



CHAPTER 6

Managing Zone Filters

This chapter describes how to use the Cisco DDoS MultiDevice Manager (MDM) to manage the traffic filters that the Detector and Guard use to process zone traffic.



Note

This guide refers to the Cisco Traffic Anomaly Detector Module and the Cisco Traffic Anomaly Detector appliance as *Detector* and the Cisco Anomaly Guard Module and the Cisco Guard appliance as *Guard*. When referring to both the Detector and the Guard, this guide uses the term *device*.

This chapter contains the following sections:

- [Understanding Zone Traffic Filters, page 6-1](#)
- [Managing a Flex-Content Filter, page 6-2](#)
- [Managing a Bypass Filter, page 6-11](#)
- [Managing a User Filter, page 6-14](#)

Understanding Zone Traffic Filters

Zone filters define how a device handles a specific traffic flow. You can configure the filters of a zone configuration to customize the traffic flow and control the anti-DDoS operations of the device.

Zone filters enable devices to perform the following functions:

- Analyze zone traffic for anomalies
- Bypass the device's anomaly detection (Detector) or zone protection (Guard) functions

When the device is a Guard, zone filters also enable the following actions:

- Separate legitimate traffic from malicious traffic
- Forward legitimate traffic to the zone
- Drop malicious traffic

The four types of filters are the bypass, flex-content, user, and dynamic filters.



Note

All but the dynamic filters are defined in the zone configuration. Dynamic filters are unique because they do not exist until the zone is under attack. When the zone is under attack, the device produces the dynamic filters to manage zone protection.

- Bypass filters—Prevents a device from handling a traffic flow that matches the criteria that you specify. Bypass filters enable you to specify the trusted traffic that you want to bypass the anomaly detection or zone protection functions of the device, preventing the device from analyzing the traffic. When the device is a Detector, the specified mirrored traffic is dropped immediately. When the device is a Guard, the specified diverted traffic is forwarded directly to the destination zone.
- Flex-content filters—Performs an action on a traffic flow that matches the criteria that you specify. flex-content filters provide flexible traffic filtering options, such as filtering based on fields in the IP and TCP headers, filtering based on payload content, or filtering based on complex Boolean expressions.
- User filters—(Used by the Guard only) Apply a specific protection level to the traffic flow that matches the criteria that you specify. (The Detector is preconfigured with a set of static user filters that it applies to zones that you create with a GUARD_ zone template.) User filters define the first actions that the Guard executes when it identifies abnormal or malicious traffic. Each zone configuration that you create with a GUARD_ zone template includes a default set of user filters configured to handle a wide range of attack types, enabling ondemand protection. These filters allow the Guard to protect a zone before the Guard learns the normal traffic patterns of the zone. You can modify user filters to customize the Guard protection capabilities and to establish rules that determine how the Guard manages traffic flows for the zone when it suspects an attack.
- Dynamic filters—(Created by a device when the device detects a traffic anomaly (an attack) while analyzing the zone traffic.) The dynamic filters operate as follows:
 - Detector operation—The Detector module is directed to either record the event in the Detector syslog or activate a Guard to provide zone protection.
 - Guard operation—The Guard continuously modifies this set of filters based on changes in the zone traffic and the type of DDoS attack. Dynamic filters have a limited life span and are deleted by the device when the attack ends. See the [“Managing a Dynamic Filter”](#) section on page 10-8 for more information.

The Guard uses both user filters and dynamic filters to manage zone protection during an attack. 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 that are configured to mitigate the current attack. When the Guard has to choose between applying a user filter and a dynamic filter to the traffic flow, it selects the filter type configured to address the more severe action.

Managing a Flex-Content Filter

You configure a flex-content filter to filter zone traffic based on fields in the packet header or patterns in the packet payload. Flex-content filters allow the device to identify known worm or flood attacks based on constant patterns that appear in the incoming traffic.



