



CHAPTER 8

Detecting Zone Traffic Anomalies

This chapter describes how to configure the Cisco Traffic Anomaly Detector (Detector) to detect traffic anomalies.

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 Zone Anomaly Detection](#)
- [Configuring How the Detector Performs Zone Anomaly Detection](#)
- [Configuring Guard-Protection Activation Methods](#)
- [Activating Zone Anomaly Detection](#)
- [Deactivating Zone Anomaly Detection](#)
- [Activating Remote Guards to Protect a Zone](#)

Understanding Zone Anomaly Detection

Zone anomaly detection refers to when the Detector is actively monitoring a copy of the zone traffic and looking for indications of a DDoS attack on the zone. When a traffic anomaly triggers a policy action by exceeding the policy threshold (indicating an attack), the Detector performs one of the following tasks:

- Activates a Guard that you define on the Detector remote Guard lists to mitigate the attack.
- Sends you a notification.

Before you activate anomaly detection, observe the following requirement and recommendation:

- Configure port mirroring on the switch or connect the Detector to a router using an optical splitter—You must use one of these methods to provide the Detector with a copy of the zone traffic for analysis purposes.
- Perform the learning process—We recommend that you allow the Detector to create a set of zone-specific policies and policy thresholds based on normal traffic characteristics. To perform the learning process, we recommend that you perform the following steps:
 1. Activate the policy construction phase—The Detector creates a set of policies based on the services that it detects in the zone traffic. See the [“Activating the Policy Construction Phase” section on page 7-4](#) for more information.
 2. Activate the detect and learn function—The Detector performs the threshold tuning phase of the learning process while monitoring the traffic for anomalies using the last accepted policy thresholds. If the Detector detects an attack on the zone, it stops the threshold tuning phase but continues to detect anomalies in the zone traffic. See the [“Enabling the Detect and Learn Function” section on page 7-12](#) for more information.



Note Activate the detect and learn option only when you are sure that the zone is not under attack.

- Synchronize the zone configuration with the Guard—When you associate Guards with the Detector to provide zone protection, you can synchronize the zone configuration on the Detector with the zone configuration on a Guard. See the [“Synchronizing Zone Configurations with a Guard” section on page 4-9](#) and the [“Activating Remote Guards to Protect a Zone” section on page 8-5](#) for more information.
- Define the anomaly detection characteristics—You can configure the following optional anomaly detection characteristics:
 - Operation mode—Define how the Detector performs zone anomaly detection (whether the Detector detects anomalies in the zone traffic automatically or in an interactive manner in which you determine the actions that the Detector executes). See the [“Configuring How the Detector Performs Zone Anomaly Detection” section on page 8-3](#) for more information.
 - Guard-Protection activation methods—Define how the Detector activates a remote Guard to protect the zone. The Detector can activate the remote Guard to protect a partial zone that is a part of the entire zone (for example, a specific server that is part of a protected network environment) or activate the remote Guard to protect the entire zone.

**Tip**

You can verify that the Detector is receiving a copy of the zone traffic by waiting at least 10 seconds after initiating the policy construction phase and entering the **show rates** command. Verify that the value of the *Received traffic* rate is greater than zero. A value of zero indicates that the Detector is not receiving a copy of the zone traffic. Check the configuration of the port mirroring on the switch, or use an optical splitter to check the connection of the Detector to the router.

Configuring How the Detector Performs Zone Anomaly Detection

During an attack on a zone, the Detector creates dynamic filters that determine what actions the Detector performs during the attack. You can configure the Detector to execute the action associated with each dynamic filter automatically or wait until you decide whether or not to execute the proposed action. To control the execution of the actions, you configure the Detector to perform anomaly detection in one of the following modes:

- Automatic protect mode—The Detector activates the dynamic filter actions as soon as the Detector creates the filter. This operation mode is the default.
- Interactive protect mode—The Detector saves the dynamic filters as *recommendations*. You review the list of recommendations and decide which recommendations to accept, ignore, or direct to automatic activation.

Use the **show** command in zone configuration mode to display the current operation mode of the zone.

