Cisco Guard Configuration Guide

Software Release 6.0
February 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12692-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Guard Configuration Guide
© 2007 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 12

Preface

This guide describes the Cisco Guard (Guard), how it functions, and how to perform administration tasks.

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

This preface contains the following sections:

- Audience
- How to Use This Guide
- Symbols and Conventions
- Obtaining Documentation, Obtaining Support, and Security Guidelines

Audience

The *Cisco Guard Configuration Guide* is intended primarily for the following audiences:

- Network administrators
- Engineers
- Operators
- Network security professionals

This guide assumes a thorough knowledge of networking and networking security.

How to Use This Guide

This guide is organized as follows:

Chapter	Description
Chapter 1, "Product Overview"	Describes the Cisco Guard (Guard) and outlines the Guard operation states and components.
Chapter 2, "Initializing the Guard"	Describes the initial procedures required to connect and configure the Guard. The chapter outlines the Guard CLI environment and authentication methods.
Chapter 3, "Configuring the Guard"	Describes how to configure Guard services and access control.
Chapter 4, "Configuring Traffic Diversion"	Describes the zone traffic diversion process and how to configure diversions.
Chapter 5, "Configuring Zones"	Describes how to create and manage zones.
Chapter 6, "Configuring Zone Filters"	Describes the zone filters and how to configure them.
Chapter 7, "Configuring Policy Templates and Policies"	Describes the zone policies and policy templates and how to configure them.
Chapter 8, "Learning the Zone Traffic Characteristics"	Describes the learning process and how to use the learning process to construct and tune the policies that the Guard uses for zone protection.
Chapter 9, "Protecting Zones"	Describes how to configure and activate zone protection.
Chapter 10, "Using Interactive Protect Mode"	Describes the Interactive protect mode and the recommendations, the user decision options, and the policy interactive status.
Chapter 11, "Using Attack Reports"	Describes the attack reports, the report structure, and viewing options.
Chapter 12, "Using Guard Diagnostic Tools"	Describes the Guard diagnostic tools.
Chapter 13, "Performing Maintenance Tasks"	Describes how to perform tasks that are required for Guard maintenance.
Chapter 14, "Analyzing Guard Mitigation"	Describes how to analyze the zone traffic patterns and identify configuration problems. The chapter provides a short explanation on how to identify the type of attack and recommended actions that you can take according to the analysis.
Appendix A, "Understanding Zone Traffic Diversion"	Provides additional information relating to the traffic diversion procedure including sample code lines.
Appendix B, "Troubleshooting Diversion"	Provides information about the traffic diversion troubleshooting procedure with sample screens.

Symbols and Conventions

This guide uses the following conventions:

Style or Symbol	Description
boldface font	Boldface text indicates commands and keywords that you must enter exactly as shown.
Italics font	Italic font indicates arguments arguments for which you supply the values.
`Screen` font	Screen font indicates the screen display, such as a prompt, and information that the Guard displays on the screen. Do not enter screen font as part of the command.
[x]	Square brackets indicate an optional element (keyword or argument).
[**x** | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{**x** | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.
[x {y | z}]	Braces and vertical bars within square brackets indicate a required choice within an optional element. You do not need to select one. If you do, you have some required choices.

This guide uses the zone name *scannet* and the prompt *user@GUARD-conf-zone-scannet#* in examples.

This guide uses the following symbols and conventions to identify different types of information:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.* The tips information might not be troubleshooting or even an action, but could be useful information.

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Product Overview

This chapter provides a general overview of the Cisco Guard (Guard) including its major components and how they work together to protect network elements from malicious attack traffic.

The chapter contains the following sections:

- Understanding the Guard
- Understanding DDoS Attacks
- Understanding Zones, Zone Policies, and the Learning Process
- Understanding Zone Protection
- Understanding the Protection Cycle

Understanding the Guard

The Guard is a Distributed Denial of Service (DDoS) attack mitigation device that diverts suspect traffic from its normal network path to itself for cleaning. During the traffic cleaning process, the Guard identifies and drops the attack packets and forwards the legitimate packets to their targeted network destinations.

Typically, you deploy the Guard in a distributed upstream configuration at the backbone level.

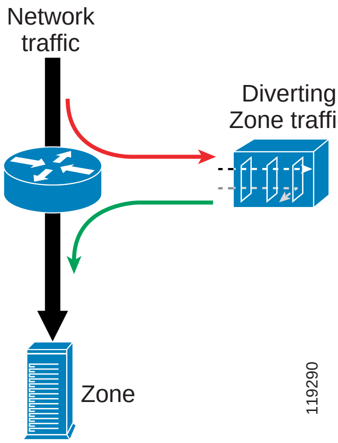
You define the network elements, or *zones*, that the Guard protects against DDoS attacks. When a zone is under attack, the Guard diverts only the network traffic that is destined for the targeted zone, identifies and drops specific attack packets, and forwards legitimate traffic packets to the zone. The Guard constantly filters the zone traffic and stays on the alert for evolving attack patterns. When the Guard determines that the attack on the zone has ended, it stops diverting the zone traffic to itself. By diverting network traffic only when needed, the Guard can assume its protective role when there is an attack but remain unobtrusively in the network background for the rest of the time.

The Guard allows you to do the following tasks:

- Traffic learning—Learn the characteristics (services and traffic rates) of normal zone traffic using an algorithm-based process. During the learning process, the Guard modifies the default zone traffic policies and policy thresholds to match the characteristics of normal zone traffic. The traffic policies and thresholds define the reference points that the Guard uses to determine when the zone traffic is normal or abnormal (indicating an attack on the zone).
- Traffic protection—Distinguish between legitimate and malicious traffic and filter the malicious traffic so that only the legitimate traffic is allowed to pass on to the zone.
- Traffic diversion—Divert the zone traffic from its normal network path to the Guard learning and protection processes and then returns the legitimate zone traffic to the network.

Figure 1-1 shows a sample network application in which the Guard diverts zone traffic to itself so it can learn the zone traffic or protect the zone from an attack.

Figure 1-1 Cisco Guard Operation



Understanding DDoS Attacks

DDoS attacks deny legitimate users access to a specific computer or network resource. These attacks are launched by individuals who send malicious requests to targets that degrade service, disrupt network services on computer servers and network devices, and saturate network links with unnecessary traffic.

This section contains the following topics:

- Understanding Spoofed Attacks
- Understanding Nonspoofed Attacks

Understanding Spoofed Attacks

A spoofed attack is a type of DDoS attack in which the packets contain an IP address in the header that is not the actual IP address of the originating device. The source IP addresses of the spoofed packets can be random or have specific, focused addresses. Spoofed attacks saturate the target site links and the target site server resources. It is easy for a computer hacker to generate high volume spoofed attacks even from a single device.

To overcome spoofed attacks, the Guard performs anti-spoofing processes that use challenge-response algorithms that can distinguish spoofed traffic from nonspoofed traffic. The Guard considers the traffic that passes the anti-spoofing mechanisms as authenticated traffic.

Understanding Nonspoofed Attacks

Nonspoofed attacks (or client attacks) are mostly TCP-based with real TCP connections that can overwhelm the application level on the server rather than the network link or operating system.

The Guard initially activates an anti-spoofing mechanism to block all spoofed packets. The Guard then performs a statistical analysis on the traffic to detect and block anomalies in the traffic that are not spoofed, such as an unusual number of SYN packets, a large number of concurrent connections, or a high traffic rate.

Client attacks from a large number of clients (or zombies) may overwhelm the server application even without any of the individual clients creating an anomaly. The zombie programs try to imitate legitimate browsers that access the target site. The Guard anti-zombie processes mitigates such HTTP attacks by using a challenge response authentication process to differentiate between legitimate browsers and zombie programs that access the attacked site.

Understanding Zones, Zone Policies, and the Learning Process

This section describes what a Guard zone represents, how zone policies detect traffic anomalies, and how the Guard learns the zone traffic characteristics.

These sections contain the following topics:

- Understanding Zones
- Understanding the Zone Policies
- Understanding the Learning Process

Understanding Zones

A zone that the Guard protects can be one 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)
- Any combination of these elements

When you create a new zone, you assign a name to it and configure the zone with network addresses. The Guard configures the zone with a default set of policies and policy thresholds to detect anomalies in the zone traffic.

The Guard can protect multiple zones at the same time if the network address ranges do not overlap.

For more information about zones, see Chapter 5, “Configuring Zones.”

Understanding the Zone Policies

When the Guard protects a zone, the policies associated with the zone configuration enable the Guard to detect anomalies in the zone traffic and mitigate attacks on the zone. When the traffic flow exceeds a policy threshold, the Guard identifies the traffic as abnormal or malicious and dynamically configures a set of filters to apply the appropriate protection level to the traffic flow according to the severity of the attack.

For more information about zone policies, see Chapter 7, “Configuring Policy Templates and Policies.”

Understanding the Learning Process

The learning process enables the Guard to analyze normal zone traffic and create a set of zone-specific policies and policy thresholds that are based on the analyzed traffic. The zone-specific policies and policy thresholds enable the Guard to more accurately detect zone traffic anomalies.

You enable the learning process to replace the default set of zone policies or to update the current set of zone policies that may not be configured properly to recognize current normal traffic services and volume. When policy thresholds are set too high compared to the current normal traffic volume, the Guard might not be able to detect traffic anomalies (attacks). When policy thresholds are set too low, the Guard may mistake legitimate traffic for attack traffic.

The learning process consists of the following two phases:

- Policy Construction Phase—Creates the zone policies for the main services that the zone traffic uses. To create zone policies, the Guard follows the rules established by the policy templates that each zone configuration contains.
- Threshold Tuning Phase—Tunes the thresholds of the zone policies to values that are appropriate for recognizing the normal traffic rates of the zone services.

For more information about the learning process, see Chapter 8, “Learning the Zone Traffic Characteristics.”

Understanding Zone Protection

You can activate zone protection on the Guard by using one of the following methods:

- Manually—You can manually access the Guard and activate protection for a zone.
- Automatically—You can configure the Guard to accept a protection activation message from a network attack detection device, such as the Cisco Traffic Anomaly Detector (Detector).

Note The Detector is the companion product of the Guard. The Detector is a DDoS attack detection device that can analyze a copy of the zone traffic and 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 section contains the following topics:

- Understanding Traffic Filters
- Understanding the Different Protection Modes
- Understanding the Protect and Learn Function
- Understanding On-Demand Protection
- Understanding Attack Reports

Understanding Traffic Filters

The Guard uses four types of traffic filters to apply the required protection level to the zone traffic. You can configure these filters to customize the traffic flow and control the DDoS protection operation.

The Guard uses the following types of filters:

- User Filters—Apply the required protection level to the specified traffic flows.
- Bypass filters—Prevent the Guard from applying DDoS protection measures to specific traffic flows.
- Flex-Content filters—Count or drop a specified traffic flow and filter according to fields in the IP and TCP headers and content bytes.
- Dynamic filters—Apply the required protection level to the specified traffic flows. The Guard creates dynamic filters only when it detects an attack on the zone and configures them based on its analysis of the traffic flow. The Guard continuously modifies this set of filters based on the the zone traffic, type of DDoS attack, and changes to the attack characteristics.

The Guard has three protection levels that enable it to apply different processes to the traffic flows:

- Analysis protection level—Allows the traffic to flow monitored, but unhindered, during zone protection if no anomalies are detected. Once the Guard detects an anomaly, it applies the appropriate protection level to the traffic.
- Basic protection level—Activates anti-spoofing and anti-zombie functions to authenticate the traffic by inspecting the suspicious traffic flow to verify its source.
- Strong protection level—Activates severe anti-spoofing functions that inspect the traffic flow packets to verify the legitimacy of the flow.

The Guard analyzes the traffic and coordinates the efforts of the zone policies that monitor the zone traffic for anomalies with the zone filters. In addition, it limits the rate of traffic that it injects on to the zone to prevent traffic overflow.

For more information about filters, see Chapter 8, “Learning the Zone Traffic Characteristics.”

Understanding the Different Protection Modes

You can activate the Guard to perform zone protection as follows:

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

For more information about the protection modes, see Chapter 10, “Using Interactive Protect Mode.”

Understanding the Protect and Learn Function

You can activate the threshold tuning phase of the learning process and activate zone protection simultaneously (the protect and learn function) to enable the Guard to learn the zone policy thresholds and at the same time monitor the traffic for anomalies. When the Guard detects an attack, it stops the learning process and begins mitigating the attack. The Guard resumes the learning process when the attack ends. This process prevents the Guard from learning malicious traffic thresholds during an attack.

For more information about the protect and learn function, see the "Enabling the Protect and Learn Function" section on page 8-11.

Understanding On-Demand Protection

You can use the default zone templates and associated default policies to protect a zone without enabling the Guard to learn the zone traffic characteristics. The default policies and filters in the Guard zone templates can protect a zone that has traffic characteristics that are unknown to the Guard.

For more information about on-demand protection, see the "Activating On-Demand Protection" section on page 9-2.

Understanding Attack Reports

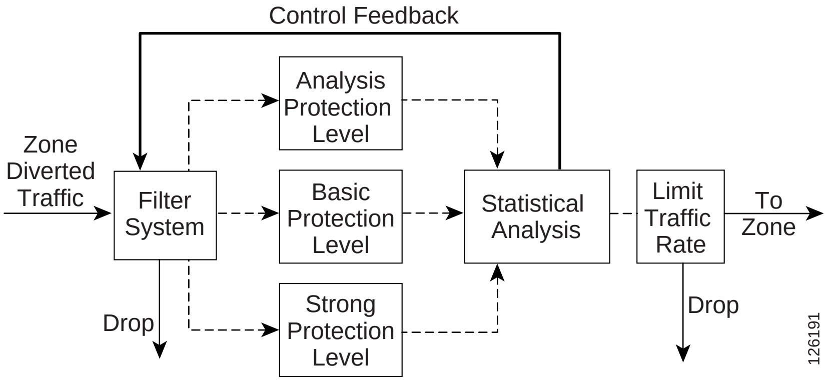
The Guard provides an attack report for every zone that provides zone status information and details of the attack, starting with the production of the first dynamic filter and ending with protection termination.

For more information about the attack reports, see Chapter 11, "Using Attack Reports."

Understanding the Protection Cycle

The Guard protection cycle applies the zone filters, zone policies, and the Guard protection levels to the traffic flow to analyze and clean the zone traffic and inject legitimate traffic only to the zone. Figure 1-2 shows the Guard protection cycle.

Figure 1-2 Guard Protection Cycle



Once zone protection is activated by you or by an anomaly detection device such as the Detector, the Guard diverts the zone traffic to itself where the policies of the zone configuration monitor the traffic flow. A policy executes an action against a particular traffic flow when the flow exceeds the policy threshold. Policy actions can range from issuing a notification to creating new filters (dynamic filters) that direct the traffic to the appropriate protection level. The Guard analyzes the traffic flow, drops the traffic that exceeds the defined rate that the zone can handle, and then injects the legitimate traffic back to the zone.

During the attack, the Guard performs a closed-loop feedback cycle in which it adjusts the zone protection measures to the dynamically changing zone traffic characteristics. The Guard adjusts the protection strategies to handle any changes to the DDoS attack and traffic flow. The Guard stops zone protection if no dynamic filters are in use, the traffic to the zone has not been dropped, or no new dynamic filters have been added over a predefined period of time.

CHAPTER 2

Initializing the Guard

This chapter describes the basic tasks required to initialize the Cisco Guard (Guard) in a network and how to manage it.

This chapter contains the following sections:

- Using the Command-Line Interface
- Accessing the Guard for the First Time
- Configuring the Guard Interfaces
- Configuring the Default Gateway
- Adding a Static Route to the Routing Table
- Configuring the Proxy IP Address
- Managing the Guard

Using the Command-Line Interface

You can control the Guard functions by using the command-line interface (CLI). The Guard user interface is divided into many different command modes and the access to the CLI is mapped according to user privilege levels. The commands that are available to you depend on which mode you are currently in.

This section contains the following topics:

- Understanding User Privilege Levels
- Understanding Command Modes
- Entering CLI Commands
- Tips for Using the CLI

Understanding User Privilege Levels

The access to the CLI is mapped according to user privilege levels. Each privilege level has its own group of commands.

Table 2-1 describes the user privilege levels.

Table 2-1 User Privilege Levels

User Privilege Level	Description
Administration (admin)	Provides access to all operations.
Configuration (config)	Provides access to all operations except for operations relating to user definition, deletion, and modification.
Dynamic (dynamic)	Provides access to monitoring and diagnostic operations, protection, and learning-related operations. Users with Dynamic privileges can also configure flex-content filters and dynamic filters.
Show (show)	Provides access to monitoring and diagnostic operations.

Note We recommend that users with Administration and Configuration privilege levels configure all filters. Users with lower privilege levels can add and remove dynamic filters.

Understanding Command Modes

This section contains summaries of the command and configuration modes used in the Guard CLI. To obtain a list of commands available for each command mode, enter **?** at the system prompt.

Table 2-2 lists and describes the Guard command modes.

Table 2-2 Guard Command Configuration Modes

Mode	Description
Global	Allows you to connect to remote devices and list system information. The Global prompt is the default prompt when you log into the Guard. The command prompt is as follows: `user@GUARD#`
Configuration	Allows you to configure features that affect the Guard operation and have restricted user access. To enter configuration mode, use the **configure** command in global mode. The command prompt is as follows: `user@GUARD-conf#`
Interface configuration	Allows you to configure the Guard networking interfaces. To enter interface configuration mode, use the **interface** command in configuration mode. The command prompt is as follows: `user@GUARD-conf-if-<interface-name>#`
Router configuration	Allows you to configure the Guard routing configuration. To enter router configuration mode, use the **router** command in configuration mode. The command prompt is as follows: `router>`

Table 2-2 Guard Command Configuration Modes (continued)

Mode	Description
Zone configuration	Allows you to configure the zone attributes. To enter zone configuration mode, use the **zone** command in configuration mode or use the **configure** command in global mode. The command prompt is as follows: `user@GUARD-conf-zone-<zone-name>#`
Policy template configuration	Allows you to configure the zone policy templates. To enter policy template configuration mode, use the **policy-template** command in zone configuration mode. The command prompt is as follows: `user@GUARD-conf-zone-<zone-name>-policy_template-<policy-template-name>#`
Policy configuration	Allows you to configure the zone policies. To enter policy configuration mode, use the **policy** command in zone configuration mode. The command prompt is as follows: `user@GUARD-conf-zone-<zone-name>-policy-<policy-path>#`

Entering CLI Commands

This section contains the following topics:

- Using the no Form of a Command
- show Command Syntax
- CLI Error Messages

Table 2-3 describes the rules for entering CLI commands.

Table 2-3 CLI Rules

Action	Keyboard Sequence
Scroll through and modify the command history	Use the **arrow** keys.
Display commands available in a specific command mode	Press **Shift** and enter the **?** (question mark) key.
Display a command completion	Type the beginning of the command and press **Tab**.
Display a command syntax completion(s)	Enter the command and press **Tab** twice.
Scroll using the **more** command	Enter the **more** *number-of-lines* command. The **more** command configures the number of additional lines displayed in the window once you press the **Spacebar**. The default is two lines less than the capability of the terminal. The *number-of-lines* argument configures the number of additional lines to be displayed once you press the **Spacebar**.

Table 2-3 CLI Rules (continued)

Action	Keyboard Sequence
Scroll on a single screen (within a command output)	Press the **Spacebar**.
Scroll back a single screen (within a command output)	Press the **b** key.
Stop scroll movement	Press the **q** key.
Search forward for a string	Press the **/** (forward slash mark) key and enter the *string*.
Search backward for a string	Press the **?** (question mark) key and enter the *string*.
Cancel the action or delete a parameter	Use the **no** form of a specific command.
Display information relating to a current operation	Enter the **show** command.
Exit from a current command group level to a higher group level	Enter the **exit** command.
Exit all command group levels and return to the root level	Enter the **end** command.
Display command output from and including the first line that contains a *string*	Enter the | (vertical bar) and then enter the **begin** *string* command.
Display command output lines that include a *string*	Enter the | (vertical bar) and then enter the **include** *string* command.
Display command output lines that do not include a *string*	Enter the | (vertical bar) and then enter the **exclude** *string* command.

Note If you enter the **exit** command at the root level, you exit the CLI environment to the operating system login screen.

Using the no Form of a Command

Almost every configuration command also has a **no** form. In general, use the **no** form of a command to disable a feature or function. Use the command without the keyword **no** to enable a disabled feature or function. For example, the **event monitor** command turns on the event monitor, and the **no event monitor** command turns it off.

show Command Syntax

You can execute zone-related **show** commands from the zone configuration mode. Alternatively, you can execute these commands from the global or configuration modes.

The following is the syntax for the **show** command in global or configuration modes:

show zone *zone-name parameters*

The following is the syntax for the **show** command in zone configuration mode:

show *parameters*

Note This publication uses the **show** command syntax from the zone configuration mode unless explicitly specified.

CLI Error Messages

The Guard CLI displays error messages in the following situations:

- The syntax of the command is incomplete or incorrect.
- The command does not match the system configuration.
- The operation could not be performed due to a system failure. In this situation, an entry is created in the system log.

Tips for Using the CLI

This section provides tips for using the CLI and includes the following topics:

- Using Help
- Using the Tab Completion
- Understanding Conventions of Operation Direction
- Abbreviating a Command
- Using Wildcard Characters

Using Help

The CLI provides context-sensitive help at every mode of the command hierarchy. The help information tells you which commands are available at the current command mode and provides a brief description of each command.

To get help, type **?**.

To display help for a command, type **?** after the command.

To display all commands available in a mode along with a short description, enter **?** at the command prompt.

The help displays commands available in the current mode only.

Using the Tab Completion

You can use tab completion to reduce the number of characters that you need to type for a command. Type the first few characters of a command and press **Tab** to complete the command.

After entering a command that has a value with multiple options, press **Tab** twice to display a list of possible input parameters, including system-defined parameters and user-defined parameters. For example, if you press **Tab** twice after entering the **policy-template** command in zone configuration mode, the list of policy template names is displayed. If you press Tab twice after entering the **zone** command in configuration mode, zones that are already defined are displayed.

If multiple commands match for a Tab completion action, nothing is displayed; the system repeats the current line that you entered.

The tab completion feature displays only commands available for the current mode.

You can disable tab completion for zone names in all commands in global and configuration modes such as the **zone** command and the **show zone** commands 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.

Understanding Conventions of Operation Direction

The order of keywords in the command syntax define the direction of the operation. When you enter the keyword before you enter the command, the Guard copies the data from the Guard to the server. When you enter the command before you enter the keyword, the Guard copies the data from the server to the Guard. For example, the **copy log ftp** command copies the log file from the Guard to the FTP server. The **copy ftp new-version** command copies the new software version file from the FTP server to the Guard.

Abbreviating a Command

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation.

For example, you can abbreviate the **show** command to **sh**.

Using Wildcard Characters

You can use an asterisk (*) as a wildcard.

For example, if you enter the **learning policy-construction *** command**,** the policy construction phase is activated for all the zones that are configured on the Guard.

If you enter the **learning policy-construction scan *** command**,** the policy construction phase is activated for all the zones that are configured on the Guard with names that begin with scan (such as scannet, scanserver, and so on).

If you enter the **no zone *** command**, all zones are removed.**

Accessing the Guard for the First Time

This section shows how to establish the initial session with the Guard by using the preconfigured username that has an administration user privilege level. During this process, the CLI prompts you to assign passwords to the following default user accounts:

- admin—Provides access to all administrative and configuration operations.
- riverhead—Provides access to monitoring and diagnostic operations, zone protection, and learning-related operations. This user can also configure flex-content filters and dynamic filters.
- root—Provides access to the Linux shell for certain administrative operations.