Note

We recommend that you limit the use of flex-content filters because these filters can consume a large amount of CPU resources which may affect the performance level of the device. If you need to monitor traffic for a specific attack that can be identified using either a dynamic or a flex-content filter, we recommend that you use the dynamic filter.

The flex-content filter is a combination of Berkley Packet filter and a pattern filter with very selective filtering capabilities. Use the flex-content filters to drop or 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 Syntax of the Flex-Content Filter Expression, page 6-3](#)
- [Understanding the Syntax of the Flex-Content Filter Pattern, page 6-5](#)
- [Adding a Flex-Content Filter, page 6-6](#)
- [Displaying a List of Flex-Content Filters, page 6-8](#)
- [Modifying a Flex-Content Filter Configuration, page 6-10](#)
- [Deleting a Flex-Content Filter, page 6-10](#)

Understanding the Syntax of the Flex-Content Filter Expression

The flex-content filter expression is created using the Berkley Packet filter format and specifies the expression to be matched with the packet.

The flex-content filter 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 default is **host**.
- Direction qualifiers—Define the transfer direction. Possible directions are **src**, **dst**, **src or dst**, and **src and dst**. The default is **src or dst**.
- 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.



Note

You can create a flex-content filter expression to filter traffic based on a destination port and protocol. However, due to performance considerations, we recommend that you specify destination port and protocol match criteria using the Protocol and Dest Port fields in the Flex-Content Filter Form.

Table 6-1 describes the tcpdump-expression elements.

Table 6-1 Elements Used in the Flex-Content Filter Expression

| Element | 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 <i>net mask mask</i> | Traffic to a specific network. |
| net <i>net/len</i> | Traffic to a specific subnet. |
| dst port <i>destination_port_number</i> | TCP or UDP traffic to a destination port number. |

Table 6-1 Elements Used in the Flex-Content Filter Expression (continued)

| Element | Description |
|---|---|
| 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 representing one of the following protocols: ICMP, UDP, and TCP. |
| ip broadcast | Broadcast IP packets. |
| ip multicast | Multicast IP packets. |
| ether proto <i>protocol</i> | Ether 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 6-2 describes the tcpdump-expression rules. |

[Table 6-2](#) describes the flex-content filter expression rules.

Table 6-2 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 flex-content filter 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 example, `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 TCP RST packets:

```
user@GUARD-conf-zone-scannet# user@GUARD-conf-zone-scannet# flex-content-filter enabled
tcp[13]&4!=0
```

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

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

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

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

Understanding the Syntax of the Flex-Content Filter Pattern

The flex-content filter pattern is a regular expression that describes a string of characters, or set of strings, without actually listing its elements. A flex-content filter pattern is made up 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 device performs on the flex-content filter pattern (see [Table 6-3](#)). The flex-content filter matches the pattern 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 6-3 describes the special characters that you can use in a flex-content filter pattern.