To enable the interactive detect mode, use the following command in zone configuration mode:

```
interactive
```

To disable the interactive detect mode and use the automatic detect mode, use the following command in zone configuration mode:

```
no interactive
```

See [Chapter 9, “Using Interactive Detect Mode”](#) for information about the following interactive protection operations:

- Enabling the interactive protect mode when you create a new zone.
- Managing the protection recommendations.
- Determining when you must switch to the automatic protect mode.

Configuring Guard-Protection Activation Methods

Guard-protection activation methods define how a remote Guard that you associate with the Detector activates zone protection. The activation methods focus on the zone protection requirements and save Guard resources.

To activate the Guard-protection activation methods, use the following command in zone configuration mode:

```
protect-ip-state { entire-zone | dst-ip-by-name | dst-ip-by-ip | policy-type }
```

The Detector supports the following Guard-protection activation methods:

- **entire-zone**—Activates a Guard to protect the entire zone when it detects an anomaly in the zone traffic. This method saves Guard resources because it reduces the number of active zones that the Guard protects. Use this method when the zone consists of related subzones.
- **dst-ip-by-name**—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. You can activate a Guard to protect the attacked IP address but avoid diverting the traffic of the entire zone to the Guard. If the Detector cannot associate the traffic anomaly with a particular IP address, it does not activate a Guard to protect the zone. Use this method when the zone consists of unrelated subzones.
- **dst-ip-by-ip**—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. The IP address must be in the address range of one of the zones that is defined on the Guard. However, the zone name on the Detector does not have to be identical to the zone name on the Guard. The **dst-ip-by-ip** Guard-protection activation method is equivalent to using the **protect ip-address** command on the Guard. Use this method when the zone names on the Detector are not identical to the zone names on the Guard or when the zone consists of unrelated subzones.



Note To ensure that the Guard activates zone protection for the attacked IP address only and avoids diverting the traffic of the entire zone to itself, make sure that the zone is defined on the Guard with an activation extent of **ip-address-only**.

- **policy-type**—Activates the Guard to protect the entire zone or to protect a particular IP address within the zone address range according to the policy that caused the Detector to activate the Guard. The Detector activates the Guard to protect a particular IP address if it detects an anomaly in the zone traffic that is destined to that IP address (for example, if the policy that caused the remote activation has traffic characteristics of **dst_ip**). If the Detector cannot associate the traffic anomaly with a particular IP address, it activates the Guard to protect the entire zone (for example, if the policy that caused the remote activation has traffic characteristics of **global**).

Use this method when the zone consists of related subzones so that you can prevent a targeted zone from causing damage to the entire zone.

The following example shows how to configure the Guard-protection activation method:

```
user@DETECTOR-conf-zone-scanner# protect-ip-state entire-zone
```

Activating Zone Anomaly Detection

You can activate zone anomaly detection by using the following command in zone configuration mode:

```
detect [learning]
```

The optional **learning** keyword enables the Detector to detect anomalies in the zone traffic and tune the zone policy thresholds using the detect and learn function (see the “[Enabling the Detect and Learn Function](#)” section on page 7-12 for more information).

The following example shows how to activate anomaly detection for the zone scannet:

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

Deactivating Zone Anomaly Detection

You can deactivate zone anomaly detection by using one of the following commands in zone configuration mode:

- **no detect**—Ends zone anomaly detection. If you have the detect and learn function enabled when you enter the **no detect** command, the Detector ends zone anomaly detection but continues with the policy threshold phase of the learning process (see the “[Enabling the Detect and Learn Function](#)” section on page 7-12 for more information).
- **deactivate**—Ends both zone anomaly detection and the threshold tuning phase of the learning process.

Activating Remote Guards to Protect a Zone

When the Detector detects a zone traffic anomaly, it creates dynamic filters that can activate the Guards that you associate with the Detector. If you do not associate any Guards with the Detector, then the dynamic filters instruct the Detector to log the event only.

You can use the Detector to activate a remote Guard in one of the following ways:

- Using a remote Guard list—Use Secure Sockets Layer (SSL) to enable remote activation and zone synchronization, or use SSH to enable remote activation only.
- Using Border Gateway Protocol (BGP)—Configure the Detector to send a BGP message to the adjacent router to divert the zone traffic to a remote Guard.
- Activating offline—Configure the Detector to issue a notification when an attack on the zone occurs.
- Activating manually—Create a dynamic filter to activate remote Guards.

