



CHAPTER 5

Configuring Zone Filters

This chapter describes how to configure the zone filters that process the zone traffic on the Cisco Traffic Anomaly Detector Module (Detector module).

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the *Cisco Anomaly Guard Module Configuration Guide* or the *Cisco Guard Configuration Guide*.

This chapter contains the following sections:

- [Understanding Zone Filters](#)
- [Managing Bypass Filters](#)
- [Managing Flex-Content Filters](#)
- [Managing User Filters for GUARD Zones](#)

Understanding Zone Filters

The Detector module uses zone filters to manage traffic flow when protecting the zone or learning the zone traffic characteristics. Zone filters enable the Detector module to perform the following functions:

- Analyze zone traffic for anomalies
- Bypass the Detector module anomaly detection features

You can configure a set of zone filters that provide the Detector module with zone-specific rules for traffic management and Distributed Denial of Service (DDoS) attack anomaly detection. When you modify the configuration of a zone filter, the change is saved to the zone configuration and takes effect immediately.

The Detector module uses the following types of filters:

- Bypass filters—Prevent the Detector module from handling specific traffic flows. You can prevent the Detector module from analyzing trusted traffic by directing the traffic away from the Detector module anomaly detection features.
- Flex-content filters—Count a specific traffic flow that can filter according to fields in the IP and TCP headers, the payload content, and complex Boolean expressions.
- Dynamic filters—Apply the required protection level to the specified traffic flow. The Detector module creates dynamic filters based on the analysis of traffic flow and continuously modifies this set of filters to zone traffic and the type of DDoS attack. The dynamic filters have a limited life span and are deleted when the attack ends.

If you create a zone with a GUARD zone template, the zone configuration contains a set of user filters. You can configure the user filters on the Detector module and then copy the zone configuration to a Guard. The user filters are used only by the Guard and apply a specific protection level to the traffic flow. Until the Guard has had enough time to analyze the attack, the user filters provide the first line of defense against the attack. Once the Guard analyzes the attack, it begins producing dynamic filters. When the Guard attempts to apply both a user filter and a dynamic filter to the traffic flow, it selects the filter with the more severe action.

Managing Bypass Filters

The bypass filter prevents the Detector module from analyzing specific traffic flows. You can configure a bypass filter to direct trusted traffic away from the Detector module anomaly detection features.

When you display the list of bypass filters in the following procedures, the Count column indicates the current bypass filter traffic rate, which is measured in packets per second (pps).

This section contains the following topics:

- [Adding a Bypass Filter](#)
- [Deleting a Bypass Filter](#)

Adding a Bypass Filter

To add a bypass filter, perform the following steps:

-
- Step 1** From the navigation pane, select a zone. The zone main menu appears.
 - Step 2** From the zone main menu, choose **Configuration > Filters > Bypass filters**. The Bypass Filters screen appears.
 - Step 3** Click **Add**. The Add Bypass Filters screen appears.
 - Step 4** Configure the parameters of the new bypass filter. [Table 5-1](#) describes the filter parameters listed in the Bypass Filter form.

Table 5-1 *Bypass Filter Parameters*

Parameter	Description
Source IP	Source IP address of the traffic that you want to bypass the Detector module anomaly detection features. To specify any source IP address, leave this field blank or enter an asterisk (*).
Source subnet	Source subnet of the traffic that you want to bypass the Detector module anomaly detection features. Choose the subnet from the Source subnet drop-down list.

Table 5-1 *Bypass Filter Parameters (continued)*

Parameter	Description
Protocol	Protocol of the traffic that you want to bypass the Detector module anomaly detection features. Enter the protocol number. To specify any protocol, leave this field blank or enter an asterisk (*).
Dst Port	Zone destination port of the traffic that you want to bypass the Detector module anomaly detection features. Enter the destination port number. To specify any source destination port, leave this field blank or enter an asterisk (*).
Fragments	Traffic type to be handled by the filter. From the Fragments drop-down list, choose one of the following options: <ul style="list-style-type: none"> • without—Bypass filter processes nonfragmented traffic. • with—Bypass filter processes fragmented traffic. • *—Bypass filter processes both fragmented and nonfragmented traffic.

Step 5 Choose one of the following options:

- **OK**—Saves the new bypass filter configuration. The Bypass Filters screen appears. If the zone was created using a Guard zone template, the bypass filter is added to both the Guard and the Detector module portion of the configuration files.
- **Cancel**—Exits the Bypass Filters form without saving any information. The Bypass filters screen appears.