Table 6-3 Special Characters Used in the Flex-Content Filter Pattern

| Special character | Description |
|-------------------|---|
| . | Matches a string that may be present and can contain zero or more characters. For example, the pattern goo.*s matches the patterns goos, goods, good for dds, 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 expression parameters are nonspecific.

```
user@GUARD-conf-zone-scanner# flex-content-filter enabled drop * * expression " " pattern
\x89\xE5Qh\d11he132hkernQhounthickChGetTf\xB911
Qh32\ .dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

Adding a Flex-Content Filter

Flex-content filters are activated in the order in which they appear in the Flex-Content Filter table. When you add a new flex-content filter, make sure that you place it in the correct location of the table.



Note

A Guard stops activating the flex-content filters when the zone traffic matches a flex-content filter with a drop action.

To add a flex-content filter, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > Flex-Content Filters**. The Flex-Content Filters screen appears displaying the list of existing flex-content filters.
- Step 3** Click **Add**. One of the following Add Filter screens appears:
 - The Add Filter – Step 2 screen appears if this is the first flex-content filter that you are configuring for the zone. Skip to Step 6.
 - The Add Filter – Step 1 screen appears if you have one or more flex-content filters already configured for the zone. Proceed to Step 4.

- Step 4** In the Insert column, select the row below where you want to insert the flex-content filter. The Insert Here text appears, indicating that the new flex-content filter will be inserted above the row that you selected.
- Step 5** Click **Next**. The Add Filter – Step 2 screen appears with the Flex-Content Filter Form.
- Step 6** Configure the match criteria of the flex-content filter parameters. [Table 6-4](#) describes the filter parameters listed in the Flex-Content Filter Form.

Table 6-4 Flex-Content Filter Parameters

| Parameter | Description |
|--------------|--|
| Description | Description for the flex-content filter. |
| Protocol | <p>Protocol number. Enter a protocol number from 0 to 255. To specify any protocol type, leave this field blank or enter an asterisk (*).</p> <p>For a list of valid protocol number, see the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/protocol-numbers</p> |
| Dst Port | <p>Destination port number. Enter a destination port number from 0 to 65535. To define a specific port number, you must define a specific protocol number.</p> <p>To specify any destination port, enter an asterisk (*). You can use an asterisk if you configure the protocol number to 6 (TCP) or 17 (UDP).</p> <p>For a list of valid port numbers, see the IANA website: http://www.iana.org/assignments/port-numbers</p> |
| Expression | <p>Expression to match with the packet. The expression is in the Berkley Packet filter format. Refer to the “Understanding the Syntax of the Flex-Content Filter Expression” section on page 6-3 for more information and configuration examples.</p> <p>Enter a string with up to 180 tokens that are separated by spaces. If you use spaces in the expression, enclose the expression in quotation marks (“ ”).</p> <p>To use a quotation mark in the expression, use the backslash escape character before the quotation mark (“”).</p> |
| Pattern | <p>Regular expression data pattern to match with the packet payload. See the “Understanding the Syntax of the Flex-Content Filter Pattern” section on page 6-5 for more information and configuration examples.</p> <p>Enter the data pattern to use. If you use spaces in the expression, enclose the expression in quotation marks (“ ”).</p> <p>To use a quotation mark in the expression, use the backslash escape character before the quotation mark (“”).</p> |
| Match Case | Case sensitivity of the flex-content filter pattern. Check the check box to define the pattern as case sensitive. |
| Start Offset | <p>Offset, in bytes, from the beginning of the packet payload, where the pattern matching for the flex-content filter pattern begins. The default is 0, which is the start of the payload. Enter an integer from 0 to 1800.</p> <p>The start offset applies to the Pattern field.</p> |

Table 6-4 Flex-Content Filter Parameters (continued)

| Parameter | Description |
|------------|---|
| End Offset | Offset, in bytes, from the beginning of the packet content, where the pattern matching for the flex-content filter pattern ends. The default is the packet length, which is the end of the payload. Enter an integer from 0 to 1800. The end offset applies to the Pattern field. |
| Action | Action that the flex-content filter performs on the zone traffic. The actions from the Action drop-down list are as follows: <ul style="list-style-type: none"> count—Counts the packets that match the filtering criteria. drop—Drops the packets that match the filtering criteria. |