You place the Detector downstream from the Guard. When no attack is in progress, the Detector sees all inbound traffic destined for the protected zone. During an attack when the Guard diverts traffic from the targeted zone for mitigation, the Detector sees the legitimate traffic that the Guard forwards to the zone.

This section contains the following topics:

- [Activating Remote Guards Using Remote Guard Lists](#)
- [Activating Remote Guards Using BGP](#)
- [Activating Remote Guards Offline](#)
- [Activating Remote Guards Manually](#)

Activating Remote Guards Using Remote Guard Lists

You can configure the Detector with a list of Guards (known as the remote Guard lists) that it activates to protect a zone. The Detector maintains two types of remote Guard lists as follows:

- Zone remote Guard lists—The Detector activates the Guards on this zone-specific list to protect the zone and may synchronize the zone configuration with the Guard.
- Default remote Guard list—The Detector searches the default list only if the zone remote Guard list is empty or does not contain both SSL and Secure Shell communication methods.

You can configure a Guard in more than one remote Guard list.



Note

If you add a Guard to the remote Guard lists, you must establish a communication channel with that remote Guard. See the [“Establishing Communication with the Guard”](#) section on page 3-17 for more information.

Each remote Guard list supports two communication methods:

- SSL—The Detector communicates with the Guards using SSL. The Detector can activate the Guards to protect the zone and synchronize the zone configuration with the Guards.

The Detector can synchronize the zone configuration with the Guards on the remote Guard lists before activating the Guard to protect the zone. See the [“Synchronizing Zone Configurations with a Guard”](#) section on page 4-9 for more information.

- Secure Shell (SSH)—The Detector communicates with the Guards using SSH (version2). The Detector can activate the Guards to protect the zone but cannot synchronize the zone configuration with the Guards.

The Detector activates a Guard in the default remote Guard list only if a Guard with the same communication method was not defined in the zone remote Guard list.



Caution

If you change the remote Guard lists, you must regenerate the SSL certificates that the Detector uses for the communication channel with the remote Guards or the communication fails. See the [“Regenerating SSL Certificates”](#) section on page 3-19 for more information.

Verify that the Detector has at least one Guard defined in one of the remote Guard lists (the default remote Guard list or the zone remote Guard list). If no remote Guard is defined in any one of the remote Guard lists, the Detector records the event in its log file.

This section contains the following topics:

- [Activating a Remote Guard and Synchronizing Zone Configuration](#)
- [Configuring the Default Remote Guard List](#)
- [Configuring the Zone Remote Guard Lists](#)

Activating a Remote Guard and Synchronizing Zone Configuration

To activate a remote Guard and synchronize zone configuration, perform the following steps:

-
- Step 1** Create and configure a new zone using one of the Guard zone templates.
See the [“Creating a New Zone” section on page 4-4](#).
- Step 2** Add the remote Guard IP address to either of the following lists:
- Zone remote Guard list—A list of remote Guards that the Detector activates to protect the zone.
See the [“Configuring the Zone Remote Guard Lists” section on page 8-8](#) for more information.
 - Detector default remote Guard list—The default list of remote Guards. The Detector activates these remote Guards if the zone remote Guard list is empty.
See the [“Configuring the Default Remote Guard List” section on page 8-7](#) for more information.
- Step 3** Configure the communication channel with the remote Guard.
See the [“Establishing Communication with the Guard” section on page 3-17](#) for more information.
- Step 4** Configure the zone Guard-protection forms (**protect-ip-state**) to determine the method that the Detector uses to activate a remote Guard.
See the [“Configuring Guard-Protection Activation Methods” section on page 8-4](#) for more information.
- Step 5** Create a new zone on the remote Guard by using one of the following methods:
- Synchronize the zone configuration from the Detector to the Guard using SSL.
See the [“Synchronizing Zone Configurations with a Guard” section on page 4-9](#) for more information.
 - Create a new zone on the remote Guard. The zone name on the Guard must be identical to the zone name on the Detector unless you configure the Detector to activate protection on the Guard based on the attacked IP address only by using the **protect-ip-state dst-ip-by-ip** command.
See the [“Configuring Guard-Protection Activation Methods” section on page 8-4](#) for more information about the **protect-ip-state** command.
- Step 6** Configure the timer that the remote Guard uses to terminate zone protection by using the **protection-end-timer** command in the remote Guard. If the value of the protection-end-timer is **forever**, the remote Guard does not terminate zone protection when the attack ends.
-

Configuring the Default Remote Guard List

The Detector activates a remote Guard in the default remote Guard list if both the following conditions apply:

- A zone remote Guard list is empty or does not contain Guards with both SSL and SSH communication methods.
- The remote Guard in the default list is configured with the communication method that is not defined in the zone-specific remote Guard list.

