Monitoring Attack Filtering Using CLI Commands

- [How to display a specified attack detector configuration, page 11-23](#)
- [How to display the default attack detector configuration, page 11-24](#)
- [How to display all attack detector configurations, page 11-25](#)
- [How to display filter state \(enabled or disabled\), page 11-25](#)
- [How to display configured threshold values and actions, page 11-25](#)
- [How to display the current counters, page 11-27](#)
- [How to display all currently handled attacks, page 11-27](#)
- [How to display all existing force-filter settings, page 11-27](#)
- [How to display all existing don't-filter settings, page 11-27](#)
- [How to display the list of ports selected for subscriber notification, page 11-27](#)
- [How to find out whether hardware attack filtering has been activated, page 11-28](#)

Use these commands to monitor attack detection and filtering:

- **show interface linecard 0 attack-detector**
- **show interface linecard 0 attack-filter**
- **show interface linecard 0 attack-filter query**
- **show interface linecard 0 attack-filter current-attacks**
- **show interface linecard 0 attack-filter don't-filter**
- **show interface linecard 0 attack-filter force-filter**
- **show interface linecard 0 attack-filter subscriber-notification ports**

## How to display a specified attack detector configuration

- [Options, page 11-23](#)
- [Example, page 11-23](#)

The following information is displayed:

- Protocol Side — Whether the attack detector applies to attacks originating at the subscriber or network side.
- Direction — Whether the attack detector applies to single sided or dual sided attacks. Action to take if an attack is detected.
- Thresholds:
  - open-flows-rate — Default threshold for rate of open flows (new open flows per second).
  - suspected-flows-rate — Default threshold for rate of suspected DDoS flows (new suspected flows per second).
  - suspected-flows-ratio — Default threshold for ratio of suspected flow rate to open flow rate.
- Subscriber notification — enabled or disabled.
- Alarm: sending an SNMP trap enabled or disabled.

### Options

The following option is available:

- **number** — the number of the attack detector to display

---

**Step 1** From the SCE> prompt, type **show interface linecard 0 attack-detector *number*** and press **Enter**.

---

### Example

```
SCE>show interface LineCard 0 attack-detector 1
Detector #1:
Comment: 'Sample'
Access-list: 1
Effective only for TCP port(s) 21,23,80
Effective for all UDP ports
Protocol|Side|Direction ||Action| Thresholds |Sub- |Alarm
 || || |Open flows|Ddos-Suspected flows|notif| |
 || || |rate |rate |ratio |
 || || |-----|-----|-----|-----|
TCP |net.|source-only| | | | | |
TCP |net.|dest-only | | | | | |
TCP |sub.|source-only| | | | | |
TCP |sub.|dest-only | | | | | |
TCP |net.|source+dest| | | | | |
TCP |sub.|source+dest| | | | | |
TCP+port |net.|source-only|Block| | | | |Yes
TCP+port |net.|dest-only | | | | | |
TCP+port |sub.|source-only|Block| | | | |Yes
TCP+port |sub.|dest-only | | | | | |
TCP+port |net.|source+dest| | | | | |
TCP+port |sub.|source+dest| | | | | |
UDP |net.|source-only| | | | | |
UDP |net.|dest-only | | | | | |
UDP |sub.|source-only| | | | | |
UDP |sub.|dest-only | | | | | |
```

|          |      |             |  |  |  |  |     |  |
|----------|------|-------------|--|--|--|--|-----|--|
| UDP      | net. | source+dest |  |  |  |  |     |  |
| UDP      | sub. | source+dest |  |  |  |  |     |  |
| UDP+port | net. | source-only |  |  |  |  |     |  |
| UDP+port | net. | dest-only   |  |  |  |  |     |  |
| UDP+port | sub. | source-only |  |  |  |  |     |  |
| UDP+port | sub. | dest-only   |  |  |  |  |     |  |
| UDP+port | net. | source+dest |  |  |  |  |     |  |
| UDP+port | sub. | source+dest |  |  |  |  |     |  |
| ICMP     | net. | source-only |  |  |  |  |     |  |
| ICMP     | net. | dest-only   |  |  |  |  |     |  |
| ICMP     | sub. | source-only |  |  |  |  | Yes |  |
| ICMP     | sub. | dest-only   |  |  |  |  |     |  |
| other    | net. | source-only |  |  |  |  |     |  |
| other    | net. | dest-only   |  |  |  |  |     |  |
| other    | sub. | source-only |  |  |  |  |     |  |
| other    | sub. | dest-only   |  |  |  |  |     |  |

Empty fields indicate that no value is set and configuration from the default attack detector is used.

