



CHAPTER 9

Activating Zone Protection

This chapter describes how to activate zone protection on the Cisco Guard (Guard) manually using the Guard CLI or the WBM, or automatically using an external triggering device, such as a Cisco Traffic Anomaly Detector (Detector).

The Detector, which is the companion product of the Guard, is a Distributed Denial of Service (DDoS) attack detection device that analyzes a copy of the zone traffic. The Detector can activate the Guard attack mitigation services when the Detector determines that the zone is under attack. The Detector can also synchronize zone configurations with the Guard. For more information about the Detector, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* and *Cisco Traffic Anomaly Detector Configuration Guide*.

This chapter contains the following sections:

- [Understanding the Zone Protection Activation Options](#)
- [Managing Zone Protection](#)
- [Managing Dynamic Filters](#)
- [Activating Automatic or Interactive Protect Mode](#)
- [Managing Guard Recommendations for Dynamic Filters](#)

Understanding the Zone Protection Activation Options

When zone protection is activated, the Guard applies the zone policies to the traffic flow. When a traffic anomaly triggers a policy action by exceeding the policy threshold (indicating an attack), the Guard begins producing dynamic filters to mitigate the attack. The Guard determines the attack is over when it no longer needs to produce dynamic filters for the traffic.

The Guard provides you with several options for performing zone protection. For example, you can allow the Guard to manage all aspects of the zone protection operation or you can monitor and direct the Guard actions during an attack. You can also define the following zone protection characteristics:

- Activation method—Activate the zone according to the zone name, the zone address range, or the received traffic. You should configure the activation method if zone protection is activated by an external device (such as a Detector).
- Activation extent—Activate zone protection for the entire zone address range or only for a specific IP address within the zone. The activation extent applies to zones where zone protection is activated by an external device, such as a Detector only.
- Protection termination timeout—Define the timeout after which the Guard terminates zone protection.

This section contains the following topics:

- [Understanding On-Demand Protection](#)
- [Understanding the Protect and Protect and Learn Functions](#)
- [Automatic and Interactive Zone Operation Modes](#)
- [Protection Activation Methods](#)

Understanding On-Demand Protection

If you need to protect a zone before you have an opportunity to allow the Guard to learn the zone traffic, you can use one of the predefined zone templates to protect a zone, which is known as *on-demand protection*. The predefined policies and filters in the zone template can protect a zone that has traffic characteristics that are unknown to the Guard. The default thresholds of these zone policies are tuned so that the Guard activates the anti-spoofing functions quickly if it identifies traffic anomalies in the zone traffic.

Because the Guard does not know the specific zone traffic patterns, the predefined thresholds that are used to block (drop) source IP addresses are set to high values. On-demand protection requires that you intervene during mitigation of nonspoofed attacks. You must monitor the legitimate and malicious traffic rates of the zone and view the Guard mitigation actions.

You may require on-demand protection for a zone if there is an attack on the zone and one of the following conditions apply:

- The zone is in the learning process.
- You have enabled the Protect and Learn function but the Guard has not learned the zone traffic characteristics.
- You have accepted policy thresholds that you think do not represent the zone traffic.

When you allow the Guard to learn the zone traffic, the Guard replaces the zone configuration policies used for on-demand protection with policies that it creates specifically for the zone.

Understanding the Protect and Protect and Learn Functions

When you manually activate zone protection, the Guard provides you with the following zone protection options:

- **Protect**—The Guard analyzes the zone traffic and begins producing dynamic filters when it detects anomalies in the zone traffic.
- **Protect and Learn**—The Guard begins the threshold tuning phase of the learning process while monitoring the zone traffic for anomalies using the last accepted threshold values. While analyzing the traffic for the threshold tuning phase, the Guard can automatically adjust the policy thresholds of the zone configuration with new threshold information. If the Guard detects an attack while analyzing the traffic, it suspends the threshold tuning phase to prevent it from learning attack traffic threshold values while it mitigates the attack. When the attack on the zone ends, the Guard resumes the threshold tuning phase.

