



## CHAPTER 5

# Configuring Zone Filters

---

This chapter describes how to configure the Cisco Traffic Anomaly Detector (Detector) network traffic filters.

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector. 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 determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector 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](#)
- [Configuring Flex-Content Filters](#)
- [Configuring Bypass Filters](#)
- [Configuring Dynamic Filters](#)

## Understanding Zone Filters

Zone filters define how the Detector handles a specific traffic flow. You can configure filters to customize the methods that the Detector uses to detect traffic anomalies.

Zone filters enable the Detector to perform the following functions:

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

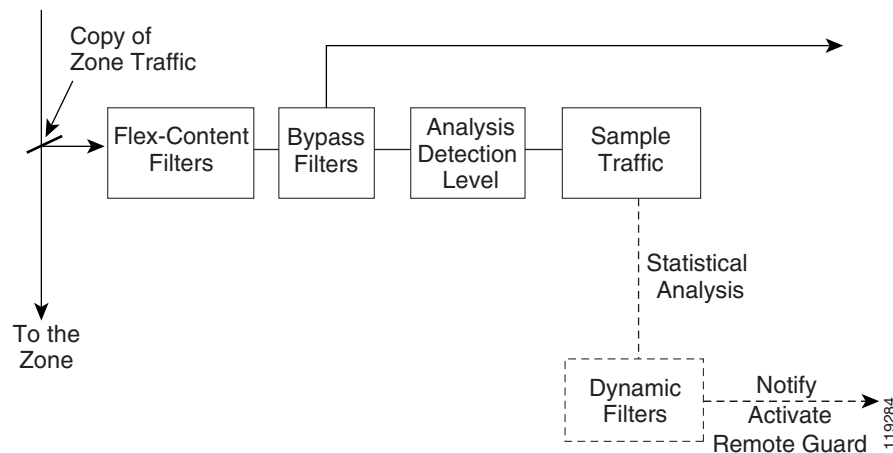
The Detector has the following types of filters:

- Bypass filters—Prevent the Detector from analyzing specific traffic flows. You can direct trusted traffic away from the Detector anomaly detection features. See the [“Configuring Bypass Filters” section on page 5-10](#) for more information.
- Flex-content filters—Count a specific traffic flow. Flex-content filters provide extremely flexible filtering capabilities, such as filtering according to fields in the IP and TCP headers, filtering based on the payload content, and filtering based on complex Boolean expressions. See the [“Configuring Flex-Content Filters” section on page 5-2](#) for more information.

- Dynamic filters—Apply the required protection level to the specified traffic flow. The Detector 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 by the Detector when the attack ends. See the “Configuring Dynamic Filters” section on page 5-12 for more information.

Figure 5-1 displays the Detector filter system.

**Figure 5-1** Detector Filter System



The Detector applies the analysis detection level to a copy of the zone traffic flow to analyze the traffic.

To perform a statistical analysis of the traffic flow, the Detector uses the zone policies which are all configured to handle specific types of traffic. The zone policies constantly measure traffic flows and take action against a particular traffic flow if they identify that flow as malicious or abnormal, which occurs when the flow exceeds the policy threshold. When the Detector identifies anomalies in the zone traffic, it creates new filters (dynamic filters) which can activate a Guard to protect the zone, or the Detector records the event in its syslog.

## Configuring Flex-Content Filters

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

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 tcpdump-expression value.
3. Performs pattern matching with the pattern-expression value on the remaining packets.



### Note

Flex-content filters consume 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. If you are using a flex-content filter to detect 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.

This section contains the following topics:

- [Adding a Flex-Content Filter](#)
- [Displaying Flex-Content Filters](#)
- [Deleting Flex-Content Filters](#)
- [Changing the State of a Flex-Content Filter](#)

## Adding a Flex-Content Filter

The Detector creates a list of flex-content filters that you create and activates the filters in an ascending order. When you add a new flex-content filter, make sure that you place it in the correct location in the filter list.

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

- Step 1** Display the list of flex-content filters and identify the location in the list in which you want to add the new filter (see the “[Displaying Flex-Content Filters](#)” section on page 5-8).
- Step 2** If the current row numbers are consecutive, renumber the flex-content filters in increments that allow you to insert the new flex-content filter by entering the following command in zone configuration mode:

```
flex-content-filter renumber [start [step]]
```

[Table 5-1](#) provides the arguments for the **flex-content-filter renumber** command.