The Detector activates all remote Guards with the same communication method.

To add a Guard to the default remote Guard list, use the following command in configuration mode:

```
remote-guard {ssh | ssl} remote-guard-address [description]
```

Table 8-1 provides the arguments and keywords for the **remote-guard** command.

Table 8-1 Arguments and Keywords for the remote-guard Command

Parameter	Description
ssh	Specifies the SSH communication method.
ssl	Specifies the SSL communication method.
<i>remote-guard-address</i>	IP address of the remote Guard.
<i>description</i>	(Optional) Description of the remote Guard. The description can have a maximum of 63 alphanumeric characters.

The following example shows how to add a remote Guard to the default remote Guard list using an SSL communication method:

```
user@DETECTOR-conf# remote-guard ssl 192.168.100.33
```

To display the default lists of remote Guards, use the **show remote-guards** command in global or configuration mode.

Configuring the Zone Remote Guard Lists

The Detector activates all the remote Guards that you define in the zone remote Guard lists.

To add a Guard to a zone remote Guard list, use the following command in zone configuration mode:

```
remote-guard {ssh | ssl} remote-guard-address [description]
```

Table 8-2 provides the arguments and keywords for the **remote-guard** command.

Table 8-2 Arguments for the remote-guard Command

Parameter	Description
ssh	Specifies the SSH communication method.
ssl	Specifies the SSL communication method.
<i>remote-guard-address</i>	IP address of the remote Guard.
<i>description</i>	(Optional) Description of the remote Guard. The description can have a maximum of 63 alphanumeric characters.

The following example shows how to add a Guard to the zone remote Guard list using an SSL communication method:

```
user@DETECTOR-conf-zone-scannet# remote-guard ssl 192.168.100.33
```

To display the zone remote Guard lists, use the **show remote-guards** command in zone configuration mode.

Activating Remote Guards Using BGP

Use Border Gateway Protocol (BGP) to activate a remote Guard to protect the zone if you do not want to establish a communication channel between the Detector and the remote Guard. For example, you can use BGP to activate a remote Guard if the Detector is located at the customer premises and the remote Guard is located at the Internet Service Provider (ISP) premises. You can configure the Detector to send a BGP update message to the adjacent router when it detects an attack on the zone to divert the zone traffic to the remote Guard, and you can configure the remote Guard to activate zone protection when it identifies traffic that is destined to the zone.

The Detector sends a BGP update message to the adjacent router to divert the zone traffic to a remote Guard when it creates a dynamic filter with an action of remote-activate Detector; the Detector sends a BGP withdraw message to the adjacent router when the dynamic filter is deleted.

The remote Guard cannot notify the Detector that an attack on the zone has ended because there is no communication channel between the Detector and the remote Guard. To enable the Detector to continue monitoring the zone traffic after the attack ends, perform each of the following tasks:

- Configure a timeout for the dynamic filters with an action of remote-activate. By default, the timeout for each policy is 600 seconds.

See the [“Configuring the Policy Timeout” section on page 6-19](#) and the [“Deleting Dynamic Filters” section on page 5-16](#) for more information.

- Configure the remote Guard to send a BGP update message to the adjacent router to divert the zone traffic to the remote Guard. The adjacent router lists the remote Guard as the next hop to the zone so that if the Detector sends a BGP withdraw message to the adjacent router, the router continues to divert the zone traffic to the remote Guard.
- Configure the remote Guard to send a BGP withdraw message when the attack ends to the adjacent router to stop diverting the zone traffic to the remote Guard.

If the remote Guard is installed at the backbone level and the Detector is installed on the site of the zone, the Detector will monitor only traffic that was handled by the remote Guard until traffic resumes flowing in the original data path.

**Note**

To enable the Detector to activate a remote Guard using BGP, you must have access rights to configure routing on the Detector, the adjacent routers, and the remote Guard.