Automatic and Interactive Zone Operation Modes

You can configure the Guard to protect a zone in either one of the following modes of operation:

- Automatic protect mode—Automatically activates the dynamic filters that it creates during an attack.
- Interactive protect mode—Creates dynamic filters during an attack but does not activate them. Instead, the Guard groups the dynamic filters as *recommendations*. You review the recommendations and decide whether to accept, ignore, or direct them to automatic activation.

You can change the operation mode setting of a zone configuration at any time.

Protection Activation Methods

Depending on how you configured the zone, the Guard activates zone protection based on the zone name or the information it extracts from the traffic you divert to it. The follow protection activation methods are available:

- Zone name—The Guard activates zone protection based on the zone name.
- IP address—The Guard activates zone protection when it receives an external indication that consists of an IP address or subnet that is part of the zone address range.
- Packet—The Guard activates zone protection when it receives packets for a zone in its database.
- IP Address or Packet—The Guard activates zone protection when it receives traffic (packet) that is destined to the zone or when it receives an external indication that consists of an IP address or subnet that is part of the zone address range.

For more information about the protection activation methods, refer to the “[Understanding the Protection Activation Methods](#)” section in [Chapter 4, “Creating and Configuring Zones.”](#)

Managing Zone Protection

This section describes how to manually activate zone protection, deactivate zone protection, and verify traffic diversion and protection after activating zone protection.

This section contains the following topics:

- [Activating Zone Protection](#)
- [Activating On-Demand Protection](#)
- [Protecting an IP Address When the Zone Name is Not Known](#)
- [Verifying Zone Traffic Diversion and Protection](#)
- [Deactivating Zone Protection](#)

Activating Zone Protection


To activate zone protection, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to activate zone protection:

- To activate Protect only, click **Protect** or choose **Protection > Protect** from the zone main menu.
- To activate Protect and Learn, click **Protect & Learn**.

The Guard diverts the zone traffic to itself and begins analyzing the traffic flow for anomalies. The legitimate traffic is injected back into the network where it is forwarded to its intended destination. The malicious traffic is filtered by the Guard and dropped.

The zone name is added to the Protected Zones zone listing in the navigation pane and the Recent Events table lists an event type of *protection-start* with a detail listing of *Zone is protected*.


The zone status icon changes to Protection .

Activating On-Demand Protection

On-demand protection allows you to protect a zone before the Guard can learn the zone-specific traffic characteristics and configure the zone policies accordingly. To use on-demand protection, you create a new zone using one of the zone templates and the Guard protects the zone using the predefined policies and policy thresholds of the zone template. You may require on-demand protection for a zone if there is an attack on the zone and one of the following conditions apply:

- You have activated the learning process, but the Guard zone has not completed the process of learning the zone traffic characteristics.
- You have activated the Protect and Learn function but the Guard has not learned the zone traffic characteristics.
- You have accepted policy thresholds that may not accurately represent the zone traffic rates.

To activate on-demand protection, perform the following steps:

- Step 1** Create a new zone to handle the attack by performing the following steps:
- a. From the navigation pane, click **Guard Summary** to display the Guard summary menu.
 - b. From the Guard summary menu, choose **Zones > Create Zone**.
 - c. Configure the parameters of the zone configuration.
- See the “[Creating a Zone from a Zone Template](#)” section in [Chapter 4, “Creating and Configuring Zones](#)” for more information.
- Step 2** Choose the zone that you just created from the navigation pane. The zone main menu and the zone status screen appear.
- Step 3** Click **Protect** to activate zone protection. The Guard diverts the zone traffic to itself and begins analyzing the traffic flow for anomalies. The legitimate traffic is injected back into the network where it is forwarded to its intended destination. The malicious traffic is filtered by the Guard and dropped.
- The zone name is added to the Protected Zones zone listing in the navigation pane and the Recent Events table lists an event type of *protection-start* with a detail listing of *Zone is protected*.
- The zone status icon changes to Protection .
- Step 4** Analyze the zone traffic patterns (see the “[Viewing the Zone Counters](#)” section in [Chapter 10, “Monitoring Guard and Zone Operations](#)”).

Protecting an IP Address When the Zone Name is Not Known

You can protect a specific IP address even if you do not know the name of the zone that contains the IP address in its IP address range. The Guard activates zone protection for the zone that contains the IP address in its IP address range based on the IP address activation method. See the “[Understanding the Protection Activation Methods](#)” section in [Chapter 4, “Creating and Configuring Zones](#)” for more information.