**Table 5-1 Arguments for the flex-content-filter renumber Command**

Parameter	Description
<i>start</i>	(Optional) Integer from 1 to 9999 that denotes the new starting number of the flex-content filter list. The default is 10.
<i>step</i>	(Optional) Integer from 1 to 999 that defines the increment between the flex-content filter row numbers. The default is 10.

- Step 3** (Optional) Filter a pattern expression of an ongoing attack or an attack that you have previously recorded. Activate the Detector to generate a signature of the attack by using the **show packet-dump signatures** command. See the “[Generating Attack Signatures from Packet-Dump Capture Files](#)” section on page 11-18 for more information.

- Step 4** Add a new flex-content filter by entering the following command:

```
flex-content-filter row-num {disabled | enabled} {drop | count} protocol port [start start-offset [end end-offset]] [ignore-case] expression tcpdump-expression pattern pattern-expression
```

[Table 5-2](#) provides the arguments and keywords for the **flex-content-filter** command.

**Table 5-2 Arguments and Keywords for the flex-content-filter Command**

Parameter	Description
<i>row-num</i>	Unique number from 1 to 9999 that identifies the filter and defines the priority among the flex-content filters. The Detector operates the filters in ascending row-number order.
<b>disabled</b>	Sets the filter state to disabled. The filter does not monitor traffic.

**Table 5-2 Arguments and Keywords for the flex-content-filter Command (continued)**

Parameter	Description
<b>enabled</b>	<p>Sets the filter state to enabled. The Detector monitors traffic and performs the action (drop or count) on the flow that matches the filter.</p> <p>This is the default state.</p>
<b>drop</b>	<p>Drops the flow that matches the filter. You can configure the drop action in Guard configuration mode if you have created the zone from the Guard zone templates. The drop action is applicable to the Guard only.</p>
<b>count</b>	<p>Counts the flow that matches the filter.</p>
<b>protocol</b>	<p>Traffic from a specific protocol. Use an asterisk (*) to indicate any protocol. Enter an integer from 0 to 255.</p> <p>Review possible protocol numbers at the Internet Assigned Numbers Authority (IANA) website:  <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a></p>
<b>port</b>	<p>Traffic destined to a specific destination port. Enter an integer from 0 to 65535. To define a specific port number, you must define a specific protocol number.</p> <p>Use an asterisk (*) to indicate any destination port. You can use an asterisk if you configure the protocol number to 6 (TCP) or 17 (UDP).</p> <p>Review possible port numbers at the Internet Assigned Numbers Authority (IANA) website:  <a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></p>
<b>start-offset</b>	<p>Offset, in bytes, from the beginning of the packet payload, where the pattern matching for the <i>pattern-expression</i> argument begins. The default is 0, which is the start of the payload. Enter an integer from 0 to 1800.</p> <p>If you copy the pattern from the <b>show packet-dump signatures</b> command output, copy this argument from the Start Offset field in the command output.</p>
<b>end-offset</b>	<p>Offset, in bytes, from the beginning of the packet payload, where the pattern matching for the <i>pattern-expression</i> argument ends. The default is the packet length, which is the end of the payload. Enter an integer from 0 to 1800.</p> <p>If you copy the pattern from the <b>show packet-dump signatures</b> command output, copy this argument from the End Offset field in the command output.</p>
<b>ignore-case</b>	<p>Defines the <i>pattern-expression</i> argument as case insensitive.</p> <p>By default, the <i>pattern-expression</i> argument is case sensitive.</p>
<b>tcpdump-expression</b>	<p>Expression that is matched with the packet. The expression is in Berkeley Packet filter format. See the “Configuring the tcpdump-expression Syntax” section on page 5-5 for more information and configuration examples.</p> <p>If you use spaces in the expression, enclose the expression in quotation marks (“ ”).</p> <p>To enter an empty expression, use double quotation marks (“ ”).</p> <p>To use a quotation mark in the expression, use the backslash escape character before the quotation mark (\”).</p> <p><b>Note</b> Help is not available for the tcpdump-expression syntax.</p>

