CHAPTER 9

Activating Anomaly Detection

This chapter describes how to activate anomaly detection using the WBM. When you activate anomaly detection for a zone, the Cisco Traffic Anomaly Detector Module (Detector module) applies the zone policies to the copy of the zone traffic that it receives. When a traffic anomaly triggers a policy action by exceeding the policy threshold (indicating an attack), the Detector module either sends you a notification or activates a Cisco Anomaly Guard (Guard).

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

This chapter contains the following sections:

Understanding the Anomaly Detection Activation Options

The Detector module provides you with several options for performing anomaly detection. For example, you can allow the Detector module to manage all aspects of the anomaly detection operation or you can monitor and direct the Detector module during an attack.

This section contains the following topics:

Detect, Detect and Learn

When you activate zone anomaly detection, the Detector module provides you with the following options:

- Detect—Analyzes the zone traffic and begins producing dynamic filters when it detects a traffic anomaly.
- Detect and Learn—Analyzes zone traffic for traffic anomalies and at the same time begins the threshold tuning phase of the learning process. While analyzing the traffic for the threshold tuning phase, the Detector module can automatically adjust the policy thresholds of the zone configuration with new threshold information. If the Detector module detects an attack while analyzing the traffic, it stops the threshold tuning phase to prevent it from learning attack traffic threshold values.

Automatic and Interactive Operation Modes

You can configure the Detector module to detect traffic anomalies in a zone in either one of the following modes of operation:

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

Managing Anomaly Detection

This section describes how to manually activate and deactivate zone traffic anomaly detection.

This section contains the following topics:

Activating Anomaly Detection

To activate zone anomaly detection, perform the following steps:

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

Step 2 Use one of the following methods to activate anomaly detection:

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

The Detector module begins analyzing the traffic flow for traffic anomalies.

The zone name is added to the Under Detection zone listing in the navigation pane and the Recent Events table lists an event type of *detection-start* with a detail listing of *Zone is under detection*.

The zone status icon changes to Detection  .

Verifying Traffic Anomaly Detection

From the zone status screen, you can view the traffic counter to verify that the anomaly detection process is functioning properly.

Click a zone under detection from the navigation pane to display the zone status screen. Anomaly detection is functioning if the following conditions exist:

- The Recent Events table lists an event type of *detection-start* with a detail listing of *Zone is under detection*.
- The Traffic Rate table shows the Received traffic rate is greater than zero.

Deactivating Anomaly Detection

To deactivate anomaly detection, perform the following steps:

Step 1 From the navigation pane, click a zone under detection. The zone main menu and the zone status page appear.

Step 2 Use one of the following methods to deactivate anomaly detection:

- From the zone status screen, click **Deactivate.**
- From the zone main menu, choose **Detection > Deactivate.**

If the Detect function was enabled, the Detector module stops analyzing zone traffic and the zone status changes to Standby  .

If the Detect and Learn function was enabled, the Deactivate window appears (continue to Step 3).

Step 3 Check the **Stop Detection** check box.

Step 4 (Optional) Check the **Stop Learning** check box to stop the threshold tuning phase of the learning process and define how the Detector module 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. Define the threshold selection method to use.

  Table 9-1 describes the threshold selection method parameters.

Table 9-1 Threshold Terminating Method

Parameter	Description
Threshold selection method	Method for selecting the thresholds to accept. Choose one of the following options from the drop-down list: • Accept new thresholds—Saves the results of the learning 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: new-threshold = (learned-threshold * Weight + current-threshold * (100 – 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	Defines the weight that the Detector module uses to calculate new thresholds. This option is active only when you choose the Accept weighted thresholds method. Enter a weight value for the Detector module to use in the following formula: new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100

Step 5 Click **OK** to confirm your selection.

The Detector module stops analyzing zone traffic, and the zone name is removed from the Under Detection list in the navigation pane.