To activate protection for a specific IP address, perform the following steps:

-
- Step 1** From the navigation pane, click **Guard Summary**. The Guard summary menu appears.
 - Step 2** From the Guard summary menu, choose **Main > Protect IP**. The Protect IP screen appears.
 - Step 3** Enter the IP address to protect as described in [Table 9-1](#).

Table 9-1 Protect IP Address Definition

Parameter	Description
IP address	Specific IP address within a zone address range. Enter the IP address in dotted-decimal notation. For example, enter 192.168.5.6.
IP mask	Subnet mask for which zone protection is activated. Enter the IP address in dotted-decimal notation. For example, enter 255.255.255.252.

- Step 4** Click **OK** to activate protection.
-

Verifying Zone Traffic Diversion and Protection

From the zone status screen, you can view the traffic counters to verify that the zone traffic has been successfully diverted to the Guard and that the protection process is functioning.

From the navigation pane, click on a zone to display the zone status screen. Traffic diversion is functioning if the following items display in the zone status screen:

- The Traffic Rate table shows a legitimate traffic rate that is greater than zero.
- The Recent Events table lists an event type of *protection-start* with a detail listing of *Zone is protected*.

If the malicious traffic rate is greater than zero, an attack is in progress. To verify that zone protection is functioning properly while an attack is in progress, check the following items in the zone status screen:

- The Zone Status table shows the number of active dynamic filters as greater than zero.

If you have configured the zone for interactive protect mode, the number of pending dynamic filters may be greater than zero. You must activate the pending dynamic filters. See the “[Managing Guard Recommendations for Dynamic Filters](#)” section for more information.

- The Traffic Rate table shows that the legitimate traffic rate as greater than zero.


When there is no attack on the zone and no indications of suspicious traffic, the Guard considers all diverted traffic as legitimate and forwards the traffic to the zone, resulting in the Legitimate traffic counter rate being equal to the Received traffic counter rate. See [Chapter 10, “Monitoring Guard and Zone Operations”](#) for details about viewing the Received traffic counter and using other Guard diagnostic tools.

Deactivating Zone Protection

When there is no attack on a zone and you rely on another source for detecting zone traffic anomalies (such as the Detector), you may want to deactivate zone protection and end traffic diversion to the Guard.

To deactivate zone protection, perform the following steps:

-
- Step 1** From the navigation pane, choose a protected zone. The zone main menu and the zone status screen appear.
- Step 2** From the zone status and attack reports screens, verify that the zone is not currently being attacked before deactivating zone protection.
- Step 3** Use one of the following methods to deactivate zone protection:
- From the zone status screen, click **Deactivate**.
 - From the zone main menu, choose **Protection > Deactivate**.

If the Protect function only was enabled, the Guard stops diverting the zone traffic to itself and the zone status changes to Standby .

If the Protect and Learn function was enabled, the Deactivate window appears. Continue to Step 4.

- Step 4** Check the **Stop Protection** check box.
- Step 5** (Optional) Check the **Stop Learning** check box to stop the threshold tuning phase of the learning process and define how the Guard handles the new thresholds by choosing one of the following options from the Deactivate window:
- **Reject**—Ignores the current results of the threshold tuning phase.
 - **Accept**—Uses the current results of the threshold tuning phase in the zone configuration. You can define the threshold selection method to use.

[Table 9-2](#) describes the threshold selection method parameters.

Table 9-2 Threshold Terminating Method

Parameter	Description
Threshold selection method	<p>Method for selecting the thresholds to accept. Choose one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> Accept new thresholds—Saves the results of the leaning process to the zone configuration. Accept max. thresholds—Compares the current policy threshold to the learned threshold and saves the higher of the two to the zone configuration. This is the default method. Accept weighted thresholds—Calculates the policy thresholds to save based on the following formula: $\text{new-threshold} = (\text{learned-threshold} * \text{Weight} + \text{current-threshold} * (100 - \text{Weight})) / 100$ Enter the weight value in the Weight field. Keep current thresholds—Rejects all of the suggested threshold values of the learning process and the policies retain their current thresholds
Weight	<p>Defines the weight that the Guard uses to calculate new thresholds. This option is active only when you choose the Accept weighted thresholds method. Enter a weight value for the Guard to use in the following formula:</p> $\text{new-threshold} = (\text{learned-threshold} * \text{Weight} + \text{current-threshold} * (100 - \text{Weight})) / 100$

- Step 6** Click **OK** to confirm your selection. The Guard stops diverting the zone traffic to itself and the zone name is removed from the Protected Zones list in the navigation pane.

