



CHAPTER 5

Configuring Zones

This chapter describes how to create and manage zones on the Cisco Guard (Guard).

This chapter refers to the Cisco Detector (Detector), the companion product of the Guard. The Detector 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 Zones](#)
- [Using Zone Templates](#)
- [Creating a New Zone](#)
- [Configuring Zone Attributes](#)
- [Configuring the Zone IP Address Range](#)
- [Synchronizing Zone Configurations with a Detector](#)

Understanding Zones

A zone is a network element that the Guard protects against Distributed Denial of Service (DDoS) attacks. A zone can be any combination of the following elements:

- A network server, client, or router
- A network link, subnet, or an entire network
- An individual Internet user or a company
- An Internet Service Provider (ISP)

The Guard can protect different zones simultaneously providing their network address ranges do not overlap.

The zone configuration process consists of the following tasks:

- **Creating a zone**—You create a zone by defining the zone name and the zone description. See the [“Creating a New Zone” section on page 5-3](#) for more information.
- **Configuring the zone network definition**—You configure the zone network definitions that include the network IP address and subnet mask. See the [“Configuring Zone Attributes” section on page 5-5](#) for more information.

- Configuring the zone filters—You can configure the zone filters. The zone filters apply the required protection level to the zone traffic and define the way the Guard handles specific traffic flows. See [Chapter 6, “Configuring Zone Filters,”](#) for more information.
- Learning the zone traffic characteristics—You can create the zone protection policies that enable the Guard to analyze a particular traffic flow and take action if the traffic flow exceeds a policy threshold. The Guard constructs the policies in a learning process that consists of two phases: policy construction and threshold tuning. See [Chapter 8, “Learning the Zone Traffic Characteristics,”](#) for more information.

Using Zone Templates

A zone template defines the default configuration of a zone.

[Table 5-1](#) displays the zone templates.

Table 5-1 Zone Templates

Template	Description
GUARD_DEFAULT	Default zone template. The Guard may change the packet source IP address to the Guard TCP-proxy IP address. You can use this zone template if you do not use ACLs ¹ , access policies, or load-balancing policies that are based on the incoming IP address for the zone network.
GUARD_LINK Templates	<p>Zone templates designed for on-demand protection of large subnets segmented according to zones with a known bandwidth. We recommend that you activate zone protection on these zones for the attacked address range only so that you can focus on the zone protection requirements and save Guard resources. Configure the method that the Guard uses to activate zone protection for the attacked subnet or range by using the activation-extent ip-address-only command. To enable a Detector to activate zone protection on the Guard for the attacked IP address or subnet only, use the protect-ip-state dst-ip-by-name command on the Detector.</p> <p>The following bandwidth-limited link zone templates are available for 128-Kb, 1-Mb, 4-Mb, and 512-Kb links:</p> <p>GUARD_LINK_128K GUARD_LINK_1M GUARD_LINK_4M GUARD_LINK_512K</p>
GUARD_LINK Templates (continued)	You cannot perform the policy construction phase of the learning process for zones that were created from these templates.
GUARD_TCP_NO_PROXY	Zone template designed for a zone for which no TCP proxy is to be used. You can use this zone template if the zone is controlled based on the IP addresses, such as an IRC ² server-type zone, or if you do not know the type of services running on the zone.

Table 5-1 Zone Templates (continued)

Template	Description
GUARD_VOIP	<p>Zone template designed for a zone that contains a VoIP³ server that uses SIP⁴ over UDP to establish VoIP sessions and RTP/RTCP⁵ to transmit voice data between SIP end points after sessions are established.</p> <p>Zones that are created from the GUARD_VOIP zone template contain specific policies to handle VoIP traffic that are produced from the sip_udp policy template (see the “Understanding and Configuring Policy Templates” section on page 7-2 for more information).</p>

1. ACL = Access Control List
2. IRC = Internet Relay Chat
3. VoIP = Voice over IP
4. SIP = Session Initiation Protocol
5. RTP/RTCP = Real-Time Transport Protocol/Real-Time Control Protocol

Creating a New Zone

You can create a zone and configure the zone name, description, network address, operation definitions, and networking definitions. When you create a new zone, you can use an existing zone as a template or you can create a zone using a predefined zone template. The zone template that you use defines the initial policy and filter configurations of the zone.