Managing Dynamic Filters

Dynamic filters apply the required protection level to the traffic flow and define how to handle the attack. The Detector module 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 Distributed Denial of Service (DDoS) attack. You can view and manage dynamic filters only when the zone is under attack because the Detector module creates dynamic filters only when you have anomaly detection activated and the zone is under attack.

To manually control zone anomaly detection during an attack, you can add or delete a dynamic filter during an attack. The Detector module deletes all dynamic filters when the attack ends. The Detector module supports a maximum of 150,000 dynamic filters that are concurrently active in all zones.

This section contains the following topics:

Displaying the Dynamic Filters List

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

Step 1 From the navigation pane, choose a zone under detection. 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 **Detection > Dynamic filters.**
- From the Zone Status table, click **Active Dynamic filters.**

The Dynamic Filters screen appears.

The Dynamic Filters table displays the dynamic filters filtered according to the policy that created them and provides information about the ongoing attack. Table 9-2 describes the information in the Dynamic Filters table.

Table 9-2 Field Descriptions for Dynamic Filters

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 dynamic filter was activated.
Expiration	Time that the filter is due to expire. After this time, the dynamic filter is deleted.
Src IP	Source IP address of the traffic that the filter processes.

Table 9-2 Field Descriptions for Dynamic Filters (continued)

Field	Description
Dst IP	Destination IP address on which the dynamic filter is applied. The Detector module activates protection on the Guard based on the destination IP address and the value of the Protect-IP state that is configured for the zone.
Protocol	Protocol number of the traffic that the filter processes.
Dst Port	Destination port of the traffic that the filter processes.
Fragments	Fragmentation settings of the traffic flow, which specifies whether the attack stream contains fragmented packets.
Action	Action taken by the dynamic filter.
Rate (pps)	Current traffic rate in packets per second that is measured for this filter.
Details	Indication that additional information is available for this filter. Click **i** to view additional information.

The Src IP, Protocol, and Dst 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.

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 zone under detection. 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 **Detection > Dynamic filters.**
- From the Zone Status table, click **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 information:

- The policy that created the dynamic filter.
- Information about the attack flow.
- Information about the trigger that created the dynamic filter. Table 9-3 describes the trigger parameters.

Table 9-3 Field Descriptions for Triggers

Field	Description
Policy Threshold	Policy threshold that was exceeded by the attack flow.
Triggering rate	Approximate attack rate that triggered the creation of the dynamic filter.

Adding Dynamic Filters

During an attack on the zone, you can add a dynamic filter to manage zone anomaly detection. You can configure a dynamic filter to activate the Guards that are defined in the remote Guard lists to protect the zone. The destination IP address of the dynamic filter must match the Protect-IP state and the address range that is configured for the zone or the remote Guard activation fails. 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, enter an asterisk (*) in the Destination IP field or leave the field blank.

  You must configure the Protect-IP state of the zone to 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, enter the IP address in the Destination IP field.

  You must configure the Protect-IP state of the zone to Only Dst IP (only destination IP address).

You can configure remote Guard lists using the CLI only. See the *Cisco Traffic Anomaly Detector Configuration Guide* for information about using the CLI.

See the "Configuring Guard Zones" section in Chapter 4, "Creating and Configuring Zones" for more information about the zone Protect-IP state.

To add a dynamic filter, perform the following steps:

Step 1 Choose a zone under detection from the navigation pane. 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 **Detection > 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 9-4.

Table 9-4 Field Descriptions for Dynamic Filters

Field	Description
Destination IP	The Detector module activates protection on the remote Guard based on the destination IP address and the value of the Protect-IP state that is configured for the zone. Leave blank or enter an asterisk (*) for any IP address.