Managing Dynamic Filters

Dynamic filters apply the required protection level to the traffic flow and define how to mitigate the attack. The Guard creates dynamic filters when it identifies an anomaly in the zone traffic, which occurs when the flow exceeds the zone policy thresholds, and continuously adapts this set of filters to the zone traffic and the type of DDoS attack. You can view and manage dynamic filters only when the zone is under attack because the Guard creates dynamic filters only when you have zone protection activated and the zone is under attack.

When the dynamic filter timeout expires, the Guard determines whether or not the dynamic filter should be deactivated based on current traffic conditions. If the Guard determines that the dynamic filter should not be deactivated, the filter remains active for a time span defined by the policy timeout parameter. The Guard deactivates dynamic filters if **one** of the following conditions applies:

- The total zone malicious traffic rate, which equals the sum of the spoofed and dropped traffic, is less than or equal to the zone-malicious-rate termination threshold.
- The dynamic filter measures the traffic rate (the filter rate counter does not display N/A) and the Filter-rate termination threshold is equal to or greater than both of the following:
 - The dynamic filter current traffic rate.

- The dynamic filter average traffic rate during a user-configured time span. This time span is defined by the policy timeout parameter.



Note Dynamic filters with an action of to-user-filters, block-unauthenticated, redirect/zombie, or notify do not measure traffic rate.

To manually control zone protection during an attack, you can add or delete a dynamic filter during an attack. The Guard removes all dynamic filters when the attack ends.

This section contains the following topics:

- [Displaying the Dynamic Filters List](#)
- [Displaying Dynamic Filter Details](#)
- [Adding a Dynamic Filter](#)
- [Deleting a Dynamic Filter](#)
- [Preventing the Production of Dynamic Filters](#)

Displaying the Dynamic Filters List

To display the list of dynamic filters, perform the following steps:

- Step 1** From the navigation pane, choose a protected zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to display the list of dynamic filters:
- From the zone main menu, choose **Protection > Dynamic filters**.
 - From the Zone Status table, click **Active dynamic filters**.

The Dynamic Filters screen appears.

The Dynamic Filters table displays the dynamic filters according to the policy that created them and provides information about the ongoing attack. [Table 9-3](#) describes the information displayed in the Dynamic Filters table.

Table 9-3 *Field Descriptions for Dynamic Filters Table*

Field	Description
Created by	Policy that created the dynamic filter. Click on the policy name to display the policy details.
Activation	Date and time that the filter was activated.
Expiration	Filter expiration time. Once the filter expires, the Guard decides whether or not to deactivate the dynamic filter based on the dynamic filter termination criteria. If the Guard determines that the dynamic filter should not be deactivated, the filter remains active for a time span defined by the policy timeout parameter.
Src IP	Source IP address on which the dynamic filter is applied.
Protocol	Protocol number on which the dynamic filter is applied.

Table 9-3 *Field Descriptions for Dynamic Filters Table (continued)*

Field	Description
Dst Port	Destination port on which the dynamic filter is applied.
Fragments	Fragmentation settings of the traffic flow, which specifies whether the attack stream contains fragmented packets.
Action	Action taken by the dynamic filter. Choose one of the following dynamic filter actions: <ul style="list-style-type: none"> to-user-filters—Forwards the traffic to the user filters. If you have modified the default user filters, you must make sure that there is a user filter to handle the dynamic filter. filter/strong—Applies Strong protection anti-spoofing functions to the specific traffic. filter/drop—Drops the traffic. block-unauthenticated-basic—Enhances the Basic anti-spoofing functions so that they drop traffic flows that have not been authenticated. block-unauthenticated-strong—Enhances the Strong anti-spoofing functions so that they drop traffic flows that have not been authenticated. block-unauthenticated-dns—Drops traffic flows flowing to Domain Name System (DNS) UDP servers (protocol=UDP, port=53) that the DNS anti-spoofing functions have defined as unauthenticated. redirect/zombie—Enhances authentication for all user filters with an action of basic/redirect.
Rate (pps)	Approximate attack rate in packets per second.
Details	Indication that additional information is available for this filter. Click i for additional information.