| State | Operating state of the flex-content filter. The operating states from the State drop-down list are as follows: <ul style="list-style-type: none"> enable—Sets the filter state to enabled. The device monitors traffic and performs the action (drop or count) on the flow that matches the filtering criteria. This is the default state. disable—Sets the filter state to disabled. The filter does not monitor traffic. |

Step 7 Click **OK**. The MDM saves the modified zone configuration on the master device.

Step 8 (Optional) Synchronize the new information with the other zone devices by using one of the following methods:

- Manually by choosing **Activation > Sync** from the zone menu.
- Automatically according to how you configured the synchronization feature in the zone configuration (see the [“Modifying the Zone General Configuration Attributes”](#) section on page 5-9).

Displaying a List of Flex-Content Filters



To display a list of existing flex-content filters and their configurations, follow these steps:

Step 1 From the navigation pane, choose a zone. The zone menu appears.

Step 2 From the zone menu, choose **Configuration > Filters > Flex-Content Filters**. The Flex-Content Filters screen appears displaying the list of existing flex-content filters.

Table 6-5 describes the fields in the Flex-Content Filters table.

Table 6-5 Field Descriptions for the Flex-Content Filters Table

| Field | Description |
|---------------------|---|
| ! | Filter consolidation error. The MDM encountered a problem when attempting to obtain and consolidate zone configuration information from the zone devices. A filter consolidation error can be caused by one of the following conditions: <ul style="list-style-type: none"> The filter is configured on the master device but is not part of the zone configuration on the other zone devices. If you have automatic synchronization enabled, the error icon will disappear after the next synchronization period. If you do not have automatic synchronization enabled, perform a manual synchronization to eliminate the error condition. The MDM cannot communicate with one of the zone Guards. |
| Protocol | Protocol number. |
| Dst Port | Destination port number. |
| Expression | Expression that is matched with the packet. See the “Understanding the Syntax of the Flex-Content Filter Expression” section on page 6-3 for more information and configuration examples. |
| Pattern | Regular expression data pattern that is matched with the packet payload. See the “Understanding the Syntax of the Flex-Content Filter Pattern” section on page 6-5 for more information and configuration examples. |
| Match Case | Case sensitivity of the flex-content filter pattern. A check mark indicates that the flex-content filter pattern is case sensitive. |
| Start Offset | Offset, in bytes, from the beginning of the packet payload, where the pattern matching for the flex-content filter pattern begins. |
| End Offset | Offset, in bytes, from the beginning of the packet content, where the pattern matching for the flex-content filter pattern ends. |
| Action | Action that the flex-content filter performs on the zone traffic. The action can be one of the following: <ul style="list-style-type: none"> count—Counts the packets that match the filter drop—Drops the packets that match the filter |
| State | Operating state of the flex-content filter. The state can be one of the following: <ul style="list-style-type: none">  Enabled—The filter is enabled. The device monitors traffic and performs the action (drop or count) on the flow that matches the filter.  Disabled—The filter is disabled and does not monitor traffic. |
| Guard Rate (PPS) | Current traffic rate in packets per second for traffic that matches the criteria of the filter. The value shown is the sum of the individual rate values collected from all of the zone Guard devices using the filter. |
| Detector Rate (PPS) | Current traffic rate in packets per second for traffic that matches the criteria of the filter. The value shown is the individual rate value collected from the zone Detector master device. |

Modifying a Flex-Content Filter Configuration

You can modify the configuration of a flex-content filter, including the operating state of the filter. For example, you can change the filter state to disable, preventing the device from filtering traffic based on the match criteria of the filter. The filter remains in the flex-content filter list and is reactivated (enabled) when needed. If the filter is no longer needed, you can delete it from the flex-content filter list (see the [“Deleting a Flex-Content Filter”](#) section on page 6-10).



Note

You cannot change the action associated with a flex-content filter.

To modify the configuration of a flex-content filter, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > Flex-Content Filters**. The Flex-Content Filters screen appears displaying the list of existing flex-content filters.