Deleting a Bypass Filter

To delete a bypass filter, perform the following steps:

- Step 1** From the navigation pane, choose a zone. The zone main menu appears.
- Step 2** From the zone main menu, choose **Configuration > Filters > Bypass filters**. The Bypass Filters screen appears.

Step 3 Check the check box next to each bypass filter that you want to delete and then click **Delete**. The bypass filter is deleted from the list of filters. To delete all the bypass filters listed, check the check box next to Src IP and then click **Delete**.

If you created the zone using a Guard zone template, the bypass filter is deleted from both the Guard and the Detector module portion of the configuration files.

Managing Flex-Content Filters

Flex-content filters filter zone traffic based on fields in the packet header or patterns in the packet payload. You can identify attacks that are based on patterns that appear in the incoming traffic. These patterns can identify known worms or flood attacks that have a constant pattern.



Note

A flex-content filter consumes a lot of CPU resources. We recommend that you limit the use of flex-content filters because they might affect the performance of the Detector module. If you are using a flex-content filter to monitor a specific attack that can be identified by a dynamic filter, such as TCP traffic to a specified port, we recommend that you filter the traffic using a dynamic filter.

The flex-content filter is a combination of a Berkley Packet Filter and a pattern filter with very selective filtering capabilities. Use the flex-content filters to count a desired packet flow and to identify a specific malicious source of traffic.

The flex-content filter applies the filtering criteria in the following order:

1. Filters packets based on the protocol and the port parameter values.
2. Filters packets based on the expression value.
3. Performs pattern matching with the pattern value on the remaining packets.

This section contains the following topics:

- [Understanding the Flex-Content Expression Syntax](#)
- [Understanding the Flex-Content Filter Pattern Syntax](#)
- [Adding a Flex-Content Filter](#)
- [Deleting a Flex-Content Filter](#)

Understanding the Flex-Content Expression Syntax

The `tcpdump-expression` is in the Berkley Packet Filter format and specifies the expression to be matched with the packet.



Note

You can use the `tcpdump-expression` to filter traffic based on the destination port and protocol. However, for network performance considerations, we recommend that you filter traffic based on these criteria using the flex-content filter `protocol` and `port` arguments.

The expression contains one or more elements. Elements usually consist of an ID (name or number) preceded by one or more qualifiers.

There are three types of qualifiers:

- **Type qualifiers**—Define the ID (name or number). Possible types are **host**, **net**, and **port**. The **host** type qualifier is the default.
- **Direction qualifiers**—Define the transfer direction. Possible directions are **src**, **dst**, **src or dst**, and **src and dst**. The direction qualifier **src or dst** is the default.
- **Protocol qualifiers**—Restrict the match to a particular protocol. Possible protocols are **ether**, **ip**, **arp**, **rarp**, **tcp**, and **udp**. If you do not specify a protocol qualifier, all protocols that apply to the type are matched. For example, port 53 means TCP or UDP port 53.

Table 5-2 describes the flex-content filter expression elements.

Table 5-2 Flex-Content Filter Expression Elements

Parameter	Description
dst host <i>host_ip_address</i>	Traffic to a destination host IP address.
src host <i>host_ip_address</i>	Traffic from a source host IP address.
host <i>host_ip_address</i>	Traffic to and from both source and destination host IP addresses.
net net mask <i>mask</i>	Traffic to a specific network.
net <i>net/len</i>	Traffic to a specific subnet.

Table 5-2 Flex-Content Filter Expression Elements (continued)

Parameter	Description
dst port <i>destination_port_number</i>	TCP or UDP traffic to a destination port number.
src port <i>source_port_number</i>	TCP or UDP traffic from a source port number.
port <i>port_number</i>	TCP or UDP traffic to and from both source and destination port numbers.
less <i>packet_length</i>	Packets with a length equal to or less than the specific length in bytes.
greater <i>packet_length</i>	Packets with a length equal to or greater than the specific length in bytes.
ip proto <i>protocol</i>	Packets with a protocol number of the following protocols: ICMP, UDP, and TCP.
ip broadcast	Broadcast IP packets.
ip multicast	Multicast packets.
ether proto <i>protocol</i>	Ether protocol packets of a specific protocol number or name such as IP, Address Resolution Protocol (ARP), or Reverse Address Resolution Protocol (RARP). The protocol names are also keywords. If you enter the protocol name, you must use a backslash (\) as an escape character before the name.
<i>expr relop expr</i>	Traffic that complies with the specific expression. Table 5-3 describes the tcpdump-expression rules.