Table 9-4 Field Descriptions for Dynamic Filters (continued)

Field	Description
Action	Action that the Detector module performs when the traffic matches the filter. The Detector module supports the remote-activate action only, which enables it to activate the remote Guards that you have defined in the remote Guard lists to protect the zone. Use the CLI to configure the remote Guard lists. For more information about accessing and using the Detector module CLI, see the *Cisco Traffic Anomaly Detector Module Configuration Guide*.
Timeout (Sec)	Minimum time that the filter is active. Choose one of the following filter timeout options: • Check the Forever check box for an infinite amount of time. • Check the seconds check box and enter the amount of time in seconds.

Step 5 Click **OK** to activate the dynamic filter.

Deleting Dynamic Filters

You can delete a dynamic filter, but deleting the filter is effective for a limited period of time only because the Detector module continues to configure new dynamic filters as changes to the attack traffic occur. To prevent the Detector module from producing unwanted dynamic filters, see the "Preventing the Creation of Unwanted Dynamic Filters" section.

To delete a dynamic filter, perform the following steps:

Step 1 From the navigation pane, choose a zone under detection. 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 **Detection > 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 Creation of Unwanted Dynamic Filters

You can prevent the Detector module from producing unwanted 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" for information about changing the policy operating state. 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. For information about configuring a bypass filter, see the "Managing Bypass Filters" section in Chapter 5, "Configuring Zone Filters."
- Increase the threshold of the policy that produced the undesired dynamic filter. For information about modifying the policy threshold, see the "Modifying Policy Parameters" section in Chapter 8, "Managing Zone Policies".

Activating Automatic or Interactive Detect Mode

You can control activation of the zone dynamic filters by configuring the Detector module to operate in one of the following modes when detecting anomalies in the zone traffic:

- Automatic detect mode—The Detector module activates the dynamic filter as soon as it creates the filter for the zone. This operation mode is the default.
- Interactive detect mode—The Detector module does not automatically activate the dynamic that it creates for the zone. Instead, it saves the dynamic filters and groups them as recommendations. You review the list of recommendations and decide which recommendations to accept, ignore, or direct to automatic activation.

You configure the anomaly detection operating mode as part of the zone configuration and can change the operating mode setting at any time, including when the zone is under attack.

This section contains the following topics:

Activating Automatic Detect Mode

To activate the zone in automatic detect 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 Choose **Configuration > General** from the zone main menu. The General screen appears.

Step 3 Click **Config**. The Config screen displays.

Step 4 From the Operation Mode parameter drop-down list, choose **automatic.**

Step 5 Click **OK**. The Detector module updates the zone configuration with the new operation mode setting. If the zone operation is currently active, the Detector module automatically activates all pending and new dynamic filters.

Activating Interactive Detect Mode

To activate the zone in interactive detect 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 Choose **Configuration > General** from the zone main menu. The General screen appears.

Step 3 Click **Config**. The Config screen displays.

Step 4 From the Operation Mode parameter drop-down list, choose **interactive.**

Step 5 Click **OK**. The Detector module updates the zone configuration with the new operation mode setting. If anomaly detection is currently active, the Detector module produces recommendations when an attack is detected.

Taking Action When the Number of Pending Dynamic Filters Exceeds 1000

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

- Displays an error message that instructs 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 Detector module has more than 1000 pending dynamic filters you must configure the zone for automatic detect mode 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 Detector module stops anomaly detection 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 anomaly detection setting.

Step 6 Click **Protect**. The Detector module begins the automatic detect mode operation and activates all dynamic filters as it creates them.

Managing Detector Module Recommendations for Dynamic Filters

When the Detector module performs anomaly detection for the zone in interactive detect mode, it generates a list of the dynamic filters that it creates during an attack. The dynamic filters on the list are known as *pending dynamic filters*. The Detector module groups the pending dynamic filters according to the policies that produced them and presents them to you as Detector module *recommendations*.

The recommendations provide a summary of the pending filters and include information about the name of the policy that caused the creation of the pending dynamic filters, the data on the traffic anomaly that resulted in the policy activation, the number of pending dynamic filters, and the recommended action. You can choose to act on a Detector module 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:

Viewing Recommendations

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

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

When the Detector module has new recommendations, the number of pending dynamic filters is greater than zero. The Detector module displays the number of pending dynamic filters in the zone status screen in the Zone Status table.