- Step 3** Click any one of the fields of the flex-content filter that you want to configure. The Flex-Content-Filter Form screen appears.
- Step 4** Modify the configuration of the flex-content filter. See [Table 6-4](#) for a description of the fields in the Flex-Content Filter Form screen.
- Step 5** Click **OK**. The MDM saves the modified zone configuration on the master device.
- Step 6** (Optional) Synchronize the new information with the other zone devices by using one of the following methods:
 - Manually by choosing **Activation > Sync** from the zone menu.
 - Automatically according to how you configured the synchronization feature in the zone configuration (see the [“Modifying the Zone General Configuration Attributes”](#) section on page 5-9).

Deleting a Flex-Content Filter

You can delete a flex-content filter that you no longer need. Deleting a flex-content filter permanently removes the filter from the zone configuration. If you might need the filter in the future, you should change the operating state of the filter to disable rather than delete the filter (see the [“Modifying a Flex-Content Filter Configuration”](#) section on page 6-10).

To delete one or more flex-content filters, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone 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 the flex-content filter to delete. Select all of the existing flex-content filters by checking the check box in the header row.
- Step 4** Click **Delete**. The MDM saves the modified zone configuration on the master device.

- Step 5** (Optional) Synchronize the new information with the other zone devices by using one of the following methods:
- Manually by choosing **Activation > Sync** from the zone menu.
 - Automatically according to how you configured the synchronization feature in the zone configuration (see the “[Modifying the Zone General Configuration Attributes](#)” section on page 5-9).

Managing a Bypass Filter

You can configure a bypass filter to specify the traffic that you want to bypass the device functions. Any traffic flow that matches the criteria of the bypass filter is not analyzed by the device. Depending on the device type, the matching traffic is either immediately dropped (Detector) or forwarded directly to the zone (Guard).



Note

A Guard takes traffic that matches the criteria of a bypass filter and injects it back into the network without limiting the traffic rate based on the rate and the burst parameters of the zone configuration (see [Table 5-3](#) for more information).

This section contains the following topics:

- [Adding a Bypass Filter, page 6-11](#)
- [Displaying a List of Bypass Filters, page 6-12](#)
- [Deleting a Bypass Filter, page 6-13](#)

Adding a Bypass Filter

To add a bypass filter, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > Bypass filters**. The Bypass Filters screen appears.
- Step 3** Click **Add**. The Add Bypass Filter screen appears.
- Step 4** Configure the match criteria of the bypass filter parameters. [Table 6-6](#) describes the parameters in the Bypass Filters screen.

Table 6-6 Bypass Filters Screen Parameters

| Parameter | Description |
|---------------|---|
| Source IP | Source IP address. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1). To specify any source IP address, leave this field blank or enter an asterisk (*). |
| Source subnet | Source subnet mask. Choose the subnet from the Source Subnet drop-down list. |

Table 6-6 Bypass Filters Screen Parameters (continued)

| Parameter | Description |
|-----------|---|
| Protocol | <p>Protocol number.</p> <p>Enter the protocol number. To specify any protocol, leave this field blank or enter an asterisk (*).</p> <p>For a list of possible protocol numbers, see the IANA website: http://www.iana.org/assignments/protocol-numbers</p> |
| Dst Port | <p>Destination port number.</p> <p>Enter the destination port number. To specify any destination port, leave this field blank or enter an asterisk (*).</p> <p>For a list of possible port numbers, see the IANA website: http://www.iana.org/assignments/port-numbers</p> |
| Fragments | <p>Defines the filter processes fragmented traffic as follows:</p> <ul style="list-style-type: none"> • without—nonfragmented traffic • with—fragmented traffic • *—fragmented and nonfragmented traffic <p>Note To configure the value of the Fragments parameter to with or *, configure the value of the Dst Port parameter to any destination port by entering an asterisk (*) or leaving the Dst Port blank.</p> |

- Step 5** Click **OK**. The MDM saves the modified zone configuration on the master device.
- Step 6** (Optional) Synchronize the new information with the other zone devices by using one of the following methods:
- Manually by choosing **Activation > Sync** from the zone menu.
 - Automatically according to how you configured the synchronization feature in the zone configuration (see the “[Modifying the Zone General Configuration Attributes](#)” section on page 5-9).

Displaying a List of Bypass Filters