Table 5-3 describes the tcpdump-expression rules.

Table 5-3 Flex-Content Filter Expression Rules

Expression Rule	Description
<i>relop</i>	>, <, >=, <=, =, !=
<i>expr</i>	Arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+ , - , * , / , & ,], a length operator, and special packet data accesses. To access data inside the packet, use the following syntax: <i>proto [expr: size]</i>
<i>proto</i>	Protocol layer for the index operation. The possible values are ether, ip, tcp, udp, or icmp. The byte offset, relative to the indicated protocol layer, is given by the <i>expr</i> value. To access data inside the packet, use the following syntax: <i>proto [expr: size]</i> The <i>size</i> argument is optional and indicates the number of bytes in the field. The argument can be 1, 2, or 4. The default is 1.

You can combine primitives using the following methods:

- A parenthesized group of primitives and operators (parentheses are special to the Shell and must be escaped)
- Negation—Use **!** or **not**
- Concatenation—Use **&&** or **and**
- Alternation—Use **||** or **or**

Negation has the highest precedence. Alternation and concatenation have equal precedence and are associated left to right. Explicit **and** tokens, not juxtaposition, are required for concatenation. If you specify an identifier without a keyword, the most recent keyword is used.

For a detailed explanation on the Berkley Packet filter configuration options, go to this website:

<http://www.freesoft.org/CIE/Topics/56.htm>

The following example shows how to count only the unfragmented datagram and fragment zero of fragmented datagrams. This filter is implicitly applied to the TCP and UDP index operations. For instance, `tcp[0]` always indicates the first byte of the TCP header and never indicates the first byte of an intervening fragment:

```
ip[6:2]&0x1fff=0
```

The following example shows how to drop all TCP RST packets:

```
tcp[13]&4!=0
```

The following example shows how to count all ICMP packets that are not echo requests/echo reply (ping):

```
"icmp [0]!=8 and icmp[0] != 0"
```

The following example shows how to count all TCP packets destined to port 80 that did not originate from port 1000:

```
"tcp and dst port 80 and not src port 1000"
```

Understanding the Flex-Content Filter Pattern Syntax

The pattern syntax is a regular expression that describes a string of characters. The pattern describes a set of strings without actually listing its elements. This expression is made up of normal characters and special characters. Normal characters include all printable ASCII characters that are not considered as special characters. Special characters are characters that have a special meaning and specify the type of matching that the Detector module performs on the pattern expression. The flex-content filter matches the pattern expression with the content of the packet (the packet payload). For example, the three strings *version 3.1*, *version 4.0*, and *version 5.2* are described by the following pattern: *version .*\.**

Table 5-4 describes the special characters that you can use.

Table 5-4 Flex-Content Pattern Field Descriptions

Special character	Description
.*	Matches a string that may be present and can contain zero or more characters. For example, the pattern <i>goo.*s</i> matches <i>goos</i> , <i>goods</i> , <i>good for ddos</i> , and so on.
\	Removes the special meaning of a special character. To use the special characters in this list as single-character patterns, remove the special meaning by preceding each character with a backslash (\). For example, two backslashes (\\) match one backslash (\), and one backslash and a period (\.) match one period (.). You must also precede an asterisk (*) with a backslash.
\xHH	Matches a hexadecimal value where H is a hexadecimal digit and is not case sensitive. Hexadecimal values must be exactly two digits. For example, the pattern \x41 matches the hexadecimal value A.