To access the Guard for the first time, perform the following steps:

Step 1 Press the power control button on the front of the Guard.

After the Guard boot process completes, the software prompts you to enter a username.

Note During power-up, the green power LED on the front of the Guard is on.

Step 2 Enter **admin** for the username and **rhadmin** for the password.

Step 3 Enter a password for the root user account that consists of 6 to 24 characters.

Retype the new password to verify it.

Step 4 Enter a password for the admin user account that consists of 6 to 24 characters.

Retype the new password to verify it.

Step 5 Enter a password for the riverhead user account that consists of 6 to 24 characters.

Retype the new password to verify it.

Note You can change the passwords for the admin and riverhead user accounts at any time. See the "Changing Your Password" section on page 3-7 for more information.

Step 6 Enter configuration mode to configure the Guard by entering the following command:

configure [**terminal**]

The following example shows how to enter configuration mode:

```
user@GUARD# configure
user@GUARD-conf#
```

Configuring the Guard Interfaces

The Guard has several Network Interface Cards (NICs). The eth0 and the eth1 10/100/1000 Ethernet interfaces comprise the out-of-band NICs used for management traffic.

The giga0 and giga1 (Gigabit Ethernet) interfaces comprise the in-band NICs that the Guard uses for management and zone traffic. The giga0 and giga1 interfaces provide the physical interface on which virtual interfaces (VLANs and tunnels) are configured. Configuring the Guard interfaces serves as a basis for the traffic diversion procedures. See Chapter 4, "Configuring Traffic Diversion," for more information.

You configure a Guard interface by entering the **interface** command and specifying the interface type and number. Many Guard features are enabled on a per-interface basis.

The following guidelines apply to all physical and virtual interface configuration processes:

- Each interface must be configured with an IP address and an IP subnet mask unless you configure IP addresses for individual VLANs.
- You must activate each interface using the **no shutdown** command.

To display the status or configuration of an interface, enter the **show** or **show running-config** commands.

This section contains the following topics:

- Configuring a Physical Interface

- Configuring a VLAN
- Configuring a Loopback Interface
- Configuring a Tunnel
- Clearing the Counters of a Physical Interface

Configuring a Physical Interface

Configure a physical interface to connect the Guard to a network. The Guard has four physical interfaces: eth0, eth1, giga0, and giga1. The out-of-band interfaces are eth0 and eth1 (10/100/1000 Ethernet sockets for out-of-band management).

The in-band interfaces (copper or fiber socket) are giga0 and giga1.

Caution Do not configure two interfaces on the same subnet or the Guard routing may not work properly.

To configure a physical interface, perform the following steps:

Step 1 Enter interface configuration mode by entering the following command in configuration mode:

```
interface if-name
```

The *if-name* argument specifies the interface name. The Guard supports the following interfaces:

- eth0 or eth1—Out-of-band interfaces
- giga0 or giga1—In-band interfaces

Step 2 Set the interface IP address by entering the following command:

```
ip address ip-addr ip-mask
```

The *ip-addr* and *ip-mask* arguments define the interface IP address. Enter the IP address and subnet mask in dotted-decimal notation (for example, an IP address of 192.168.100.1 and a subnet mask of 255.255.255.0).

Step 3 (Optional) Define the interface maximum transmission unit (MTU) by entering the following command:

```
mtu integer
```

The *integer* argument is an integer between 576 and 1800 for all interfaces. The default MTU value is 1500 bytes.

Step 4 (Optional) For the giga0 or giga1 in-band interface only, configure the interface speed and duplex mode by entering the following command:

```
speed {auto | half speed | full speed}
```

Table 2-4 provides the arguments and keywords for the **speed** command.

Table 2-4 Arguments and Keywords for the speed Command

Parameter	Description
auto	Enables the interface autonegotiation capability. The interface automatically operates at 10/100/1000 Mbps and half or full duplex, depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration. The default setting is **auto**.
half	Specifies half-duplex operation.
full	Specifies full-duplex operation.
speed	Interface speed in megabits per second (Mbps). Enter **10**, **100**, or **1000**.

Step 5 Activate the interface by entering the following command:

```
no shutdown
```

After activating or deactivating a giga0 or giga1 in-band interface, you must reload the Guard for the configuration change to take effect.

The following example shows how to configure and activate interface eth1:

```
user@GUARD-conf# interface eth1
user@GUARD-conf-if-eth1# ip address 10.10.10.33 255.255.255.252
user@GUARD-conf-if-eth1# no shutdown
```

To deactivate a physical interface, use the **shutdown** command.

Configuring a VLAN

You can define VLANs on the in-band interfaces only.

To define a VLAN on the Guard, perform the following steps:

Step 1 Enter VLAN interface configuration mode, if one exists, or define a new VLAN by entering the following command in configuration mode:

```
interface gigaX.vlan-id
```

The *vlan-id* argument is an integer that specifies the VLAN ID number. The VLAN ID is a TAG IEEE 802.1Q number.

The *x* argument specifies the interface. Enter 0 or 1 for the in-band interface.

Step 2 Set the VLAN IP address by entering the following command:

```
ip address ip-addr ip-mask
```

The *ip-addr* and *ip-mask* arguments define the interface IP address. Enter the IP address and subnet mask in dotted-decimal notation (for example, an IP address of 192.168.100.1 and a subnet mask of 255.255.255.0).

Step 3 (Optional) Define the interface MTU by entering the following command:

```
mtu integer
```

The *integer* argument is an integer between 576 and 1824 bytes. The default MTU value is 1500 bytes.

Step 4 Activate the interface by entering the following command:

```
no shutdown
```

The following example shows how to configure a VLAN on the Guard:

```
user@GUARD-conf# interface giga1.2
user@GUARD-conf-if-giga1.2# ip address 192.168.5.8 255.255.255.0
user@GUARD-conf-if-giga1.2# no shutdown
```

Configuring a Loopback Interface

You can specify a virtual interface called a loopback interface to emulate a physical interface. You can use the loopback interface to configure advanced traffic diversion configurations, such as the long traffic diversion process.

In applications where other routers or access servers attempt to reach this loopback interface, you must configure a routing protocol to distribute the subnet assigned to the loopback address.

To configure the loopback interface, perform the following steps:

Step 1 Enter the loopback interface configuration mode, if one exists, or define a new loopback interface by entering the following command in configuration mode:

```
interface if-name
```

The *if-name* argument specifies the loopback interface name. The interface name is **lo:***integer* where *integer* is an integer between 0 and 99.

Step 2 Set the loopback interface IP address by entering the following command:

```
ip address ip-addr ip-mask
```

The *ip-addr* and *ip-mask* arguments define the interface IP address. Enter the IP address and subnet mask in dotted-decimal notation (for example, an IP address of 192.168.100.1 and a subnet mask of 255.255.255.0).

The following example shows how to configure a loopback interface:

```
user@GUARD-conf# interface lo:0
user@GUARD-conf-if-lo:0# ip address 1.1.1.1 255.255.255.255
```

Configuring a Tunnel

You can define a Generic Routing Encapsulation (GRE) or an IP in IP (IPIP) tunnel for the Guard to use in the traffic diversion process.

To define a tunnel, perform the following steps:

Step 1 Enter the tunnel interface configuration mode, if one exists, or define a new tunnel by entering the following command in configuration mode:

interface {**gre**X | **ipip**Y}

The X argument is an integer between 0 and 1024 bytes assigned to a GRE tunnel.

The Y argument is an integer between 0 and 1024 bytes assigned to an IPIP tunnel.

Step 2 Set the tunnel IP address by entering the following command:

ip address *ip-addr* [*ip-mask]*

The *ip-addr* and *ip-mask* arguments define the interface IP address. Enter the IP address and subnet mask in dotted-decimal notation (for example, an IP address of 192.168.100.1 and a subnet mask of 255.255.255.0). The default subnet mask is 255.255.255.255.

Step 3 Set the tunnel source IP address by entering the following command:

tunnel source *source ip*

The *source ip* argument specifies the tunnel source IP address. This IP address will be used as the source address for the packets in the tunnel. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1).

Step 4 Set the tunnel destination IP address by entering the following command:

tunnel destination *destination-ip*

The *destination ip* argument specifies the tunnel destination IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.100.1).

Step 5 (Optional) Define the interface MTU by entering the following command:

mtu *integer*

The *integer* argument is an integer between 576 and 1480. The default value for an IPIP tunnel is 1480 bytes. The default value for a GRE tunnel is 1476 bytes.

Step 6 Activate the interface. Enter the following command:

no shutdown

The following example shows how to configure a GRE tunnel:

```
user@GUARD-conf# interface gre2
user@GUARD-conf-if-gre2# ip address 192.168.121.1 255.255.255.0
user@GUARD-conf-if-gre2# tunnel source 192.168.8.8
user@GUARD-conf-if-gre2# tunnel destination 192.168.250.2
user@GUARD-conf-if-gre2# no shutdown
```

Checking the Status of a GRE Tunnel

You can configure the Guard to send keepalive messages over a GRE tunnel at specific times to keep the interface active. You can also specify the number of times that the Guard sends a keepalive packet without receiving a response before the Guard brings the tunnel down.

You configure the keepalive time interval in 1-second increments. If you do not change the retries default value, the Guard declares a GRE tunnel down after 10 consecutive intervals have passed without the Guard receiving a keepalive packet response.

Caution When the Guard declares a GRE tunnel down, the Guard stops using the tunnel for injection. If no other means of traffic injection exist, the Guard suspends zone traffic diversion along with traffic learning or zone protection.

The Guard continues to send keepalive messages even when the GRE tunnel is declared down. If the tunnel end returns the keepalive message, the Guard activates the tunnel and resumes traffic diversion along with zone learning or zone protection.

To enable keepalive messages on a GRE tunnel, use the following command in GRE interface configuration mode:

keepalive [*refresh-time* [*retries*]]

Table 2-5 provides the arguments for the **keepalive** command.

Table 2-5 Arguments for the keepalive Command

Parameter	Description
refresh-time	(Optional) Time interval in seconds at which keepalive messages are sent. Enter an integer from 1 to 32767. The default refresh time is 3 seconds.
retries	(Optional) Number of times that the Guard continues to send keepalive packets without a response before bringing the tunnel interface protocol down. Enter an integer from 1 to 255. The default number of retries is 10.

The following example shows how to enable keepalive messages on a GRE tunnel:

```
user@GUARD-conf-if-gre2# keepalive 60 5
```

Clearing the Counters of a Physical Interface

You can clear the counters of physical interfaces that are used for data (giga1 or giga2) if you are going to perform testing and want to be sure that the counters include information from the testing session only.

To clear the interface counters, use the following command in interface configuration mode:

clear counters

The following example shows how to clear the counters of the interface giga1:

```
user@GUARD-conf-if-giga1# clear counters
```

Configuring the Default Gateway

The default gateway receives and forwards packets containing IP addresses that are unknown to the local network. In most cases, the Guard default gateway IP address is the adjacent router located between the Guard and the Internet. The default gateway IP address must be on the same network as one of the IP addresses of the Guard network interfaces.

Caution If you do not configure the default gateway IP address, the Guard may not be accessible to the network.

To assign a default gateway address, use the following command in configuration mode:

default-gateway *ip-addr*

The *ip-addr* argument specifies the default gateway IP address. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1).

To modify the default gateway address, reenter the command.

The following example shows how to configure the default gateway:

```
user@GUARD-conf# default-gateway 192.168.100.1
```

Adding a Static Route to the Routing Table

You can add a static route to the Guard routing table to specify routes for servers or networks outside the local networks that are associated with the Guard IP interfaces. The static route is added permanently and is not removed after the Guard is rebooted.

To add a static route to the Guard routing table, use the following command in configuration mode:

ip route *ip-addr ip-mask nexthop-ip* [*if-name*]

Table 2-6 provides the arguments for the **ip route** command.

Table 2-6 Arguments for the ip route Command

Parameter	Description
ip-addr	Network destination of the route. The destination can be an IP network address (where the host bits of the network address are set to 0) or a host route IP address. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).
ip-mask	Subnet mask associated with the network destination. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0).
nexthop-ip	Forwarding or the next-hop IP address over which the set of addresses that are defined by the network destination and subnet mask are reachable. The next-hop IP address should be within the interface subnet. For local subnet routes, the next-hop IP address is the IP address that is assigned to the interface that is attached to the subnet. For remote routes available across one or more routers, the next-hop IP address is a neighboring router IP address that is directly accessible.

Table 2-6 Arguments for the ip route Command (continued)

Parameter	Description
if-name	(Optional) Interface on the Guard over which the destination is reachable. If you do not specify an interface, the next-hop IP address in the Guard routing table determines the interface used.

The following example shows how to configure a static route:

```
user@GUARD-conf# ip route 172.16.31.5 255.255.255.255 192.168.100.34
```

To display the routing table, enter the **show ip route** command.

Configuring the Proxy IP Address

The Guard proxy IP address is required for the proxy mode anti-spoofing protection mechanisms in which the Guard serves as a TCP proxy to the zone. The Guard first authenticates new connections and only then initiates a connection with the zone using its own IP address as the source IP address. You must configure a proxy IP address before activating zone protection.

⚠ **Caution** You cannot activate zone protection without defining a proxy IP address.

Do not assign the Guard with a proxy IP address while zone protection is enabled.

We recommend that you configure three to four proxy IP addresses if your network uses load balancing to distribute network overload or if your network requires a high number of concurrent connections.

You can configure up to 60 proxy IP addresses; however, we recommend that you do not configure more than 20 proxy IP addresses because more proxy IP addresses consume more memory resources.

To configure a Guard anti-spoofing proxy IP address, use the following command in configuration mode:

proxy *ip-addr*

The *ip-addr* argument specifies the proxy IP address. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).

You must verify the route between every zone and the Guard proxy IP address. The Guard does not answer ping requests to its proxy IP address.

To configure additional proxy IP addresses, reenter the command.

The following example shows how to configure a proxy IP address:

```
user@GUARD-conf# proxy 192.168.100.34
```

Managing the Guard

Initially, you can manage the Guard locally from a console. The console connection provides access to the CLI and allows you to run the initial setup procedures when you first turn on the Guard. See the "Assigning Privilege Levels with Passwords" section on page 3-9 for more information.

After you configure the Guard networking (see the "Configuring the Guard Interfaces" section on page 2-7), you can access and manage the Guard using one of the following methods:

- Access using a Secure Shell (SSH) session.
- Access the Guard using a Web-Based Manager (WBM).
- Access the Guard using the MultiDevice Manager (MDM).
- Access from a DDoS-sensing network element. Refer to the appropriate documentation for more information.

This section contains the following topics:

- Managing the Guard with a Web-Based Manager
- Managing the Guard with the Cisco DDoS MultiDevice Manager
- Accessing the Guard with SSH

Managing the Guard with a Web-Based Manager

You can manage the Guard using the WBM and a web browser.

To enable the WBM and manage the Guard, perform the following steps:

Step 1 Enable the WBM service by entering the following command in configuration mode:

```
service wbm
```

Step 2 Permit access to the Guard from the remote manager IP address by entering the following command in configuration mode:

```
permit wbm {* | ip-addr [ip-mask]}
```

Table 2-7 provides the arguments for the **permit wbm** command.

Table 2-7 Arguments for the permit wbm Command

Parameter	Description
*	Asterisk wildcard character that allows access by all remote manager IP addresses. ⚠ **Caution** For security reasons, we do not recommend that you permit access to a service from all IP addresses.
ip-addr	IP address of the remote manager. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).
ip-mask	(Optional) Subnet mask. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0).

Step 3 Open the browser and enter the following address:

```
https://Guard-ip-address/
```

The *Guard-ip-address* argument is the IP address of the Guard.

The Guard WBM window appears.

Note HTTPS, not HTTP, is used to enable web-based management control.

Step 4 Enter your username and password and click **OK**. After you enter the username and password correctly, the Guard home page displays.

If you have the Guard configured to use Terminal Access Controller Access Control Plus (TACACS+) authentication, the Guard uses the TACACS+ user database for user authentication instead of using its local database. If you have configured advanced authentication attributes on the TACACS+ server, such as password expiry, the Guard may prompt you for a new password based on the configuration of the user on the TACACS+ server or notify you when the password is about to expire.

The following example shows how to enable the Guard WBM:

```
user@GUARD-conf# service wbm
user@GUARD-conf# permit wbm 192.168.30.32
```

For information about using the WBM to manage your Guard, see the appropriate *Cisco Web-Based Manager Configuration Guide*.

Managing the Guard with the Cisco DDoS MultiDevice Manager

The Cisco DDoS MultiDevice Manager (MDM) is a server-based application that allows you to manage one or more Guards from the web using a web browser. To use the MDM to manage your network of Guards, perform the following actions:

- Install and configure the MDM software on a network server (see the *Cisco DDoS MultiDevice Manager Configuration Guide*).
- Enable the MDM service on your Guard and permit access by the MDM as described in the following procedure.

To enable the MDM service on the Guard, perform the following steps:

Step 1 Enable the MDM service by entering the following command in configuration mode:

```
service mdm
```

Step 2 Permit access to the Guard from the MDM by entering the following command in configuration mode:

```
mdm server ip-addr
```

The *ip-addr* argument defines the IP address of your MDM server. Enter the IP address in dotted-decimal notation.

The following example shows how to enable the MDM service and permit access by the MDM:

```
user@GUARD-conf# service mdm
user@GUARD-conf# mdm server 192.168.30.32
```

For information about using the MBM to manage your Guards, see the *Cisco DDoS MultiDevice Manager Configuration Guide*.

Accessing the Guard with SSH

You can access the Guard using a Secure Shell (SSH) connection.

The SSH service is enabled by default.

To access the Guard with SSH, perform the following steps:

Step 1 Permit access to the Guard from the remote network IP address by entering the following command in configuration mode:

```
permit ssh {ip-addr [ip-mask] | *}
```

Table 2-8 provides the arguments for the **permit ssh** command.

Table 2-8 Arguments for the permit ssh Command

Parameter	Description
ip-addr	IP address of the remote network. Enter the IP address in dotted-decimal notation (for example, enter 192.168.100.1).
ip-mask	(Optional) Subnet mask. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0).
*****	Asterisk wildcard character that allows access by any remote network. **Caution** For security reasons, we recommend that you not permit access to all remote networks.

Step 2 Establish a connection from the remote network address and enter your login username and password.

If you have the Guard configured to use TACACS+ authentication, the Guard uses the TACACS+ user database for user authentication instead of using its local database. If you have configured advanced authentication attributes on the TACACS+ server, such as password expiry, the Guard may prompt you for a new password based on the configuration of the user on the TACACS+ server or notify you when the password is about to expire.

To enable the SSH connection without entering a login username and password, perform the following:

- Configure the Guard to use a locally configured login and password for authentication. See the "Configuring Authentication" section on page 3-4 for more information.
- Add the remote connection SSH public key to the Guard SSH key list. See the "Managing SSH Keys" section on page 3-23 for more information.

The following example shows how to enable an SSH connection to the Guard:

```
user@GUARD-conf# permit ssh 192.168.30.32
```

CHAPTER 3

Configuring the Guard

This chapter describes how to configure the Cisco Guard (Guard) services.

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:

Activating Guard Services

The Guard has several service options which you can activate by enabling the service and then defining the IP address that is permitted access to the service. With the exception of the Secure Shell service which is always active, this section describes how to activate the services.

The Guard services are as follows:

- Internode communication service—The Guard uses this service when establishing a communication channel with the Cisco Traffic Anomaly Detector. See the "Establishing Communication with the Detector" section on page 3-17 for more information.
- Network Time Protocol (NTP) service—The Guard provides a time synchronization service that allows you to synchronize the Guard with a time synchronization server. To enable time synchronization, you must configure an NTP server. See the "Synchronizing the Guard Clock with an NTP Server" section on page 3-22 for more information.
- Simple Network Management Protocol **(**SNMP) server service—You can access the Guard using SNMP to retrieve information as defined by the following MIBs:
  - Riverhead private MIB
  - MIB2 (RFC1213-MIB)—All of the MIB groups with the exceptions of the EGP and transmission MIB groups.
  - UCDAVIS (UCD-SNMP-MIB)—Only the following MIB groups: memory, latable, systemStats, version, and snmperrs.

  See the MIB file that is released with the software version for information about the MIB definitions.

  Note The Riverhead MIB contains 64-bit counters. To read the MIB, you must use a browser that supports SNMP version 2.

- SNMP trap service—When you activate the snmp-trap service, the Guard generates SNMP traps. See the "Enabling SNMP Traps" section on page 3-26 for more information.
- Secure Shell service—The SSH service is always active. See the "Accessing the Guard with SSH" section on page 2-17 and the "Managing SSH Keys" section on page 3-23 for more information.
- Web-Based Manager (WBM) service—You can monitor and control the Guard from the web using a web browser. See the "Managing the Guard with a Web-Based Manager" section on page 2-15 for more information.
- MultiDevice Manager (MDM) service—Using a web browser, you can monitor and control the Guard and other Guard and Detector devices from the MDM server. See the "Managing the Guard with the Cisco DDoS MultiDevice Manager" section on page 2-16 for more information.

By default, all Guard services, except SSH, are disabled.

To activate a Guard service, perform the following steps:

Step 1 Enable the Guard service by entering the following command in configuration mode:

```
service {internode-comm | mdm | ntp | snmp-server | snmp-trap | wbm}
```

Table 3-1 provides the keywords for the **service** command.

Table 3-1 Keywords for the service Command

Service	Description
internode-comm	Specifies the internode communication service.
mdm	Specifies the MDM service.
ntp	Specifies the NTP service.
snmp-server	Specifies the SNMP server service.
snmp-trap	Specifies the SNMP trap service.
wbm	Specifies the WBM service.

Step 2 Permit access to the Guard service by entering one of the following commands:

- For the MDM service, permit access to the Guard service from the MDM by entering the following command in configuration mode:

  ```
  mdm server ip-addr
  ```

  The *ip-addr* argument defines the IP address of your MDM server. Enter the IP address in dotted-decimal notation.

- For all other services, permit access to the Guard service and enable connectivity by entering the following command in configuration mode:

  ```
  permit {internode-comm | ntp | snmp-server | ssh | wbm}
  {* | ip-address-general [ip-mask]}
  ```

  Table 3-2 provides the arguments and keywords for the **permit** command.

Table 3-2 Arguments and Keywords for the permit Command

Parameter	Description
internode-comm	Specifies the internode communication service.
ntp	Specifies the NTP service.
snmp-server	Specifies the SNMP server service.
ssh	Specifies the SSH service.
wbm	Specifies the WBM service.
*	Wildcard character that permits access to a service by all device IP addresses. ⚠ **Caution** For security reasons, we do not recommend that you permit access to a service from all IP addresses.
ip-address-general	IP address from which to permit access. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
ip-mask	(Optional) IP subnet mask. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0). The default subnet mask is 255.255.255.255.

The following example shows how to activate the WBM service:

```
user@GUARD-conf# service wbm
user@GUARD-conf# permit wbm 192.168.10.35
```

Configuring Access Control Using AAA

Authentication, Authorization, and Accounting (AAA) is a method for controlling user access to the Guard and the Guard services. AAA provides the following features:

- Authentication—Identifies a user before the user is allowed access to the system and system services.
- Authorization—Determines what a user is allowed to perform once access to the system is obtained. This process occurs after the user is authenticated.
- Accounting—Records what a user is performing or has performed. Accounting allows you to track the services that users are accessing.