To display a list of existing bypass filters and their configurations, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > Bypass Filters**. The Bypass Filters screen appears displaying the list of existing bypass filters.

Table 6-7 describes the fields in the Bypass Filters table.

Table 6-7 Field Descriptions for the Bypass Filters Table

| Field | Description |
|----------------|---|
| ! | Filter consolidation error. The MDM encountered a problem when attempting to obtain and consolidate zone configuration information from the zone devices. A filter consolidation error can be caused by one of the following conditions: <ul style="list-style-type: none"> The filter is configured on the master device but is not part of the zone configuration on the other zone devices. If you have automatic synchronization enabled, the error icon will disappear after the next synchronization period. If you do not have automatic synchronization enabled, perform a manual synchronization to eliminate the error condition. The MDM cannot communicate with one of the zone Guards. |
| Src IP | Source IP address. The IP address is displayed in classless interdomain routing (CIDR) format (for example, 192.168.100.1/24). |
| Protocol | Protocol number. |
| Dst Port | Destination port number. |
| Fragments | Defines the filter processes fragmented traffic as follows: <ul style="list-style-type: none"> without—nonfragmented traffic with—fragmented traffic *—fragmented and nonfragmented traffic |
| Guard Count | Current traffic rate in packets per second for traffic matching the criteria of the filter. The value shown is the sum of the individual rate values collected from all of the zone Guard devices using the filter. |
| Detector Count | Current traffic rate in packets per second for traffic matching the criteria of the filter. The value shown is the individual rate value collected from the zone Detector master device. |

Deleting a Bypass Filter

To delete one or more bypass filters, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > Bypass Filters**. The Bypass Filters screen appears displaying the list of existing bypass filters.
- Step 3** Check the check box next to the bypass filters to delete and click **Delete**. To select all of the existing Bypass filters, check the check box in the header row.
- Step 4** Click **Delete**. The MDM saves the modified zone configuration on the master device.

- Step 5** (Optional) Synchronize the new information with the other zone devices by using one of the following methods:
- Manually by choosing **Activation > Sync** from the zone menu.
 - Automatically according to how you configured the synchronization feature in the zone configuration (see the [“Modifying the Zone General Configuration Attributes”](#) section on page 5-9).

Managing a User Filter

User filters are Guard-specific filters that search for traffic that matches the criteria of the filter. When the Guard identifies abnormal or malicious traffic, the user filters define the initial zone protection actions that the Guard executes. User filters can perform the following actions:

- Permit the traffic to pass without applying any antispoofing and antizombie protection measures
- Apply the required protection level
- Drop the traffic



Note

You can only configure user filters for zones that were created with a Guard zone template.

Each zone configuration includes a default set of user filters that are preconfigured to handle a wide range of attack types for ondemand protection. You can modify user filters to customize the Guard zone protection capabilities and to establish rules that relate to how the Guard handles specific traffic flows when it suspects an attack.

When you divert zone traffic to the Guard, the Guard continuously analyzes the traffic and looks for abnormal traffic patterns that indicate an attack on the zone. If the Guard detects abnormal traffic patterns, it produces dynamic filters that define how to mitigate the attack. The Guard, by default, creates an initial dynamic filter that directs all traffic to the user filters. The user filters provide the first line of defense against the evolving DDoS attack by providing the Guard with the time that it needs to analyze the attack characteristics. Once the Guard analyzes the attack, it produces dynamic filters with protection measures (actions) that are determined by the characteristics of the attack. The Guard continues to produce new dynamic filters as the attack evolves.

During an attack, the Guard examines the user and the dynamic filters before it decides how to manage the specific traffic flow. It compares the first user filter that matches the flow with the dynamic filters and chooses the most severe protection measure suggested by the two filter types. The Guard applies the appropriate protection level to the traffic flow to authenticate the traffic. Dynamic filters with actions of redirect/zombie and block-unauthenticated are applied even if a user filter to handle the same type of traffic exists because the dynamic filters affect the Guard authentication functions and do not directly affect the traffic flow.