**Table 5-2 Arguments and Keywords for the flex-content-filter Command (continued)**

Parameter	Description
<i>pattern-expression</i>	<p>Regular expression data pattern that is to be matched with the packet payload. See the “<a href="#">Configuring the pattern-expression Syntax</a>” section on page 5-8 for more information.</p> <p>You can activate the Detector to generate the signature by using the <b>show packet-dump signatures</b> command. See the “<a href="#">Generating Attack Signatures from Packet-Dump Capture Files</a>” section on page 11-18.</p> <p>If you use spaces in the expression, enclose the expression in quotation marks (“ ”).</p> <p>To enter an empty expression, use double quotation marks (“ ”).</p> <p>To use a quotation mark in the expression, use the backslash escape character before the quotation mark (“\”).</p> <p><b>Note</b> Help is not available for the pattern-expression syntax.</p>

You can change the filter state to enable or disable at any time (see the “[Changing the State of a Flex-Content Filter](#)” section on page 5-10).

The following example shows how to configure the flex-content filter:

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * * expression "ip[6:2]
& 0x1fff=0" pattern
"/ HTTP/1.1\ x0D\0AAccept: .*/.*\x0D\x0AAccept-Language: en*\x0D\x0AAccept-Encoding:
gzip, deflate\x0D\x0AUser-Agent: Mozilla/4.0"
```

This section contains the following topics:

- [Configuring the tcpdump-expression Syntax](#)
- [Configuring the pattern-expression Syntax](#)

## Configuring the tcpdump-expression Syntax

The tcpdump-expression is in the Berkeley 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, but the performance of the Detector may be affected. 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 which usually consist of an ID 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 5-3 describes the tcpdump-expression elements.

**Table 5-3 tcpdump-expression Elements**

Element	Description
<b>dst host</b> <i>host_ip_address</i>	Specifies traffic to a destination host IP address.
<b>src host</b> <i>host_ip_address</i>	Specifies traffic from a source host IP address.
<b>host</b> <i>host_ip_address</i>	Specifies traffic to and from both source and destination host IP addresses.
<b>net net mask</b> <i>mask</i>	Specifies traffic to a specific network.
<b>net</b> <i>net/len</i>	Specifies traffic to a specific subnet.
<b>dst port</b> <i>destination_port_number</i>	Specifies TCP or UDP traffic to a destination port number.
<b>src port</b> <i>source_port_number</i>	Specifies TCP or UDP traffic from a source port number.
<b>port</b> <i>port_number</i>	Specifies TCP or UDP traffic to and from both source and destination port numbers.
<b>less</b> <i>packet_length</i>	<b>Specifies packets with a length equal to or less than the specific length in bytes.</b>
<b>greater</b> <i>packet_length</i>	Specifies packets with a length equal to or greater than the specific length in bytes.
<b>ip proto</b> <i>protocol</i>	Specifies packets with a protocol number of the following protocols: ICMP, UDP, and TCP.
<b>ip broadcast</b>	Specifies broadcast IP packets.
<b>ip multicast</b>	Specifies multicast packets.
<b>ether proto</b> <i>protocol</i>	Specifies either protocol packets of a specific protocol number or name such as IP, ARP, or 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 5-4 describes the tcpdump-expression rules.

Table 5-4 describes the tcpdump-expression rules.

**Table 5-4 Flex-Content Filter Expression Rules**

Expression Rule	Description
<i>relop</i>	>, <, >=, <=, =, !=

**Table 5-4 Flex-Content Filter Expression Rules (continued)**

Expression Rule	Description
<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. <b>The possible values are</b> 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 expression elements using the following methods:

- A group of elements and operators in parentheses—The operators are the normal binary operators [+ , - , \* , / , & , |] and a length operator.



**Note** To use a parenthesis in the expression, use the backslash escape character before the parenthesis ( \ ( ).

- 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 from 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 of the Berkeley Packet filter configuration options, go to this location:

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

The following example shows how to count unfragmented datagrams and fragmented zeros of fragmented datagrams only. 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 as shown in this example:

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * * expression
ip[6:2]&0x1fff=0 pattern ""
```

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

```
user@DETECTOR-conf-zone-scannet# user@DETECTOR-conf-zone-scannet# flex-content-filter
enabled count * * expression tcp[13]&4!=0 pattern ""
```

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

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * * expression "icmp
[0]!=8 and icmp[0] != 0" pattern ""
```

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

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * * expression "tcp and
dst port 80 and not src port 1000" pattern ""
```

## Configuring the pattern-expression Syntax

The pattern-expression syntax is a regular expression that describes a string of characters. The pattern-expression describes a set of strings without actually listing its elements. This expression consists of normal characters and special characters. Normal characters include all printable ASCII characters that are not considered to be special characters. Special characters have a special meaning and specify the type of matching that the Detector 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 5-5 describes the special characters that you can use.