The Guard is preconfigured with the following system user accounts:

- admin—The admin user account is configured with the administration access rights, allowing access to the Guard CLI and all its functionality. When connecting to the Guard CLI for the first time, you are required to set a password for this account. Use the admin user account to configure additional user accounts.
- riverhead—The riverhead user account is configured with dynamic access rights. The Guard uses this user account to establish the initial communication channel with the Cisco Traffic Anomaly Detector. When you connect to the Guard CLI for the first time, you are required to set a password for this account.

You cannot delete system user accounts.

You can divide the Guard user community into domains and assign passwords for secure management access. We recommend that you create new user accounts and avoid using the system user accounts after the initial configuration so that you can monitor user actions.

The section contains the following topics:

- Configuring Authentication
- Configuring Authorization
- Configuring Accounting
- Configuring the TACACS+ Server Attributes

Configuring Authentication

You can configure which authentication method that the Guard uses when a user tries to log into the Guard or requests a higher privilege level (using the **enable** command). The Guard offers the following authentication options:

- Local authentication—Uses locally configured login and enable passwords for authentication. This authentication method is the default. See the "Configuring Local Authentication" section on page 3-6 for more information.
- Terminal Access Controller Access Control System Plus (TACACS+) authentication—Remote user authentication using one or more TACACS+ servers.

Note When you define a user to authenticate on the TACACS+ server, you must also define authorization for the user or the user will have access to **show** commands only (see the "Configuring Authorization" section on page 3-8).

You can configure the Guard to use one or both of the user authentication methods. When using Terminal Access Controller Access-Control System Plus (TACACS+) authentication, you can define multiple TACACS+ servers. Defining more than one authentication method provides a backup in case the initial method fails due to a communication error.

The Guard authenticates a user by using each of the methods that you define and in the order in which you define them on the Guard. To view the list of defined authentication methods, enter the **show running config** command. The Guard attempts to authenticate the user using the first method on the list. If the first authentication method does not respond, the Guard sequentially selects the next authentication method on the list until it finds one that responds.

You can configure the action that the Guard takes when it receives a response from the first TACACS+ server by using the **tacacs-server first-hit** command. If you disable the first-hit option (the default setting) and the first server rejects the authentication, the Guard sequentially scans the other TACACS+ servers to find a server that accepts the authentication. User authentication fails when no defined TACACS+ servers accept the authentication or the Guard cannot communicate with any of the servers. If you enable the first-hit option, the Guard accepts the authentication response (reject or accept) of the first TACACS+ server to respond as the final decision. By default, the first-hit option is disabled. For more information about the **tacacs-server first-hit** command, see the "Configuring the TACACS+ Search Method" section on page 3-16.

Note You can configure the Guard to use its local database as a fallback for user authentication when the Guard cannot communicate with the TACACS+ servers (see the "Configuring Authentication Methods" section).

This section contains the following topics:

- Configuring Authentication Methods
- Configuring Local Authentication

Configuring Authentication Methods

To configure the authentication method that the Guard uses, perform the following steps:

Step 1 Configure the TACACS+ server connection if TACACS+ authentication is required. See the "Configuring the TACACS+ Server Attributes" section on page 3-14 for more information.

Step 2 Define the authentication method by entering the following command in configuration mode:

```
aaa authentication {enable | login} {local | tacacs+} [tacacs+ | local]
```

Table 3-3 provides the keywords for the **aaa authentication** command.

Table 3-3 Keywords for the aaa authentication Command

Parameter	Description
enable	Allows the Guard to authenticate when a user enters a higher privilege level.
login	Allows the Guard to authenticate when a user logs in.
local	Specifies the local database that the Guard uses to authenticate a user.
tacacs+	Allows a TACACS+ server to authenticate a user.
tacacs+ | **local**	(Optional) Specifies an alternative authentication method if the configured method fails.

If you access the Guard from a console session, it uses the local user database for authentication regardless of the defined authentication method.

To change the authentication method, reenter the command.

The following example shows how to configure authentication on entering a higher privilege level. The primary authentication method is configured to TACACS+, and the secondary authentication method is configured to the local user database.

```
user@GUARD-conf# aaa authentication enable tacacs+ local
```

Configuring Local Authentication

The Guard initially has a preconfigured username (called a user definition) with administration privileges, which allows you to create new users. A user definition allows you to divide the Guard user community into domains and to assign passwords for secure management access.

To enable authentication of CLI users with a TACACS+ server, see the "Configuring Authentication" section on page 3-4.

This section contains the following topics:

- Adding a User
- Changing Your Password
- Changing the Passwords of Other Users
- Deleting a User from the Local User Database

Adding a User

To add a user to the Guard local database, use the following command in configuration mode:

username *username* {**admin** | **config** | **dynamic** | **show**} [*password*]

Table 3-4 provides the arguments and keywords for the **username** command.

Table 3-4 Arguments and Keywords for the username Command

Parameter	Description
username	Username. A case-sensitive alphanumeric string from 1 to 63 characters that starts with an alphabetic letter. The string cannot contain spaces but can contain underscores.
admin	Provides access to all operations.
config	Provides access to all operations except for operations relating to user definition, deletion, and modification.
dynamic	Provides access to monitoring and diagnostic operations, protection, and learning-related operations. Users with Dynamic privileges can also configure flex-content filters and dynamic filters.
show	Provides access to monitoring and diagnostic operations.
password	(Optional) Password associated with the username. Enter an alphanumeric case-sensitive 6- to 24-character string with no spaces. If you do not enter a password, you are prompted for it.

The following example shows how to configure a new user and set the password:

```
user@GUARD-conf# username Robbin config 1234
```

Users enter passwords in clear text but the Guard configuration file displays passwords in an encrypted manner. This example displays the Guard configuration file (running-config):

```
username Richard config encrypted 840xdMk3
```

The **encrypted** keyword in the previous example indicates that the password is encrypted.

To display the list of users configured on the Guard, use the **show running-config** or **show guard** commands.

To display a list of the users currently logged into the CLI, use the **show users** command.

Changing Your Password

You can change your own password. Administrators can change their own password and the passwords of other users (see the "Changing the Passwords of Other Users" section on page 3-8).

To change your own password, perform the following steps:

Step 1 Enter the following command in global mode:

```
password
```

Step 2 Enter your current password. The system prompts you for a new password.

Step 3 Enter a new password. The password must be an alphanumeric, 6- to 24-character string with no spaces. The password is case sensitive. The system prompts you to confirm the new password by typing it again.

The following example shows how to change your password:

```
user@GUARD# password
Old Password: <old-password>
New Password: <new-password>
Retype New Password: <new-password>
```

Changing the Passwords of Other Users

You must have administration user privileges to change the password of other users.

To change the password of another user, perform the following steps:

Step 1 Enter the following command in global mode:

password *username-password*

The *username-password* argument is the user whose password you are changing.

Step 2 Enter a new password.

The password must be an alphanumeric, 6- to 24-character string with no spaces. The password is case sensitive. The system prompts you to confirm the new password by typing it again.

The following example shows how the administrator changes the password of the user Jose:

```
user@GUARD# password Jose
New Password: <new-password>
Retype New Password: <new-password>
```

Deleting a User from the Local User Database

When you delete a user from the local user database, the associated user cannot access the Guard if authentication is performed using the local user database only.

To delete a user from the Guard local user database, use the **no username** *username* command.

The following example shows how to delete a user from the local user database:

```
user@GUARD-conf# no username Robbin
```

Configuring Authorization

You can limit the services available to a user. When you enable authorization, the Guard verifies the user profile, which is located either in the local user database or on a TACACS+ security server. The user is permitted access to the requested service only if the information in the user profile allows it.

You can configure which authorization method that the Guard uses when a user tries to execute a command. The Guard offers the following authorization options:

- TACACS+ authorization—Authorizes users through a TACACS+ server. Access to a subsequent server is initiated, if a server is defined, only if communication to a server fails.

  Two types of TACACS+ authorization are supported:

  - EXEC authorization—Determines the user privilege level once when the user is authenticated upon logging into the Guard.

- Command authorization—Consults a TACACS+ server to get authorization for each command after the user enters the command.

TACACS+ authorization enables you to specify access rights for each command.

Caution We recommend that you limit authorization to the **copy running-config** command because using the **copy running-config** command allows a user to access all configuration commands, regardless of whether the user is actually authorized every command in the configuration file.

- Local authorization—Uses locally configured user profiles for command group access control. Authorization is defined for all commands at the specified privilege level. This authorization method is the default.

The Guard can use local authorization when communication to the TACACS+ server fails.

You can configure a sequential authorization list that defines the methods for authorizing a user, allows you to designate one or more methods to be used for authorization, and provides a backup if communication to the initial method fails.

The Guard uses the first method that you listed to authorize users; if that method does not respond, the Guard selects the second authorization method. The authorization fails only if both authorization methods do not succeed.

To configure the Guard to consider an authentication rejection as final and stop further searching with other TACACS+ servers or the local user database, you can configure the TACACS+ server attributes. See the "Configuring the TACACS+ Server Attributes" section on page 3-14 for more information.

This section contains the following topics:

- Configuring Local Authorization
- Configuring Authorization Methods
- Disabling Tab Completion of Zone Names

Configuring Local Authorization

Access to Guard operations depends on the user privilege level. You can limit the operations available to a user. The Guard checks the user profile to verify the user access rights. Once authorized, the user is granted access to the requested operation only if the information in the user profile allows it. See Table 2-1 for more information about user privilege levels.

This section contains the following topics:

- Assigning Privilege Levels with Passwords
- Moving Between User Privilege Levels

Assigning Privilege Levels with Passwords

You can set passwords that restrict access to user privilege levels. After you specify the privilege level and the password, you can give the password to a user who needs to access this level. Without knowing the privilege level password, the user cannot move to the password-protected level.

To set a local password to control access to a privilege level, use the following command in configuration mode:

enable password [**level** *level*] [*password*]

Table 3-5 provides the arguments for the **enable password** command.

Table 3-5 Arguments for the enable password Command

Parameter	Description
level *level*	(Optional) Specifies the user privilege level. The level can be one of the following: • **admin**—Provides access to all operations. • **config**—Provides access to all operations except for operations relating to user definition, deletion, and modification. • **dynamic**—Provides access to monitoring and diagnostic operations, protection, and learning-related operations. Users with Dynamic privileges can also configure flex-content filters and dynamic filters. • **show**—Provides access to monitoring and diagnostic operations. The default level is admin.
password	(Optional) Password for the privilege level. The password must be an alphanumeric, 6- to 24-character string with no spaces. The password is case sensitive. If you do not enter a password, you are prompted for it.

The following example shows how to assign a password to the user privilege level admin:

```
user@GUARD-conf# enable password level admin <password>
```

Moving Between User Privilege Levels

Authorized users can move between user privilege levels.

To move between user privilege levels, perform the following steps:

Step 1 Enter the following command in global mode:

```
enable [level]
```

Table 3-6 provides the values for the optional *level* argument which specifies the user privilege level.

Table 3-6 Keywords for the enable Command

Parameter	Description
admin	Provides access to all operations. This is the default.
config	Provides access to all operations except for operations relating to user definition, deletion, and modification
dynamic	Provides access to monitoring and diagnostic operations, protection, and learning-related operations. Users with Dynamic privileges can also configure flex-content filters and dynamic filters.
show	Provides access to monitoring and diagnostic operations.

Step 2 Enter the privilege level password.

The following example shows how to switch to the admin privilege level:

```
user@GUARD> enable admin
Enter enable admin Password: <password>
```

To return to the show privilege level (as described in Table 3-5), use the **disable** command.

Configuring Authorization Methods

To configure the authorization method, perform the following steps:

Step 1 Configure the TACACS+ server connection if TACACS+ authorization is required. See the "Configuring the TACACS+ Server Attributes" section on page 3-14 for more information.

Step 2 Define the authorization method by entering one of the following commands in configuration mode:

- **aaa authorization exec tacacs+**
- **aaa authorization commands** *level* **tacacs+**

To remove an authorization method, use the **no** form of the command.

Table 3-7 provides the arguments and keywords for the **aaa authorization** command.

Table 3-7 Arguments and Keywords for the aaa authorization Command

Parameter	Description
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. The Guard consults the TACACS+ server to determine the privilege level for an authenticated user. **Caution** You must configure authentication for the user on a TACACS+ server before configuring user authorization or the user may not be able to access the Guard module (see the "Configuring Authorization" section on page 3-8).
commands	Runs authorization for all commands at the specified privilege level. To configure authorization for more than one privilege level, use the command for each privilege level that requires authorization.
level	Authorization for the specified privilege level. The level can be one of the following: • **admin**—Provides access to all operations. • **config**—Provides access to all operations except for operations relating to user definition, deletion, and modification. • **dynamic**—Provides access to monitoring and diagnostic operations, protection, and learning-related operations. Users with Dynamic privileges can also configure flex-content filters and dynamic filters.
tacacs+	Verifies the user access rights with a TACACS+ server.

We recommend that you do not configure authorization for **show** privilege level commands because it may affect Guard performance.

Note No TACACS+ authorization is performed for commands that you enter from console sessions.

The following example shows how to configure authorization for commands that require the config privilege level:

```
user@GUARD-conf# aaa authorization commands config tacacs+
```

Caution You must grant access to the dynamic user privilege level or specify access rights to the **configure** command to enable access to the configuration command mode.

TACACS+ Server Sample Configuration

You can specify authorization for each command in the TACACS+ server database.

The following example shows how to configure authorization on a TACACS+ server for the user Zoe:

```
user=Zoe {
    cmd = protect {
        permit .*
    }
    cmd = "no protect" {
        permit .*
    }
    cmd = learning {
        deny policy*
    }
    cmd = "no learning" {
        deny .*
    }
    cmd = dynamic-filter {
        permit .*
    }
    cmd = "no dynamic-filter" {
        permit .*
    }
    cmd = flex-filter {
        deny .*
    }
    cmd = "no flex-filter" {
        deny .*
    }
}
```

Disabling Tab Completion of Zone Names

You can limit the access to the zone configurations to authorized users only by disabling the tab completion feature when entering the zone names. This setting applies to all commands in which you specify the zone name.

When you enter commands in global or configuration mode, such as the **zone** command, **no zone** command, **show zone** command, and **deactivate** command, the Guard no longer displays or completes the zone name. You must enter the complete zone name to configure a zone, change the zone operation mode, or display zone statistics.

The Guard sends the **tab-complete zone-list** command to the TACACS+ server when you disable tab completion of zone names. Configure authorization for the **tab-complete zone-list** command on the TACACS+ server to enable tab completion of zone names to authorized users.

The following example shows how to disable tab completion of zone names for all the **zone** commands:

```
user@GUARD-conf# aaa authorization commands zone-completion tacacs+
```

To enable tab completion of zone names, use the **no** form of the command.

Configuring Accounting

Accounting management allows you to track the services that users are accessing and save the accounting information on a TACACS+ server. You can enable accounting of requested services for billing, reporting, or security purposes. By default, the Guard is configured with accounting management disabled.

To configure accounting, perform the following steps:

Step 1 Configure the TACACS+ server connection. See the "Configuring the TACACS+ Server Attributes" section on page 3-14 for more information.

Step 2 Configure accounting by entering the following command in configuration mode:

```
aaa accounting commands {show | dynamic | config | admin} stop-only {local | tacacs+}
```

Table 3-8 provides the keywords for the **aaa accounting** command.

Table 3-8 Keywords for the aaa accounting Command

Parameter	Description
show | dynamic | config | admin	Defines accounting for the specified privilege level (see Table 2-1 for information on user privilege levels).
stop-only	Records the action when the command execution terminates.
tacacs+	Uses a TACACS+ server database to record accounting information.
local	Does not save accounting information.

To configure accounting for more than one privilege level, enter the **aaa accounting** command for each privilege level for which accounting is required.

We recommend that you enable accounting management for the config user privilege level only. Tracking and saving accounting data may affect Guard performance.

Use the **no** form of the command to remove the accounting management for a privilege level.

The following example shows how to configure accounting for commands that require the config privilege level on a TACACS+ server:

```
user@GUARD-conf# aaa accounting commands config stop-only tacacs+
```

Configuring the TACACS+ Server Attributes

You must configure the TACACS+ server attributes to enable authentication, authorization, or accounting with a TACACS+ server.

Caution You must configure the TACACS+ server attributes before you apply the TACACS+ authentication method or you may not be able to access the Guard.

To configure the TACACS+ server attributes, perform the following steps:

Step 1 Configure the IP address of the TACACS+ server by entering the **tacacs-server host** *ip-address* command.

See the "Configuring a TACACS+ Server IP Address" section on page 3-15 for more information.

Step 2 Configure the encryption key that the Guard uses to access the TACACS+ server by entering the **tacacs-server key** *tacacs-key* command.

See the "Configuring the TACACS+ Server Encryption Key" section on page 3-15 for more information.

Step 3 (Optional) Configure the search method that the Guard uses for authentications by entering the **tacacs-server first-hit** command.

See the "Configuring the TACACS+ Search Method" section on page 3-16 for more information.

Step 4 (Optional) Configure the TACACS+ server connection timeout by entering the **tacacs-server timeout** *timeout* command.

See the "Configuring the TACACS+ Server Connection Timeout" section on page 3-16 for more information.

Step 5 Display the TACACS+ server connection statistics by entering the **show tacacs statistics** command.

See the "Displaying TACACS+ Server Statistics" section on page 3-17 for more information.

The Guard user privilege levels relate to the TACACS+ privilege numeration as follows:

- **admin** = 15
- **config** = 10
- **dynamic** = 5
- **show** = 0

This section contains the following topics:

- Configuring a TACACS+ Server IP Address
- Configuring the TACACS+ Server Encryption Key

- Configuring the TACACS+ Search Method
- Configuring the TACACS+ Server Connection Timeout
- Displaying TACACS+ Server Statistics

Configuring a TACACS+ Server IP Address

You can configure the Guard to use a sequential list of TACACS+ servers for authentication, authorization, and accounting. The Guard uses the TACACS+ server list to authenticate or authorize users or send an accounting event; if that server does not respond, the Guard selects the second server. Authentication or authorization fails only if all servers listed do not respond.

Alternatively, you can configure the Guard to use only the first TACACS+ server on the list to authenticate users (see the "Configuring the TACACS+ Search Method" section on page 3-16 for more information).

You must define the IP address of each TACACS+ server on the list. You can define a maximum of nine TACACS+ servers.

To add a TACACS+ server to the list and assign its IP address, use the following command in configuration mode:

tacacs-server host *ip-address* [**port** *port_number*]

The *ip-address* argument specifies the IP address of the TACACS+ server.

Table 3-9 provides the arguments and keywords for the **tacacs-server host** command.

Table 3-9 Arguments and Keywords for the tacacs-server host Command

Parameter	Description
ip-address	IP address of the TACACS+ server. Enter the IP address in dotted-decimal notation (for example, an IP address of 192.168.100.1).
port *port_number*	(Optional) Specifies the port number to use. If you do not specify a port number, the Guard uses port 49 by default.

The TACACS+ servers are added to the list in the order in which you enter them. You can add a maximum of nine servers to the list.

The following example shows how to add a server to the TACACS+ server list:

```
user@GUARD-conf# tacacs-server host 192.168.33.45 port 60
```

Configuring the TACACS+ Server Encryption Key

You must configure the encryption key to access a TACACS+ server. The key must match the key on the TACACS+ servers. The key cannot contain spaces.

To configure the server encryption access key, use the following command in configuration mode:

tacacs-server key *tacacs-key*

The argument *tacacs-key* is an alphanumeric string that contains up to 100 characters.

Note You can define only one encryption key. When using several TACACS+ servers, the Guard uses the same key to encrypt communication with all TACACS+ servers.

The following example shows how to set the TACACS+ server encryption key to MyKey:

```
user@GUARD-conf# tacacs-server key MyKey
```

Configuring the TACACS+ Search Method

You can configure the Guard to consider an authentication rejection as final and stop further searching with other TACACS+ servers by using the **tacacs-server first-hit** command in configuration mode. The Guard performs user authentication using only the first TACACS+ server on the server list to respond. If the first TACACS+ server does not respond, the Guard selects the next server on the list. The Guard regards the first user authentication approval or rejection received as the final decision and stops attempting to authenticate the user with other TACACS+ servers.

To configure the Guard to continue a sequential search of the defined TACACS+ servers in an attempt to find a server that accepts the user authentication, use the **no tacacs-server first-hit** command in configuration mode. This method is the default setting for the first-hit operation. User authentication fails if all of the defined TACACS+ servers reject the user authentication or the Guard cannot communicate with any of the servers.

The following example shows how to configure the TACACS+ search method so that the Guard uses only the first TACACS+ server on the list to authenticate users:

```
user@GUARD-conf# tacacs-server first-hit
```

Configuring the TACACS+ Server Connection Timeout

You can configure the amount of time that the Guard waits for a reply from the TACACS+ server. When the timeout ends, the Guard either attempts to establish a connection with the next TACACS+ server (if a server was configured) or falls back to local AAA (if a fallback was configured). Authentication and authorization fail if no fallback method is configured.

Note The same server timeout is used for communication with all TACACS+ servers.

To configure the TACACS+ server connection timeout, use the following command in configuration mode:

tacacs-server timeout *timeout*

The *timeout* argument specifies the amount of time (in seconds) that the Guard waits for a TACACS+ server to reply. The default timeout is 0.

The following example shows how to configure the TACACS+ server connection timeout to 600 seconds:

```
user@GUARD-conf# tacacs-server timeout 600
```

Tip You may want to increase the timeout value if you have network problems or if the TACACS+ servers are slow to respond and cause persistent timeouts.

Displaying TACACS+ Server Statistics

You can display statistical information for the TACACS+ servers that you define by using the **show tacacs statistics** command in configuration mode.

To clear the TACACS+ statistics, use the **clear tacacs statistics** command in configuration mode.

Table 3-10 displays the fields in the **show tacacs statistics** command output.

Table 3-10 Field Descriptions in the show tacacs statistics Command Output

Field	Description
PASS	Specifies the number of times that the Guard accessed the TACACS+ server successfully and was granted access.
FAIL	Specifies the number of times that the Guard accessed the TACACS+ server successfully and was denied access.
ERROR	Specifies the number of times that the Guard could not access the TACACS+ server.

Establishing Communication with the Detector

You can establish a secure communication channel between a Detector and the Guards that you define on the Detector remote Guard lists. The secure communication channel enables the Detector to perform the following tasks:

- Activate the Guard—When the Detector detects a zone traffic anomaly, it uses the communication channel to activate the Guard that provides zone protection and to poll the Guard during zone protection.
- Synchronize a zone configuration—The Detector uses the communication channel to exchange zone configuration information with the Guard.

After you configure the communication channel parameters on both the Detector and Guard, from the Detector you initiate a connection with the Guard which enables the Detector to exchange the keys and certificates that are required to establish a secure communication channel with the Guard. The Detector then closes the connection and establishes the communication channel when it needs to activate the Guard, synchronize a zone configuration, or poll the Guard.

The Detector and Guard support the following two types of communication channels:

- Secure Shell (SSH) version 2—Enables the Detector to activate the Guard.
- Secure Sockets Layer (SSL)—Enables the Detector to activate the Guard, poll the Guard, and synchronize zone configurations.

You use the zone remote Guard list and default remote Guard list on the Detector to specify the Guards that the Detector communicates with for zone protection and synchronization. When you specify a Guard on a remote Guard list, you select the type of communication channel that the Detector is to establish with the Guard: SSH or SSL. Both devices require the SSH service for establishing a SSH or SSL communication channel. By default, the SSH service is always enabled on both devices. When you establish an SSL communication channel, the Detector uses the SSH communication channel only for the initial connection with a Guard, during which time the devices exchange their keys and certificates.