The three ways that you can create a new zone are as follows:

- Using one of the predefined zone templates—Creates a new zone with the templates default policies and filters. The default policies are tuned for on-demand protection; however, if there is no immediate need to protect the zone, we recommend that you allow the Guard to learn the zone traffic characteristics. See the [“Activating On-Demand Protection”](#) section on page 9-2 for more information.

After you create a new zone using a predefined zone template, you must configure the zone attributes.

- Duplicating an existing zone—Creates a zone using an existing zone as the zone template. Use this method if the new zone has traffic patterns that are similar to those of the existing zone.
- Copying a zone configuration from the Detector—Copies the zone configuration that you create on the Detector to the Guard using the synchronization process. See the [“Synchronizing Zone Configurations with a Detector”](#) section on page 5-8.

You must initiate synchronization process from the Detector. See the *Cisco Traffic Anomaly Detector Configuration Guide* for more information.

See the [“Configuring Zone Attributes”](#) section on page 5-5 for information about how to modify the zone configuration settings.

This section contains the following topics:

- [Creating a New Zone from a Zone Template](#)
- [Creating a New Zone by Duplicating an Existing Zone](#)

Creating a New Zone from a Zone Template

When you use a zone template to create a new zone, the zone template provides a set of predefined policies and policy thresholds for the new zone configuration. The predefined policy settings are tuned for on-demand protection (see the [“Activating On-Demand Protection”](#) section on page 9-2).

To create a new zone using a predefined zone template, use the following command in configuration mode:

```
zone zone-name [template-name] [interactive]
```

Table 5-2 provides the arguments and keywords for the **zone** command.

Table 5-2 Arguments and Keywords for the zone Command

Parameter	Description
<i>zone-name</i>	Name of the zone. Enter one of the following zone name types: <ul style="list-style-type: none"> New zone name—Enter an alphanumeric string from 1 to 63 characters. The name must start with an alphabetic letter and can contain underscores but cannot contain any spaces. Existing zone name—Enter the name of an existing zone to delete the current zone configuration and create a new zone using the same zone name and the configuration attributes of the zone template that you specify.
<i>template-name</i>	(Optional) Zone template that defines the zone configuration. If you entered a new zone name and do not specify a zone template, the Guard creates the zone using the GUARD_DEFAULT template (see the “Using Zone Templates” section on page 5-2 for more information on the zone templates). If you enter the name of an existing zone without specifying a zone template, the Guard enters the zone configuration mode of the existing zone without making any changes to its configuration. See Table 5-1 for a list of available zone templates.
interactive	(Optional) Configures the Guard to perform zone protection in the interactive detect mode. See Chapter 10, “Using Interactive Protect Mode,” for more information.

When you enter the **zone** command, the Guard enters the configuration mode of the new zone.

The following example shows how to create a new zone configured for interactive protect mode:

```
user@GUARD-conf# zone scannet interactive
user@GUARD-conf-zone-scannet#
```

To delete a zone, use the **no zone** command. When deleting a zone, you can use an asterisk (*) as a wildcard character at the end of the zone name. The wildcard allows you to remove several zones with the same prefix in one command.

To display the zone templates, use the **show templates** command in global or configuration mode. To display the zone template default policies, use the **show templates template-name policies** command in global or configuration mode.

Creating a New Zone by Duplicating an Existing Zone

You can create a new zone by creating a copy of an existing zone. When using an existing zone as a template for the new zone, all properties of the source zone are copied to the new zone. If you specify a zone snapshot as the source zone, the zone policies are copied from the snapshot.

To create a copy of a zone, use one of the following commands:

- **zone new-zone-name copy-from-this** [*snapshot-id*]
—Use this command in zone configuration mode to create a new zone with the configuration of the current zone.
- **zone new-zone-name copy-from** zone-name [*snapshot-id*]
—Use this command in configuration mode to create a new zone with the configuration of the specified zone.

Table 5-3 provides the arguments and keywords for the **zone** command.

Table 5-3 Arguments and Keywords for the zone Command

Parameter	Description
<i>new-zone-name</i>	Name of a new zone. The name is an alphanumeric string from 1 to 63 characters. The string must start with an alphabetic letter and can contain underscores but cannot contain any spaces.
copy-from-this	Creates a new zone by copying the configuration of the current zone.
copy-from	Creates a new zone by copying the configuration of the specified zone.
<i>zone-name</i>	Name of an existing zone.
<i>snapshot-id</i>	(Optional) Identifier of an existing snapshot. See the “ Displaying Snapshots ” section on page 8-15 for more information.