An asterisk (*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

See the “[Displaying Dynamic Filter Details](#)” section for information about viewing the details of a specific dynamic filter.

Displaying Dynamic Filter Details

To display detailed information for a specific dynamic filter, perform the following steps:

-
- Step 1** From the navigation pane, choose a protected zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to view the list of dynamic filters:
- From the zone main menu, choose **Protection > Dynamic filters**.
 - From the Zone Status table, click **Active dynamic filters** (this link is only active when there are active dynamic filters).

The Dynamic Filters screen appears.

- Step 3** Click **i** in the Details column of the dynamic filter for which you want to display the details. The Dynamic Filter Details screen appears.

The Dynamic Filter Details screen contains three tables that describe the following attack information:

- The policy that created the filter.
- The attack that was mitigated. The mitigated flow can have a wider range than the detected attack flow. For example, a non-spoofed attack on port 80 blocks all TCP traffic from the originating source IP and not only port 80.
- The trigger that created the filter. [Table 9-4](#) describes the trigger parameters.

Table 9-4 Field Descriptions for Triggers

Field	Description
Policy Threshold	Policy threshold that the attack traffic exceeded.
Triggering rate	Approximate attack rate that triggered the production of the filter.

Adding a Dynamic Filter

During an attack on the zone, you can add a dynamic filter to control zone protection.

To add a dynamic filter, perform the following steps:

- Step 1** From the navigation pane, choose a protected zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to display the list of dynamic filters:
- From the zone main menu, choose **Protection > Dynamic filters**.
 - From the zone status table on the zone status page, click **Active dynamic filters**.
- The Dynamic filters screen appears.
- Step 3** Click **Add**. The Add Dynamic Filter screen appears.
- Step 4** Define the dynamic filter parameters as described in [Table 9-5](#).

Table 9-5 Field Descriptions for Dynamic Filters

Field	Description
Source IP	Directs traffic from a specific IP address to the dynamic filter. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1). Use an asterisk (*) or leave blank to indicate any IP address.
Source Subnet	Directs traffic from a specific subnet to the dynamic filter. Choose the subnet from the Source Subnet drop-down list.
Protocol	Directs traffic from a specific protocol to the dynamic filter. Use an asterisk (*) or leave blank to specify any protocol. Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid protocol numbers: http://www.iana.org/assignments/protocol-numbers

Table 9-5 *Field Descriptions for Dynamic Filters (continued)*

Field	Description
Dst Port	<p>Directs traffic destined for a specific port to the dynamic filter. Use an asterisk (*) or leave blank to specify any destination port.</p> <p>Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid port numbers:</p> <p>http://www.iana.org/assignments/port-numbers</p>
Fragments	<p>Specifies the fragmentation settings on which the filter acts. Choose the desired traffic type from the Fragments drop-down list:</p> <ul style="list-style-type: none"> • without—Dynamic filter processes nonfragmented traffic. • with—Dynamic filter processes fragmented traffic. • *—Dynamic filter processes fragmented and nonfragmented traffic.
Action	<p>Specifies the action that the filter performs on the specific traffic type. Choose the filter action from the Action drop-down list:</p> <ul style="list-style-type: none"> • to-user-filters—Forwards the specific traffic to the user filters. If you have modified the default user filters, you must make sure that there is a user filter to handle these dynamic filters. • filter/strong—Applies the Strong protection level anti-spoofing functions to the specific traffic. • filter/drop—Drops the traffic. • block-unauthenticated-basic—Enhances the Basic protection level anti-spoofing functions so that they drop traffic flows that have not been authenticated. • block-unauthenticated-strong—Enhances the Strong protection level anti-spoofing functions so that they drop traffic flows that have not been authenticated. • block-unauthenticated-dns—Drops the traffic that flows to DNS UDP servers (protocol=UDP, port=53) that were not authenticated by the DNS anti-spoofing functions. • redirect/zombie—Enhances authentication for all user filters with an action of basic/redirect.
Timeout (Sec)	<p>Minimum time that the filter is active. Choose one of the following timeout options:</p> <ul style="list-style-type: none"> • Check the Forever check box for an unlimited time. • Check the seconds check box and enter an integer from 1 to 3,000,000 that specifies the time (in seconds) for the filter to be active.