Note Before you can establish a communication channel between a Detector and a Guard, you must add the Guard to a remote Guard list on the Detector. For more information, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* and *Cisco Traffic Anomaly Detector Configuration Guide*.

This section contains the following topics:

- Configuring the SSL Communication Channel Parameters
- Configuring the SSH Communication Channel Parameters

Configuring the SSL Communication Channel Parameters

Configure an SSL communication channel between the Detector and the Guard when you need the Detector to interact with the Guard as follows:

- Activate the Guard when the Detector detects a traffic anomaly.
- Synchronize zone configurations with the Guard.
- Poll the Guard to identify that an attack on the zone has ended. If you enable the detect and learn process on the Detector, the Detector suspends the learning process (threshold tuning) when it detects an attack on the zone. The Detector polls the Guard that it activated to mitigate the attack to determine when the attack is over, at which point, the Detector automatically resumes the learning process.
- Monitor communication with the Guard and notify you if remote actions fail, such as activating the Guard to protect the zone.

An SSL communication channel provides secure connections through a combination of authentication and data encryption and relies upon digital certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters for this level of security. SSL encrypts the data so that only the intended recipient can decipher the data.

Each Guard and Detector uses a digital certificate to authenticate the device attempting to communicate with it over the communication channel. The identity of the Guard and the Detector in the SSL certificates is associated with the device IP address. To ensure a secure connection, the Detector generates a private-public key pair and distributes its public key to the Guards that you define on the remote Guard lists.

After you configure the SSL communication parameters on both the Guard and the Detector, you must establish the communication channel between the two devices, which you perform from the Detector. During the initial connection to the Guard, the Detector establishes an SSH communication channel with the user riverhead on the Guard and then the devices exchange the keys and certificates that are required to secure the communication channel. After the initial connection, the Detector establishes an SSL communication channel when needed to activate the Guard, poll the Guard, or synchronize zone configurations.

If you replace one the devices on either end of an SSL communication channel or change one of their IP addresses, then you must regenerate the SSL certificates in both devices so that the two devices can successfully authenticate each other.

This section contains the following topics:

- Enabling an SSL Communication Channel
- Regenerating SSL Certificates

Enabling an SSL Communication Channel

To enable an SSL communication channel, you must configure the Guard and the Detector to allow the following connection types:

- SSH—The Detector establishes the initial connection with the Guard using an SSH communication channel to exchange the keys and certificates.
- SSL—The Detector uses an SSL communication channel to establish all connections with the Guard after the initial connection.

Caution If the Guard is authenticating users using TACACS+ authentication, you must define the user riverhead on the TACACS+ server to enable the Detector to establish the SSH communication channel during the initial connection with the Guard.

To enable an SSL communication channel, perform the following steps on both the Guard and the Detector:

Step 1 Permit access to the SSH service by the companion device IP address by entering the **permit ssh** *ip-address-general* [*ip-mask*] in configuration mode.

The *ip-address-general* and *ip-mask* arguments define the IP address of the companion device.

Step 2 Enable the communication channel service by entering the **service internode-comm** command in configuration mode.

Step 3 Permit access to the communication channel service by the companion device IP address by entering the **permit internode-comm** *ip-address-general* [*ip-mask*] command in configuration mode.

The *ip-address-general* and *ip-mask* arguments define the IP address of the companion device.

After you configure the Guard and the Detector to enable the SSL communication channel, you can establish the communication channel between them. For information on establishing the communication channel, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* or the *Cisco Traffic Anomaly Detector Configuration Guide*.

Regenerating SSL Certificates

The key that identifies the Guard and the Detector in the SSL certificates is associated with the device IP addresses. You must regenerate new SSL certificates for the Guard and the Detector on both ends of a communication channel when you make the following changes:

- Change the IP address of one of the devices.
- Replace one of the devices.

The process of regenerating new SSL certificates includes deleting the current certificates from both devices. To display the current SSL certificates, use the **show internode-comm certs** command.

To regenerate the current SSL certificates, perform the following steps:

Step 1 From the Detector, delete the SSL certificate of the Guard by using the following command in configuration mode:

```
cert remove cert-host-ip
```

The *cert-host-ip* argument specifies the IP address of the Guard. Enter an asterisk (*) to delete the SSL certificates of all Guards.

The following example shows how to delete an SSL certificate:

```
user@DETECTOR-conf# cert remove 10.56.36.4
```

Step 2 From the Guard, delete the SSL certificate of the Detector by using the following command in configuration mode:

```
cert remove cert-host-ip
```

The *cert-host-ip* argument specifies the IP address of the Detector. Enter an asterisk (*) to delete the SSL certificates of all Detectors that have established communication channels with the Guard.

Step 3 If you replace the Guard, then you must also delete its SSH host key from the Detector. From the Detector, use the following command in configuration mode to delete Guard SSH host keys:

```
no host-keys ip-address-general
```

The *ip-address-general* argument specifies the IP address of the remote device.

Step 4 From the Detector, regenerate new SSL certificates by establishing a new SSL communication channel between the Guard and the Detector. For information about establishing a communication channel, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* or the *Cisco Traffic Anomaly Detector Configuration Guide*.

Configuring the SSH Communication Channel Parameters

Configure an SSH communication channel between the Detector and the Guard when the only interaction between the two devices that you need is for the Detector to activate the Guard when it detects a traffic anomaly. An SSH communication channel does not allow the Detector to perform the following tasks with the Guard:

- Synchronize zone configurations with the Guard.
- Poll the Guard to identify that an attack on the zone has ended. If you enable the detect and learn process on the Detector, the Detector suspends the learning process (threshold tuning) when it detects an attack on the zone. Because the Detector cannot poll the Guard to determine when the attack is over, it is unable to automatically resume the learning process when the attack ends.
- Monitor communication with the Guard and notify you if remote actions fail, such as activating the Guard to protect the zone.

To allow the Detector to perform these tasks, you must configure an SSL communication channel (see the "Configuring the SSL Communication Channel Parameters" section on page 3-18).

To ensure a secure SSH communication channel, the Detector generates a private-public SSH key pair and distributes the public SSH key to the Guards listed in the remote Guard lists.

After you enable the SSH communication channel, you must establish the communication channel between the Detector and the Guard, which you perform from the Detector.

If you replace a Guard at one end of an SSH communication channel, then you must regenerate the SSH private (host) and public keys on the Detector so that it can successfully authenticate itself with the new Guard.

This section contains the following topics:

- Enabling an SSH Communication Channel
- Regenerating SSH Communication Channel Keys

Enabling an SSH Communication Channel

To enable an SSH communication channel between a Guard and a Detector, permit access to the SSH service on the Guard from the Detector IP address by entering the **permit ssh** command in configuration mode

Caution If the Guard is authenticating users using TACACS+ authentication, you must define the user riverhead on the TACACS+ server to enable the Detector to establish the SSH communication channel.

After you enable the SSL communication channel between the Guard and the Detector, you can establish the communication channel between them. For information on establishing the communication channel, see the *Cisco Traffic Anomaly Detector Module Configuration Guide* or the *Cisco Traffic Anomaly Detector Configuration Guide*.

Regenerating SSH Communication Channel Keys

If you replace a Guard that a Detector communicates with over an SSH communication channel, then you must perform the following steps to regenerate the SSH communication channel keys:

Step 1 Delete the SSH host key from the Detector by entering the **no host-keys** *ip-address-general* configuration mode command on the Detector.

The *ip-address-general* argument specifies the IP address of the remote device.

To display the host keys listed on the Guard, use the **show host-keys** command.

Step 2 Configure the SSH key on the remote Guard by performing one of the following actions:

- Establish a new SSH communication channel from the Detector.
- Add the Detector public key manually to the remote Guard. You can copy the Detector public SSH key, and paste it into the list of SSH keys that the Guard maintains.

  To display the Detector public SSH key, use the **show public-key** command on the Detector.

  To add the Detector public SSH key to the list of SSH keys that the Guard maintains, use the **key add** command on the Guard. See the "Adding SSH Keys" section on page 3-23 for more information.

Configuring a Date and a Time

You can set the time and the date by using the following command in configuration mode:

date *MMDDhhmm[[CC]YY][.ss]*

Table 3-11 provides the arguments for the **date** command.

Table 3-11 Arguments for the date Command

Parameter	Description
MM	Month in numeric figures.
DD	Day of the month.
hh	Hour in a 24-hour clock.
mm	Minutes.
CC	(Optional) First two digits of the year (for example, **20**05).
YY	(Optional) Last two digits of the year (for example, 20**05**).
.ss	(Optional) Seconds (the decimal point must be present).

The following example shows how to configure the date to October 8 of the year 2007 and the time to 5:10 pm (1710) and 17 seconds:

```
user@GUARD-conf# date 1008171003.17
Wed Oct  8 17:10:17 EDT 2003
```

Synchronizing the Guard Clock with an NTP Server

To configure the Guard system clock to synchronize with a Network Time Protocol (NTP) server, perform the following steps in configuration mode:

Step 1 Configure the date and time locally by entering the following command:

```
date MMDDhhmm[[CC]YY][.ss]
```

See the "Configuring a Date and a Time" section on page 3-21 for more information.

Step 2 Configure the Guard system time zone by entering the following command:

```
timezone timezone-name
```

The *timezone-name* argument specifies the name of the time zone. The name is composed of the *continent* /*city* options.

The following are the continent options:

- Africa, America, Antarctica, Arctic, Asia, Atlantic, Australia, Europe, Indian, Pacific
- Etc—Wildcard for a desired time zone

Tip The time zone name is case sensitive. Type the desired continent name and press **TAB** twice for a list of relevant cities.

Step 3 Enable the NTP service by entering the following command:

```
service ntp
```

Step 4 Permit access to the NTP service from a network address by entering the following command:

```
permit ntp ip-address
```

Step 5 Configure the IP address of the desired NTP server by entering the following command:

```
ntp server ip-address
```

The *ip-address* argument specifies the NTP server IP address.

Step 6 Reload the Guard configuration.

The following example shows how to configure an NTP server:

```
user@GUARD-conf# date 1008171003.17
user@GUARD-conf# timezone Africa/Timbuktu
user@GUARD-conf# service ntp
user@GUARD-conf# permit ntp 192.165.200.224
user@GUARD-conf# ntp server 192.165.200.224
```

Managing SSH Keys

The Guard supports SSH for secure remote login. You can add a list of SSH keys to enable secure communication from a remote device to the Guard without entering a login and password.

The section describes how you can manage the Guard SSH key list and contains the following topics:

- Adding SSH Keys
- Deleting SSH Keys

Adding SSH Keys

You can enable an SSH connection without entering a login and password by adding the remote connection SSH public key to the Guard SSH key list.

Enter the following command in configuration mode:

key add [*user-name*] {**ssh-dsa** | **ssh-rsa**} *key-string comment*

Table 3-12 provides the arguments and keywords for the **key add** command.

Table 3-12 Arguments and Keywords for the key add Command

Parameter	Description
user-name	(Optional) Name of the user to which the SSH key is added. Only an administrator can add an SSH key for other users. The default is to add the SSH key for the current user.
ssh-dsa	Specifies the SSH2-DSA key type.
ssh-rsa	Specifies the SSH2-RSA key type.

Table 3-12 Arguments and Keywords for the key add Command (continued)

Parameter	Description
key-string	Public SSH key that was created on a Cisco Traffic Anomaly Detector or remote terminal. The key string is limited to 8192 bits. You must copy the complete key and exclude the key type identification (ssh-rsa or ssh-dsa).
comment	Device description. The comment format is usually in the format of user@hostname for the user and machine used to generate the key. For example, the default comment used for the SSH public keys that the Cisco Traffic Anomaly Detector generates is root@DETECTOR.

The following example shows how to add an SSH RSA key:

```
user@GUARD-conf# key add ssh-rsa 14513797528175730. . .user@Guard.com
```

Deleting SSH Keys

You can remove an SSH key from the list. If you remove the SSH key, you must authenticate the next time that you establish an SSH session with the Guard.

To remove an SSH key from the Guard, use the following command in configuration mode:

key remove [*user-name*] *key-string*

Table 3-13 provides the arguments for the **key remove** command.

Table 3-13 Arguments for the key remove Command

Parameter	Description
user-name	(Optional) Name of the user from which the SSH keys are removed. Only an administrator can delete an SSH key for other users. The default is to delete the SSH key for the current user.
key-string	Public SSH key to delete. Paste the SSH public key onto the prompt. Paste only the key without the identification field (ssh-rsa or ssh-dsa).

The following example shows how to view a user key so that it can be cut and pasted into the **key remove** command:

```
user@GUARD-conf# show keys Lilac
ssh-rsa 2352345234523456... user@Guard.com
user@GUARD-conf# key remove Lilac 2352345234523456...
```

Configuring the Keys for SFTP and SCP Connections

Secure File Transfer Protocol (SFTP), which is layered on top of SSH2, and Secure Copy Protocol (SCP), which relies on SSH, provide a secure and authenticated method for copying files. SFTP and SCP use public key authentication and strong data encryption, which prevents login, data, and session information from being intercepted or modified in transit.

To configure the keys for SFTP and SCP connections, perform the following steps:

Step 1 Display the Guard public key on the Guard by entering the **show public-key** command in configuration mode.

If the key exists, skip Step 2 and proceed to Step 3.

If no key exists, proceed to Step 2.

Step 2 Generate a private-public key pair on the Guard by entering the **key generate** command in configuration mode.

If an SSH key pair already exists, the following message appears:

```
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

Type **y** to regenerate the key.

The Guard creates the public-private key pair. To display the Guard public key, use the **show public-key** command in configuration mode.

Step 3 Copy the public key from the Guard and paste it into the key file on the network server.

For example, if you are connecting to a network server that is installed on a Linux operating system with the username user account, add the Guard public key to the /home/username/.ssh/authorized_keys2 file.

Make sure that the key is copied as a single line. If the key is copied as two lines, delete the new line character at the end of the first line.

Note If you do not copy the public key and paste it into the key file on the network server, you cannot configure automatic export functions (such as the **export reports** command) and you have to enter your password each time that you manually connect to the network server.

Changing the Hostname

You can change the hostname of the Guard. The change takes effect immediately, and the new hostname is automatically integrated into the CLI prompt string.

To change the Guard hostname, use the following command in configuration mode:

hostname *name*

The *name* argument specifies the new hostname.

The following example shows how to change the hostname of the Guard:

```
user@GUARD-conf# hostname CiscoGuard
admin@CiscoGuard-conf#
```

Enabling SNMP Traps

You can enable the Guard to send SNMP traps and notify you of significant events that occur on the Guard. In addition, you can configure the Guard SNMP trap generator parameters and define the scope of the SNMP trap information that the Guard reports.

A trap is logged in the Guard event log and displayed in the event monitor when a trap condition occurs, regardless of whether the SNMP agent sends the trap.

To configure the Guard to send SNMP traps, perform the following steps:

Step 1 Enable the SNMP trap generator service by entering the following command in configuration mode:

```
service snmp-trap
```

Step 2 Configure the SNMP trap generator parameters (the trap destination IP address and the trap information scope) by entering the following command:

```
snmp trap-dest ip-address [community-string [min-severity]]
```

Table 3-14 provides the arguments for the **snmp trap-dest** command.

Table 3-14 Arguments for the snmp trap-dest Command

Parameter	Description
ip-address	Destination host IP address.
community-string	(Optional) Community string that is sent with the trap. This string must match the community string defined for the destination host. The default community string is *public*. Enter an alphanumeric string from 1 to 15 characters. The string cannot contain spaces.
min-severity	(Optional) Trap information scope. Define the scope by stating the minimum severity-level coverage. The trap then displays all specified severity-level events and above. For example, if you specify Warnings, the trap displays all severity-level events from Warnings to Emergencies. The following list states the severity-level options: • Emergencies—System is unusable (severity=0). • Alerts—Immediate action needed (severity=1). • Critical—Critical conditions (severity=2). • Errors—Error conditions (severity=3). • Warnings—Warning conditions (severity=4). • Notifications—Normal but significant conditions (severity=5). • Informational—Informational messages (severity=6). • Debugging—Debugging messages (severity=7). By default, the report displays all severity-level events.

To delete SNMP trap generator parameters, use the **no snmp trap-dest** command. Enter an asterisk **(*)** to remove all SNMP trap destination parameters.

The following example shows that traps with a severity level equal to or higher than errors are sent to the destination IP address 192.168.100.52 with the SNMP community string of tempo:

```
user@GUARD-conf# snmp trap-dest 192.168.100.52 tempo errors
```

Table 3-15 lists the SNMP traps that the Guard generates.

Table 3-15 SNMP Traps

SNMP Trap	Severity	Description
rhExcessiveUtilizationTrap	EMERGENCY	The Guard cannot add new dynamic filters because more than 150,000 dynamic filters are active concurrently in all the Guard zones.
rhExcessiveUtilizationTrap	EMERGENCY	The anomaly detection engine memory limit was reached (higher than 90 percent).
rhGeneralTrap	EMERGENCY	The Guard failed to activate zone protection by using the packet activation method and will send subsequent traps with an ALERT severity level.
rhGeneralTrap	EMERGENCY	The Guard failed to activate diversion.
rhGeneralTrap	EMERGENCY	The Guard restored diversion.
rhGeneralTrap	ALERT	The Guard failed to activate zone protection by using the packet activation method, and a trap with an EMERGENCY severity level was already generated.
rhGeneralTrap	ALERT	The disk space is 80 percent.
rhExcessiveUtilizationTrap	CRITICAL	The Gigabit interface link utilization in bps[1] is above 85 percent.
rhExcessiveUtilizationTrap	CRITICAL	The memory utilization is above 85 percent.
rhExcessiveUtilizationTrap	CRITICAL	The accelerator card CPU utilization is above 85 percent.
rhGeneralTrap	CRITICAL	The HW diagnostics card reported an error.
rhLinkStatusTrap	CRITICAL	The link is down.
rhDynamicFilterTrap	ERROR	The number of pending dynamic filters is 1000, and new pending dynamic filters will be discarded.
rhZoneGenericTrap	ERROR	The Guard failed to synchronize the zone configuration.

Table 3-15 SNMP Traps (continued)

SNMP Trap	Severity	Description
rhGeneralTrap	ERROR	The Guard failed to activate zone protection as follows: • From protect or from learn to protect and learn • From protect and learn to protect or to learn The Guard deactivated zone protection and the learning process.
rhDynamicFilterTrap	WARNING	The Guard failed to add dynamic filters.
rhExcessiveUtilizationTrap	WARNING	The Guard has more than 135,000 dynamic filters that are active concurrently in all the zones. When the number of active dynamic filters reaches 150,000, the Guard cannot add new dynamic filters.
rhGeneralTrap	WARNING	The disk space is 75 percent.
rhPolicyConstructionTrap	WARNING	The policy construction phase of the learning process has failed.
rhProtectionTrap	WARNING	The Guard failed to start zone protection.
rhReloadTrap	WARNING	The Guard has restarted. The trap contains a MIB2 warm-start or cold-start trap and information on what caused the Guard to restart.
rhReloadTrap	WARNING	The Guard has shut down. The trap contains a a MIB2 warm-start or cold-start trap and information on what caused the Guard to shut down.
rhThresholdTuningTrap	WARNING	The threshold tuning phase of the learning process has failed.
rhAttackTrap	NOTIFICATIONS	An attack has started.
rhAttackTrap	NOTIFICATIONS	An attack has ended.
rhLinkStatusTrap	NOTIFICATIONS	The link is up.
rhPolicyConstructionTrap	NOTIFICATIONS	The policy construction phase of the learning process has been started.
rhPolicyConstructionTrap	NOTIFICATIONS	The policy construction phase of the learning process has been accepted.
rhPolicyConstructionTrap	NOTIFICATIONS	The policy construction phase of the learning process has been stopped.
rhProtectionTrap	NOTIFICATIONS	The zone protection has started.
rhProtectionTrap	NOTIFICATIONS	The zone protection has ended.
rhThresholdTuningTrap	NOTIFICATIONS	The threshold tuning phase of the learning process has been started.
rhThresholdTuningTrap	NOTIFICATIONS	The threshold tuning phase of the learning process has been accepted.

Table 3-15 SNMP Traps (continued)

SNMP Trap	Severity	Description
rhThresholdTuningTrap	NOTIFICATIONS	The threshold tuning phase of the learning process has been stopped.
rhZoneGenericTrap	NOTIFICATIONS	The Guard has started to synchronize the zone configuration.
rhZoneTrap	NOTIFICATIONS	A new zone has been created.
rhZoneTrap	NOTIFICATIONS	A zone has been deleted.
rhDynamicFilterControlTrap	INFO	The number of attack-detection events that the Guard did not send for a specific policy.
rhDynamicFilterControlTrap	INFO	The Guard has more than 1000 active dynamic filters and will not send traps for dynamic filters that it deletes.
rhDynamicFilterTrap	INFO	A dynamic filter has been added.
rhDynamicFilterTrap	INFO	A dynamic filter has been deleted.
rhDynamicFilterTrap	INFO	A pending dynamic filter has been added.

[1] bps = bits per second

Configuring SNMP Community Strings

You can access the Guard SNMP server and retrieve information as defined by the Management Information Base 2 (MIB2) and the Cisco Riverhead proprietary MIB. The community string acts like a password and permits read access from the Guard SNMP agent. You can configure the Guard SNMP community string and enable access to the SNMP agent from clients in different organizational units and with different community strings.

To add an SNMP community string, use the following command in configuration mode:

snmp community *community-string*

The *community-string* argument specifies the desired Guard community string. Enter an alphanumeric string from 1 to 15 characters. The string cannot contain spaces. The Guard default community string is riverhead. You can specify as many community names as you want. To delete a community string, use the **no community string** command. Enter an asterisk (*****) to remove all SNMP community strings.

The following example shows how to configure the SNMP community string:

```
user@GUARD-conf# snmp community tempo
```

Configuring the Login Banner

The login banner is the text that appears on the screen before user authentication when you open an SSH session, a console port connection, or a WBM session to the Guard.

You can configure a login banner to warn users against unauthorized access, describe what is considered the proper use of the system, and to alert users that the system is being monitored to detect improper use and other illicit activity.

The Guard displays the login banner in the following locations:

- CLI—Before the password login prompt or as a popup window (depending on the SSH client that you are using).
- WBM—On the right side of the Guard login window.

This section contains the following topics:

- Configuring the Login Banner from the CLI
- Importing the Login Banner
- Deleting the Login Banner

Configuring the Login Banner from the CLI

You can create a single or multiple message banner by using the **login-banner** command. If you enter more than one login banner, the new login banner is appended to the existing login banner as a new line.

To configure the login banner, use the following command in configuration mode:

login-banner *banner-str*

The *banner-str* argument specifies the banner text. The maximum string length is 999 characters. If you use spaces in the expression, enclose the expression in quotation marks (" ").

To display the login banner, use the **show login-banner** command.

The following example shows how to configure and display the login banner:

```
user@GUARD-conf# login-banner "Welcome to the Cisco Guard"
user@GUARD-conf# login-banner "Unauthorized access is prohibited."
user@GUARD-conf# login-banner "Contact sysadmin@corp.com for access."
user@GUARD-conf# show login banner
Welcome to the Cisco Guard
Unauthorized access is prohibited.
Contact sysadmin@corp.com for access.
```

Importing the Login Banner

You can import a text file from a network server to replace the existing login banner by entering one of the following commands in global mode or in configuration mode:

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

The maximum length of each line in the file that you import is 999 characters.

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information on how to configure the key that the Guard uses for secure communication.

Table 3-16 provides the arguments and keywords for the **copy login-banner** command.

Table 3-16 Arguments and Keywords for the copy login-banner Command

Parameter	Description
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Complete name of the file. If you do not specify a path, the server copies the file from your home directory.
login	(Optional) The server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for it.

The following example shows how to import the login banner from an FTP server:

```
user@GUARD-conf# copy ftp login-banner 10.0.0.191 /root/login-banner <user> <password>
```

Deleting the Login Banner

If you no longer want to display a message before user authentication, delete the login banner.

To delete the login banner, use the **no login-banner** command in configuration mode.

The following example shows how to delete the login banner:

```
user@GUARD-conf# no login-banner
```

Configuring the WBM Logo

To customize your end-user interface, you can add a company logo or any customized logo to the WBM web pages.

The new logo appears in the following places:

- On the Guard login page, under the Cisco Systems logo.
- On all WBM pages, except for the Guard login page, on the right side of the Cisco Systems logo.

The new logo must be in GIF format. We recommend that the size of the new logo is as follows: width = 87 pixels and height = 41 pixels.

This section contains the following topics:

- Importing the WBM Logo
- Deleting the WBM Logo

Importing the WBM Logo

To import a new logo from a network server, use the following command in global mode or in configuration mode:

- **copy ftp wbm-logo** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **wbm-logo** *server full-file-name login*

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for a password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information on how to configure the key that the Guard uses for secure communication.

Table 3-17 provides the arguments and keywords for the **copy wbm-logo** command.

Table 3-17 Arguments and Keywords for the copy wbm-logo Command

Parameter	Description
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Complete name of the file including the GIF file extension. If you do not specify a path, the server copies the file from your home directory.
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for it.

The following example shows how to import the WBM logo file from an FTP server:

```
user@GUARD-conf# copy ftp wbm-logo 10.0.0.191 /root/WBMlogo.gif <user> <password>
```

Deleting the WBM Logo

To delete the WBM logo, use the **no wbm-logo** command in configuration mode.

The following example shows how to delete the login banner:

```
user@GUARD-conf# no wbm-logo
```

Configuring the Session Timeout

The session timeout is the amount of time that a session remains active when there is no activity. If there is no activity for the configured time, a timeout occurs, and then you must log in again. The session timeout is disabled by default.

The session timeout applies to the CLI only and does not apply to the WBM.

You can configure the number of minutes until the Guard disconnects an idle session automatically by entering the following command in configuration mode:

session-timeout *timeout-val*

The *timeout-val* argument specifies the number of minutes until the Guard disconnects an idle session automatically. Valid values are from 1 to 1440 minutes (one day).

The following example shows how to configure the Guard to disconnect an idle session after 10 minutes:

```
user@GUARD-conf# session-timeout 10
```

To prevent the Guard from disconnecting idle sessions automatically, use the **no session-timeout** command.

To display the value of the session timeout, use the **show session-timeout** command.

CHAPTER 4

Configuring Traffic Diversion

This chapter describes how to configure traffic diversion with the Cisco Guard (Guard).

Traffic diversion configuration is topology independent. The configuration procedures for Layer 2 and Layer 3 topologies are identical.

To save all configuration changes to the Guard memory, use the **write memory** command in router configuration mode.

Note Information provided in this document regarding Cisco router configuration is for informational purposes only. Refer to the appropriate user guides for detailed information.

This chapter contains the following sections:

- Understanding the BGP Diversion Method
- Understanding Traffic Forwarding Methods
- Long Diversion Method

Understanding the BGP Diversion Method

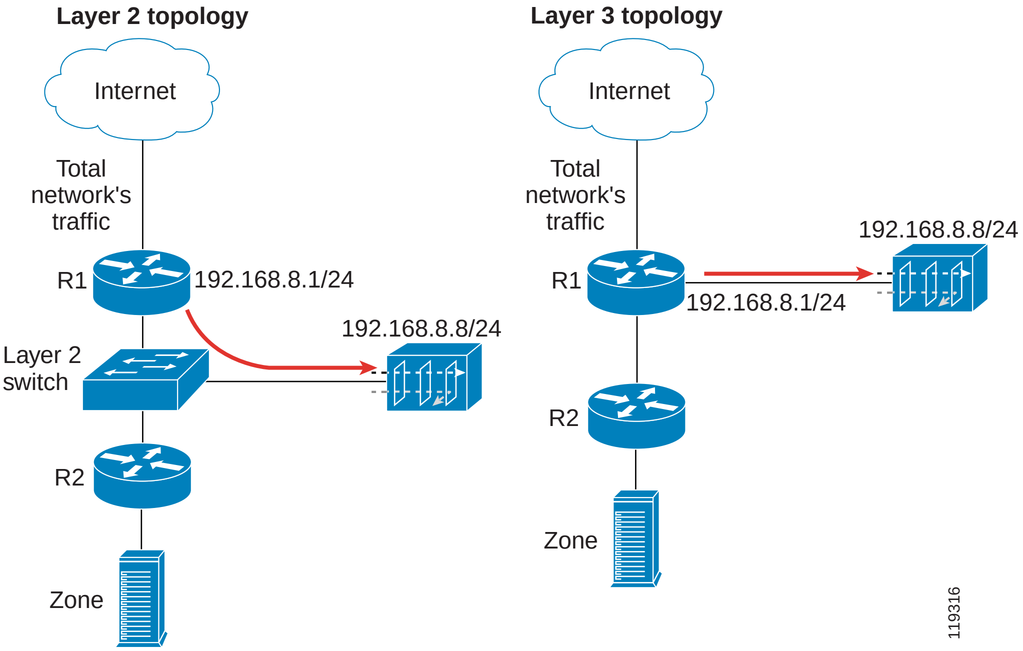
Following standard Border Gateway Protocol (BGP) routing definitions, routers select the routing path with the longest matching prefix (also known as the “most specific”). After establishing a BGP session with the router, the Guard sends a routing update where the Guard is listed as the best path for the protected zone. The network prefix that the Guard announces is longer than the one already listed in the router’s routing table, overriding the router's routing table definition. The prefix subnet is configured per zone subnet IP address. BGP is configured similarly in all networks.

To configure traffic diversion in Layer 2 and Layer 3 network topologies, perform the following:

1. Configure traffic diversion using BGP (see the “Guard BGP Configuration” section for more information).
2. Configure the appropriate traffic forwarding method (the “Understanding Traffic Forwarding Methods” section for more information).

Figure 4-1 provides examples of Layer 2 and Layer 3 network topologies. In both network topologies, the Guard diverts the traffic from router R1.

Figure 4-1 ***BGP Configuration***



After BGP diversion is established, the router's routing tables points to the Guard as the best route to the zone and the router forwards all traffic destined to the zone's IP address to the Guard.

This section contains the following topics:

- BGP Configuration Guidelines
- Guard BGP Configuration
- Cisco Router BGP Configuration

BGP Configuration Guidelines

This section provides general guidelines for BGP configuration on the Guard and on a divert-from router.

Note The guidelines provided in this section apply to the BGP configuration on any router from which the Guard diverts the traffic. The sample BGP configurations in the following sections is presented using the syntax of the Cisco IOS software.

Note The following examples are provided using common External Border Gateway Protocol (eBGP). You should consider the network configuration and determine whether eBGP or Internal Border Gateway Protocol (iBGP) should be implemented in your network.

Follow these guidelines when the Guard and adjacent routers operate using common eBGP:

1. Configure the Guard with an easily recognizable Autonomous System (AS) number.

The Guard sends routing information only when it diverts traffic. This route appear in the router's routing tables. Using a recognizable value allows you to easily identify the Guard in the router's routing tables.

2. To ensure that the Guard's routing information is not redistributed to other internal and external BGP neighboring devices, perform the following:
   - Configure the Guard to not send routing information and to drop incoming BGP routing information.
   - Set the Guard BGP community attribute values to **no-export** and **no-advertise**.

   A match in the community attributes enables the Guard to filter BGP announcements on the router and enforce this policy.
3. Enter the **soft-reconfiguration inbound** command during the setup procedures. This command is useful for troubleshooting and allows you to restore a routing table without reconnecting to the neighboring device.

See the "BGP Diverting Method" section on page A-5 for more information about BGP.

Guard BGP Configuration

You can configure BGP on the Guard using the Zebra application (see http://www.zebra.org for more information about the Zebra application).

Note We recommend that you configure a zone's diversion when the zone is in standby mode.

To enter diversion configuration on the Guard, perform the following steps:

Step 1 From the Configuration command group level, enter the following command:

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

The following prompt appears, indicating that the system has entered the Zebra application in nonprivileged mode:

```
router>
```

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

Step 2 Switch to the privileged mode by entering the following command:

```
router> enable
```

The following prompt appears, indicating that the system has entered the Zebra application privileged mode:

```
router#
```

Note To quit the Zebra application, enter the **exit** command from the router command level. To exit from the current command group level to a higher group level, enter the **exit** command.

Step 3 Switch to terminal configuration mode by entering the following command:

```
router# config terminal
```

The following prompt appears, indicating that the system has entered the Zebra application configuration mode:

```
router(config)#
```

Step 4 Configure routing on the Guard using the commands shown in the following example. These commands observe the following conventions:

- Items in bold represent commands.
- Items in bold italic represent names. You may replace these names.
- Items in italics enclosed in angle brackets (< >) represent values that you must supply. Replace the terms in italics with the Guard and router (a divert-from router) values indicated. Do not include the angle brackets.

Note You can use the prefix-list, route-map, or distribute-list method for filtering outgoing routing information about a router. The following example describes the distribute-list method. You can use the prefix-list or route-map filtering method types as long as the routing information is not sent to the Guard.

The following commands must be entered on the Guard:

```
router(config)# router bgp <Guard-AS-number>
router(config-router)# bgp router-id <Guard-IP-address>
router(config-router)# redistribute guard
router(config-router)# neighbor <Router-IP-address> remote-as <Router-AS-number>
router(config-router)# neighbor <Router-IP-address> description <description>
router(config-router)# neighbor <Router-IP-address> soft-reconfiguration inbound
router(config-router)# neighbor <Router-IP-address> distribute-list nothing-in in
router(config-router)# neighbor <Router-IP-address> route-map Guard-out out
router(config-router)# exit
router(config)# access-list nothing-in deny any
router(config)# route-map Guard-out permit 10
router(config-route-map)# set community no-export no-advertise
```

This section contains the following topics:

- Guard BGP Configuration Example
- Displaying the Guard Router Configuration File

Guard BGP Configuration Example

To display the Guard router configuration, enter the **show running-config** command from the router command level. In the following example, the router's AS number is 100, and the Guard's AS number is 64555.

The following partial sample output is displayed:

```
router# show running-config
... ... ...
router bgp 64555
bgp router-id 192.168.8.8
redistribute guard
neighbor 192.168.8.1 remote-as 100
neighbor 192.168.8.1 description divert-from router
neighbor 192.168.8.1 soft-reconfiguration inbound
neighbor 192.168.8.1 distribute-list nothing-in in
neighbor 192.168.8.1 route-map Guard-out out
!
access-list nothing-in deny any
!
route-map Guard-out permit 10
set community 100:64555 no-export no-advertise
... ... ...
```

Displaying the Guard Router Configuration File

You can display the Guard router configuration file by entering the following command from the Global command group level:

show running-config router

The information that displays is the same information that displays when you enter the **show running-config** command from the router command level (see the "Guard BGP Configuration Example" section.

Cisco Router BGP Configuration

This section describes the router BGP configuration used when you configure a traffic diversion. The syntax in the commands is taken from the BGP configuration on a Cisco router.

These commands observe the following conventions:

- Items in bold represent commands.
- Items in bold italic represent names. You may replace these names.
- Items in italics enclosed in angle brackets (< >) represent values that you must supply. Replace the terms in italics with the Guard and router (a divert-from router) values indicated. Do not include the angle brackets.

The following configuration example shows the commands to use to configure BGP on a Cisco router:

```
R7200(config)# router bgp <Router-AS>
R7200(config-router)# bgp log-neighbor-changes
R7200(config-router)# neighbor <Guard-IP-address> remote-as GuardAS
R7200(config-router)# neighbor <Guard-IP-address> description <description>
R7200(config-router)# neighbor <Guard-IP-address> soft-reconfiguration inbound
R7200(config-router)# neighbor <Guard-IP-address> distribute-list routesToGuard out
R7200(config-router)# neighbor <Guard-IP-address> route-map Guard-in in
R7200(config-router)# no synchronization
R7200(config-router)# exit
R7200(config)# ip bgp-community new-format
R7200(config)# ip community-list expanded <Guard-community-name> permit no-export
no-advertise
R7200(config)# route-map Guard-in permit 10
R7200(config-route-map)# match community <Guard-community-name> exact match
R7200(config-route-map)# exit
R7200(config)# ip access-list standard routestoGuard
R7200(config-std-nacl)# deny any
```

The **no synchronization** command prevents the distribution of the Guard BGP routing updates into Interior Gateway Protocol (IGP).

Cisco Router BGP Configuration Example

To display the router configuration, enter the **show running-config** command from the router global command level. In the following example, the router's AS number is 100, and the Guard's AS number is 64555.

The following partial sample output is displayed:

```
R7200# show running-config
... ... ...
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.8.8 remote-as 64555
neighbor 192.168.8.8 description Guard
neighbor 192.168.8.8 soft-reconfiguration inbound
neighbor 192.168.8.8 distribute-list routesToGuard out
neighbor 192.168.8.8 route-map Guard-in in
no synchronization
!
ip bgp-community new-format
ip community-list expanded Guard permit 100:64555 no-export no- advertise
!
route-map Guard-in permit 10
match community Guard exact match
ip access-list standard routesToGuard
 deny any
... ... ...
```

Understanding Traffic Forwarding Methods

This section provides details on traffic forwarding methods. Traffic forwarding methods are used to forward the cleaned traffic from the Guard to the next-hop router. See the "Understanding the Traffic Forwarding Methods" section on page A-6 for more information.

The following terminology is used in this section:

- Divert-from router—Router from which the Guard diverts the destination zone traffic.
- Inject-to router—Router to which the Guard forwards the clean destination zone traffic.
- Next-hop router—Router that is the next hop to the zone according to the routing table on the divert-from router before the Guard activated traffic diversion.

This section contains the following topics:

- Layer-2 Forwarding Method
- Policy-Based Routing Destination Forwarding Method
- VPN Routing Forwarding Destination Forwarding Method
- Policy-Based Routing VLAN Forwarding Method
- VPN Routing Forwarding VLAN Forwarding Method
- Tunnel Diversion Forwarding Method

Layer-2 Forwarding Method

The Layer-2 Forwarding (L2F) method is used in a Layer 2 topology when all three devices—the Cisco Guard, the divert-from router, and the next-hop router—are located in one shared IP network (Figure 4-2).

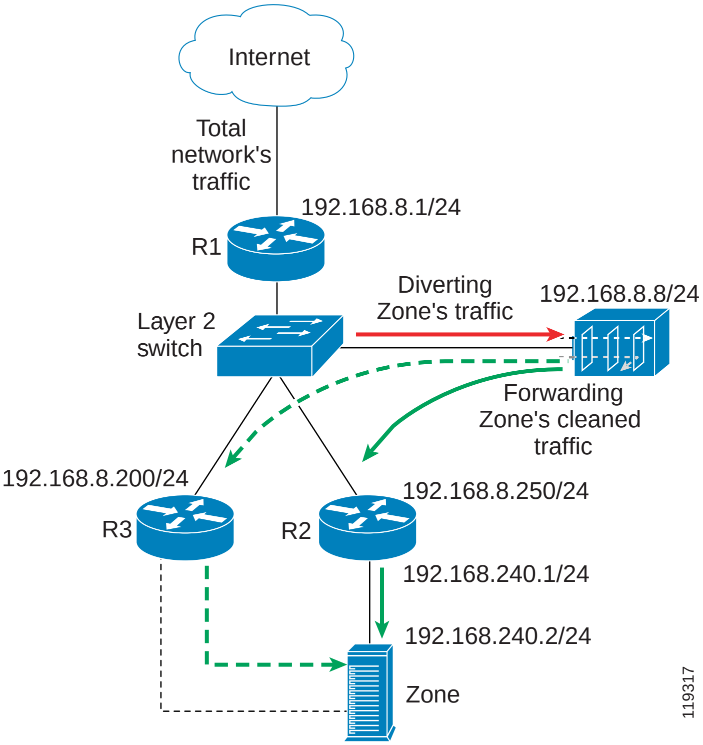
In a Layer 2 topology, a divert-from router and an inject-to router are two separate devices. The next-hop router and the inject-to router are the same device.

The Guard issues an ARP query to resolve the MAC address of the inject-to/next-hop router and then forwards the traffic. For this reason, no configuration on the routers is required when using the L2F method.

The zone may be connected as follows:

- Directly to a Layer 2 switch. In this case, connect the zone to the same IP subnet as the Guard and configure the zone's IP address as the inject-to router. The Guard forwards the traffic directly to the zone.
- Using an IP forwarding router. In this case, you must define the IP forwarding router as the Guard's next-hop router.

Figure 4-2 Layer-2 Forwarding Method



This section contains the following topics:

- Guard L2F Configuration
- Router L2F Configuration

Guard L2F Configuration

This section describes the Guard L2F configurations and contains the following topics:

- Interface Statements
- BGP Statements
- Injection Configuration

Interface Statements

You can configure the Guard's out-of-band interface as described in the "Configuring a Physical Interface" section.

The following example shows how to configure out-of-band interface giga1:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the "Guard BGP Configuration" section.

In the following example, the Guard's AS is 64555. The router's AS is 100 and the IP address is 192.168.8.1:

```
router bgp 64555
 redistribute guard
 neighbor 192.168.8.1 remote-as 100
 neighbor 192.168.8.1 description C7513
 neighbor 192.168.8.1 distribute-list nothing-in in
 neighbor 192.168.8.1 soft-reconfiguration inbound
 neighbor 192.168.8.1 route-map filt-out out
!
route-map filt-out permit 10
 set community no-advertise no-export 100:64555
!
access-list nothing-in deny any
```

Injection Configuration

You can configure traffic injection from the Guard to the zone by adding a static route to the zone or the next-hop router according to the network topology. You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) through the next-hop router (192.168.8.250):

```
router# configure terminal
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.8.250
```

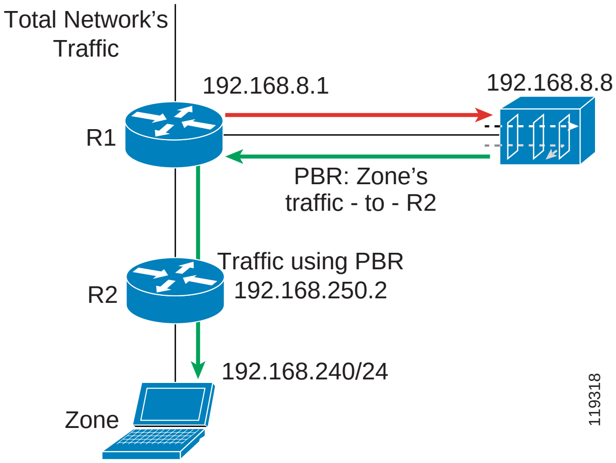
Router L2F Configuration

No configuration is required on the router.

Policy-Based Routing Destination Forwarding Method

Policy-Based Routing (PBR) destination is a static forwarding method that is deployed in Layer 3 network topologies, where the Guard forwards the filtered traffic to the same router from which the traffic was diverted (Figure 4-3).

Figure 4-3 PBR Destination Forwarding Method



To enable the Guard to divert the zone's traffic from the router, the Guard modifies the zone's route in the router's routing table and the Guard is listed as the best path to the zone.

An endless routing loop could occur if the router's routing table is not changed. Because the only entry for the traffic destined to the zone in the router's routing table is the Guard, filtered traffic from the Guard is sent back to the Guard.

To overcome routing loops, you can configure PBR destination on the inject-to router. PBR destination allows you to create rules that override the rules in the router's routing table and avoid endless routing loops. PBR destination enables you to add rules that are applied to the filtered traffic. These rules instruct the router to forward the filtered traffic to the zone, regardless of the routing table entries.

To configure the diversion in this network topology, you can configure the traffic diversion process using BGP (see the "Guard BGP Configuration" section for more information).

This section contains the following topics:

- PBR Destination Configuration Guidelines
- Guard PBR Destination Configuration
- Cisco Router PBR Destination Configuration Examples

PBR Destination Configuration Guidelines

The guidelines provided in this section apply to PBR destination configurations on any inject-to router.

To configure PBR destination on an inject-to router, follow these guidelines:

1. You must apply PBR destination on the router interface that is connected to the Guard.

Note You can apply PBR destination only to the traffic that comes from the Guard.

2. You must forward the traffic that is selected by PBR destination to the next-hop router. The next-hop router should have the following characteristics:
   - The next-hop router is connected directly to the divert-from router. In Layer 3 topology, the next-hop router and the inject-to router are the same device.
   - The divert-from router is not part of the next-hop router's route to the zone. (A configuration where the divert-from router is part of the next-hop router's route to the zone would result in a routing loop between the divert-from and the next-hop routers.)

PBR destination is applied using the **route-map** command and the **match** and **set** commands to define the conditions for policy routing packets. To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. The user must enable PBR destination for the configured route map on a particular interface. All packets arriving on the specified interface that match the match clause are subject to PBR destination.

A PBR destination configuration consists the following three parts:

- Sequence—Specifies the position that a new route map will have in the list of route maps already configured with the same name. Cisco routers process sequence numbers in ascending order.

  You can define a separate route-map entry and sequence number for traffic that is to be forwarded to the zone and for all other traffic.

  The sequence is configured using the **route-map** command. Using the **route-map** command puts the router into route-map configuration mode.
- Matching statement—Specifies the conditions under which policy routing occurs. You should specify the conditions under which an IP address is matched by using the **match** command. A match determines whether the next hop is modified.
- Forwarding statement—Specifies the routing actions to perform if the criteria enforced by the **match** commands are met. The **set ip next-hop route-map** configuration command indicates where to send packets that pass a match clause of a route map for policy routing.

Guard PBR Destination Configuration

The configuration in the following example refers to the network in Figure 4-3.

- BGP Statements—You can enter the Guard router BGP configuration as described in the "Guard BGP Configuration" section.
- Injection Configuration to the Next-Hop Router—The next-hop router in the example is R2 (see Figure 4-3). To configure traffic injection from the Guard to the zone, add a static route to the inject-to router. You should configure the static route at the Guard's router configuration level.

  The following example shows how to configure a static route for the zone's network (192.168.240.0/24):

  ```
  router# configure terminal
  router(config)# ip route 192.168.240.0 255.255.255.0 192.168.8.1
  ```

Cisco Router PBR Destination Configuration Examples

The following example shows the router PBR destination configuration used when configuring a diversion.