You cannot modify the configuration of a user filter. If a user filter requires a configuration change, you must first delete the existing user filter and then add a new user filter with the required configuration.

This section contains the following topics:

- [Understanding User Filter Actions, page 6-15](#)
- [Displaying a List of User Filters, page 6-15](#)
- [Adding a User Filter, page 6-16](#)
- [Deleting a User Filter, page 6-18](#)

Understanding User Filter Actions

The action associated with a user filter represents the operation that the Guard executes when zone traffic conforms to the match criteria of the filter. [Table 6-8](#) describes the possible actions associated with a user filter.

Table 6-8 User Filter Actions

| User Filter Action | Function |
|--------------------|--|
| permit | Prevents the Guard from performing any statistical analysis of the flow or applying any antispoofing and antizombie protection functions on the flow. We recommend that you set a rate and burst limit to this filter because it is not handled by other protection functions (see Table 5-3 on page 5-10 for more information). |
| basic/redirect | Authenticates applications over Hypertext Transfer Protocol (HTTP). |
| basic/reset | Authenticates applications over Transmission Control Protocol (TCP). We recommend that you use an action of basic/redirect for HTTP traffic flows. |
| basic/default | Authenticates non-TCP traffic flows. |
| basic/dns-proxy | Authenticates TCP Domain Name System (DNS) traffic flows. |
| 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. |
| basic/sip | Authenticates Voice over IP (VoIP) applications that use Session Initiated Protocol (SIP) over User Datagram Protocol (UDP) to establish the VoIP sessions and Real-Time Transport Protocol/Realtime Control Protocol (RTP/RTCP) to transmit voice data between the SIP end points after sessions are established. |
| drop | Drops the specified traffic flow. |
| strong | Enables strong authentication for a traffic flow. Use this filter when strong authentication is required or when the previous filters do not seem suitable for the application. Authentication is performed for every connection. For TCP incoming connections, the Guard serves as a proxy. Do not use the strong authentication action for connections if you use ACLs, access policies, or load-balancing policies that are based on the incoming IP address in the network. |

Displaying a List of User Filters

To display a list of existing user filters and their configurations, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > User Filters**. The User Filters screen appears displaying the list of existing user filters.



Note

The MDM displays only user filters that appear in the zone configuration on the master device.

Table 6-9 describes the fields in the User Filters table.

Table 6-9 Field Descriptions for the User Filters Table

| Field | Description |
|------------|---|
| ! | Filter consolidation error. The MDM encountered a problem when attempting to obtain and consolidate zone configuration information from the zone devices. A filter consolidation error can be caused by one of the following conditions: <ul style="list-style-type: none"> The filter is configured on the master device but is not part of the zone configuration on the other zone devices. If you enable automatic synchronization, the error icon will disappear after the next synchronization period. If you do not have automatic synchronization enabled, perform a manual synchronization to eliminate the error condition. The MDM cannot communicate with one of the zone Guards. |
| Src IP | Source IP address. The IP address is displayed in classless interdomain routing (CIDR) format (for example, 192.168.100.1/24). |
| Protocol | Protocol number. |
| Dst Port | Destination port number. |
| Fragments | Defines the filter processes fragmented traffic as follows: <ul style="list-style-type: none"> without—nonfragmented traffic with—fragmented traffic *—fragmented and nonfragmented traffic |
| Rate | Limit on the traffic rate that the user filter can handle. |
| Burst | Traffic burst limit that the filter allows for the specific flow. |
| Action | Action that the filter executes when the traffic flow matches the filter match criteria. See the “ Understanding User Filter Actions ” section on page 6-15 for more information. |
| Rate (pps) | Current traffic rate in packets per second that is measured for this filter. The value shown is the sum of the individual rate values collected from all of the zone Guard devices. |

Adding a User Filter

When adding a new user filter, be sure to place it in the correct location within the User Filter table because the Guard activates the user filters in the order in which they appear in the table (see the “[Displaying a List of User Filters](#)” section on page 6-15).