**Table 5-5** Special Characters Used in the pattern-expression

Special character	Description
<code>.*</code>	Matches a string that may be present and can contain zero or more characters. For example, the pattern <code>goo.*s</code> matches the patterns <code>goos</code> , <code>goods</code> , <code>good for ddos</code> , and <code>so on</code> .
<code>\</code>	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 ( <code>\</code> ). For example, two backslashes ( <code>\\</code> ) match one backslash ( <code>\</code> ), and one backslash and a period ( <code>\.</code> ) match one period ( <code>.</code> ).  You must also precede an asterisk ( <code>*</code> ) with a backslash.
<code>\xHH</code>	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 <code>\x41</code> matches the hexadecimal value A.

By default, the pattern-expression is case sensitive. To define the pattern-expression as case insensitive, use the `flex-content-filter` command with the `ignore-case` keyword. See the “Adding a Flex-Content Filter” section on page 5-3 for more information.

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` parameters are nonspecific.

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled drop * * expression " "
pattern \x89\xE5Qh\.\dllhel132hkernQhounthickChGetTf\xB911
Qh32\.\dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

## Displaying Flex-Content Filters

To display the flex-content filters, use the following command in zone configuration mode:

```
show flex-content-filters
```

Table 5-6 describes the fields in the **show flex-content-filters** command output.

**Table 5-6 Field Descriptions for the show flex-content-filters Command**

Field	Description
Row	Flex-content filter priority.
State	Filter state (enabled or disabled).
Action	Action that the filter performs on the specific traffic type.
Protocol	Protocol number of the traffic that the filter processes.
Port	Destination port of the traffic that the filter processes.
Start	Offset, in bytes, from the beginning of the packet payload where the pattern matching begins. This offset applies to the <i>pattern</i> field.
End	Offset, in bytes, from the beginning of the packet payload where the pattern matching ends. This offset applies to the <i>pattern</i> field.
Match-case	Whether the pattern expression that the filter matches is case sensitive or not case sensitive. yes=case-sensitive no=case-insensitive
TCPDump-expression	tcpdump-expression to be matched with the packet in Berkeley Packet filter format. See the “ <a href="#">Configuring the tcpdump-expression Syntax</a> ” section on <a href="#">page 5-5</a> for the information about the tcpdump-expression syntax.
Pattern-filter	Regular expression data pattern to be matched with the packet payload. See the “ <a href="#">Configuring the pattern-expression Syntax</a> ” section on <a href="#">page 5-8</a> for information about the pattern-expression syntax.
RxRate (pps)	Current traffic rate in packets per second that is measured for this filter.

## Deleting Flex-Content Filters

You can delete a flex-content filter when you no longer need it to filter packets based on the filter expression.



### Note

Do not delete a flex-content filter if you might need it at a later date. You can disable the flex-content filter and then enable it when needed (see the “[Changing the State of a Flex-Content Filter](#)” section on [page 5-10](#)).

To delete a flex-content filter, enter the following command in zone configuration mode:

```
no flex-content-filter row-num
```

The *row-num* argument specifies the flex-content filter row number to delete. To display the list of flex-content filters and identify the row number of the flex-content filter to delete, use the **show flex-content-filters** command (See the “[Displaying Flex-Content Filters](#)” section on [page 5-8](#)). To delete all flex-content filters, enter an asterisk (\*) for the row number.

This example shows how to delete a flex-content filter:

```
user@DETECTOR-conf-zone-scannet# no flex-content-filters 5
```

## Changing the State of a Flex-Content Filter

You can disable a flex-content filter to prevent the Detector from filtering packets based on the filter expression and to prevent it from filtering specific types of traffic. When you disable the filter, it remains in the flex-content filter list, which allows you to enable the filter again if needed.