The following example shows how to drop packets with a specific pattern in the packet payload. The pattern in the example was extracted from the Slammer worm. The protocol, port, and tcpdump-expression are nonspecific.

```
\x89\xE5Qh\ .dllhel32hkernQhounthickChGetTf\xB911
Qh32\ .dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

Adding a Flex-Content Filter

To add a flex-content filter, perform the following steps:

- Step 1** From the navigation pane, choose a zone. The zone main menu appears.
- Step 2** From the zone main menu, choose **Configuration > Filters > Flex-Content filters**. The Flex-Content Filters screen appears and displays the list of existing flex-content filters.
- Step 3** Click **Add**. The Add Filter Step 2 screen appears.

Step 4 Configure the flex-content filter parameters.

[Table 5-5](#) describes the filter parameters listed in the Flex-Content Filter form.

Table 5-5 Flex-Content Filter Parameters

Parameter	Description
Description	Provides a description for the flex-content filter.
Protocol	Processes traffic using a specific protocol. Enter a protocol number from 0 to 255. To specify any protocol type, enter an asterisk (*). Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid protocol numbers: http://www.iana.org/assignments/protocol-numbers
Dst Port	Processes traffic that flows to a specific destination port. Enter a destination port number from 0 to 65535. To specify any destination port, enter an asterisk (*). Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid port numbers: http://www.iana.org/assignments/port-numbers
Expression	Filters traffic based on the specified expression (see the “ Understanding the Flex-Content Expression Syntax ” section). Enter a string with up to 180 space-separated tokens.
Pattern	Specifies the regular expression data pattern that is to be matched with the packet content (see the “ Understanding the Flex-Content Filter Pattern Syntax ” section). Enter the data pattern to use.
Match Case	Specifies whether or not the data pattern expression is case sensitive. Check the check box to define the data pattern expression as case sensitive.
Start Offset	Specifies the offset (in bytes) from the beginning of the packet content where the pattern matching begins. The default is 0, which is the start of the payload. The start offset applies to the pattern field. Enter an integer from 0 to 2047.

Table 5-5 Flex-Content Filter Parameters (continued)

Parameter	Description
End Offset	Specifies the offset (in bytes) from the beginning of the packet content where the pattern matching ends. The default is the packet length, which is the end of the payload. The end offset applies to the pattern field. Enter an integer from 0 to 2047.
Action	Specifies the action that the Detector module performs when the traffic matches the filter. The Detector module supports the count action only, which enables it to count the traffic flow packets that match the filter.
Guard Action	Specifies the action that the Guard performs when the traffic matches the filter. The Guard Action field is applicable only if you created the zone using a GUARD zone template. Choose one of the following actions from the Guard Action drop-down list: <ul style="list-style-type: none"> count—Counts the traffic flow packets that match the filter drop—Drops the traffic flow packets that match the filter
State	Specifies the operating state of the flex-content filter. Choose one of the following operating states from the State drop-down list: <ul style="list-style-type: none"> enable—The Detector module applies the filter to the traffic flow and executes the configured action on the flow that matches the filter. disable—The Detector module does not apply the filter to the traffic flow.

Step 5 Choose one of the following options:

- **OK**—Saves the new flex-content filter. The Flex-Content Filters screen appears. If the zone was created using a Guard zone template, the flex-content filter is added to both the Guard and the Detector module portion of the configuration files.

- **Clear**—Reverts the form information back to the default values and clears any information that you added.
 - **Cancel**—Exits the Flex-Content Filters screen without saving any information. The Flex-Content Filters screen appears.
-

Deleting a Flex-Content Filter

To delete a flex-content filter, perform the following steps:

- Step 1** From the navigation pane, choose a zone. The zone main menu appears.
- Step 2** From the zone main menu, choose **Configuration > Filters > Flex-Content filters**. The Flex-Content Filters screen appears and displays the list of existing flex-content filters.
- Step 3** Check the check box next to each flex-content filter that you want to delete and then click **Delete**. The flex-content filter is deleted. To delete all the flex-content filters listed, click the check box next to Src IP, and then click **Delete**.

If the zone was created using a Guard zone template, the flex-content filter is deleted from both the Guard and the Detector module portion of the configuration files.

Managing User Filters for GUARD Zones

You can only configure user filters for zones that you create using a GUARD zone template because user filters are used by the Guard only. When you create a zone using a GUARD zone template, you can configure the user filters on the Detector module and then copy the zone configuration to a Guard.

The Guard activates user filters in the order in which they appear in the user filter list. User filters are activated in an ascending row-number order. When you add a new user filter, it is important that you place it in the desired location in the list.

To verify that a zone was created from a GUARD zone template, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone. The zone main menu appears.