The following example shows how to create a new zone from the current zone:

```
user@GUARD-conf-zone-scannet# zone mailserver copy-from-this
user@GUARD-conf-zone-mailserver#
```

When you enter the **zone** command, the Guard enters the configuration mode of the new zone. The Guard marks the policies of the new zone as untuned (not tuned to zone-specific values). We recommend that you perform the threshold tuning phase of the learning process to tune the policy thresholds to the zone traffic (see the “[Activating the Threshold Tuning Phase](#)” section on page 8-6). If the traffic characteristics of the new zone are identical or very similar to the traffic characteristics of the originating zone, you can mark the policy thresholds as tuned (see the “[Marking the Policies as Tuned](#)” section on page 8-10).

The activation interface of the new zone is set to **zone-name-only**, regardless of the configuration of the source zone. See the “[Configuring the Protection Activation Method](#)” section on page 9-4 for more information.

Configuring Zone Attributes

Configure the attributes of a zone by performing the following steps:

-
- Step 1** Enter zone configuration mode. Skip this step if you are in zone configuration mode already.

To enter zone configuration mode, use one of the following commands:

- **conf** *zone-name* (from global mode)
- **zone** *zone-name* (from configuration mode or zone configuration mode)

The *zone-name* argument specifies the name of an existing zone.



Note You can disable tab completion for zone names in the **zone** command by using the **aaa authorization commands zone-completion tacacs+** command. See the “Disabling Tab Completion of Zone Names” section on page 3-13 for more information.

Step 2 Define the zone IP address by entering the following command:

```
ip address [exclude] ip-addr [ip-mask]
```

You must define at least one IP address that is not excluded to enable the Guard to learn the zone traffic and protect the zone.

See the “Configuring the Zone IP Address Range” section on page 5-7 for more information.

Step 3 (Optional) Limit the traffic bandwidth that the Guard injects back into the zone according to the traffic rate that you think the zone can handle by entering the following command:

```
rate-limit {no-limit | rate burst-size rate-units}
```

We recommend that you set the bandwidth value to the highest bandwidth that was measured entering the zone. If you do not know what this value is, leave the default bandwidth value (no-limit).

Table 5-4 provides the arguments and keywords for the **rate limit** command.

Table 5-4 Arguments and Keywords for the rate limit Command

Parameter	Description
no-limit	Configures the zone with no rate limit.
<i>rate</i>	Integer greater than 64 that specifies the amount of traffic that is allowed to pass to the zone. The units are specified by the <i>rate-units</i> argument. The <i>rate</i> limit can be up to 10 times greater than the <i>burst</i> limit.
<i>burst</i>	Integer greater than 64 that specifies the highest traffic peak allowed to pass to the zone. The units are bits, kilobits, kilopackets, megabits, and packets that correspond to the rate units that are specified by the <i>rate-units</i> argument. The <i>burst</i> limit can be up to eight times greater than the <i>rate</i> limit.
<i>rate-units</i>	Rate units. The units are as follows: <ul style="list-style-type: none"> • bps—Bits per second • kbps—Kilobits per second • kpps—Kilopackets per second • mbps—Megabits per second • pps—Packets per second

Step 4 (Optional) Add a description to the zone for identification purposes by entering the following command:

```
description string
```

The maximum string length is 80 characters. If you use spaces in the expression, enclose the expression in quotation marks (“ ”).

To modify a zone description, reenter the zone description. The new description overrides the previous description.

- Step 5** (Optional) Display and verify the configuration of the newly configured zone by entering the **show running-config** command.

The configuration information consists of CLI commands that are executed to configure the Guard with the current settings. Refer to the specific command entries for more information.