```
R7200(config)# interface FastEthernet 0/2
R7200(config-if)# description <Interface connected to the Guard>
R7200(config-if)# ip address <Router interface IP address> <Router interface IP mask>
R7200(config-if)# no ip directed-broadcast
```

```
R7200(config-if)# ip policy route-map <Guard-PBR-name>
R7200(config-if)# exit
R7200(config)# ip access-list extended <Zone-name>
R7200(config-ext-nacl)# permit ip any host <Zone IP address>
R7200(config-ext-nacl)# exit
R7200(config)# route-map <Guard-PBR-name> permit 10
R7200(config-route-map)# match ip address <Zone-name>
R7200(config-route-map)# set ip next-hop <next-hop router IP address>
R7200(config-route-map)# exit
R7200(config)# route-map < Guard-PBR-name > permit 100
R7200(config-route-map)# description let thru all other packets without modifying next-hop
```

This example shows a PBR destination traffic forwarding configuration for the sample network in Figure 4-3. To display the router configuration, you enter the **show running-config** command.

The following partial example screen is displayed:

```
R7200# show running-config
... ... ...
interface FastEthernet0/2
description Interface connected to the Guard
    ip address 192.168.8.1 255.255.255.0
    no ip directed-broadcast
    ip policy route-map GuardPbr
!
ip access-list extended zone-A
    permit ip any host 192.168.240.2
!
route-map GuardPbr permit 10
    match ip address zone-A
    set ip next-hop 192.168.250.2
!
route-map GuardPbr permit 100
description let thru all other packets without modifying next-hop
```

VPN Routing Forwarding Destination Forwarding Method

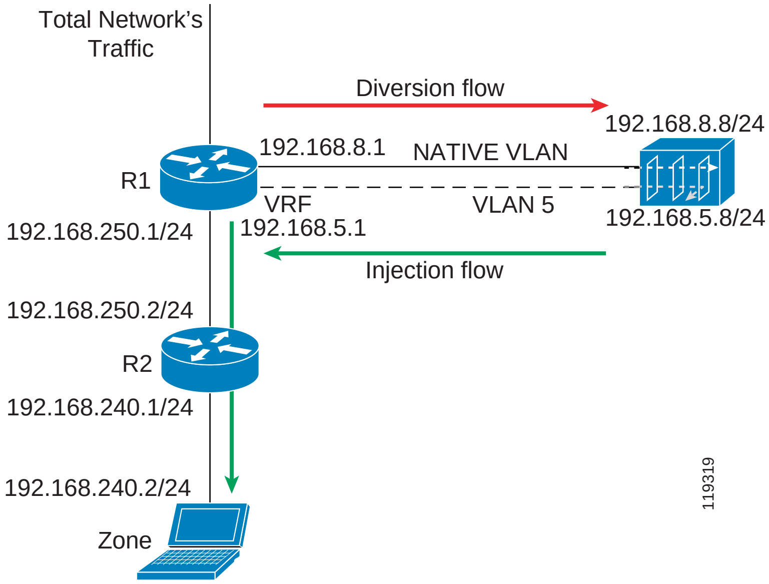
VPN Routing Forwarding Destination (VRF-DST) is a static forwarding method that is deployed in Layer 3 network topologies, where the Guard forwards the filtered traffic to the same router from which the traffic was diverted (Figure 4-4).

To enable the Guard to divert the zone's traffic from the router, the Guard modifies the zone's route in the router's routing table to make the Guard the best path to the zone.

An endless routing loop could occur if the router's routing table is not changed. Because the only entry for the traffic destined to the zone in the router's routing table is the Guard, the filtered traffic from the Guard is sent back to the Guard.

VRF-DST allows you to create another routing and forwarding table (called the VRF table) in addition to the main routing and forwarding tables. The additional routing table is configured to route traffic that is handled by the router's interface that faces the Guard.

Figure 4-4 VRF DST Forwarding Method



This section contains the following topics:

- VRF-DST Configuration Guidelines
- Guard VRF-DST Configuration

VRF-DST Configuration Guidelines

To configure VRF-DST on an inject-to router, configure two separate interfaces on the router's physical interface facing the Guard as follows:

- NATIVE VLAN interface—This interface is used to divert traffic from the router to the Guard. Traffic on this VLAN is forwarded according to the global routing table. The Guard sends BGP announcements to divert the traffic to the Guard on this interface.
- A Second VLAN interface—This interface is used to divert the returned traffic from the Guard to the router. You configure a VRF table on this interface. The VRF table contains a static route to forward all zone traffic to a specified next-hop router.

Note Use the VRF-DST method only when the next-hop router is static for each zone.

Guard VRF-DST Configuration

This section describes the Guard VRF-DST configuration. The configuration in the following examples refers to the network in Figure 4-4.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Interface VLAN Statements

The following example shows how to configure VLAN 5 on the in-band interface:

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the "Guard BGP Configuration" section.

Injection Configuration

The next-hop router in the example is R2 (see Figure 4-3). To configure traffic injection from the Guard to the zone, add a static route to the next-hop router.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the VLAN interface on R1, 192.168.5.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

Note VRF is supported from Cisco IOS Release 12.0(17) S/ST.

Creating a VRF Table

The following example shows how to create a VRF table on the inject-to router:

```
R7200(config)# ip vrf Guard-vrf
R7200(config)# rd 100:1
R7200(config)# route-target export 100:1
R7200(config)# route-target import 100:1
```

Interface Native VLAN Statements

The following example shows how to configure the Native VLAN on the divert-from router:

```
R7200(config)# interface fastEthernet1/0.1
R7200(config-if)# encapsulation dot1Q 1 native
R7200(config-if)# description << VLAN TO GUARD-DIVERSION >>
R7200(config-if)# ip address 192.168.8.1 255.255.255.0
R7200(config-if)# no ip directed-broadcast
```

Interface VLAN 5 Statements

The following example shows how to configure the VLAN 5 interface on the inject-to router:

```
R7200(config)# interface fastEthernet 1/0.5
R7200(config-if)# encapsulation dot1Q 5
R7200(config-if)# description << VLAN TO GUARD-INJECTION >>
R7200(config-if)# ip vrf forwarding Guard-vrf
R7200(config-if)# ip address 192.168.5.1 255.255.255.0
```

Interface to Zone Statements

The following example shows how to configure the router interface to the zone:

```
R7200(config)# interface fastEthernet 2/0
R7200(config-if)# description << LINK TO ZONE >>
R7200(config-if)# ip address 192.168.250.1 255.255.255.0
```

BGP Statements

Enter the router, R1, BGP configuration as described in the "Cisco Router BGP Configuration" section.

Static VRF-DST Statements

The following example shows how to configure static VRF on the inject-to router. The static VRF specifies the route to the zone. The parameter **global** indicates that the inject-to router's VRF table receives a copy of next-hop properties (outbound interface, MAC address) from global routing table.

```
R7200(config)# ip route vrf Guard-vrf 192.168.240.2 255.255.255.0 192.168.250.2 global
```

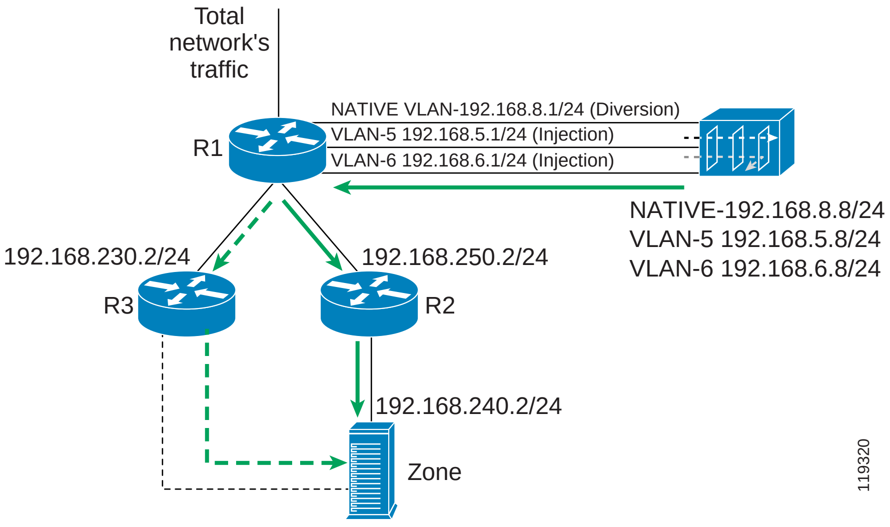
Policy-Based Routing VLAN Forwarding Method

You can use the Policy-Based Routing VLAN (PBR-VLAN) method when there is more than one possible next-hop router (Figure 4-5). You configure multiple VLAN (Virtual LAN, 802.1Q) trunks between the Guard and router R1 (the divert-from and inject-to router). Each VLAN in the trunk is associated with a different next-hop router. In addition, you configure PBR on each VLAN logical interface to forward the traffic on the VLAN to its corresponding next-hop router.

The Guard forwards packets to a particular next-hop router by transmitting the packets over the appropriate VLAN. This action allows the Guard to change the next-hop router of a zone by changing the VLAN on which the packets are forwarded.

The native VLAN is used for traffic diversion. On this interface, the Guard sends the BGP announcements to the router.

Figure 4-5 PBR-VLAN Forwarding Method



This section contains the following topics:

- Guard PBR-VLAN Configuration
- Cisco Router PBR-VLAN Configuration

Guard PBR-VLAN Configuration

This section describes the Guard PBR-VLAN configuration. The following examples refer to the network in Figure 4-5.

PBR-VLAN is applied on R1's interface facing the Guard. Zone traffic on VLAN-5 is forwarded to R2. Zone traffic on VLAN-6 is forwarded to R3.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Interface VLAN-5 Statements

The following example shows how to configure VLAN-5 on the in-band interface:

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

Interface VLAN-6 statements

The following example shows how to configure VLAN-6 on the in-band interface:

```
admin@GUARD-conf# interface giga1.6
admin@GUARD-conf-if-giga1.5# ip address 192.168.6.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the "Guard BGP Configuration" section.

Injection Configuration to R2

To configure traffic injection from the Guard to the zone, add a static route to the next-hop router R2.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the VLAN interface on R1, 192.168.5.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

Injection Configuration to R3

You can configure traffic injection from the Guard to the zone by adding a static route to the next-hop router R3.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone’s network (192.168.240.0/24) via the VLAN interface on R1, 192.168.6.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.6.1
```

Cisco Router PBR-VLAN Configuration

This section describes the Cisco router PBR-VLAN configurations.

Interface Native VLAN Statements

The following example shows how to configure the native VLAN for traffic diversion:

```
interface fastEthernet 1/0
 description << NATIVE VLAN TO GUARD-DIVERSION >>
 ip address 192.168.8.1 255.255.255.0
 no ip directed-broadcast
```

VLAN-5 Creation

The following example shows how to create VLAN-5 on router R1:

```
interface fastEthernet 1/0.1
 encapsulation dot1Q 5
 description << VLAN-5 TO GUARD-INJECTION >>
 ip address 192.168.5.1 255.255.255.0
 ip policy route-map next-hop_R2
 no ip directed-broadcast
```

VLAN-6 Creation

The following example shows how to create VLAN-6 on router R1:

```
interface fastEthernet 1/0.2
 encapsulation dot1Q 6
 description << VLAN-6 TO GUARD-INJECTION >>
 ip address 192.168.6.1 255.255.255.0
 ip policy route-map next-hop_R3
 no ip directed-broadcast
```

Next-Hop Interface Configuration

The following example shows how to configure the interfaces to the next-hop routers:

```
interface fastEthernet 2/0
 ip address 192.168.250.1 255.255.255.0
 Description << LINK TO NEXT-HOP R2 >>
 exit
interface fastEthernet 3/0
 ip address 192.168.230.1 255.255.255.0
 description << LINK TO NEXT-HOP R3 >>
```

BGP Statements

You can enter the router, R1, BGP configuration as described in the “Cisco Router BGP Configuration” section.

Route-Map Statements (PBR)

The following example shows how to configure PBR for the next-hop routers:

```
route-map next-hop_R2 permit 10
 set ip next-hop 192.168.250.2

route-map next-hop_R3 permit 10
 set ip next-hop 192.168.230.2
```

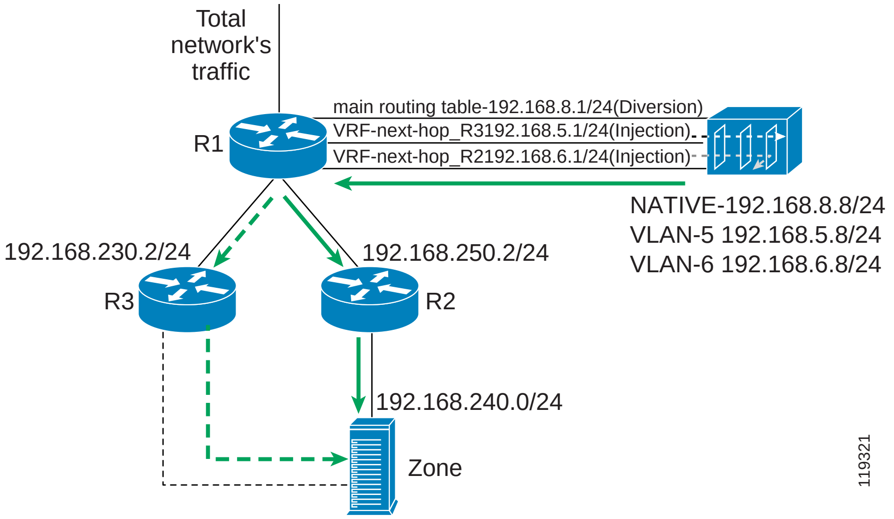
VPN Routing Forwarding VLAN Forwarding Method

The VPN Routing Forwarding VLAN (VRF-VLAN) method is similar to the PBR-VLAN method. A VRF table is associated with each VLAN on the inject-to router rather than a PBR table. Each VRF table directs the traffic on the VLAN to the corresponding next-hop router (Figure 4-6).

The Guard forwards packets to a particular next-hop router by transmitting the packets over the appropriate VLAN. This action allows the Guard to change the next-hop router to the zone by changing the VLAN on which the packets are forwarded.

The native VLAN is used for traffic diversion. On this interface, the Guard sends the BGP announcements to the router.

Figure 4-6 VRF-VLAN Forwarding Method



This section contains the following topics:

- Guard VRF-VLAN Configuration
- Cisco Router VRF-VLAN Configuration

Guard VRF-VLAN Configuration

This section describes the Guard VRF-VLAN configuration. The following examples refer to the network in Figure 4-6.

VRF-VLAN is applied on R1’s interface facing the Guard. Zone traffic on VLAN-5 is forwarded to R2. Zone traffic on VLAN-6 is forwarded to R3.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Interface VLAN-5 Statements

The following example shows how to configure VLAN-5 on the in-band interface:

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

Interface VLAN-6 Statements

The following example shows how to configure VLAN-6 on the in-band interface:

```
admin@GUARD-conf# interface giga1.6
admin@GUARD-conf-if-giga1.5# ip address 192.168.6.8 255.255.255.0
```

BGP Statements

You can enter the Guard router BGP configuration as described in the "Guard BGP Configuration" section.

Set the neighbor IP address to 192.168.8.1.

Injection Configuration to R2

You can configure traffic injection from the Guard to the zone by adding a static route to the next-hop router R2.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the VLAN interface on R1, 192.168.5.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

Injection Configuration to R3

You can configure traffic injection from the Guard to the zone by adding a static route to the next-hop router R3.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the VLAN interface on R1, 192.168.6.1:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.6.1
```

Cisco Router VRF-VLAN Configuration

This section describes the Cisco router VRF-VLAN configurations.

First VRF Table Production

The following example shows how to create the VRF table associated with router R2:

```
ip vrf next-hop_R2
```

```
 rd 100:1
 route-target export 100:1
 route-target import 100:1
Second VRF Table Production
Create the VRF table associated with router R3:
ip vrf next-hop_R3
 rd 100:1
 route-target export 100:1
 route-target import 100:1
```

Native VLAN Production

The following example shows how to configure the native VLAN on router R1:

```
interface fastEthernet 1/0
 description <<NATIVE VLAN TO GUARD-DIVERSION>>
 ip address 192.168.8.1 255.255.255.0
 no ip directed-broadcast
```

VLAN-5 Creation

The following example shows how to create VLAN-5 on router R1:

```
interface fastEthernet 1/0.1
 encapsulation dot1Q 5
 description << VLAN-5 TO GUARD-INJECTION >>
 ip address 192.168.5.1 255.255.255.0
 ip vrf forwarding next-hop_R2
 no ip directed-broadcast
```

VLAN-6 Creation

The following example shows how to create VLAN-6 on router R1 with the second VRF association:

```
interface fastEthernet 1/0.2
 encapsulation dot1Q 6
 description << VLAN-6 TO GUARD-INJECTION >>
 ip address 192.168.6.1 255.255.255.0
 ip vrf forwarding next-hop_R3
 no ip directed-broadcast
```

Next-Hop Interfaces

The following example shows how to configure the interfaces to the next-hop routers:

```
interface fastEthernet 2/0
 ip address 192.168.250.1 255.255.255.0
 Description << LINK TO NEXT-HOP R2 >>
!
interface fastEthernet 3/0
 ip address 192.168.230.1 255.255.255.0
 description << LINK TO NEXT-HOP R3 >>
```

BGP Statements

You can enter the router, R1, BGP configuration as described in the “Cisco Router BGP Configuration” section.

Static VRF Routes

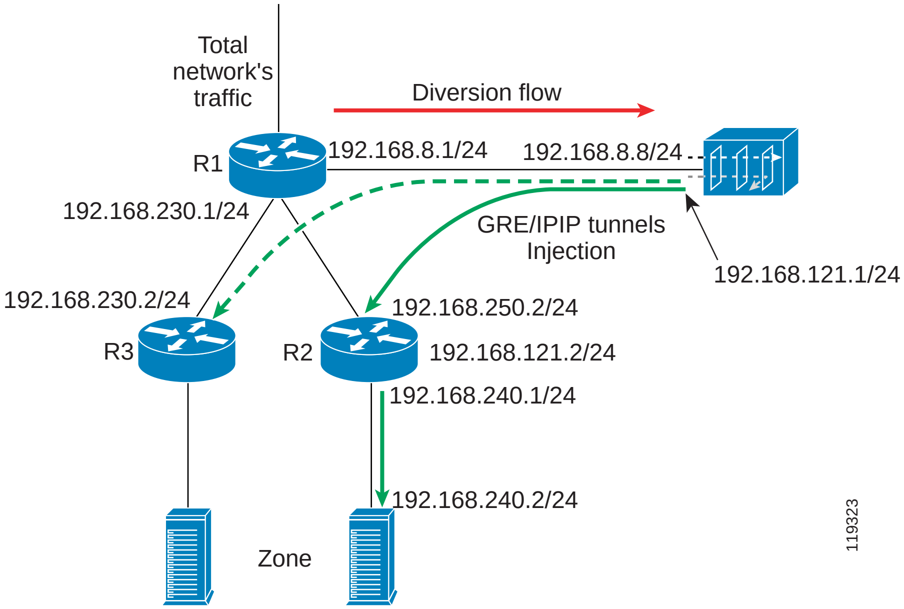
The following example shows how to configure static VRF on the inject-to router. The static VRF specifies the route to the zone. The parameter global indicates that the route to the next hop is learned from the global routing table.

```
R7200(config)# ip route vrf next-hop_R3 192.168.240.2 255.255.255.255 192.168.230.2 global
R7200(config)# ip route vrf next-hop_R2 192.168.240.2 255.255.255.255 192.168.250.2 global
```

Tunnel Diversion Forwarding Method

In the tunnel diversion method, a tunnel (GRE or IPIP) is created between the Guard and each of the next-hop routers (Figure 4-7). The Guard sends the traffic destined to the zone over the tunnel to the appropriate next-hop router. This action allows the Guard to change the next-hop router to a specified zone by changing the tunnel that the packets are forwarded on. Because the clean traffic from the Guard to the zone is encapsulated in the tunnel, the inject-to router performs a routing decision on the tunnel interface end point, not on the zone's address.

Figure 4-7 Tunnel Diversion Forwarding Method



This section contains the following topics:

- Guard Tunnel Diversion Configuration
- Cisco Router Tunnel Diversion Configuration

Guard Tunnel Diversion Configuration

This section describes the Guard tunnel diversion configuration. The following examples refer to the network in Figure 4-7.

Native Interface Statements

The following example shows how to configure the in-band interface:

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

Tunnel Interface Statements

The following example shows how to configure a Generic Routing Encapsulation (GRE) tunnel.

```
admin@GUARD-conf# interface gre1
admin@GUARD-conf-if-gre1# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-gre1# tunnel source 192.168.8.8
admin@GUARD-conf-if-gre1# tunnel destination 192.168.250.2
```

The following example shows how to configure an IP in IP (IPIP) tunnel.

```
admin@GUARD-conf# interface ipip1
admin@GUARD-conf-if-ipip1# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-ipip1# tunnel source 192.168.8.8
admin@GUARD-conf-if-ipip1# tunnel destination 192.168.250.2
```

BGP Statements

You can enter the Guard router BGP configuration as described in the "Guard BGP Configuration" section.

Set the neighbor IP address to 192.168.8.1.

Injection Configuration

The next-hop router in the example is R2. To configure traffic injection from the Guard to the zone, add a static route to the next-hop router.

You should configure the static route at the Guard's router configuration level.

The following example shows how to configure a static route for the zone's network (192.168.240.0/24) via the tunnel interface on R1, 192.168.121.2:

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.121.2
```

Cisco Router Tunnel Diversion Configuration

Tunnel forwarding requires that you configure the router at the end of the tunnel (R2 in Figure 4-7). The diversion process requires that you configure the divert-from router (R1 in Figure 4-7).

R1 Diversion Configuration: BGP Statements

You can enter the router, R1, BGP configuration as described in the "Cisco Router BGP Configuration" section.

R2 Forwarding Configuration: Tunnel Interface on R2

The following example shows how to configure the tunnel on router R2:

```
interface tunnel 1
 description << GRE tunnel to Guard  >>
 ip address 192.168.121.2 255.255.255.252
 load-interval 30
```

```
tunnel source 192.168.250.2
tunnel destination 192.168.8.8
```

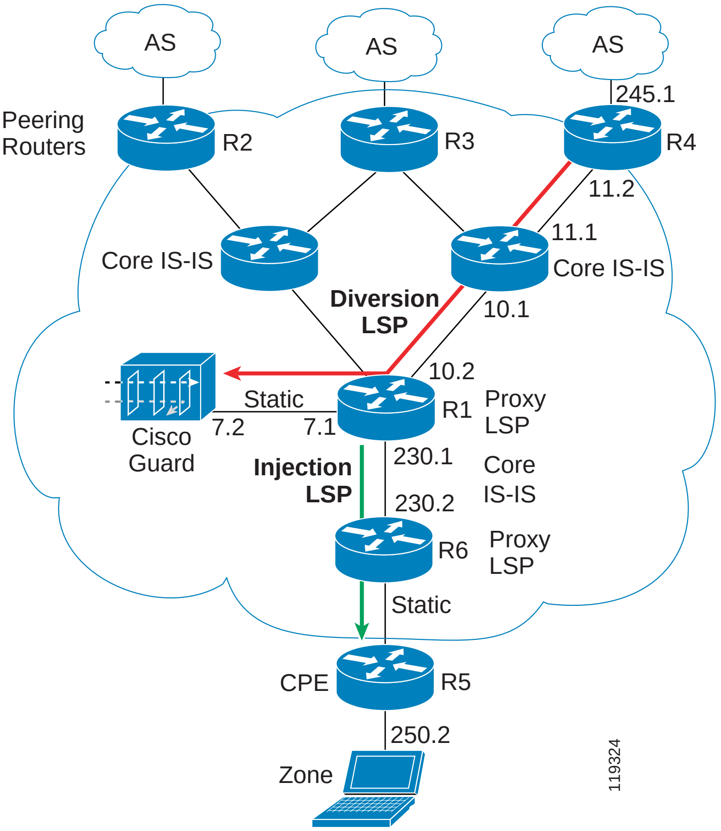
Long Diversion Method

Unlike standard diversion techniques where the Guard diverts traffic only from an adjacent directly connected router, the long diversion method diverts traffic from remotely located peering routers that may reside several hops away from the Guard.

Figure 4-8 includes the following network elements:

- Peering router (R4)
- Guard's adjacent router (R1)
- Zone's edge router (R6)
- Cisco Guard

Figure 4-8 Long Diversion Configuration



This section contains the following topics:

- Packet Flow Example
- Long Diversion Configuration

Packet Flow Example

The traffic flows to the zone's IP addresses (based on the loopback address that holds the Label Switched Path [LSP]).

Once an attack is identified, you activate the Guard to protect the attacked zone. The following steps automatically take place:

1. The Guard informs the peering routers (R2, R3, R4) about a new route to the zone. The next hop is defined as the Guard's loopback interface.
2. The zone's traffic is routed by the peering routers over the diversion LSP to the zone.
3. The Guard forwards the clean traffic to R1.
4. R1 performs an IP lookup and routes the packets, on the appropriate LSP, to the zone.

Long Diversion Configuration

The configuration in the following example refers to the network in Figure 4-8.

Guard Long Diversion Configuration

This section describes the Guard long diversion configurations.

Guard CLI Loopback Configuration

The following example shows how to add a loopback interface to the Guard:

```
admin@GUARD# configure
admin@GUARD-conf# interface lo:2
admin@GUARD-conf-if-lo:2# ip address 1.1.1.1 255.255.255.255
admin@GUARD-conf-if-lo:2# no shutdown
admin@GUARD-conf-if-lo:2# exit
For changes to take effect you need to reload the software.
Type 'yes' to reload now, or any other key to reload manually later
yes
reloading...
```

Zebra CLI Loopback Configuration

The following example shows how to use the Zebra application to add a loopback interface to the routing configuration.

Note For more information about the Zebra application, see http://www.zebra.org.