To enable the Detector to activate a remote Guard using BGP, perform the following steps:

- Step 1** Configure the Detector to send a BGP announcement to the adjacent router each time that it detects an anomaly in the zone traffic.
See the [“Configuring the Detector to Send BGP Announcements” section on page 8-10](#) for more information.
- Step 2** Configure the adjacent router to divert the zone traffic to the remote Guard when it receives a BGP announcement from the Detector.
See the [“Configuring a Router to Divert the Zone Traffic to a Remote Guard” section on page 8-12](#) for more information.
- Step 3** Configure the remote Guard to activate protection when it receives traffic that is destined to the zone and to send a BGP announcement to the adjacent router that lists itself as the next hop to the zone.

See the “[Configuring a Remote Guard to Send BGP Announcements](#)” section on page 8-12 for more information.

This section contains the following topics:

- [Configuring the Detector to Send BGP Announcements](#)
- [Configuring a Router to Divert the Zone Traffic to a Remote Guard](#)
- [Configuring a Remote Guard to Send BGP Announcements](#)

Configuring the Detector to Send BGP Announcements

If BGP routing is configured on the Detector, the Detector sends a BGP update message as long as a dynamic filter with an action of remote-activate exists. You can configure the Detector to send a BGP update message to the adjacent router when it detects an attack on the zone so that the router diverts the zone traffic to a remote Guard.



Note

The Detector sends the BGP update message based on the routing configuration of the Detector. If the routing configuration on the Detector is global and does not specify zone IP addresses, the Detector sends the same BGP update message for each of the zones that it detects an attack on, regardless of the zone configuration.

To configure the Detector to send a BGP routing message when it detects an attack on the zone, perform the following steps:

Step 1 Enable the routing service by entering the **service router** command in configuration mode.

See the “[Activating Detector Services](#)” section on page 3-2 for more information.

Step 2 Enter router configuration mode by entering the **router** command in configuration mode:

```
user@DETECTOR-conf# router
```

The following prompt appears:

```
router>
```

The Detector uses the Zebra application to configure routing (see <http://www.zebra.org> for more information about the Zebra application).



Tip

At each command level of the router configuration mode, you can press the question mark (?) key to display the list of commands available at this mode.

Step 3 Switch to the privileged mode by entering the following command:

```
router> enable
```

The following prompt appears:

```
router#
```

**Note**

To exit router configuration mode, use the **exit** command in router configuration mode. To exit from a current configuration mode to a previous configuration mode, use the **exit** command.

Step 4 Enter terminal configuration mode by entering the following command:

```
router# config terminal
```

The following prompt appears:

```
router(config)#
```

Step 5 Configure the Detector to send a BGP routing message to the adjacent router, which is identified by the community string, and redistribute the routes that the Detector defined by using the **redistribute detector** command.

Step 6 Save all routing configuration changes to the Detector memory by entering the **write memory** command.

Step 7 Verify the following information on the adjacent router:

- The router received the BGP message—Use the **show ip bgp neighbors detector-ip-address received-routes** command.
- The router learned the correct prefixes—Use the **show ip bgp** command.

Step 8 (Optional) Configure the Guard-protection activation method that the zone uses by entering the **protect-ip-state** command. The Guard-protection activation method is designed to focus on the zone protection requirements and save remote Guard resources. The Detector sends a BGP announcement to divert the traffic of the entire zone or of the attacked IP address or subnet to the remote Guard based on the value of the Guard-protection activation method.

**Note**

You can configure the remote Guard to activate protection for the entire zone or for the attacked IP address or subnet only by using the **activation-extent** command on the remote Guard.

See the [“Configuring Guard-Protection Activation Methods” section on page 8-4](#) for more information.

Step 9 (Optional) Configure a timeout for the dynamic filters with an action of remote-activate by entering the **policy set-timeout** command or the **timeout** command.

See the [“Configuring the Policy Timeout” section on page 6-19](#) and the [“Deleting Dynamic Filters” section on page 5-16](#) for more information.

If the timeout of the policy and the dynamic filters that the policy produces is **forever**, the Detector continues sending BGP update messages to the adjacent router to divert the zone traffic to the remote Guard.

The default timeout for each policy is 600 seconds.

To display all policies with an action of remote-activate, use the **show policies | include remote-activate** command. To display dynamic filters, use the **show dynamic-filters** command.