SCE#>

## How to display the default attack detector configuration

**Step 1** From the SCE> prompt, type **show interface linecard 0 attack-detector default** and press **Enter**.

### Example

SCE>show interface LineCard 0 attack-detector default

Default detector:

| Protocol | Side | Direction   | Action | Thresholds         |                              |       | Sub-  | Alarm |
|----------|------|-------------|--------|--------------------|------------------------------|-------|-------|-------|
|          |      |             |        | Open flows<br>rate | Ddos-Suspected flows<br>rate | ratio | notif |       |
| -----    | ---- | -----       | -----  | -----              | -----                        | ----- | ----- | ----- |
| TCP      | net. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| TCP      | net. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| TCP      | sub. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| TCP      | sub. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| TCP      | net. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| TCP      | sub. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| TCP+port | net. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| TCP+port | net. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| TCP+port | sub. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| TCP+port | sub. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| TCP+port | net. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| TCP+port | sub. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| UDP      | net. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| UDP      | net. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| UDP      | sub. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| UDP      | sub. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| UDP      | net. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| UDP      | sub. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| UDP+port | net. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| UDP+port | net. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| UDP+port | sub. | source-only | Report | 1000               | 500                          | 50    | No    | No    |
| UDP+port | sub. | dest-only   | Report | 1000               | 500                          | 50    | No    | No    |
| UDP+port | net. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| UDP+port | sub. | source+dest | Report | 100                | 50                           | 50    | No    | No    |
| ICMP     | net. | source-only | Report | 500                | 250                          | 50    | No    | No    |
| ICMP     | net. | dest-only   | Report | 500                | 250                          | 50    | No    | No    |
| ICMP     | sub. | source-only | Report | 500                | 250                          | 50    | No    | No    |
| ICMP     | sub. | dest-only   | Report | 500                | 250                          | 50    | No    | No    |



```

other |net.|source-only|Report| 500| 250|50| No| No
other |net.|dest-only ||Report| 500| 250|50| No| No
other |sub.|source-only|Report| 500| 250|50| No| No
other |sub.|dest-only ||Report| 500| 250|50| No| No
SCE#>

```

## How to display all attack detector configurations

**Step 1** From the SCE> prompt, type **show interface linecard 0 attack-detector all** and press **Enter**.

## How to display filter state (enabled or disabled)

**Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter** and press **Enter**.

### Example

```

SCE>show interface LineCard 0 attack-filter
Enabled state:

```

```

Protocol	Direction	State
TCP |source-only|enabled
TCP |dest-only |enabled
TCP |dest+source|enabled
TCP+port |source-only|enabled
TCP+port |dest-only |enabled
TCP+port |dest+source|enabled
UDP |source-only|enabled
UDP |dest-only |enabled
UDP |dest+source|enabled
UDP+port |source-only|enabled
UDP+port |dest-only |enabled
UDP+port |dest+source|enabled
ICMP |source-only|enabled
ICMP |dest-only |enabled
other |source-only|enabled
other |dest-only |enabled
SCE#>

```

## How to display configured threshold values and actions

Use this command to display the configured threshold values and actions a specified IP address (and port), taking into account the various specific attack detector access list configurations

### Options

In addition to the attack detector options described above, the following options are available:

- **ip-address** — the IP address for which to display information.  
If **attack -direction** is dual-sided, an IP address must be configured for both the source (*source-ip-address*) and the destination (*dest-ip-address*) sides.
- **portnumber** — the port number for which to display information.

- Step 1** From the SCE#> prompt, type **show interface linecard 0 attack-filter query ((single-sided ip ip-address)|(dual-sided source-IP source-ip-address destination-IP dest-ip-address)) [dest-port portnumber] configured** and press **Enter**.

## Examples

### Example 1

This example shows a query for a single IP address.

```
SCE#>show interface linecard 0 attack-filter query single-sided ip 10.1.1.1 configured
```

| Protocol | Side | Dir. | Action | Thresholds         |                    |                | don't-<br>filter | force-<br>filter | Sub-<br>notif | Alarm |
|----------|------|------|--------|--------------------|--------------------|----------------|------------------|------------------|---------------|-------|
|          |      |      |        | Open flows<br>rate | Ddos-Susp.<br>rate | flows<br>ratio |                  |                  |               |       |
| TCP      | net. | src. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| TCP      | net. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| TCP      | sub. | src. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| TCP      | sub. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP      | net. | src. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP      | net. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP      | sub. | src. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP      | sub. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| ICMP     | net. | src. | Report | 500                | 250                | 50             | No               | No               | No            | No    |
| ICMP     | net. | dst. | Report | 500                | 250                | 50             | No               | No               | No            | No    |
| ICMP     | sub. | src. | Report | 500                | 250                | 50             | No               | No               | Yes           | No    |
| (1)      |      |      |        |                    |                    |                |                  |                  |               |       |
| ICMP     | sub. | dst. | Report | 500                | 250                | 50             | No               | No               | No            | No    |
| other    | net. | src. | Report | 500                | 250                | 50             | No               | No               | No            | No    |
| other    | net. | dst. | Report | 500                | 250                | 50             | No               | No               | No            | No    |
| other    | sub. | src. | Report | 500                | 250                | 50             | No               | No               | No            | No    |
| other    | sub. | dst. | Report | 500                | 250                | 50             | No               | No               | No            | No    |