Step 5 Choose one of the following options:

- **OK**—Saves the dynamic filter information. The Guard activates the new dynamic filter.
- **Cancel**—Exits the Add Dynamic filter screen without saving any information. The Dynamic Filters screen appears.

Deleting a Dynamic Filter

You can delete a dynamic filter to prevent the Guard from applying the dynamic filter action on the traffic flow. Deleting a dynamic filter is only effective for a limited period of time because the Guard continues to configure new dynamic filters when zone protection is enabled and there are changes in the attack traffic flow. To prevent the Guard from producing unwanted dynamic filters, see the [“Preventing the Production of Dynamic Filters”](#) section.

To delete a dynamic filter, perform the following steps:

-
- Step 1** From the navigation pane, choose a protected zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to view the dynamic filters:
- From the zone main menu, choose **Protection > Dynamic filters**.
 - From the Zone Status table, click **Active dynamic filters**.
- The Dynamic filters screen appears.
- Step 3** Check the check box next to the dynamic filter that you want to delete.
- Step 4** Click **Delete** to delete the dynamic filter.
-

Preventing the Production of Dynamic Filters

If the Guard is applying dynamic filters to traffic that you want to forward to the zone, you can prevent the Guard from producing these dynamic filters by performing one of the following actions:

- Deactivate the policy that produces the dynamic filters (see the [“Modifying Policy Parameters”](#) section in [Chapter 8, “Managing Zone Policies”](#)). To view the list of dynamic filters and find out which policy produced the unwanted dynamic filters, see the [“Displaying the Dynamic Filters List”](#) section.
- Configure a bypass filter for the desired traffic flow. See the [“Managing Bypass Filters”](#) section in [Chapter 5, “Configuring Zone Filters”](#) for more information.
- Increase the threshold of the policy that produced the undesired dynamic filter. See the [“Modifying Policy Parameters”](#) section in [Chapter 8, “Managing Zone Policies”](#) for more information.

Activating Automatic or Interactive Protect Mode

You can control activation of the zone dynamic filters by configuring the Guard to operate in one of the following modes when protecting the zone:

- Automatic protect mode—The Guard activates all dynamic filters as it creates them. This operation mode is the default.
- Interactive protect mode—The Guard does not automatically activate the dynamic that it creates for the zone. Instead, it saves the dynamic filters and groups them as recommendations. You are required to act on the dynamic filter recommendations that the Guard produces during an attack. You review the recommendations and decide which ones to accept, ignore, or direct to automatic activation.

You configure the protect mode operation for a zone as part of the zone configuration and can change the zone protect mode setting at any time, including when the Guard is mitigating an attack on the zone.

This section contains the following topics:

- [Activating Automatic Protect Mode](#)
- [Activating the Zone in Interactive Protect Mode](#)
- [Taking Action When the Number of Pending Dynamic Filters Exceeds 1000](#)

Activating Automatic Protect Mode

To activate the zone in automatic protect mode, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
 - Step 2** From the zone main menu, choose **Configuration > General**. The General screen appears.
 - Step 3** Click **Config**. The Config screen displays.
 - Step 4** From the Operation Mode drop-down list, choose **automatic**.
 - Step 5** Click **OK**. The Guard updates the zone configuration with the new zone operation mode setting. If zone protection is currently active, the Guard automatically activates all the pending dynamic filters and new dynamic filters.
-

Activating the Zone in Interactive Protect Mode

To activate the zone in interactive protect mode, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
 - Step 2** From the zone main menu, choose **Configuration > General**. The General screen appears.
 - Step 3** Click **Config**. The Config screen displays.
 - Step 4** From the Operation Mode drop-down list, choose **interactive**.