```
router(config)# router bgp 100
router(config-router)# redistribute Guard
router(config-router)# bgp router-id 192.168.8.16
router(config-router)# neighbor 192.168.8.1 remote-as 100
router(config-router)# neighbor 192.168.8.1 description << iBGP session to peering Router
>>
router(config-router)# neighbor 192.168.8.1 soft-reconfiguration inbound
router(config-router)# neighbor 192.168.8.1 route-map _new_next-hop out
router(config-router)# exit
router(config)# route-map _new_next-hop permit 10
router(config-route-map)# set ip next-hop 1.1.1.1
router(config)# ip route 0.0.0.0 0.0.0.0 192.168.7.1
```

Cisco Router Long Diversion Configuration

This section describes the Cisco router long diversion configuration.

Peering Router Configuration (R2, R3, and R4)

The sample configuration in this section applies to the peering routers: R2, R3, and R4 (see Figure 4-8). This section displays only the commands relevant to long diversion configuration.

The following example shows how to configure Multiprotocol Label Switching (MPLS) on the peering routers:

```
mpls ip
ip cef
```

The following example shows how to configure the loopback 0 interface. This interface will be used to build the LSP via Intermediate System-to-Intermediate System (IS-IS).

```
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
 no ip directed-broadcast
 load-interval 30
```

The following example shows how to configure the network connectivity interfaces:

```
interface fastEthernet 5/0
 ip address 192.168.11.2 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 tag-switching ip (enable MPLS)
 no cdp enable
```

The following example shows how to configure IS-IS:

```
router isis
 redistribute static ip
 net 49.0001.0000.0000.0003.00
```

The following example shows how to configure iBGP to the Guard:

```
router(config)# router bgp 100
R7200(config-router)# no synchronization
R7200(config-router)# bgp log-neighbor-changes
R7200(config-router)# neighbor 192.168.8.16 remote-as 100
R7200(config-router)# neighbor 192.168.8.16 description << iBGP to the Guard >>
R7200(config-router)# neighbor 192.168.8.16 soft-reconfiguration inbound
```

Adjacent Router Configuration (R1)

The sample configuration in this section applies to the adjacent router R1 (see Figure 4-8). This section displays only the commands relevant to long diversion configuration.

The following example shows how to configure the loopback 0 interface. This interface will be used to build the LSP via IS-IS.

```
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
 no ip directed-broadcast
```

The following example shows how to configure the network connectivity interfaces:

```
interface fastEthernet 5/0
 ip address 192.168.10.2 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 tag-switching ip (enable MPLS)
 no cdp enable
```

The following example shows how to configure the interface to the Guard.

Note MPLS is not configured on this interface.

```
interface FastEthernet1/0
 ip address 192.168.7.1 255.255.255.0
 no ip directed-broadcast
```

The following example shows how to configure the interface to the Guard.

Note MPLS is configured on this interface.

```
interface fastEthernet 0/1/1
 ip address 192.168.230.1 255.255.255.0
 tag-switching ip (enable MPLS)
 no cdp enable
```

The following example shows how to configure IS-IS:

```
router isis
 redistribute static ip
 net 49.0001.0000.0000.0002.00
```

The following example shows how to configure a static route on the egress proxy-LSR to the Guard loopback IP address (the IP address 1.1.1.1 is the loopback address configured on the Guard):

```
ip classless
ip route 1.1.1.1 255.255.255.255 192.168.7.2
```

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	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. The following bandwidth-limited link zone templates are available for 128-Kb, 1-Mb, 4-Mb, and 512-Kb links: GUARD_LINK_128K GUARD_LINK_1M GUARD_LINK_4M GUARD_LINK_512K
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	Zone template designed for a zone that contains a VoIP[3] server that uses SIP[4] over UDP to establish VoIP sessions and RTP/RTCP[5] to transmit voice data between SIP end points after sessions are established. 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).

[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
zone-name	Name of the zone. Enter one of the following zone name types: • 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.
template-name	(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. SeeTable 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
new-zone-name	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.
zone-name	Name of an existing zone.
snapshot-id	(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.
rate	Integer greater than 64 that specifies the amount of traffic that is allowed to pass to the zone. The units are specified by the *rate-units* argument. The *rate* limit can be up to 10 times greater than the *burst* limit.
burst	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 *rate-units* argument. The *burst* limit can be up to eight times greater than the *rate* limit.
rate-units	Rate units. The units are as follows: • **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.
ip-addr	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.
ip-mask	(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
zone *zone-name*	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.
server	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
full-file-name	Complete name of the file. If you do not specify a path, the server saves the file in your home directory.
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Detector prompts you for it.
file-server-name	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.
destination-file-name	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.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	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
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for it.
source-file-name	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.

CHAPTER 6

Configuring Zone Filters

This chapter describes how to configure the Cisco Guard (Guard) network traffic filters.

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 Zone Filters
- Configuring Flex-Content Filters
- Configuring Bypass Filters
- Configuring User Filters
- Configuring Dynamic Filters

Understanding Zone Filters

Zone filters define how the Guard handles a specific traffic flow. You can configure filters to customize the traffic flow and control the Distributed Denial of Service (DDoS) attack mitigation operation.

Zone filters enable the Guard to perform the following functions:

- Analyze zone traffic for anomalies
- Apply the basic or strong level of protection to separate legitimate traffic from malicious traffic
- Drop malicious packets
- Forward traffic directly to the zone, bypassing the Guard protection features

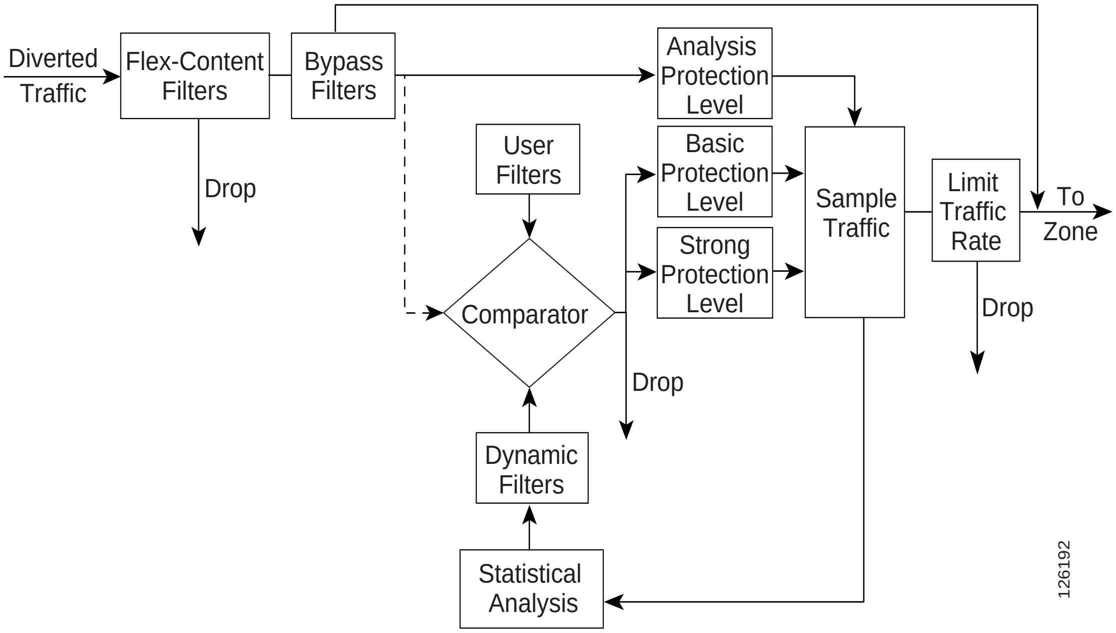
The Guard has the following types of filters:

- User filters—Apply the required protection level to the specified traffic flow. User filters define the first actions that the Guard takes when it identifies abnormal or malicious traffic. The zone configuration includes a default set of user filters configured for on-demand protection that can handle a wide range of attack types. You can modify user filters to customize the Guard protection capabilities and to set rules about how the Guard handles traffic flows when an attack is suspected. See the "Configuring User Filters" section on page 6-13 for more information.

- Bypass filters—Prevent the Guard from analyzing specific traffic flows. You can direct trusted traffic away from the Guard protection features and forward it directly to the zone. See the "Configuring Bypass Filters" section on page 6-11 for more information.
- Flex-content filters—Count or drop a specific traffic flow. Flex-content filters provide extremely flexible filtering capabilities, such as filtering according to fields in the IP and TCP headers, filtering based on the payload content, and filtering based on complex Boolean expressions. See the "Configuring Flex-Content Filters" section on page 6-3 for more information.
- Dynamic filters—Apply the required protection level to the specified traffic flow. The Guard creates dynamic filters based on the analysis of traffic flow and continuously modifies this set of filters to zone traffic and the type of DDoS attack. The dynamic filters have a limited life span and are deleted by the Guard when the attack ends. See the "Configuring Dynamic Filters" section on page 6-18 for more information.

Figure 6-1 displays the Guard filter system.

Figure 6-1 Guard FIlter System



When zone protection is enabled either by a user action or by a remote network-sensing DDoS element, such as the Detector, the Guard diverts the zone traffic to itself and analyzes the traffic.

The Guard monitors the rate of the traffic that flows to the zone. It drops traffic that exceeds the defined rate and forwards the legitimate traffic to the zone. The Guard performs statistical analysis of zone traffic and performs a closed-loop feedback cycle to adjust the protection measures to the dynamically changing zone traffic characteristics and the changing DDoS attack types.

To perform statistical analysis of traffic flow, the Guard uses the zone policies which are all configured to handle specific types of traffic. The zone policies constantly measure traffic flows and take action against a particular traffic flow if they identify that flow as malicious or abnormal, which occurs when the flow exceeds the policy threshold.

When the Guard identifies a traffic anomaly, it performs the following tasks:

1. Produces dynamic filters that are configured with actions to handle the attack. The Guard, by default, adds an initial dynamic filter that directs all traffic to user filters which provide the first line of defense against an evolving DDoS attack. Once the Guard has had enough time to analyze the attack, it begins producing dynamic filters to mitigate the attack.
2. Changes the flow of traffic within the Guard. Abnormal traffic flows into the Comparator, which is a component that receives input from the dynamic filters and the user filters. The Comparator compares the first user filter that matches the flow with the dynamic filters and chooses the most severe protection measure suggested. It applies the relevant protection level to authenticate the traffic.

By default, the Guard protects the zone until you deactivate zone protection.

Configuring Flex-Content Filters

Flex-content filters filter the zone traffic based on the fields in the packet header or the patterns in the packet payload. You can identify attacks that are based on the patterns that appear in the traffic. These patterns can identify known worms or flood attacks that have a constant pattern.

Use the flex-content filters to drop or count a desired packet flow and to identify a specific malicious source of traffic.

The flex-content filter applies the filtering criteria in the following order:

1. Filters packets based on the protocol and the port parameter values.
2. Filters packets based on the tcpdump-expression value.
3. Performs pattern matching with the pattern-expression value on the remaining packets.

Note Flex-content filters consume a lot of CPU resources. We recommend that you limit the use of flex-content filters because they might affect the performance of the Guard. If you are using a flex-content filter to protect a specific attack that can be identified by a dynamic filter, such as TCP traffic to a specified port, we recommend that you filter the traffic using a dynamic filter.

This section contains the following topics:

- Adding a Flex-Content Filter
- Displaying Flex-Content Filters
- Deleting Flex-Content Filters
- Changing the State of a Flex-Content Filter

Adding a Flex-Content Filter

The Guard creates a list of flex-content filters that you create and activates the filters in an ascending order. When you add a new flex-content filter, make sure that you place it in the correct location in the filter list.

The Guard stops activating the flex-content filters when traffic matches a flex-content filter with a drop action.

To configure a flex-content filter, perform the following steps:

Step 1 Display the list of flex-content filters and identify the location in the list in which you want to add the new filter (see the "Displaying Flex-Content Filters" section on page 6-9).

Step 2 If the current row numbers are consecutive, renumber the flex-content filters in increments that allow you to insert the new flex-content filter by entering the following command in zone configuration mode:

```
flex-content-filter renumber [start [step]]
```

Table 6-1 provides the arguments for the **flex-content-filter renumber** command.

Table 6-1 Arguments for the flex-content-filter renumber Command

Parameter	Description
start	(Optional) Integer from 1 to 9999 that denotes the new starting number of the flex-content filter list. The default is 10.
step	(Optional) Integer from 1 to 999 that defines the increment between the flex-content filter row numbers. The default is 10.

Step 3 (Optional) Filter a pattern expression of an ongoing attack or an attack that you have previously recorded. Activate the Guard to generate a signature of the attack by using the **show packet-dump signatures** command. See the "Generating Attack Signatures from Packet-Dump Capture Files" section on page 12-18 for more information.

Step 4 Add a new flex-content filter by entering the following command:

```
flex-content-filter row-num {disabled | enabled} {drop | count} protocol port [start
start-offset [end end-offset]] [ignore-case] expression tcpdump-expression pattern
pattern-expression
```

Table 6-2 provides the arguments and keywords for the **flex-content-filter** command.

Table 6-2 Arguments and Keywords for the flex-content-filter Command

Parameter	Description
row-num	Unique number from 1 to 9999 that identifies the filter and defines the priority among the flex-content filters. The Guard operates the filters in ascending row-number order.
disabled	Sets the filter state to disabled. The filter does not monitor traffic.
enabled	Sets the filter state to enabled. The Guard monitors traffic and performs the action (drop or count) on the flow that matches the filter. This is the default state.
drop	Drops the flow that matches the filter.
count	Counts the flow that matches the filter.
protocol	Traffic from a specific protocol. Use an asterisk (*****) to indicate any protocol. Enter an integer from 0 to 255. Review possible protocol numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/protocol-numbers

Table 6-2 Arguments and Keywords for the flex-content-filter Command (continued)

Parameter	Description
port	Traffic destined to a specific destination port. Enter an integer from 0 to 65535. To define a specific port number, you must define a specific protocol number. Use an asterisk (*****) to indicate any destination port. You can use an asterisk if you configure the protocol number to 6 (TCP) or 17 (UDP). Review possible port numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/port-numbers
start-offset	Offset, in bytes, from the beginning of the packet payload, where the pattern matching for the *pattern-expression* argument begins. The default is 0, which is the start of the payload. Enter an integer from 0 to 1800. If you copy the pattern from the **show packet-dump signatures** command output, copy this argument from the Start Offset field in the command output.
end-offset	Offset, in bytes, from the beginning of the packet payload, where the pattern matching for the *pattern-expression* argument ends. The default is the packet length, which is the end of the payload. Enter an integer from 0 to 1800. If you copy the pattern from the **show packet-dump signatures** command output, copy this argument from the End Offset field in the command output.
ignore-case	Defines the *pattern-expression* argument as case insensitive. By default, the *pattern-expression* argument is case sensitive.
tcpdump-expression	Expression that is matched with the packet. The expression is in Berkeley Packet filter format. See the "Configuring the tcpdump-expression Syntax" section on page 6-6 for more information and configuration examples. If you use spaces in the expression, enclose the expression in quotation marks (" "). To enter an empty expression, use double quotation marks (" "). To use a quotation mark in the expression, use the backslash escape character before the quotation mark (\"). **Note** Help is not available for the tcpdump-expression syntax.
pattern-expression	Regular expression data pattern that is to be matched with the packet payload. See the "Configuring the pattern-expression Syntax" section on page 6-8 for more information. You can activate the Guard to generate the signature by using the **show packet-dump signatures** command. See the "Generating Attack Signatures from Packet-Dump Capture Files" section on page 12-18. If you use spaces in the expression, enclose the expression in quotation marks (" "). To enter an empty expression, use double quotation marks (" "). To use a quotation mark in the expression, use the backslash escape character before the quotation mark (\"). **Note** Help is not available for the pattern-expression syntax.

You can change the filter state to enable or disable at any time. See the "Changing the State of a Flex-Content Filter" section on page 6-10 for more information.

You can delete a filter at any time (see the “Deleting Flex-Content Filters” section on page 6-10).

The following example shows how to configure the flex-content filter:

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * * expression “ip[6:2] &
0x1fff=0” pattern
“/ HTTP/1\.1\ x0D\0AAccept: .*/.*\x0D\x0AAccept-Language: en*\x0D\x0AAccept-Encoding:
gzip, deflate\x0D\x0AUser-Agent: Mozilla/4\.0”
```

This section contains the following topics:

- Configuring the tcpdump-expression Syntax
- Configuring the pattern-expression Syntax

Configuring the tcpdump-expression Syntax

The tcpdump-expression is in the Berkeley Packet filter format and specifies the expression to be matched with the packet.

Note You can use the tcpdump-expression to filter traffic based on the destination port and protocol, but the performance of the Guard may be affected. We recommend that you filter traffic based on these criteria using the flex-content filter *protocol* and *port* arguments.

The expression contains one or more elements which usually consist of an ID preceded by one or more qualifiers.

There are three types of qualifiers:

- Type qualifiers—Define the ID (name or number). Possible types are **host**, **net**, and **port**. The **host** type qualifier is the default.
- Direction qualifiers—Define the transfer direction. Possible directions are **src**, **dst**, **src or dst**, and **src and dst**. The direction qualifier **src or dst** is the default.
- Protocol qualifiers—Restrict the match to a particular protocol. Possible protocols are **ether**, **ip**, **arp**, **rarp**, **tcp**, and **udp**. If you do not specify a protocol qualifier, all protocols that apply to the type are matched. For example, port 53 means TCP or UDP port 53.

Table 6-3 describes the tcpdump-expression elements.

Table 6-3 tcpdump-expression Elements

Element	Description
dst host *host_ip_address*	Traffic to a destination host IP address.
src host *host_ip_address*	Traffic from a source host IP address.
host *host_ip_ address*	Traffic to and from both source and destination host IP addresses.
net *net* **mask** *mask*	Traffic to a specific network.
net *net/len*	Traffic to a specific subnet.
dst port *destination_port_number*	TCP or UDP traffic to a destination port number.

Table 6-3 tcpdump-expression Elements (continued)

Element	Description
src port *source_port_number*	TCP or UDP traffic from a source port number.
port *port_number*	TCP or UDP traffic to and from both source and destination port numbers.
less *packet_length*	**Packets with a length equal to or less than the specific length in bytes.**
greater *packet_length*	Packets with a length equal to or greater than the specific length in bytes.
ip proto *protocol*	Packets with a protocol number of the following protocols: ICMP, UDP, and TCP.
ip broadcast	Broadcast IP packets.
ip multicast	Multicast packets.
ether proto *protocol*	Ether protocol packets of a specific protocol number or name such as IP, ARP, or RARP. The protocol names are also keywords. If you enter the protocol name, you must use a backslash (\) as an escape character before the name.
expr relop expr	Traffic that complies with the specific expression. Table 6-4 describes the tcpdump-expression rules.

Table 6-4 describes the tcpdump-expression rules.

Table 6-4 Flex-Content Filter Expression Rules

Expression Rule	Description
relop	>, <, >=, <=, =, !=
expr	Arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+, -, *, /, &, |], a length operator, and special packet data accesses. To access data inside the packet, use the following syntax: *proto* [*expr*: *size*]
proto	Protocol layer for the index operation. **The possible values are** ether, ip, tcp, udp, or icmp. The byte offset, relative to the indicated protocol layer, is given by the *expr* value. To access data inside the packet, use the following syntax: *proto* [*expr*: *size*] The *size* argument is optional and indicates the number of bytes in the field. The argument can be 1, 2, or 4. The default is 1.

You can combine expression elements using the following methods:

- A group of elements and operators in parentheses—The operators are the normal binary operators [+, -, *, /, &, |] and a length operator.

Note To use a parenthesis in the expression, use the backslash escape character before the parenthesis (\( ).

- Negation—Use **!** or **not**.
- Concatenation—Use **&&** or **and**.
- Alternation—Use || or **or**.

Negation has the highest precedence. Alternation and concatenation have equal precedence and are associated from left to right. Explicit and tokens, not juxtaposition, are required for concatenation. If you specify an identifier without a keyword, the most recent keyword is used.

For a detailed explanation of the Berkeley Packet filter configuration options, go to this location:

http://www.freesoft.org/CIE/Topics/56.htm.

The following example shows how to count unfragmented datagrams and fragmented zeros of fragmented datagrams only. This filter is implicitly applied to the TCP and UDP index operations. For instance, tcp[0] always indicates the first byte of the TCP header and never indicates the first byte of an intervening fragment as shown in this example:

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * * expression
ip[6:2]&0x1fff=0 pattern ""
```

The following example shows how to drop all TCP RST packets:

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled drop * * expression tcp[13]&4!=0
pattern ""
```

The following example shows how to count all ICMP packets that are not echo requests/echo replies (ping):

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * * expression "icmp
[0]!=8 and icmp[0] != 0" pattern ""
```

The following example shows how to count all TCP packets that are destined to port 80 and that did not originate from port 1000:

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled count * * expression "tcp and
dst port 80 and not src port 1000" pattern ""
```

Configuring the pattern-expression Syntax

The pattern-expression syntax is a regular expression that describes a string of characters. The pattern-expression describes a set of strings without actually listing its elements. This expression consists of normal characters and special characters. Normal characters include all printable ASCII characters that are not considered to be special characters. Special characters have a special meaning and specify the type of matching that the Guard performs on the pattern-expression. The flex-content filter matches the pattern-expression with the content of the packet (the packet payload). For example, the three strings version 3.1, version 4.0, and version 5.2 are described by the following pattern: version .*\..*

Table 6-5 describes the special characters that you can use.