(N) below a value means that the value is set through attack-detector #N.  
SCE#>

### Example 2

This example shows a query for a single IP address, with a specified port.

```
SCE#>show interface linecard 0 attack-filter query single-sided ip 10.1.1.1 dest-port 21 configured
```

| Protocol | Side | Dir. | Action | Thresholds         |                    |                | don't-<br>filter | force-<br>filter | Sub-<br>notif | Alarm |
|----------|------|------|--------|--------------------|--------------------|----------------|------------------|------------------|---------------|-------|
|          |      |      |        | Open flows<br>rate | Ddos-Susp.<br>rate | flows<br>ratio |                  |                  |               |       |
| TCP+port | net. | src. | Block  | 1000               | 500                | 50             | No               | No               | No            | Yes   |
| (1)      |      |      |        |                    |                    |                |                  |                  |               |       |
| TCP+port | net. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| TCP+port | sub. | src. | Block  | 1000               | 500                | 50             | No               | No               | No            | Yes   |
| (1)      |      |      |        |                    |                    |                |                  |                  |               |       |
| TCP+port | sub. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP+port | net. | src. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP+port | net. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP+port | sub. | src. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |
| UDP+port | sub. | dst. | Report | 1000               | 500                | 50             | No               | No               | No            | No    |

(N) below a value means that the value is set through attack-detector #N.  
SCE#>

## How to display the current counters

Use this command to display the current counters for the specified attack detector for attack types for a specified IP address.

- 
- Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter query ((single-sided ip ip-address)|(dual-sided source-IP source-ip-address destination-IP dest-ip-address)) [dest-port portnumber] current** and press **Enter**.
- 

## How to display all currently handled attacks

- 
- Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter current-attacks** and press **Enter**.
- 

## How to display all existing force-filter settings

- 
- Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter force-filter** and press **Enter**.
- 

## How to display all existing don't-filter settings

- 
- Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter dont-filter** and press **Enter**.
- 

## How to display the list of ports selected for subscriber notification

- 
- Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter subscriber-notification ports** and press **Enter**.
-

## How to find out whether hardware attack filtering has been activated

- Step 1** From the SCE> prompt, type **show interface linecard 0 attack-filter current-attacks** and press **Enter**. In the output from this command, look for the "HW-filter" field. If this field is "yes", the user must take into account the probable inaccuracies in the attack reporting.

This information also appears in the attack log file.

```

---|-----|-----|-----|-----|-----|-----|
---|Source IP -----|Side / |Open rate / |Handled |Action|HW- |force-
---| Dest IP|Protocol |Susp. rate | flows / | |filter|filter
---		Duration				
10.1.1.1	Subscriber	523	4045	Report	No	No
	*TCP	0	9			
---|-----|-----|-----|-----|-----|-----|

```

## Viewing the Attack Log

- [The Attack Log, page 11-28](#)
- [How to View the Attack Log, page 11-29](#)
- [How to Copy the Attack Log to a File, page 11-29](#)

## The Attack Log

The attack-log contains a message for each specific-IP detection of attack beginning and attack end. Messages are in CSV format.

The message for detecting attack beginning contains the following data:

- IP address (Pair of addresses, if detected)
- Protocol Port number (If detected)
- Attack-direction (Attack-source or Attack-destination)
- Interface of IP address (subscriber or network)
- Open-flows-rate, suspected-flows-rate and suspected-flows-ratio at the time of attack detection
- Threshold values for the detection
- Action taken

The message for detecting attack end contains the following data:

- IP address (Pair of addresses, if detected)
- Protocol Port number (If detected)
- Attack-direction (Attack-source or Attack-destination)

- Interface of IP address
- Number of attack flows reported/blocked
- Action taken

As with other log files, there are two attack log files. Attack events are written to one of these files until it reaches maximum capacity, at which point the events logged in that file are then temporarily archived. New attack events are then automatically logged to the alternate log file. When the second log file reaches maximum capacity, the system then reverts to logging events to the first log file, thus overwriting the temporarily archived information stored in that file.

The following SNMP trap indicates that the attack log is full and a new log file has been opened  
ST\_LINE\_ATTACK\_LOG\_IS\_FULL

**Note**

When the attack log is large, it is not recommended to display it. Copy a large log to a file to view it.

## How to View the Attack Log

- 
- Step 1** From the SCE# prompt, type **more line-attack-log** and press **Enter**.
- 

## How to Copy the Attack Log to a File

- 
- Step 1** From the SCE# prompt, type **more line-attack-log redirect *filename*** and press **Enter**.  
Writes the log information to the specified file.
-