If you do not intend to use a flex-content filter again, you can delete it (see the “[Deleting Flex-Content Filters](#)” section on page 5-9).

To change the state of a flex-content filter, enter the following command in zone configuration mode:

```
flex-content-filter row-num {disabled | enabled}
```

The *row-num* argument specifies the flex-content filter row number. To display the list of flex-content filters and identify the row number of the flex-content filter to enable or disable, enter the **show flex-content-filters** command (see the “[Displaying Flex-Content Filters](#)” section on page 5-8).

The following example shows how to disable a flex-content filter:

```
user@DETECTOR-conf-zone-scannet# flex-content-filters 5 disabled
```

## Configuring Bypass Filters

The bypass filter prevents the Detector from analyzing specific traffic flows by directing trusted traffic away from the Detector’s anomaly detection functions.

This section contains the following topics:

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

### Adding a Bypass Filter

To add a bypass filter, use the following command in zone configuration mode:

```
bypass-filter row-num src-ip [ip-mask] protocol dest-port [fragments-type]
```

[Table 5-7](#) provides the arguments for the **bypass-filter** command.

**Table 5-7 Arguments for the bypass-filter Command**

Parameter	Description
<i>row-num</i>	Unique number from 1 to 9999. The row number identifies the filter and defines the priority among the bypass filters. The Detector operates the filters according to the ascending row-number order.
<i>src-ip</i>	Traffic from a specific IP address is processed. Use an asterisk (*) to indicate any IP address.
<i>ip-mask</i>	(Optional) Traffic from a specific subnet is processed. The subnet mask can contain only Class C values. The default subnet is 255.255.255.255.

**Table 5-7 Arguments for the bypass-filter Command (continued)**

Parameter	Description
<i>protocol</i>	Traffic from a specific protocol is processed. Use an asterisk (*) to indicate any protocol.  Review possible protocol numbers at the Internet Assigned Numbers Authority (IANA) website:  <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a>
<i>dest-port</i>	Traffic to a specific destination port is processed. Use an asterisk (*) to indicate any destination port.  Review possible port numbers at the Internet Assigned Numbers Authority (IANA) website:  <a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a>
<i>fragments-type</i>	(Optional) Whether or not the filter processes fragmented traffic. The three fragmented types are as follows: <ul style="list-style-type: none"> <li>• <b>no-fragments</b>—Nonfragmented traffic</li> <li>• <b>fragments</b>—Fragmented traffic</li> <li>• <b>any-fragments</b>—Fragmented and nonfragmented traffic</li> </ul> The default is <b>no-fragments</b> .



**Note** You cannot specify both a fragments type and a destination port. To set the fragments type, enter an asterisk (\*) for the destination port.

## Displaying Bypass Filters

To display the list of bypass filters, use the following command in zone configuration mode:

```
show bypass-filters
```

Table 5-8 describes the fields in the **show bypass-filters** command output.

**Table 5-8 Field Descriptions for the show bypass-filters Command**

Field	Description
Row	Bypass filter priority.
Source IP	Source IP address of the traffic that the filter processes.
Source Mask	Source address subnet mask of the traffic that the filter processes.
Proto	Protocol number of the traffic that the filter processes.
DPort	Destination port of the traffic that the filter processes.

**Table 5-8** Field Descriptions for the `show bypass-filters` Command (continued)

Field	Description
Frg	Fragmentation settings that the filter processes: <ul style="list-style-type: none"> <li>• <b>yes</b>—The filter processes fragmented traffic.</li> <li>• <b>no</b>—The filter processes nonfragmented traffic.</li> <li>• <b>any</b>—The filter processes both fragmented and nonfragmented traffic.</li> </ul>
RxRate (pps)	Current traffic rate in packets per second that is measured for this filter.

The source IP address, source address mask, protocol number, and destination port may be nonspecific. An asterisk (\*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

## Deleting Bypass Filters

To delete a bypass filter, enter the following command in zone configuration mode:

```
no bypass-filter row-num
```

The *row-num* argument specifies the bypass filter row number to be deleted. To display the list of bypass filters and identify the row number of the bypass filter that you want to delete, use the **show bypass-filters** command (see the “[Displaying Bypass Filters](#)” section on page 5-11). To delete all bypass filters, enter an asterisk (\*) for the row number.