The following example shows how to create a new zone and configure the zone attributes. The zone IP address range is configured to 192.168.100.32/27, but the IP address 192.168.100.50 is excluded from the zone IP address range.

```
user@GUARD-conf# zone scannet
user@GUARD-conf-zone-scannet# ip address 192.168.100.32 255.255.255.224
user@GUARD-conf-zone-scannet# ip address exclude 192.168.100.50
user@GUARD-conf-zone-scannet# rate-limit 1000 2300 pps
user@GUARD-conf-zone-scannet# description Demonstration zone
user@GUARD-conf-zone-scannet# show running-config
```

Configuring the Zone IP Address Range

You must configure at least one IP address that is not excluded before you can activate zone protection, but you can add or delete IP addresses from the zone IP address range at any time. You can configure a large subnet and then exclude specific IP addresses from that subnet so that they are not part of the zone IP address range.

To configure the zone IP address, use the following command in zone configuration mode:

```
ip address [exclude] ip-addr [ip-mask]
```

[Table 5-5](#) provides the arguments and keywords for the **ip address** command.

Table 5-5 Arguments and Keywords for the ip address Command

Parameter	Description
exclude	(Optional) Excludes the IP address from the zone IP address range.
<i>ip-addr</i>	IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1). By default, the IP address is included in the zone IP address range. The IP address must match the subnet mask. If you enter a Class A, Class B, or Class C subnet mask, the host bits in the IP address must be 0.
<i>ip-mask</i>	(Optional) IP subnet mask. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0). The default subnet mask is 255.255.255.255.

The following example shows how to configure the zone IP address range to 192.168.100.32/27 but exclude IP address 192.168.100.50 from the zone IP address range:

```
user@GUARD-conf-zone-scannet# ip address 192.168.100.32 255.255.255.224
user@GUARD-conf-zone-scannet# ip address exclude 192.168.100.50
```

If you modify the zone IP address range, perform one or both of the following tasks to update the zone configuration policies and policy thresholds:

- Define any new services—If the new IP address or subnet consists of a new service that was not previously defined in the zone configuration, activate the policy construction phase before activating zone protection or add the service manually. See the [“Activating the Policy Construction Phase” section on page 8-4](#) and the [“Adding a Service” section on page 7-8](#) for more information.
- Tune the policy thresholds—Use one of the following methods to tune the policy thresholds for the modified IP address range:
 - Protect and learn function—If you enable the protect and learn function, use the **no learning-params threshold-tuned** command to mark the zone policies as untuned.



Caution

Do not change the status of the zone policies to untuned if there is an attack on the zone. Changing the status prevents the Guard from detecting the attack and causes the Guard to learn malicious traffic thresholds.

See the [“Enabling the Protect and Learn Function” section on page 8-11](#) and [“Marking the Policies as Tuned” section on page 8-10](#) for more information.

- Threshold tuning phase—If you do not use the protect and learn function, you should activate the threshold tuning phase before activating zone protection. See the [“Activating the Threshold Tuning Phase” section on page 8-6](#).

To delete zone IP addresses, use the **no** form of the command.

To delete excluded IP addresses, use the **no ip address exclude** command.

To delete all zone IP addresses and excluded IP addresses, use the **no ip address *** command.

Synchronizing Zone Configurations with a Detector

The synchronization process allows you to maintain a copy of a zone configuration on both the Detector and the Guards that you associate with the Detector. You can also use the synchronization process to maintain copies of the Detector zone configurations on a remote server.

The synchronization process, which you perform from the Detector only, enables the following operations:

- Detector to Guard synchronization—The Detector copies the zone configuration from itself to the Guards that you define in the Detector’s remote Guard list. This option requires that you set up the Detector and the Guard so that they can communicate with each other online using a Secure Sockets Layer (SSL) communication channel (see the [“Establishing Communication with the Detector” section on page 3-17](#)).
- Guard to Detector synchronization—The Detector copies the zone configuration from the Guard to itself enabling you to update the Guard zone configuration with changes that you make to the zone configuration on the Guard. This option requires that you set up the Detector and the Guard so that they can communicate with each other online using a Secure Sockets Layer (SSL) communication channel (see the [“Establishing Communication with the Detector” section on page 3-17](#)).

- Detector to remote server export—The Detector exports the zone configuration from itself to a network server.

You can manually synchronize zone configurations or you can configure the Detector to perform the following tasks automatically:

- Synchronize the zone configuration with the Guard or remote server after accepting the results of the threshold tuning phase.
- Synchronize the zone configuration with the Guard before activating the Guard to provide zone protection.