To add a user filter, follow these steps:

-
- Step 1** From the navigation pane, choose a zone. The zone menu appears.
 - Step 2** From the zone menu, choose **Configuration > Filters > User Filters**. The User Filters screen appears displaying the list of existing user filters.
 - Step 3** Click **Add**. One of the following Add Filter screens appears:
 - The Add Filter – Step 2 screen appears if this is the first user filter that you are configuring for the zone. Skip to Step 6.

- The Add Filter – Step 1 screen appears if you have one or more user filters already configured for the zone. Proceed to Step 4.
- Step 4** In the Insert column, select the row below where you want to insert 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 user filter parameters as described in [Table 6-10](#).

Table 6-10 User Filter Parameters

| Parameter | Description |
|---------------|---|
| Source IP | Source IP address match criteria. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1). To specify any source IP address, leave this field blank or enter an asterisk (*). |
| Source subnet | Source subnet mask match criteria. Choose the subnet mask from the Source Subnet drop-down list. |
| Protocol | Protocol number match criteria. Enter a protocol number from 0 to 255. To specify any protocol type, leave this field blank or enter an asterisk (*). For a list of valid protocol numbers, see the IANA website: http://www.iana.org/assignments/protocol-numbers |
| Dst Port | Destination port match criteria. Enter a destination port number from 0 to 65535. To define a specific port number, you must define a specific protocol number. To specify any destination port, enter an asterisk (*). You can use an asterisk if you configure the protocol number to 6 (TCP) or 17 (UDP). For a list of valid port numbers, see the IANA website: http://www.iana.org/assignments/port-numbers |
| Fragments | Defines the filter processes fragmented traffic as follows: <ul style="list-style-type: none"> • without—nonfragmented traffic • with—fragmented traffic • *—fragmented and nonfragmented traffic <p>Note To configure the value of the Fragments parameter to with or *, configure the value of the Dst Port parameter to any destination port by entering an asterisk (*) or leaving the Dst Port blank.</p> |
| Rate | Rate limitation and unit of measurement. The rate limit can be up to 10 times greater than the burst limit. For the rate value, enter an integer greater than 64 in the Rate field. For the unit of measurement, choose a value from the Rate drop-down list. If you do not want the user filter to limit the traffic rate or burst rate, leave the Rate field blank and choose unlimit for the unit of measurement. This is the default. |

Table 6-10 User Filter Parameters (continued)

| Parameter | Description |
|--------------|---|
| Burst | Burst limitation. Enter an integer greater than 64 that specifies the traffic burst limit. The Burst limit can be up to eight times greater than the rate limit. The unit of measurement for Burst corresponds to the value that you select from the Rate drop-down list. If you do not want the user filter to limit the traffic rate or burst rate, leave the Rate field blank and choose unlimit for the unit of measurement. This is the default. |
| Action | Action that the filter executes when the traffic flow matches the filter match criteria. See the “ Understanding User Filter Actions ” section on page 6-15 for more information. |

- Step 7** Click **OK**. The MDM saves the modified zone configuration on the master device.
- Step 8** (Optional) Synchronize the new information with the other zone devices by using one of the following methods:
- Manually by choosing **Activation > Sync** from the zone menu.
 - Automatically according to how you configured the synchronization feature in the zone configuration (see the “[Modifying the Zone General Configuration Attributes](#)” section on page 5-9).

Deleting a User Filter



Caution

If you delete all user filters when the policy action is set to user-filter, the Guard passes unprotected traffic to the zone.

To delete one or more user filters, follow these steps:

- Step 1** From the navigation pane, choose a zone. The zone menu appears.
- Step 2** From the zone menu, choose **Configuration > Filters > User Filters**. The User Filters screen appears displaying the list of existing user filters.
- Step 3** Check the check box next to the user filters to delete. To select all of the existing user filters, check the check box in the header row.
- Step 4** Click **Delete**. The MDM saves the modified zone configuration on the master device.
- Step 5** (Optional) Synchronize the new information with the other zone devices by using one of the following methods:
- Manually by choosing **Activation > Sync** from the zone menu.
 - Automatically according to how you configured the synchronization feature in the zone configuration (see the “[Modifying the Zone General Configuration Attributes](#)” section on page 5-9).