The following example shows how to delete a bypass filter:

```
user@DETECTOR-conf-zone-scannet# no bypass-filter 10
```

## Configuring Dynamic Filters

Dynamic filters apply the required protection level to traffic flow and define how to handle the attack. The Detector creates dynamic filters when it identifies an anomaly in the zone traffic, which occurs when the flow exceeds the zone policy thresholds. The Detector creates new dynamic filters as changes occur to the zone traffic and the type of DDoS attack. The dynamic filters have a limited life span and the Detector deletes them when the attack ends. The Detector supports a maximum of 150,000 dynamic filters that are active concurrently in all zones.

Dynamic filters produce a notification record in the Detector syslog or activate remote Guards to protect the zone.

This section contains the following topics:

- [Displaying Dynamic Filters](#)
- [Adding Dynamic Filters](#)
- [Deleting Dynamic Filters](#)
- [Preventing the Production of Dynamic Filters](#)

## Displaying Dynamic Filters

You can display the dynamic filters that the Detector created by using one of the following commands in zone configuration mode:

- **show dynamic-filters [details]**—Displays a list of all dynamic filters.
- **show dynamic-filters *dynamic-filter-id* [details]**—Displays a single dynamic filter.
- **show dynamic-filters sort {action | exp-time | id}**—Displays a sorted list of all dynamic filters.

Table 5-9 provides the arguments and keywords for the **show dynamic-filters** command.

**Table 5-9 Arguments and Keywords for the show dynamic-filters Command**

Parameter	Description
<i>dynamic-filter-id</i>	Identifier of the specific dynamic filter to display. This integer is assigned by the Detector. To identify the filter ID, display the complete list of dynamic filters.
<b>details</b>	(Optional) Displays dynamic filters in detail. The details consist of additional information about the attack flow, the triggering rate, and the policy that produced it.
<b>action</b>	Displays dynamic filters by their action.
<b>exp-time</b>	Displays dynamic filters by their expiration time in ascending order.
<b>id</b>	Displays dynamic filters by the ascending ID number.



### Note

To display the pending dynamic filters when the Detector is operating in interactive detect mode, use the **show recommendations** command. See Chapter 9, “Using Interactive Detect Mode,” for more information about pending dynamic filters.



### Note

The Detector displays a maximum of 1000 dynamic filters. When more than 1000 dynamic filters are active, examine the log file or zone report for a complete list of dynamic filters.

The following example shows how to display a dynamic filter in detail:

```
user@DETECTOR-conf-zone-scannet# show dynamic-filters 876 details
```

Table 5-10 describes the fields in the **show dynamic-filters** command output.

**Table 5-10 Field Descriptions for show dynamic-filters Command Output**

Field	Description
ID	Filter identification number.
<b>Action</b>	Action that the filter performs on the traffic flow.
<b>Exp Time</b>	Amount of time that the filter is active. After the time expires, the filter is deleted.
Source IP	Source IP address of the traffic that the filter processes.
Source Mask	Source address mask of the traffic that the filter processes.

**Table 5-10** Field Descriptions for `show dynamic-filters Command Output (continued)`

Field	Description
Proto	Protocol number of the traffic that the filter processes.
DPort	Destination port of the traffic that the filter processes.
Frg	Whether or not the filter processes fragmented traffic: <ul style="list-style-type: none"> <li>• <b>yes</b>—The filter processes fragmented traffic.</li> <li>• <b>no</b>—The filter processes nonfragmented traffic.</li> <li>• <b>any</b>—The filter processes both fragmented and nonfragmented traffic.</li> </ul>
RxRate (pps)	Current traffic rate in packets per second that is measured for this filter.
Destination IP	Destination IP address of the traffic that the filter processes. The Detector activates protection on the Guard based on the destination IP address and the value of the <b>protect-ip-state</b> that is configured for the zone.

The source IP address, source address mask, protocol number, and destination port may be nonspecific. An asterisk (\*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

Table 5-11 describes the additional fields in the `show dynamic-filters details` command output.