Using the synchronization process, you can create, configure, and modify a zone on the Detector and then update the Guard with the same zone information. The synchronization process also enables the Detector to continuously learn the zone traffic characteristics to keep the zone policies updated on both itself and the Guard. When you let the Detector do the learning for the Guard, you avoid having to divert the zone traffic to the Guard.

**Note**

To use the synchronization process, you must create the zone for synchronization and synchronize the zone from the Detector. This section describes only how to synchronize a zone configuration offline between a Detector and the Guard. For information on using the other synchronization options, see the *Cisco Traffic Anomaly Detector Configuration Guide* or the *Cisco Traffic Anomaly Detector Module Configuration Guide*.

This contains the following topics:

- [Configuration Guidelines](#)
- [Synchronizing a Zone Configuration Offline](#)
- [Example Synchronization Scenario](#)

Configuration Guidelines

To synchronize zones between a Guard and a Detector, follow these guidelines:

- Create the new zone on the Detector using one of the Guard zone templates that contain configuration parameters for both device types.
- Ensure that the same type of traffic (same traffic rates, protocols, and so on) flows to both the Guard and the Detector for proper synchronization of zone policies.
- Configure the SSL communication connection channel to enable communication between the Guard and the Detector (see the “[Establishing Communication with the Detector](#)” section on page 3-17).
- Regenerate the SSL certificates that the Detector and the Guard use for secure communication if you replace a device or change the IP address of the interface that the Detector and the Guard use to communicate (see the “[Regenerating SSL Certificates](#)” section on page 3-19).
- Verify the zone configuration on the Guard. If the activation extent is **ip-address-only** and the activation method is not **zone-name-only**, we recommend that you configure the timer that the Guard uses to identify that an attack on the zone has ended by entering the **protection-end-timer** command. If you configure the value of the **protection-end-timer** to **forever**, the Guard does not terminate zone protection when the attack ends and does not delete the subzone that it had created to protect the specific IP address.

See the “Configuring the Protection Activation Method” section on page 9-4, the “Configuring the Protection Activation Extent” section on page 9-6, and the “Configuring the Protection Inactivity Timeout” section on page 9-8 for more information.

Synchronizing a Zone Configuration Offline

You can synchronize a zone configuration on the Detector with a zone configuration on the Guard even if you cannot establish a secure communication channel between the Detector and the Guard. You may need to synchronize a zone configuration offline if one of the following conditions applies:

- The Guard and Detector cannot communicate with each other.
- The Detector communicates with the Guard across a Network Address Translation (NAT) device.

To synchronize a zone configuration on the Detector with a zone configuration on the Guard offline, you must first export the zone configuration from the Detector to a network server using FTP, Secure FTP (SFTP), or Secure Copy (SCP), and then manually import the zone configuration to the Guard.

If no secure communication channel exists between the Guard and the Detector, after you synchronize the zone configuration offline, you must manually activate the Guard to protect the zone when the Detector detects anomalies in the zone traffic (see [Chapter 9, “Protecting Zones,”](#) for more information).

To perform an offline synchronization of a zone configuration on the Detector with the Guard, you must create the zone on the Detector using one of the Guard zone templates. For more information about configuring the Detector, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* and *Cisco Traffic Anomaly Detector Configuration Guide*.

To synchronize the zone on the Detector with a zone configuration on the Guard configuration offline, perform the following steps:

Step 1 Export the zone configuration from the Detector in one of the following ways:

- Automatically—Configure the Detector to export the zone configuration whenever a specific condition occurs.
- Manually—Export the zone configuration by entering one of the following commands in global mode:
 - `copy zone zone-name guard-running-config ftp server remote-path [login [password]]`
 - `copy zone zone-name guard-running-config {sftp | scp} server remote-path login`

[Table 5-6](#) provides the arguments for the `copy guard-running-config` command.

Table 5-6 Arguments and Keywords for the copy guard-running-config Command

Parameter	Description
<code>zone zone-name</code>	Specifies the name of an existing zone.
<code>guard-running-config</code>	Exports the portion of the zone configuration that is required to configure the zone on a Guard.
<code>ftp</code>	Specifies FTP.
<code>sftp</code>	Specifies SFTP.
<code>scp</code>	Specifies SCP.
<code>server</code>	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).