 - Step 2** From the zone main menu, choose **Configuration > General**. Verify that the name of the zone template begins with GUARD.
-

This section contains the following topics:

- [Adding a User Filter](#)
- [Deleting a User Filter](#)

Adding a User Filter

To add a new user filter, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone that you created using a GUARD zone template. The zone main menu appears.
 - Step 2** From the zone main menu, choose **Configuration > Filter > User filters**. The list of user filters appears.
 - Step 3** Click **Add**. The Add Filter Step 1 screen appears with the list of user filters.
 - Step 4** In the Insert column, click the row below where you want to add the user filter. The Insert Here text appears, indicating that the new user filter will be inserted above the row that you selected.

- Step 5** Click **Next**. The Add Filter Step 2 screen appears with the User Filter form.
- Step 6** Configure the parameters of the new user filter. [Table 5-6](#) describes the filter parameters listed in the User Filter form.

Table 5-6 *User Filter Parameters*

Parameter	Description
Source IP	Directs traffic from a specific IP address to the user filter. Enter the source IP address. To specify any source IP address, leave this field blank or enter an asterisk (*).
Source subnet	Directs traffic from a specific subnet to the user filter. Choose the subnet from the Source subnet drop-down list.
Protocol	Directs traffic from a specific protocol to the user filter. Enter the protocol number. To specify any protocol, leave this field blank or enter an asterisk (*).
Dst Port	Directs traffic destined to a specific port to the user filter. Enter the destination port number. To specify any destination port, leave this field blank or enter an asterisk (*).
Fragments	Specifies the traffic type to be processed by the user filter. From the Fragments drop-down list, choose one of the following: <ul style="list-style-type: none"> without—User filter processes nonfragmented traffic. with—User filter processes fragmented traffic. *—User filter processes fragmented and nonfragmented traffic.
Rate	Specifies the rate limitation. The user filter limits the traffic to the rate specified. Enter the rate limit value in the Rate field, and then choose the unit of measurement to use from the Rate drop-down list. Choose unlimit for the unit of measurement if you do not want the user filter to limit the traffic rate.
Burst	Specifies the traffic burst limit. The user filter uses the same unit of measurement for the burst that you chose for rate (see the Rate entry in this table).

Table 5-6 *User Filter Parameters (continued)*

Parameter	Description
Action	<p data-bbox="579 293 1180 383">Specifies the action that the Guard executes when the traffic matches the filter. Choose one of the following actions from the Action drop-down list:</p> <ul data-bbox="579 402 1231 1203" style="list-style-type: none"> <li data-bbox="579 402 1231 586">• permit—Prevents statistical analysis of the flow and anti-spoofing or anti-zombie protection functions from handling this flow. We recommend that you set a rate and burst limit to a filter with an action of permit because the traffic that the filter processes is not handled by other protection functions. <li data-bbox="579 605 1231 633">• basic/redirect—Authenticates applications over HTTP. <li data-bbox="579 652 1231 742">• basic/reset—Authenticates applications over TCP. We recommend that you use an action of basic/redirect for HTTP traffic flows. <li data-bbox="579 761 1231 883">• basic/safe-reset—Authenticates TCP application traffic flows that are not tolerant of a TCP connection reset. We recommend that you use an action of basic/redirect for HTTP traffic flows. <li data-bbox="579 902 1231 930">• basic/default—Authenticates non-TCP traffic flows. <li data-bbox="579 950 1231 1002">• basic/dns-proxy—Authenticates TCP DNS traffic flows. <li data-bbox="579 1021 1231 1203">• basic/sip—Authenticates Voice-over IP (VoIP) protocols using Session Initiation Protocol (SIP) over UDP to establish the VoIP sessions and the Real-Time Transport Protocol/Real-Time Control Protocol (RTP/RTCP) to transmit voice data between the SIP endpoints after sessions are established.

Table 5-6 User Filter Parameters (continued)

Parameter	Description
Action (continued)	<ul style="list-style-type: none"> strong—Provides strong authentication for a traffic flow or you can use this action when the previous filters do not seem suitable for the application. Authentication is performed for every connection. For TCP incoming connections, the Detector module serves as a proxy. We recommend that you do not use this action for connections if you use access control lists, access policies, or load-balancing policies that are based on the incoming IP address in the network. drop—Drops traffic flows.

Step 7 Choose one of the following options:

- **OK**—Saves the new user filter configuration. The User Filters screen appears.
- **Cancel**—Exits the User Filters form without saving any information. The User filters screen appears.

Deleting a User Filter



Caution

If you delete all user filters when the policy action is set to to-user-filter and then copy the zone configuration to a Guard, the Guard may pass unprotected traffic to the zone.

To delete a user filter, perform the following steps:

- Step 1** From the navigation pane, choose a zone that you created using a GUARD zone template. The zone main menu appears.
- Step 2** From the zone main menu, choose **Configuration > Filters > User filters**. The list of zone user filters appears.

- Step 3** Check the check box next to the user filter to delete.
- Step 4** Click **Delete**. The user filter is removed from the list of user filters.
-