- Step 5** Click **OK**. The Guard updates the zone configuration with the new zone operation mode setting. If zone protection is currently active, the Guard produces recommendations when it detects an anomaly in the zone traffic.
-

Taking Action When the Number of Pending Dynamic Filters Exceeds 1000

When the number of pending dynamic filters exceeds 1000, the Guard performs the following actions:

- Displays an error message instructing you to deactivate the zone and reactivate it in automatic detect mode.
- Records the recommendations in the zone log file and report and then discards them.

To detect anomalies in the zone traffic when the Guard has more than 1000 pending dynamic filters, you must configure the zone for automatic protect mode operation by performing the following steps:

- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
- Step 2** Click **Deactivate**. The Guard stops zone protection and deletes all pending dynamic filters.
- Step 3** Choose **Configuration > General** from the zone main menu. The General screen appears.
- Step 4** Click **Config**. The Config screen displays.
- Step 5** From the Operation Mode drop-down list, choose **automatic** and then click **OK**. The zone configuration is updated with the new protection setting.
- Step 6** Click **Protect**. The Guard begins the automatic protect mode operation and activates all dynamic filters as it creates them.
-

Managing Guard Recommendations for Dynamic Filters

When the Guard performs zone protection in interactive operation mode, it generates a list of the dynamic filters that it creates to mitigate an attack but does not activate. The dynamic filters on the list are known as *pending dynamic filters*. The Guard groups the pending dynamic filters based on the policies that produced them and presents them to you as *recommendations*. You can choose to act on a Guard recommendation (including all of the pending dynamic filters associated with it) or you can act on each pending dynamic filter separately.

This section contains the following topics:

- [Displaying Recommendations](#)
- [Acting on Recommendations](#)
- [Displaying the Pending Dynamic Filters of a Recommendation](#)
- [Displaying Pending Dynamic Filter Details](#)
- [Accepting Pending Dynamic Filters](#)

Displaying Recommendations

The Guard displays the recommendations icon  in the following locations when new recommendations are available:

- The navigation pane, next to the zone icon in the **All Zones** list
- The navigation pane, next to the zone icon in the **Protected Zones** list
- The zone pages, in the zone status bar
- The Zone List table

When the Guard has new recommendations, the number of pending dynamic filters that the zone status screen displays is greater than zero.

To view the list of recommendations, perform the following steps:

- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to display the list of recommendations:
- From the zone main menu, choose **Protection > Recommendations**.
 - From the Zone Status table, click **Pending Dynamic filters**.

The Recommendations screen appears.

Table 9-6 describes the fields in the Recommendations table.

Table 9-6 *Field Descriptions for Recommendations Table*

Field	Description
ID	Identification number that the Guard assigned to the recommendation.
Recommendation	Action that the Guard recommends.
Created By	Policy that created the filter. Click on the policy name to view the policy details.
# of PFs	Number of pending dynamic filters that are associated with the recommendation. Each pending filter was created as a result of traffic flow that exceeded the policy threshold. Click on the number to view the pending dynamic filters associated with the recommendation.
Attack flow	Attack flow information. The following attack flow details are provided: <ul style="list-style-type: none"> • Src IP—Source IP address • Protocol—Protocol number • Dst Port—Destination port • Dst IP—Destination IP address
Thr.	Policy threshold that the attack flow exceeded.
Min.	Minimum attack rate. The rate of the lowest pending dynamic filter is displayed for recommendations that include several pending filters.
Max.	Maximum attack rate. The rate of the highest pending dynamic filter is displayed for recommendations that include several pending dynamic filters.
Creation	Date and time that the recommendation was created.

The Guard uses an asterisk (*) as a wildcard for one of the parameters to indicate the following:

- The value is undetermined.
- More than one value was measured for the parameter. To display the different values, view the complete list of pending dynamic filters.

