



CHAPTER 4

Configuring Zones

This chapter describes how to create and manage zones on the Cisco Traffic Anomaly Detector (Detector).

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

This chapter contains the following sections:

- [Understanding Zones](#)
- [Using Zone Templates](#)
- [Creating a New Zone](#)
- [Configuring Zone Attributes](#)
- [Configuring the Zone IP Address Range](#)
- [Synchronizing Zone Configurations with a Guard](#)

Understanding Zones

A zone is a network element that the Detector monitors for DDoS attacks. A zone can be any combination of the following elements:

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

When the Detector identifies a DDoS attack, it can activate a Guard automatically to protect the zone against the attack, or it can notify you to activate the Guard manually. The Detector can analyze the traffic for 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 4-4 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 4-6 for more information.
- Configuring the zone filters—You can configure the zone filters. The zone filters apply the required detection level to the zone traffic and define the way the Detector handles specific traffic flows. See [Chapter 5, “Configuring Zone Filters,”](#) for more information.
- Learning the zone traffic characteristics—You can create the zone detection policies that enable the Detector to analyze a particular traffic flow and take action if the traffic flow exceeds a policy threshold. The Detector constructs the policies in a learning process that consists of two phases: policy construction and threshold tuning. See [Chapter 7, “Learning the Zone Traffic Characteristics,”](#) for more information.

Using Zone Templates

A zone template defines the default configuration of a zone.

The Detector contains two sets of zone templates with the following prefixes:

- DETECTOR_—Zone templates designed for Detector use only. Select the DETECTOR_ version of the zone template when you are not going to share the zone configuration with a Guard.
- GUARD_—Zone templates designed for use on the Detector and the Guard. You can configure both Detector and Guard attributes for zones that were created from these templates and copy the zone configuration to the Guard. Select the GUARD_ version of the zone template when you plan to synchronize the zone configuration with a Guard.

See the “[Creating a Zone for Synchronization](#)” section on page 4-10 for more information about how to configure zones that you create using GUARD_ templates.

[Table 4-1](#) displays the zone templates.

Table 4-1 Zone Templates

Template	Description
DETECTOR_DEFAULT	Default Detector-only zone template. You can use this zone template to protect a VoIP ¹ server. If you create a zone using this zone template, you cannot detect TCP worm attacks on the zone.
DETECTOR_WORM	Zone template that enables the Detector to detect TCP worm attacks on the zone. Zones that are created from the DETECTOR_WORM zone template contain policies that are produced from the worm_tcp policy template (see the “ Understanding Worm Policies ” section on page 6-19 for more information).

Table 4-1 Zone Templates (continued)

Template	Description
DETECTOR_LINK Templates	<p>Zone templates designed for detection of large subnets segmented according to zones with known bandwidth. You can activate zone detection for zones defined by these zone templates without undergoing the learning process. To enable the Detector to activate zone protection on a Guard for the attacked IP address or subnet only, use the protect-ip-state dst-ip-by-name command. See the “Configuring Guard-Protection Activation Methods” section on page 8-3 for more information about the protect-ip-state command.</p> <p>The following bandwidth-limited link zone templates are available for 128-Kb, 1-Mb, 4-Mb, and 512-Kb links:</p> <p>DETECTOR_LINK_128K DETECTOR_LINK_1M DETECTOR_LINK_4M DETECTOR_LINK_512K</p> <p>You cannot perform the policy construction phase of the learning process for zones that were created from these templates.</p>
GUARD_DEFAULT	Default zone template.
GUARD_LINK templates	<p>Zone templates designed for zones with a known bandwidth. The following 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> <p>You cannot perform policy construction for zones that were created from these templates. You can activate zone detection for zones that were created from the GUARD_LINK zone templates without undergoing the threshold tuning phase.</p> <p>We recommend that you define such a zone with a Guard protection activation method of dst-ip-by-name (the Detector activates a Guard to protect a particular IP address when it detects an anomaly in the zone traffic that is destined to that IP address) by using the protect-ip-state command. See the “Configuring Guard-Protection Activation Methods” section on page 8-3 for more information.</p>
GUARD_TCP_NO_PROXY	Zone template designed for a zone for which no TCP proxy is to be used. You may use this zone template if the zone is controlled based on IP addresses, such as an IRC ² server-type zone, or if you do not know the type of services running on the zone.