To view the list of Detector module 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 **Detection > Recommendations**.
- From the zone status table on the zone status screen, click **Pending Dynamic filters**.

The Recommendations screen appears.

Table 9-5 describes the fields in the Recommendations table.

Table 9-5 Field Descriptions for Recommendations Table

Field	Description
ID	Identification number that the Detector module assigned to the recommendation.
Recommendation	Action that the Detector module 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: • **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 filters.
Creation	Date and time that the recommendation was created.

The Detector module 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.

Managing Recommendations

You can decide whether or not to activate Detector module recommendations. You can apply your decision to all recommendations, a specific recommendation, or to a specific pending dynamic filter. Your decisions determine whether or not the pending dynamic filters in a policy become dynamic filters and for how long.

You can instruct the Detector module to automatically activate the pending dynamic filters of a specific policy. You can also instruct the Detector module to prevent policies from producing recommendations.

The Detector module policies continue to produce recommendations if the zone is in interactive protect mode and a DDoS attack is in progress. We recommend that you display the zone status when you manage recommendations in order to verify the zone status and determine if additional actions are required.

To manage 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 **Detection > Recommendations**.
- From the zone status table on the zone status screen, 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 that you want to accept.

Step 5 Choose one of the required actions:

- **accept**—Accepts the specific recommendation. The Detector module activates the pending dynamic filters associated with the recommendation.
- **always-accept**—Accepts the specific recommendation. The decision applies automatically whenever the recommendation policy produces new recommendations. Pending dynamic filters automatically become dynamic filters. If you take this action, the Detector module no longer displays such recommendations.
- **always-ignore**—Ignores the specific recommendation. No dynamic filter or pending dynamic filters are produced. The decision automatically applies to all future recommendations produced by the policy. If you decide to always ignore a recommendation, the Detector module no longer displays it. 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").

Note You can change an **always-ignore** 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 pending dynamic filters associated with a recommendation. See the "Accepting a Pending Dynamic Filter" section for more information.

Viewing the Pending Dynamic Filters of a Recommendation

To view the pending dynamic filters associated with a Detector module 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 **Detection > Recommendations**.
- From the zone status table on the zone status screen, 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. The Pending dynamic filters screen appears.

Table 9-6 describes the fields in the Pending Dynamic Filters table.

Table 9-6 Field Descriptions for Pending Dynamic Filters

Field	Description
Created by	Policy that created the 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 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 filter, which indicates if the attack stream contains fragmented packets.
Action	Action taken by the filter.
Recent rate	Current attack rate measured by the filter.
Rate (pps)	Triggering rate. The approximate attack rate that triggered the production of the pending dynamic filter.
Details	Status of whether or not additional information is available for this filter. Click **i** for additional information.

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

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

The Detector module activates the pending dynamic filters that are produced by the policies for at least a user-defined time span (filter timeout).

Viewing 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 **Detection > Recommendations**.
- From the zone status table on the zone status screen, click **Pending Dynamic filters**.

The Recommendations screen appears.

Step 3 Click the numeric value listed in the # of PFs (Pending Filters) column of the recommendation. The Pending Dynamic Filters screen appears.

Step 4 Click **i** in the details column of the desired pending dynamic filter. The Filter Details screen appears.

The Filter Details screen contains three tables that provide the following information:

- Policy that created the filter.
- Attack flow.
- Trigger for the filter creation (displays the policy threshold that the attack flow exceeded and the approximate attack rate that triggered the production of the filter).

Accepting a Pending Dynamic Filter

To selectively accept a pending 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 **Detection > Recommendations**.
- From the Zone Status table on the zone status screen, 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. The Pending Dynamic Filters screen appears.

Step 4 In the Filters timeout box, enter the timeout value 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** to activate the pending dynamic filters.