The following example shows how to enable the routing service, enter routing configuration mode, and configure the Detector to send a BGP routing message to the adjacent router:

```
user@DETECTOR-conf# service router
user@DETECTOR-conf# router
router> enable
router# config terminal
```

```

router(config)# router bgp 64555
router(config-router)# bgp router-id <Detector-IP>
router(config-router)# redistribute detector
router(config-router)# neighbor <router-IP> remote-as 55
router(config-router)# neighbor <router-IP> advertisement-interval 1
router(config-router)# neighbor <router-IP> ebgp-multihop 255
router(config-router)# neighbor <router-IP> send-community
router(config-router)# neighbor <router-IP> route-map COMMUNITY out
router(config-router)# exit
router(config)# route-map COMMUNITY permit 10
router(config-route-map)# set community 55:55
router(config-route-map)# exit
router(config)# write memory
router(config)# exit
router# exit
user@DETECTOR-conf# zone <zonename>
user@DETECTOR-conf-zone-<zonename># protect-ip-state dst-ip-by-ip
user@DETECTOR-conf-zone-<zonename># policy * set-timeout 900

```

Configuring a Router to Divert the Zone Traffic to a Remote Guard

Configure the router to use the remote Guard as the next hop to the zone when it receives a BGP update message with a specified community string. The community string must be identical to the community string that you have configured on the Detector and on the remote Guard.

The following example shows how to configure the adjacent router to divert the zone traffic to the Guard:

```

RouterR0# conf term
RouterR0(config)# router bgp 55
RouterR0(config-router)# neighbor <Detector-IP> remote-as 64555
RouterR0(config-router)# neighbor <Detector-IP> route-map COMMUNITY in
RouterR0(config-router)# neighbor Detectors peer-group
RouterR0(config-router)# neighbor <Detector-IP> peer-group Detectors
RouterR0(config-router)# neighbor <Detector-IP> route-map COMMUNITY in
RouterR0(config-router)# exit
RouterR0(config)# ip community-list 55 permit 55:55
RouterR0(config)# route-map COMMUNITY permit 10
RouterR0(config-route-map)# match community 55
RouterR0(config-route-map)# set ip next-hop <remote-Guard-IP>

```

Configuring a Remote Guard to Send BGP Announcements

The Detector may send a BGP withdraw message to the adjacent router so that the router deletes the routes that the Detector listed. To ensure that the adjacent router continues to forward the zone traffic to a remote Guard so that it can continue to protect the zone, you can configure the remote Guard to send a BGP update message to the adjacent router to list the remote Guard as the next hop to the zone.

The remote Guard sends a BGP withdraw message to the adjacent router when the attack ends. When the adjacent router receives the BGP withdraw message, it deletes the routes that the remote Guard added so that the remote Guard is no longer listed as the next hop to the zone and the zone traffic resumes flowing in its original path. The remote Guard reverts to working in the background, and the Detector monitors the zone traffic for additional anomalies.



Note

See the *Cisco Guard Configuration Guide* or the *Cisco Anomaly Guard Module Configuration Guide* for more information about the remote Guard CLI commands.

To configure the remote Guard to send a BGP routing message to the adjacent router when it detects an attack on the zone and to configure how the remote Guard activates zone protection, perform the following steps on the remote Guard:

- Step 1** Configure the method that the remote Guard uses to activate zone protection by entering the **activation-interface** command with one of these keywords: **packet-or-ip-address divert** or **packet divert**.



Note You must use the **divert** keyword for the remote Guard to send BGP announcements to the adjacent router.

The remote Guard activates zone protection when it receives traffic that is destined to the zone that consists of an IP address or subnet that is part of the zone address range.

If you have configured several zones with an address range that includes the received packet IP address, the remote Guard activates the zone with the longest prefix match (the zone that has the most specific address range that includes the received packet IP address). The received IP address or subnet must be completely included in the zone IP address range.

- Step 2** (Optional) Configure the protection activation extent, which defines whether the remote Guard activates zone protection for the entire zone or for a partial zone, by entering the **activation-extent** command.
- Step 3** (Optional) Configure the minimum packet rate that causes the remote Guard to activate zone protection by using the **protect-packet activation-sensitivity** command (the default is 0 pps). The packet rate is measured as the rate to a single zone destination IP address.
- Step 4** Configure the timer that the remote Guard uses to identify that an attack on the zone has ended by entering the **protection-end-timer** command.