Acting on Recommendations

To act on recommendations, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
- Step 2** Use one of the following methods to display the list of recommendations:
- From the zone main menu, choose **Protection > Recommendations**.
 - From the Zone Status table, click **Pending Dynamic filters**.
- The Recommendations screen appears.
- Step 3** In the Filters timeout box, enter the timeout value (in seconds) for the filter.
- Step 4** Check the check box next to the recommendations on which you want to act.
- Step 5** Click one of the following buttons:
- **accept**—Accepts the specific recommendation. The Guard activates the pending dynamic filters that are associated with the recommendation.
 - **always-accept**—Accepts the specific recommendation. During the current attack period, the Guard automatically accepts the recommendations of the policy that produced the recommendation. If you take this action, the Guard no longer displays such recommendations.
 - **always-ignore**—Ignores the specific recommendation. During the current attack period, the Guard automatically ignores the recommendations of the policy that produced the recommendation. To prevent a policy from producing recommendations in future attacks, disable or deactivate the policy (see the “[Modifying Policy Parameters](#)” section in [Chapter 8, “Managing Zone Policies](#)”).

You can change an always-ignore or always-accept decision made on a specific recommendation by changing the interactive-status of the policy that created the pending dynamic filters of the recommendation.

You can selectively accept pending dynamic filters instead of accepting all the dynamic filters associated with a recommendation. See the “[Displaying the Pending Dynamic Filters of a Recommendation](#)” section for more information.

Displaying the Pending Dynamic Filters of a Recommendation

To display the pending dynamic filters that make up a recommendation, perform the following steps:

-
- Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

Step 2 Use one of the following methods to display the list of recommendations:

- From the zone main menu, choose **Protection > Recommendations**.
- From the Zone Status table, click **Pending Dynamic filters**.

The Recommendations screen appears.

Step 3 Click the numeric value that is listed in the # of PFs (Pending Filters) column of the recommendation that you want to display. The Pending Dynamic Filters screen appears.

Table 9-7 describes the fields in the Pending Dynamic Filters table.

Table 9-7 Field Descriptions for Pending Dynamic Filters

Field	Description
Created by	Policy that created the pending dynamic filter. Click on the policy name to display the Policy details. See Chapter 8, “Managing Zone Policies” for more information.
Activation	Date and time that the pending dynamic filter was created.
Src IP	Source IP address of the attack stream.
Protocol	Protocol number of the attack stream.
Dst Port	Destination port of the attack stream.
Fragments	Fragmentation setting of the attack stream, which indicates if the attack stream contains fragmented packets.
Action	Action taken by the filter.
Recent rate	Current attack rate measured by the pending dynamic filter.
Rate (pps)	Triggering rate, which is the approximate attack rate that triggered the production of the dynamic filter.
Details	Indication that additional information is available for this filter. Click i for additional information.

An asterisk (*) for any of the parameters indicates one of the following conditions:

- The value is undetermined.
- More than one value was measured for the filter parameter.

The Guard activates the pending dynamic filters produced by the policies for the period of time that you define (filter timeout).

Displaying Pending Dynamic Filter Details

To display the detailed information of a dynamic filter, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

Step 2 Use one of the following methods to display the list of recommendations:

- From the zone main menu, choose **Protection > Recommendations**.
- From the Zone Status table, click **Pending Dynamic filters**.

The Recommendations screen appears.

Step 3 Click the numeric value that is listed in the # of PFs (Pending Filters) column of the recommendation that you want to display. The Pending dynamic filters screen appears.

Step 4 In the details column of the desired pending dynamic filter that you want to display, click **i**. The Filter Details screen appears.

The pending dynamic filter details contains three tables that provide the following information:

- Policy that created the pending dynamic filter.
- Attack flow.
- Trigger for the creation of the pending dynamic filter. The Rates table displays the policy threshold that the attack traffic exceeded and the approximate attack rate that triggered the production of the pending dynamic filter.

Accepting Pending Dynamic Filters

To selectively accept pending dynamic filters, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

Step 2 Use one of the following methods to display the list of recommendations:

- From the zone main menu, choose **Protection > Recommendations**.
- From the Zone Status table, click **Pending Dynamic filters**.

The Recommendations screen appears.

Step 3 Click the numeric value that is listed in the # of PFs (Pending Filters) column of the recommendation that you want to display. The Pending Dynamic Filters screen appears.

Step 4 In the **Filters timeout** box, enter a timeout in seconds for the dynamic filter.

Step 5 Check the check box next to the pending dynamic filters that you want to activate.

Step 6 Click **Accept**. The Guard activates the selected pending dynamic filters.