**Table 5-11** Field Descriptions for `show dynamic-filters details Command`

Field	Description
Attack flow	Attack flow characteristics. The attack flow contains the Source IP, Source Mask, Proto, DPort, and Frg fields that are described in Table 5-10.
Triggering Rate	Rate of the attack flow that exceeded a policy threshold.
Threshold	Policy threshold that was exceeded by the attack flow.
Policy	Policy that produced the dynamic filter. See Chapter 6, “Configuring Policy Templates and Policies,” for more information.

## Adding Dynamic Filters

During an attack on the zone, you can add a dynamic filter to manipulate zone anomaly detection. You can configure a dynamic filter to activate the Guards that you define in the remote Guard lists (remote Guard) to protect the zone. The remote activation will fail if the destination IP address of the dynamic filter does not match the Guard-protection activation method that you defined for the zone by using the **protect-ip-state** command and the zone address range. You can configure the dynamic filter to activate zone protection on the remote Guard in one of the following ways:

- Activate zone protection on the remote Guard for the entire zone—To activate zone protection for the entire zone, do not enter the *dst-ip* argument. You must configure the Guard-protection activation method of the zone to be **entire-zone** or **policy-type**.
- Activate zone protection on the remote Guard for a specific IP address within the zone IP address range only—To activate zone protection for a specific IP address, use the *dst-ip* argument to specify the IP address. You must configure the Guard-protection activation method of the zone to be **dst-ip-by-name**.

See the “[Activating Remote Guards to Protect a Zone](#)” section on page 8-5 and the “[Configuring Guard-Protection Activation Methods](#)” section on page 8-3 for more information.

To add a dynamic filter, use the following command in zone configuration mode:

```
dynamic-filter remote-activate {exp-time | forever} [dst-ip]
```

You can use multiple **dynamic-filter** commands to add multiple dynamic filters.

[Table 5-12](#) provides the arguments and keywords for the **dynamic-filter** command.

**Table 5-12 Arguments and Keywords for the dynamic-filter Command**

Parameter	Description
<b>remote-activate</b>	Activates the remote Guards to protect the zone. If you do not enter the <i>dst-ip</i> argument, the activation method that the Detector uses to activate protection on the remote Guard is <b>entire-zone</b> .
<b>exp-time</b>	Integer from 1 to 3,000,000 that specifies the time (in seconds) for the filter to be active.
<b>forever</b>	Activates the filter for an unlimited time. The filter is deleted when protection ends.
<b>dst-ip</b>	(Optional) Traffic to a specific destination IP address. The Detector activates the remote Guards to protect the zone based on the specified IP address. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1).  The Detector uses the activation method of <i>dst-ip-by-name</i> to activate protection on the remote Guard.

The following example shows how to add a dynamic filter that activates protection for the entire zone on the remote Guard:

```
admin@GUARD-conf-zone-scannet# dynamic-filter remote-activate 600
```

## Deleting Dynamic Filters

When you delete dynamic filters, the deletion is effective for a limited period of time because the Detector continues to create new dynamic filters when you have zone anomaly detection enabled and the zone is under attack. See the “[Preventing the Production of Dynamic Filters](#)” section on page 5-16 for information about how to prevent the Detector from producing a dynamic filter.

To delete a dynamic filter, enter the following command in zone configuration mode:

```
no dynamic-filter dynamic-filter-id
```

The *dynamic-filter-id* argument specifies the dynamic filter identifier. To display the list of dynamic filters and identify the dynamic filter to delete, use the **show dynamic-filters** command (see the “[Displaying Dynamic Filters](#)” section on page 5-13). To delete all zone dynamic filters, enter an asterisk (\*) for the dynamic filter identifier.

The following example shows how to delete a dynamic filter:

```
user@DETECTOR-conf-zone-scannet# no dynamic-filter 876
```

## Preventing the Production of Dynamic Filters

To prevent the Detector from producing unwanted dynamic filters, perform one of the following actions:

- Deactivate the policy that produces the dynamic filters (see the [“Changing the Policy State”](#) section on page 6-13 for more information). To determine which policy produced the unwanted dynamic filters, see the [“Displaying Dynamic Filters”](#) section on page 5-13.
- Configure a bypass filter for the desired traffic flow (see the [“Configuring Bypass Filters”](#) section on page 5-10).
- Increase the threshold of the policy that produces the undesired dynamic filter (see the [“Configuring the Policy Threshold”](#) section on page 6-13).