If the value of the **protection-end-timer** is **forever**, the remote Guard does not terminate zone protection when the attack ends and does not send a BGP withdraw message to the adjacent router. As a result, the adjacent router continues to divert the zone traffic to the remote Guard and does not resume forwarding the zone traffic to the original data path.

- Step 5** Enter router configuration mode by entering the **router** command in configuration mode:

```
admin@GUARD-conf# router
```

The following prompt appears:

```
router>
```

The Detector uses the Zebra application to configure routing (see <http://www.zebra.org> for more information about the Zebra application).



Tip At each command level of the router configuration mode, you can press the question mark (?) key to display the list of commands available at this mode.

- Step 6** Switch to the privileged mode by entering the following command:

```
router> enable
```

The following prompt appears:

```
router#
```

**Note**

To exit router configuration mode, use the **exit** command in router configuration mode. To exit from a current configuration mode to a previous configuration mode, use the **exit** command.

Step 7 Switch to terminal configuration mode by entering the following command:

```
router# config terminal
```

The following prompt appears:

```
router(config)#
```

Step 8 Configure the remote Guard to send a BGP routing message that is identified by the community string to the adjacent router and to redistribute the routes that the remote Guard defined by using the **redistribute guard** command.

Step 9 Save all routing configuration changes to the remote Guard memory by using the **write memory** command.

Step 10 Verify the following information on the adjacent router:

- The router received the BGP message—Use the **show ip bgp neighbors remote-Guard-IP received-routes** command.
- The router learned the correct prefixes—Use the **show ip bgp** command.

The following example shows how to enter routing configuration mode and configure the Guard to send a BGP routing message to the adjacent router:

```
user@GUARD# zone <zonenumber>
user@GUARD-conf-zone-<zonenumber># activation-interface packet divert
user@GUARD-conf-zone-<zonenumber># activation-extent ip-address-only
user@GUARD-conf-zone-<zonenumber># protection-end-timer 600
user@GUARD-conf-zone-<zonenumber># exit
user@DETECTOR-conf# router
router> enable
router# config terminal
router(config)# router bgp 64555
router(config-router)# bgp router-id <Detector-IP>
router(config-router)# redistribute guard
router(config-router)# neighbor <router-IP> remote-as 55
router(config-router)# neighbor <router-IP> advertisement-interval 1
router(config-router)# neighbor <router-IP> ebgp-multihop 255
router(config-router)# neighbor <router-IP> send-community
router(config-router)# neighbor <router-IP> route-map COMMUNITY out
router(config-router)# exit
router(config-route-map)# route-map COMMUNITY permit 10
router(config-route-map)# set community 55:55
router(config-route-map)# exit
router(config-router)# write memory
```

Activating Remote Guards Offline

When the Detector detects an anomaly in the zone traffic, it logs the event and may generate a Simple Network Management Protocol (SNMP) trap (see the “[Enabling SNMP Traps](#)” section on page 3-28). You can then manually activate a Guard to protect the zone.

To activate a Guard offline, perform the following steps:

-
- Step 1** Configure the zone on both the Detector and the Guard or synchronize the zone configuration offline. See the [“Creating a Zone for Synchronization” section on page 4-10](#) for more information.
 - Step 2** (Optional) Configure the timer that the remote Guard uses to terminate zone protection by using the **protection-end-timer** command in the remote Guard. If you configure the value of the protection-end-timer to **forever**, the remote Guard does not terminate zone protection when the attack ends.
 - Step 3** Activate the zone on the Guard by using the **protect** command.
-

Activating Remote Guards Manually

From the Detector, you can activate a remote Guard manually to protect the zone even before the Detector detects an anomaly in the zone traffic.

To activate a remote Guard manually, perform the following steps on the Detector:

-
- Step 1** Add the remote Guard to the zone remote Guard list or to the default remote Guard list. See the [“Activating Remote Guards Using Remote Guard Lists” section on page 8-6](#) for more information.
 - Step 2** Create a dynamic filter by entering the **dynamic-filter remote-activate** command. See the [“Adding Dynamic Filters” section on page 5-15](#) for more information.
-