Table 5-6 Arguments and Keywords for the `copy guard-running-config` Command (continued)

Parameter	Description
<i>full-file-name</i>	Complete name of the file. If you do not specify a path, the server saves the file in your home directory.
<i>login</i>	(Optional) Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
<i>password</i>	(Optional) Password for the remote FTP server. If you do not enter the password, the Detector prompts you for it.
<i>file-server-name</i>	Name of a network server to which to export the configuration file. You must configure the network server using the file-server command. If you configured the network server using SFTP or SCP, you must configure the SSH key that the Detector uses for SFTP and SCP communication.
<i>destination-file-name</i>	Name of the configuration file on the remote server. The Detector saves the configuration file on the network server using the destination filename in the directory that you defined for the network server when you entered the file-server command.
*	Exports only the portion of the zone configuration that is required to configure the zone on the Guard to all the network servers that are defined in the zone remote server list and the default remote server list.

Step 2 Import the zone configuration from a network server to the Guard by entering one of the following commands in global mode:



Note Deactivate a zone before importing the zone configuration.

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy {sftp | scp} running-config** *server full-file-name login*
- **copy file-server-name running-config** *source-file-name*

Table 5-7 describes the arguments and keywords for the **copy** command.

Table 5-7 Arguments and Keywords for the `copy` Command

Parameter	Description
running-config	Specifies the running configuration.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
<i>server</i>	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
<i>full-file-name</i>	Complete name of the file. If you do not specify a path, the server copies the file from your home directory.

Table 5-7 Arguments and Keywords for the copy Command (continued)

Parameter	Description
<i>login</i>	(Optional) Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
<i>password</i>	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for it.
<i>source-file-name</i>	Name of the file.

See the [“Importing and Updating the Configuration”](#) section on page 13-4 for more information.

Example Synchronization Scenario

This example scenario shows how to synchronize a zone configuration on the Detector with a zone configuration on the Guard to protect the zone while the Detector continues to learn the zone traffic characteristics:

1. Create and configure a new zone on the Detector using one of the Guard zone templates.
The Detector displays (Guard/Detector) next to the zone ID field in the output of the **show** command in zone configuration mode.
2. Add the Guard to the zone SSL remote Guard list or the default SSL remote Guard list on the Detector.
3. Enable the Detector to construct the zone policies by entering the **learning policy-construction** command.
4. Enable the Detector to learn the zone traffic and tune the policy thresholds while detecting traffic anomalies by entering the **detect learning** command.
5. Configure the Detector to accept the policy thresholds every 24 hours to ensure that the zone policies are updated with the changing traffic patterns.
6. Configure the Detector to synchronize the zone configuration with the Guard each time that it accepts the new learned policy thresholds to ensure that when the Detector learns new zone policy thresholds, the zone policies on the Guard are also updated.
7. Configure the Detector to synchronize the zone configuration with the configuration on the Guard before activating the Guard to ensure that the zone configuration and policies on the Guard are updated when the Guard activates zone protection.

When the Detector detects an attack on the zone, it performs the following actions:

- Verifies that the zone configuration on the Guard is updated. If the zone configuration on the Guard is not the same as the zone configuration on the Detector, the Detector synchronizes the zone configuration with the Guard.
- Activates the Guard to protect the zone (the Guard activates zone protection).
- Stops the learning process for the zone to prevent it from learning malicious traffic thresholds. The Detector continues to look for anomalies in the zone traffic.

You can modify the zone policies on the Guard when the attack is in progress.

The Detector polls the Guard constantly. When the Detector identifies that the Guard has deactivated zone protection (the Guard deactivates zone protection when the attack ends) and additional traffic anomalies do not exist, then the Detector reactivates zone anomaly detection and the learning process.

8. If you manually modify the zone policies on the Guard to adjust the zone policies to the attack characteristics, you can synchronize the new policies with the Detector. This action is important if the zone traffic requires that you set certain policy thresholds as fixed or set a fixed multiplier for policy thresholds. Synchronizing the zone configuration with the Detector ensures that the Detector has the correct policy thresholds, calculates the thresholds correctly in future threshold tuning phases, and updates the Guard policies with the correct thresholds.



Note You can perform this action only from the Detector. See the *Cisco Traffic Anomaly Detector Configuration Guide* or the *Cisco Traffic Anomaly Detector Module Configuration Guide* for more information.

For more information, see the [“Setting the Threshold as Fixed”](#) section on page 7-14 and the [“Configuring a Threshold Multiplier”](#) section on page 7-15.