1. VoIP = Voice over IP
2. IRC = Internet Relay Chat

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 system-defined zone template. The zone template that you use defines the initial policy and filter configurations of the zone.

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

- Using one of the system-defined zone templates—Use this method to create a new zone with the default policies and filters of the template.

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

- Duplicating an existing zone—You can create a zone from an existing zone. Use this method if the new zone has traffic patterns that are similar to those of an existing zone.

See the “[Configuring Zone Attributes](#)” section on page 4-6 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.

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

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

[Table 4-2](#) provides the arguments and keywords for the **zone** command.

Table 4-2 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.

Table 4-2 Arguments and Keywords for the zone Command (continued)

Parameter	Description
<i>template-name</i>	<p>(Optional) Zone template that defines the zone configuration. If you entered a new zone name and do not specify a zone template, the Detector creates the zone using the DETECTOR_DEFAULT template (see the “Using Zone Templates” section on page 4-2 for more information about the zone templates).</p> <p>If you enter the name of an existing zone without specifying a zone template, the Detector enters the zone configuration mode of the existing zone without making any changes to its configuration.</p> <p>See Table 4-1 for a list of available zone templates.</p>
interactive	(Optional) Configures the Detector to perform zone anomaly detection in the interactive detect mode. See Chapter 9, “Using Interactive Detect Mode,” for more information.

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

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

```
user@DETECTOR-conf# zone scannet interactive
user@DETECTOR-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 4-3 provides the arguments and keywords for the **zone** command.

Table 4-3 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.

Table 4-3 Arguments and Keywords for the zone Command (continued)

Parameter	Description
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 7-15 for more information.

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

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

When you enter the **zone** command, the Detector enters the configuration mode of the new zone. The Detector 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 7-6](#)). 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 7-10](#)).

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 Detector to learn the zone traffic and detect the zone.

See the [“Configuring the Zone IP Address Range” section on page 4-7](#) for more information.

Step 3 (Optional) Add a description to the zone for identification purposes by entering the following command in zone configuration mode:

```
description string
```

The maximum string length is 80 alphanumeric 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 4** (Optional) Display and verify the configuration of the newly configured zone by entering the **show running-config** command in zone configuration mode.

The configuration information consists of CLI commands that are executed to configure the Detector 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@DETECTOR-conf# zone scannet
user@DETECTOR-conf-zone-scannet# ip address 192.168.100.32 255.255.255.224
user@DETECTOR-conf-zone-scannet# ip address exclude 192.168.100.50
user@DETECTOR-conf-zone-scannet# description Demonstration zone
user@DETECTOR-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 anomaly detection, 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 4-4 provides the arguments and keywords for the **ip address** command.

Table 4-4 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@DETECTOR-conf-zone-scannet# ip address 192.168.100.32 255.255.255.224
user@DETECTOR-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 detection or add the service manually. See the [“Activating the Policy Construction Phase” section on page 7-4](#) and the [“Adding a Service” section on page 6-9](#) for more information.
- Tune the policy thresholds—Use one of the following methods to tune the policy thresholds for the modified IP address range:
 - Detect and learn function—If you enable the detect 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 Detector from detecting the attack and causes the Detector to learn malicious traffic thresholds.

See the [“Enabling the Detect and Learn Function” section on page 7-11](#) and [“Marking the Policies as Tuned” section on page 7-10](#) for more information.

- Threshold tuning phase—If you do not use the detect and learn function, you should activate the threshold tuning phase before activating zone anomaly detection. See the [“Activating the Threshold Tuning Phase” section on page 7-6](#).

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

Synchronizing Zone Configurations with a Guard

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 lists. See the [“Activating Remote Guards to Protect a Zone” section on page 8-5](#) for more information about the 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 Guard” 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 Detector 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 Guard” 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.

This section contains the following topics:

- [Understanding the Configuration Guidelines for Synchronization](#)
- [Creating a Zone for Synchronization](#)
- [Configuring the Automatic Zone Synchronization and Export Parameters](#)
- [Synchronizing a Zone Configuration from the Guard to the Detector](#)
- [Synchronizing a Zone Configuration from the Detector to the Guard](#)
- [Synchronizing a Zone Configuration Offline](#)
- [Exporting a Zone Configuration Automatically to a Network Server](#)
- [Exporting a Zone Configuration Manually to a Network Server](#)
- [Example Synchronization Scenario](#)

Understanding the Configuration Guidelines for Synchronization

To synchronize zones between the Detector and a Guard, 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. See [Table 4-1](#) for more information about the available zone templates.
- 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 Detector and the Guard (see the [“Establishing Communication with the Guard”](#) 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 Detector 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 Detector 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.

Creating a Zone for Synchronization

To synchronize a zone configuration between the Detector and a Guard, you must create the zone on the Detector using one of the Guard zone templates which have two sets of definitions; one for the Guard and one for the Detector. See [Table 4-1](#) for more information about the zone templates.

When creating a zone using one the Guard zone templates, you use the following configuration modes to configure the zone:

- **Zone configuration mode**—Configures zone attributes that are unique to the Detector, such as defining the remote Guards. To enter zone configuration mode, use the **zone** command in configuration mode. The zone configuration command prompt is as follows:

```
user@DETECTOR-conf-zone-scannet#
```

- **Guard configuration mode**—Configures definitions that are unique to the Guard, such as user filters. To enter guard configuration mode, use the **guard-conf** command in zone configuration mode. The guard configuration mode command prompt is as follows:

```
user@DETECTOR-conf-zone-scannet (guard) #
```

- **Zone configuration mode or guard configuration mode**—Configures definitions that are common to both the Guard and the Detector, such as IP addresses.

If you modify a zone attribute that is common to both the Guard and the Detector, the change applies to both sets of definitions. For example, if you modify the zone IP address in zone configuration mode, the new IP address is also modified in the zone definition for the Guard. You can display the new zone definition for the Guard in guard configuration mode. If you change the operation state of a policy in guard configuration mode, the operation state is also modified in the zone definition of the Detector.

To create and configure a zone for synchronization, perform the following steps:

-
- Step 1** Create a new zone on the Detector using one of the Guard zone templates (see the [“Creating a New Zone from a Zone Template”](#) section on page 4-4).

When you create a new zone using a 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.

- Step 2** Configure the zone attributes (see the [“Configuring Zone Attributes”](#) section on page 4-6).

- Step 3** Configure characteristics that are unique to the Guard by entering guard configuration mode when you use one of the following commands:

- **guard-conf** (from zone configuration mode)
- **configure zone-name guard-conf** (from global mode)
- **zone zone-name guard-conf** (from configuration mode)

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

The Detector enters the guard configuration mode. The CLI prompt indicates the mode by adding the word *guard* in parentheses (*guard*) to the prompt.

The following example shows how to enter guard configuration mode:

```
user@DETECTOR-conf-zone-scannet# guard-conf
user@DETECTOR-conf-zone-scannet (guard) #
```

The guard configuration mode allows you to configure all zone attributes that are unique to the Guard, such as user filters, filter termination, and a policy or a filter action of drop. See the *Cisco Guard Configuration Guide* for more information.

Configuring the Automatic Zone Synchronization and Export Parameters

You can configure the Detector to perform the following tasks automatically:

- Synchronize the zone configuration with the remote Guards that you define in the zone remote Guard list as follows:
 - After the Detector accepts the results of the threshold-tuning phase.
 - Before the Detector activates the Guards to protect the zone.

If you do not define any Guards on the zone remote Guard list, then the Detector synchronizes the zone configuration with the remote Guards that you define in the Detector default remote Guard list. If synchronization with one of the remote Guards fails, the Detector continues to the next remote Guard on the list.

If both the zone remote Guard list and the Detector default remote Guard list are empty, the Detector does not synchronize the zone configuration.

If a zone with the same name exists on the Guard, the new configuration replaces the existing one.

- Export the zone configuration to all the network servers that you define in the zone remote server list when the Detector accepts the results of the threshold-tuning phase. If the zone remote server list is empty, the Detector searches the Detector default remote list. See the [“Exporting a Zone Configuration Automatically to a Network Server”](#) section on page 4-15 for more information.

If both the zone remote server list and the Detector default remote server list are empty, the Detector does not export the zone configuration.

To enable automatic synchronization and export of a zone configuration, use the following command in zone configuration mode:

```
learning-params sync {accept | remote-activate}
```

Table 4-5 provides the keywords for the **learning-params sync** command.

Table 4-5 Keywords for the *learning-params sync* Command

Parameter	Description
accept	Synchronizes the zone configuration with the remote Guard and exports the zone configuration to the remote server each time that the Detector accepts the results of the threshold-tuning phase of the learning process.
remote-activate	Synchronizes the zone configuration with the remote Guard before activating the Guard to protect the zone. The Detector synchronizes the zone configuration only if the zone configuration on the remote Guard is not up to date. The Detector does not export the zone configuration to a network server.

The following example shows how to automatically synchronize and export the zone configuration each time that the Detector accepts the results of the threshold-tuning phase of the learning process:

```
user@DETECTOR-conf-zone-scanner# learning-params sync accept
```

To disable automatic synchronization and export functions, use the **no learning-params sync** command.

Synchronizing a Zone Configuration from the Guard to the Detector

You can enable the Detector to copy a zone configuration from a Guard to the Detector. If the zone already exists on the Detector, the new configuration from the Guard overrides the existing one.

Synchronizing a zone configuration from the Guard to the Detector may be required if you manually modify the zone policies on the Guard to adjust them for attack characteristics and would like to update the Detector with the changes. You can set certain policy thresholds as fixed or set a fixed multiplier for policy thresholds to ensure the following:

- The Detector has the correct policy thresholds and can detect future DDoS attacks correctly.
- The correct zone configuration on the Guard is maintained if you synchronize the zone configuration from the Detector to the Guard in the future, which may be required if the Detector continues to learn the zone traffic characteristics.

See the [“Setting the Threshold as Fixed”](#) section on page 6-14 and the [“Configuring a Threshold Multiplier”](#) section on page 6-15 for more information.

To synchronize the zone configuration and policies from the Guard to the Detector, perform the following steps:

-
- Step 1** If the zone is currently active, deactivate the zone by using the **deactivate** command in zone configuration mode.
- Step 2** Synchronize the zone configuration from the Detector to the Guard by entering one of the following commands:
- **sync zone zone-name remote-guard-address local** (in global mode)
 - **sync remote-guard-address local** (in zone configuration mode)

[Table 4-6](#) provides the arguments for the **sync** command.

Table 4-6 Arguments and Keywords for the sync Command

Parameter	Description
zone	Synchronizes the configuration of the specified zone.
<i>zone-name</i>	Name of an existing zone.
<i>remote-guard-address</i>	IP address of the remote Guard. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1).
local	Synchronizes the zone configuration from the Detector to the Guard.

- Step 3** If the zone was active before you initiated the synchronization process, reactivate the zone by using the **detect** command or the **learning** command in zone configuration mode.

For more information, see [Chapter 8, “Detecting Zone Traffic Anomalies,”](#) and the [“Synchronizing Zone Configurations with a Guard”](#) section on page 4-8.

The following example shows how to deactivate the zone scannet and synchronize the zone configuration from a Guard with an IP address of 192.168.55.10 to the Detector. It then shows how to reactivate the zone.

```
user@DETECTOR-conf-zone-scannet# deactivate
user@DETECTOR-conf-zone-scannet# sync 192.168.55.10 local
user@DETECTOR-conf-zone-scannet# detect learning
```

Synchronizing a Zone Configuration from the Detector to the Guard

You can synchronize a Detector zone configuration with the zone on the Guard to ensure that the zone configuration and policies on the Guard are updated when the Guard activates zone protection. This process allows you to configure the zone once on the Detector, continuously learn the zone traffic characteristics, and maintain the same zone configuration and policies on the Guard without constantly diverting the zone traffic to the Guard.

The Detector copies the configuration of the zone to the Guard. If a zone with the same name exists on the Guard, the new configuration replaces the existing one.



Note

Before you initiate the zone synchronization process, ensure that the Guard is not currently protecting the zone. You must deactivate zone protection before synchronizing the zone configuration.

Synchronize the zone configuration and policies from the Detector by entering one of the following commands:

- **sync zone** *zone-name* **local** {**remote-guards** | *remote-guard-address-to*}
(in global mode)
- **sync local** {**remote-guards** | *remote-guard-address-to*}
(in zone configuration mode)

[Table 4-7](#) provides the arguments and keywords for the **sync** command.

Table 4-7 Arguments and Keywords for the sync Command

Parameter	Description
zone	Synchronizes the configuration of the specified zone.
<i>zone-name</i>	Name of an existing zone.
local	Synchronizes the zone configuration and policies from the Detector to the Guard.
remote-guards	Synchronizes the zone configuration with all remote Guards in the zone remote Guard list. If the zone remote Guard list is empty, synchronizes the zone configuration with the remote Guards that are defined in the Detector default remote Guard list.
<i>remote-guard-address-to</i>	IP address of the remote Guard. The Detector synchronizes the zone configuration with the specified remote Guard. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1).

The following example shows how to synchronize the zone configuration to all remote Guards in the zone remote Guard list:

```
user@DETECTOR# sync zone scannet local remote-guards
```

The following example shows how to synchronize the zone configuration to a remote Guard with an IP address of 192.168.100.5:

```
user@DETECTOR-conf-zone-scannet# sync local 192.168.100.5
```

Synchronizing a Zone Configuration Offline

You can synchronize a Detector zone configuration with a Guard by using the offline synchronization procedure that is described in this section. You may need to synchronize a zone configuration offline if one of the following conditions applies:

- You cannot establish a secure communication channel between the two devices (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 offline, you must first export the zone configuration from the Detector to a network server using FTP, SFTP, or SCP, and then import the zone configuration manually from the network server to the Guard.

To perform an offline synchronization of a zone configuration on the Detector with the Guard, you must perform the following tasks:

- Create the zone on the Detector using one of the Guard zone templates (see the [“Creating a New Zone from a Zone Template”](#) section on page 4-4).
- Export the configuration automatically to a network server using SFTP or SCP by configuring the SSH key that the Detector uses for SFTP communication (see the [“Configuring the Keys for SFTP and SCP Connections”](#) section on page 3-27).

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

Step 1 Create the zone on the Detector using one of the Guard zone templates (see the [“Creating a New Zone from a Zone Template”](#) section on page 4-4).

Step 2 Export the zone configuration from the Detector using one of the following methods:

- Automatically—Configure the Detector to export the zone configuration whenever a specific condition occurs (see the [“Exporting a Zone Configuration Automatically to a Network Server”](#) section on page 4-15).
- 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*

See [Table 4-9 on page 4-17](#) for a descriptions of the **copy zone** command arguments and keywords. See [“Exporting a Zone Configuration Manually to a Network Server”](#) section on page 4-16 for more information.

Step 3 From the Guard, import the zone configuration from a network server by entering one of the following commands in global mode:



Note If the Guard is currently protecting the zone, 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 4-8 describes the arguments and keywords for the **copy** command.

Table 4-8 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.
<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>source-file-name</i>	Name of the file.

See the “[Importing and Updating the Configuration](#)” section on page 12-4 for more information.



Note 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.

Exporting a Zone Configuration Automatically to a Network Server

You can configure the Detector to export the zone configuration automatically to a network server. The Detector exports the zone configuration each time that the results of the threshold-tuning phase of the learning process are accepted (see the “[Configuring Periodic Actions](#)” section on page 7-8 for more information about when the results of the threshold-tuning phase of the learning process are accepted).

To export the zone configuration automatically, you must define the network server, which can be an FTP, SFTP, or SCP network server. You can configure the network server in the following lists:

- Zone remote server list—A list of network servers to which the Detector exports the zone configuration.
- Detector default remote server list—The default list of network servers. The Detector exports the zone configuration to the servers on this list if the zone remote server list is empty.

To configure the Detector to automatically export the zone configuration to a network server, perform the following steps:

-
- Step 1** Define the network server by entering the **file-server** command in configuration mode (see the “[Configuring File Servers](#)” section on page 12-1 for more information).
- 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 (see the “[Configuring the Keys for SFTP and SCP Connections](#)” section on page 3-27).
- Step 2** (Optional) Add the network server to a zone remote server list by entering the following command in zone configuration mode:
- ```
export sync-config file-server-name
```
- The *file-server-name* argument specifies the name of the network server that you specified in Step 1. To remove a network server from the remote server list, use the **no** form of the command.
- Step 3** (Optional) Add the network server to the Detector default remote server list by entering the following command in configuration mode
- ```
export sync-config file-server-name
```
- The *file-server-name* argument specifies the name of the network server that you specified in Step 1. To remove a network server from the remote server list, use the **no** form of the command.
- Step 4** Configure the Detector to automatically export the zone configuration to the network server each time that it accepts the results of the threshold-tuning phase by entering the **learning-params sync accept** command in zone configuration mode. See the “[Configuring the Automatic Zone Synchronization and Export Parameters](#)” section on page 4-11 for more information.
-

The following example shows how to add a network server to the zone remote server list:

```
user@DETECTOR-conf-zone-scannet# export sync-config Corp-FTP-Server
```

To display the default list of network servers to which the Detector exports zone configuration, use the **show sync-config file-servers** command in configuration mode.

To display the zone remote server list, use the **show sync-config file-servers** command in zone configuration mode.

Exporting a Zone Configuration Manually to a Network Server

You can manually export the zone configuration to a network server.

Export the zone configuration to a network server by entering one of the following commands in global mode:

- **copy zone** *zone-name* **guard-running-config ftp** *server full-file-name [login password]* (Export the zone configuration to an FTP server.)
- **copy zone** *zone-name* **guard-running-config {sftp | scp}** *server full-file-name login* (Export the zone configuration to a network server using SFTP or SCP.)
- **copy zone** *zone-name* **guard-running-config** *file-server-name dest-file-name* (Export the zone configuration to a network server.)
- **copy zone** *zone-name* **guard-running-config *** (Export zone configuration to the network servers that you define in the zone file server list and the default file server list.)

Table 4-9 provides the arguments for the **copy guard-running-config** command.

Table 4-9 Arguments and Keywords for the copy guard-running-config Command

Parameter	Description
zone <i>zone-name</i>	Specifies the name of an existing zone.
guard-running-config	Exports the portion of the zone configuration that is required to configure the zone on a Guard.
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 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. See the “Configuring File Servers” section on page 12-1 for more information.
<i>dest-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. See the “Exporting a Zone Configuration Automatically to a Network Server” section on page 4-15 for more information.

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Detector uses before you enter the **copy** command with the **sftp** or **scp** option, the Detector prompts you for the password. See the “[Configuring the Keys for SFTP and SCP Connections](#)” section on page 3-27 for more information about how to configure the key that the Detector uses for secure communication.

The following example shows how to export the zone configuration to an FTP server:

```
user@DETECTOR-conf# copy zone scannet guard-running-config ftp 10.0.0.191
/root/ConfigFiles/scannet.txt <user> <password>
```

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 is learning the zone traffic characteristics:

1. Create and configure a new zone on the Detector using one of the Guard zone templates. When you create a new zone using a Guard zone template, the Detector displays (Guard/Detector) next to the zone ID field in the output of the **show** command in zone configuration mode.
For more information, see the “[Creating a New Zone from a Zone Template](#)” section on page 4-4.
2. Add the Guard to the zone remote Guard list or the default remote Guard list on the Detector.
For more information, see the “[Configuring the Default Remote Guard List](#)” section on page 8-7 and the “[Configuring the Zone Remote Guard Lists](#)” section on page 8-8.
3. Enable the Detector to learn the zone traffic and to construct the zone policies by entering the **learning policy-construction** command (see the “[Activating the Policy Construction Phase](#)” section on page 7-4).

4. Enable the Detector to learn the zone traffic and tune the policy thresholds while detecting traffic anomalies by entering the **detect learning** command (see the “[Enabling the Detect and Learn Function](#)” section on page 7-11).
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 by using the **learning-params periodic-action auto-accept** command.

For more information, see the “[Configuring Periodic Actions](#)” section on page 7-8.

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.

Use the **learning-params sync** command to configure the Detector to synchronize the zone configuration with the Guard. For more information, see the “[Configuring the Automatic Zone Synchronization and Export Parameters](#)” section on page 4-11.

7. Configure the Detector to synchronize the zone configuration with 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.

Use the **learning-params sync** command.

For more information, see the “[Configuring the Automatic Zone Synchronization and Export Parameters](#)” section on page 4-11.

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.

For more information, see the [“Setting the Threshold as Fixed” section on page 6-14](#) and the [“Configuring a Threshold Multiplier” section on page 6-15](#).

To synchronize the zone configuration and policies from the Guard to the Detector, perform the following actions:

- Deactivate the zone by entering the **deactivate** command.
- Synchronize the zone configuration from the Guard to the Detector by entering the **sync** command.
- Reactivate zone detection by entering the **detect** command.

For more information, see the [“Synchronizing a Zone Configuration from the Guard to the Detector” section on page 4-12](#) and [Chapter 8, “Detecting Zone Traffic Anomalies.”](#)