Table 6-5 Special Characters Used in the pattern-expression

Special character	Description
.*	Matches a string that may be present and can contain zero or more characters. For example, the pattern goo.*s matches the patterns goos, goods, good for ddos, and so on.
\	Removes the special meaning of a special character. To use the special characters in this list as single-character patterns, remove the special meaning by preceding each character with a backslash (\). For example, two backslashes (\\) match one backslash (\), and one backslash and a period (\.) match one period (.). You must also precede an asterisk (*) with a backslash.
\xHH	Matches a hexadecimal value, where H is a hexadecimal digit and is not case sensitive. Hexadecimal values must be exactly two digits. For example, the pattern \x41 matches the hexadecimal value A.

By default, the pattern-expression is case sensitive. To define the pattern-expression as case insensitive, use the **flex-content-filter** command with the **ignore-case** keyword. See the "Adding a Flex-Content Filter" section on page 6-3 for more information.

The following example shows how to drop packets with a specific pattern in the packet payload. The pattern in the example was extracted from the Slammer worm. The *protocol*, *port*, and *tcpdump-expression* parameters are nonspecific.

```
user@GUARD-conf-zone-scannet# flex-content-filter enabled drop * * expression " " pattern
\x89\xE5Qh\.dllhel32hkernQhounthickChGetTf\xB9ll
Qh32\.dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

Displaying Flex-Content Filters

To display the flex-content filters, use the following command in zone configuration mode:

show flex-content-filters

Table 6-6 describes the fields in the **show flex-content-filters** command output.

Table 6-6 Field Descriptions for the show flex-content-filters Command

Field	Description
Row	Flex-content filter priority.
State	Filter state (enabled or disabled).
Action	Action that the filter performs on the specific traffic type.
Protocol	Protocol number of the traffic that the filter processes.
Port	Destination port of the traffic that the filter processes.
Start	Offset, in bytes, from the beginning of the packet payload where the pattern matching begins. This offset applies to the *pattern* field.

Table 6-6 Field Descriptions for the show flex-content-filters Command (continued)

Field	Description
End	Offset, in bytes, from the beginning of the packet payload where the pattern matching ends. This offset applies to the *pattern* field.
Match-case	Whether the pattern-expression that the filter matches is case sensitive or not case sensitive. yes = case-sensitive, no = case-insensitive
TCPDump-expression	tcpdump-expression to be matched with the packet in Berkeley Packet filter format. See the "Configuring the tcpdump-expression Syntax" section on page 6-6 for the information on the tcpdump-expression syntax.
Pattern-filter	Regular expression data pattern to be matched with the packet payload. See the "Configuring the pattern-expression Syntax" section on page 6-8 for information on the pattern-expression syntax.
RxRate (pps)	Current traffic rate in packets per second that is measured for this filter.

Deleting Flex-Content Filters

You can delete a flex-content filter when you no longer need it to filter packets based on the filter expression.

Note Do not delete a flex-content filter if you might need it at a later date. You can disable the flex-content filter and then enable it when needed (see the "Changing the State of a Flex-Content Filter" section on page 6-10).

To delete a flex-content filter, enter the following command in zone configuration mode:

no flex-content-filter *row-num*

The *row-num* argument specifies the flex-content filter row number to delete. To display the list of flex-content filters and identify the row number of the flex-content filter to delete, use the **show flex-content-filters** command (see the "Displaying Flex-Content Filters" section on page 6-9). To delete all flex-content filters, enter an asterisk (*****) for the row number.

The following example shows how to delete a flex-content filter:

```
user@GUARD-conf-zone-scannet# no flex-content-filters 5
```

Changing the State of a Flex-Content Filter

You can disable a flex-content filter to prevent the Guard from filtering packets based on the filter expression and to prevent it from filtering specific types of traffic. When you disable the filter, it remains in the flex-content filter list, which allows you to enable the filter again if needed.

If you do not intend to use a flex-content filter again, you can delete it (see the "Deleting Flex-Content Filters" section on page 6-10).

To change the state of a flex-content filter, enter the following command in zone configuration mode:

flex-content-filter *row-num* {**disabled** | **enabled**}

The *row-num* argument specifies the flex-content filter row number. To display the list of flex-content filters and identify the row number of the flex-content filter to enable or disable, enter the **show flex-content-filters** command (see the "Displaying Flex-Content Filters" section on page 6-9).

The following example shows how to disable a flex-content filter:

```
user@GUARD-conf-zone-scannet# flex-content-filters 5 disabled
```

Configuring Bypass Filters

The bypass filter allows you to specify traffic that you want the Guard to forward directly to the zone without applying any traffic protection functions, including the anti-spoofing and anti-zombie functions.

Note The Guard injects traffic that passes through the bypass filters on to the zone without applying a limit on the traffic rate that was defined by using the **rate-limit** command.

This section contains the following topics:

- Adding a Bypass Filter
- Displaying Bypass Filters
- Deleting Bypass Filters

Adding a Bypass Filter

To add a bypass filter, use the following command in zone configuration mode:

bypass-filter *row-num src-ip* [*ip-mask*] *protocol dest-port* [*fragments-type*]

Table 6-7 provides the arguments for the **bypass-filter** command.

Table 6-7 Arguments for the bypass-filter Command

Parameter	Description
row-num	Unique number from 1 to 9999. The row-number identifies the filter and defines the priority among the bypass filters. The Guard operates the filters according to the ascending row-number order.
src-ip	Traffic from a specific IP address is processed. Use an asterisk (*****) to indicate any IP address.
ip-mask	(Optional) Traffic from a specific subnet is processed. The subnet mask can contain only Class C values. The default subnet is 255.255.255.255.
protocol	Traffic from a specific protocol is processed. Use an asterisk (*****) to indicate any protocol. Review possible protocol numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/protocol-numbers

Table 6-7 Arguments for the bypass-filter Command (continued)

Parameter	Description
dest-port	Traffic to a specific destination port is processed. Use an asterisk (*****) to indicate any destination port. Review possible port numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/port-numbers
fragments-type	(Optional) Whether or not the filter processes fragmented traffic. The three fragmented types are as follows: • **no-fragments**—Nonfragmented traffic • **fragments**—Fragmented traffic • **any-fragments**—Fragmented and nonfragmented traffic The default is **no-fragments**.

Note You cannot specify both a fragments type and a destination port. To set the fragments type, enter an asterisk (*****) for the destination port.

Displaying Bypass Filters

To display the list of bypass filters, use the following command in zone configuration mode:

show bypass-filters

Table 6-8 describes the fields in the **show bypass-filters** command output.

Table 6-8 Field Descriptions for the show bypass-filters Command

Field	Description
Row	Bypass filter priority.
Source IP	Source IP address of the traffic that the filter processes.
Source Mask	Source address subnet mask of the traffic that the filter processes.
Proto	Protocol number of the traffic that the filter processes.
DPort	Destination port of the traffic that the filter processes.
Frg	Fragmentation settings that the filter processes: • **yes**—The filter processes fragmented traffic. • **no**—The filter processes nonfragmented traffic. • **any**—The filter processes both fragmented and nonfragmented traffic.
RxRate (pps)	Current traffic rate in packets per second that is measured for this filter.

The source IP address, source address mask, protocol number, and destination port may be nonspecific. An asterisk (*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

Deleting Bypass Filters

To delete a bypass filter, enter the following command in zone configuration mode:

no bypass-filter *row-num*

The *row-num* argument specifies the bypass filter row number to be deleted. To delete all bypass filters, enter an asterisk (*****). To display the list of bypass filters and identify the row number of the bypass filter that you want to delete, use the **show bypass-filters** command (see the "Displaying Bypass Filters" section on page 6-12). To delete all bypass filters, enter an asterisk (*****) for the row number.

The following example shows how to delete a bypass filter:

```
user@GUARD-conf-zone-scannet# no bypass-filter 10
```

Configuring User Filters

User filters define the first actions that the Guard executes when it identifies abnormal or malicious traffic. User filters either apply the required protection level to the specified traffic flows or they drop the specified traffic.

Each zone configuration includes a default set of user filters that are configured for on-demand protection and can handle a wide range of attack types. You can modify user filters to customize the Guard protection capabilities and to set rules about how the Guard handles specific traffic flows when it suspects an attack.

During an attack on the zone, the Guard continuously analyzes the traffic going to the zone. When it detects abnormal traffic patterns, the user filters provide the first line of defense against the evolving DDoS attack. Once the Guard has had enough time to analyze the attack, it begins producing dynamic filters that define how to handle the attack.

The Guard examines both the user filters and the dynamic filters before deciding how to handle the specific traffic flow. It compares the first user filter that matches the flow with the dynamic filters and chooses the most severe protection measure suggested. It applies the appropriate protection level to the traffic flow to authenticate the traffic. See the "Configuring Dynamic Filters" section on page 6-18 for more information about Dynamic filters.

The dynamic filters and the user filters can take actions in these descending severity levels: drop, strong, basic, and permit (see Table 6-9). Dynamic filters with actions of redirect/zombie and block-unauthenticated are applied even if a user filter to handle the same type of traffic exists because dynamic filters affect the Guard traffic authentication mechanisms and do not directly affect the traffic flow.

User filters are activated in ascending row-number order. When you add a new user filter, it is important that you place it in the correct location in the list.

Table 6-9 describes the actions that a user filter can take.

Table 6-9 User Filter Actions

Action	Description
basic/default	Authenticates non-TCP traffic flows.
basic/dns-proxy	Authenticates TCP DNS traffic flows.
basic/redirect	Authenticates applications over HTTP.
basic/reset	Authenticates applications over TCP. We recommend that you use an action of basic/redirect for HTTP traffic flows.
basic/safe-reset	Authenticates TCP application traffic flows that are not tolerant of TCP connection reset. We recommend that you use an action of basic/redirect for HTTP traffic flows.
basic/sip	Authenticates VoIP[1] applications that use SIP[2] over UDP to establish the VoIP sessions and RTP/RTCP[3] to transmit voice data between the SIP end points after sessions are established.
drop	Drops traffic flows.
permit	Prevents statistical analysis of the flow and the anti-spoofing or anti-zombie protection functions from handling this flow. We recommend that you set a rate and burst limit to this filter because it is not handled by other protection mechanisms.
strong	Enables strong authentication for a traffic flow. Use this filter when strong authentication is required or when the previous filters do not seem suitable for the application. Authentication is performed for every connection. For TCP incoming connections, the Guard serves as a proxy. Do not use the strong authentication action for connections if you use ACLs[4], access policies, or load-balancing policies that are based on the incoming IP address in the network.

[1] VoIP = Voice over IP

[2] SIP = Session Initiation Protocol

[3] RTP/RTCP = Real-Time Transport Protocol/Real-Time Control Protocol

[4] ACL = Access Control List

This section contains the following topics:

- Adding User Filters
- Displaying User Filters
- Deleting User Filters

Adding User Filters

To add a user filter, perform the following steps:

Step 1 Display the list of user filters and identify the location in the list in which you want to add the new filter. See the "Displaying User Filters" section on page 6-17 for more information.

Step 2 If the current row numbers are consecutive, renumber the user filters in increments that allow you to insert the new user filters by entering the following command:

```
user-filter renumber [start [step]]
```

Table 6-10 provides the arguments for the **user-filter renumber** command.

Table 6-10 Arguments for the user-filter renumber Command

Parameter	Description
start	(Optional) Integer from 1 to 10000 that denotes the new starting number of the user filter list. The default is 10.
step	(Optional) Integer from 1 to 1000 that defines the increment between the user filter row numbers. The default is 10.

Step 3 Add a new user filter by entering the following command:

```
user-filter row-num filter-action src-ip [ip-mask] protocol dest-port [fragments-type]
[rate-limit rate burst units]
```

Table 6-11 provides the arguments for the **user-filter** command.

Table 6-11 Arguments and Keywords for the user-filter Command

Parameter	Description
row-num	Unique number from 1 to 1000 that identifies the filter and defines priority among the user filters. The Guard operates the filters according to the ascending row-number order.
filter-action	Action that the filter performs on the specific traffic type. See Table 6-9 for more information.
src-ip	Traffic from a specific IP address. Use an asterisk (*****) to indicate any IP address.
ip-mask	(Optional) Traffic from a specific subnet. The subnet mask can contain only Class C values. The default subnet is 255.255.255.255.
protocol	Traffic from a specific protocol. Use an asterisk (*****) to indicate any protocol. Review possible protocol numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/protocol-numbers
dest-port	Traffic to a specific destination port. Use an asterisk (*****) to indicate any destination port. Review possible port numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/port-numbers
fragments-type	(Optional) Type of traffic. The type can be one of the following: • **no-fragments**—Nonfragmented traffic • **fragments**—Fragmented traffic • **any-fragments**—Fragmented and nonfragmented traffic The default is **no-fragments**.
rate-limit *rate*	Specifies the rate limitation. The user filter limits the traffic to this rate. Enter an integer greater than 64. The units are specified by the *units* parameter. The default is not to limit the filter traffic rate. The *rate* limit can be up to 10 times greater than the *burst* limit.
burst	Integer greater than 64 that specifies the traffic burst limit. The units are bits, kilobits, kilopackets, megabits, and packets that correspond to the units that are specified by the *units* parameter. The *burst* limit can be up to eight times greater than the *rate* limit.
units	Rate limit units. The units can be one of the following: • **bps—**Bits per second • **kbps—**Kilobits per second • **kpps—**Kilo packets per second • **mbps—**Megabits per second • **pps—**Packets per second

The following example shows how to renumber the user filters starting from 10 in steps of 5. This example also shows how to add a user filter in row 12 that is aimed at traffic that is received from all source IP addresses of protocol 6 (TCP) and flows to destination port 25 (SMTP). The user filter limits the traffic flow rate to 600 pps and the burst size to 400 packets.

```
user@GUARD-conf-zone-scannet# user-filter renumber 10 5
user@GUARD-conf-zone-scannet# user-filter 12 permit * 6 25 rate-limit 600 400 pps
```

Displaying User Filters

You can display the user filters associated with a zone configuration by entering the **show** command or the **show running-config** command in zone configuration mode.

Tip To display the user filter configuration at the beginning of the display, use the **show** command or the **show running-config** command with the **| begin USER FILTERS** option.

Table 6-12 describes the user filter fields in the **show** command output.

Table 6-12 Field Descriptions for User Filter Fields in the show Command

Field	Description
Row	User filter priority.
Source IP	Source IP address of the traffic that the filter processes.
Source Mask	Source address mask of the traffic that the filter processes.
Proto	Protocol number of the traffic that the filter processes.
DPort	Destination port of the traffic that the filter processes.
Frg	Type of traffic that the filter processes. The type can be one of the following: • **yes**—The filter processes fragmented traffic. • **no**—The filter processes nonfragmented traffic. • **any**—The filter processes fragmented and nonfragmented traffic.
RxRate (pps)	Current traffic rate in packets per second that is measured for this filter.
Action	Action that the filter performs on the specific traffic type. See Table 6-9 for more information.
Rate	Limit on the traffic rate that the user filter can handle. The rate is displayed in the units specified by the *Units* field.
Burst	Traffic burst limit that the filter allows for the specific flow. The units are bits, kilobits, kilopackets, megabits, and packets, and correspond to the units specified in the *Units* field.
Units	Units by which the rate and the burst rate are displayed.

The source IP address, source address mask, protocol number, and destination port may be nonspecific. An asterisk (*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

Deleting User Filters

Caution If you delete all user filters when the policy action is set to **to-user-filter**, the Guard passes unprotected traffic to the zone. See the "Configuring the Policy Action" section on page 7-19 for more information.

To delete a user filter, enter the following command in zone configuration mode:

no user-filter *row-num*

The *row-num* argument specifies the user filter row number. To display the list of user filters and identify the row number of the user filter to delete, use the **show running-config** command (see the "Displaying User Filters" section on page 6-17). To delete all user filters, enter an asterisk (*****) for the row number.

The following example shows how to delete all user filters:

```
user@GUARD-conf-zone-scannet# no user-filter *
```

Configuring Dynamic Filters

Dynamic filters apply the required protection level to traffic flow and define how the Guard mitigates the attack. The Guard creates dynamic filters when it identifies an anomaly in the zone traffic, which occurs when the flow exceeds the zone policy thresholds. The Guard creates new dynamic filters as changes occur to the zone traffic and the type of DDoS attack.

Dynamic filters have a limited life span and are deleted by the Guard when the attack ends. The Guard supports a maximum of 150,000 dynamic filters that are active concurrently in all zones. You can add or delete dynamic filters when the zone is under attack and zone protection is enabled.

When the Guard detects a traffic anomaly, it uses both user filters and dynamic filters to mitigate the attack. The user filters provide the first line of defense until the Guard can analyze the attack and begin creating dynamic filters with mitigation actions designed specifically for the attack. For more information about user filters and how the Guard uses them in combination with the dynamic filters, see the "Configuring User Filters" section on page 6-13.

The dynamic filters and the user filters can take actions in these descending severity levels: drop, strong, basic, and permit (see Table 6-13). Dynamic filters with actions of redirect/zombie and block-unauthenticated are applied even if a user filter to handle the same type of traffic exists because they affect the Guard authentication functions and do not directly affect the traffic flow.

Table 6-13 describes the different actions dynamic filters can execute.

Table 6-13 Dynamic Filter Actions

Action	Description
drop	Drops the traffic.
strong	Applies the strong protection level anti-spoofing functions to the specific traffic.
to-user-filters	Forwards the traffic to the user filters. If you have modified the default user filters, you must make sure that there is a user filter to handle these dynamic filters.

Table 6-13 Dynamic Filter Actions (continued)

Action	Description
block-unauthenticated-basic	Enhances the basic protection level anti-spoofing functions so that they drop traffic flows that have not been authenticated.
block-unauthenticated-strong	Enhances the strong protection level anti-spoofing functions so that they drop traffic flows that have not been authenticated.
block-unauthenticated-dns	Drops the traffic that flows to DNS UDP servers (protocol=UDP, port=53) that were not authenticated by the DNS anti-spoofing functions.
redirect/zombie	Enhances authentication for all user filters with an action of **basic/redirect**.

Dynamic filters are configured to remain active for a specific amount of time. Depending on how the filter was created, the dynamic filter timeout parameter is configured in one of the following ways:

- Dynamic filters created by a zone policy—The dynamic filter timeout is set to the policy timeout. To modify the timeout of additional dynamic filters that are created by the policy, change the timeout of the policy that created the dynamic filter by entering the **timeout** command in policy configuration mode.
- User-defined dynamic filters—You define the dynamic filter timeout by configuring the *exp-time* argument of the **dynamic-filter** command.

When the dynamic filter timeout expires, the Guard determines whether or not the dynamic filter should be deactivated based on current traffic conditions. If the Guard determines that the dynamic filter should not be deactivated, the filter remains active for another time span. See the "Deactivating Dynamic Filters" section on page 6-23 for more information about deactivating dynamic filters.

This section contains the following topics:

- Displaying Dynamic Filters
- Adding Dynamic Filters
- Deleting Dynamic Filters
- Preventing the Production of Dynamic Filters
- Deactivating Dynamic Filters

Displaying Dynamic Filters

You can display the dynamic filters that the Guard created by using one of the following commands in zone configuration mode:

- **show dynamic-filters** [**details**]—Displays a list of all dynamic filters.
- **show dynamic-filters** *dynamic-filter-id* [**details**]—Displays a single dynamic filter.
- **show dynamic-filters sort** {**action** | **exp-time** | **id** | **filter-rate**}—Displays a sorted list of all dynamic filters.

Table 6-14 provides the arguments and keywords for the **show dynamic-filters** command.

Table 6-14 Arguments and Keywords for the show dynamic-filters Command

Parameter	Description
dynamic-filter-id	Identifier of the specific dynamic filter to display. This integer is assigned by the Guard. To identify the filter ID, display the complete list of dynamic filters.
details	(Optional) Displays dynamic filters in detail. The details consist of additional information on the attack flow, the triggering rate, and the policy that produced it.
action	Displays dynamic filters by their action, ranging from the most severe (drop) to the least severe (notify).
exp-time	Displays dynamic filters by their expiration time in ascending order.
id	Displays dynamic filters by the ascending ID number.
filter-rate	Displays dynamic filters by the triggering rate, measured in packets per second, in ascending order.

To display the pending dynamic filters, use the **show recommendations** command. See Chapter 10, "Using Interactive Protect Mode," for more information about pending dynamic filters.

Note The Guard displays a maximum of 1000 dynamic filters. When more than 1000 dynamic filters are active, examine the log file or zone report for a complete list of dynamic filters.

The following example shows how to display a dynamic filter in detail:

```
user@GUARD-conf-zone-scannet# show dynamic-filters 876 details
```

Table 6-15 describes the fields in the **show dynamic-filters** command output.

Table 6-15 Field Descriptions for show dynamic-filters Command Output

Field	Description
ID	Filter identification number.
Action	Action that the filter performs on the traffic flow. See Table 6-13 for more information.
Exp Time	Amount of time that the filter is active. After the time expires, the filter may be deleted according to the thresholds that you defined by using the **filter-termination** command.
Source IP	Source IP address of the traffic that the filter processes.
Source Mask	Source address mask of the traffic that the filter processes.
Proto	Protocol number of the traffic that the filter processes.
DPort	Destination port of the traffic that the filter processes.

Table 6-15 Field Descriptions for show dynamic-filters Command Output (continued)

Field	Description
Frg	Whether or not the filter processes fragmented traffic: • **yes**—The filter processes fragmented traffic. • **no**—The filter processes nonfragmented traffic. • **any**—The filter processes both fragmented and nonfragmented traffic.
RxRate (pps)	Current traffic rate in packets per seconds that is measured for this filter.

The source IP address, source address mask, protocol number, and destination port may be nonspecific. An asterisk (*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

Table 6-16 describes the additional fields in the **show dynamic-filters details** command output.

Table 6-16 Field Descriptions for show dynamic-filters details Command

Field	Description
Attack flow	Mitigated attack flow characteristics. The mitigated attack flow, displayed in the dynamic filters table, might have a wider range than the attack flow. For example, a nonspoofed attack on port 80 blocks all TCP traffic from the originating source IP address, not from port 80 only. The attack flow contains the Source IP, Source Mask, Proto, DPort, and Frg fields that are described in Table 6-15.
Triggering Rate	Rate of the attack flow that exceeded a policy threshold.
Threshold	Policy threshold that was exceeded by the attack flow.
Policy	Policy that produced the dynamic filter. See Chapter 7, "Configuring Policy Templates and Policies," for more information.

Adding Dynamic Filters

During an attack on the zone, you can add a dynamic filter to manipulate zone protection by using the following command in zone configuration mode:

dynamic-filter *action* {*exp-time* | **forever**} *src-ip* [*ip-mask*] *protocol dest-port* [*fragments-type*]

You can use multiple **dynamic-filter** commands to add multiple dynamic filters.

Table 6-17 provides the arguments and keywords for the **dynamic-filter** command.

Table 6-17 Arguments and Keywords for the dynamic-filter Command

Parameter	Description
action	Action that the filter performs on a specific traffic flow. See Table 6-13 for more information.
exp-time	Integer from 1 to 3,000,000 that specifies the time (in seconds) for the filter to be active.
forever	Activates the filter for an unlimited time. The filter is deleted when protection ends.

Table 6-17 Arguments and Keywords for the dynamic-filter Command (continued)

Parameter	Description
src-ip	Traffic from a specific source IP address. Enter the IP address in dotted-decimal notation (for example, enter an IP address of 192.168.100.1). Use an asterisk (*****) to indicate any IP address.
ip-mask	(Optional) Traffic from a specific subnet. Enter the subnet mask in dotted-decimal notation (for example, enter 255.255.255.0). The subnet mask can contain only Class C values. The default subnet is 255.255.255.255.
protocol	Traffic from a specific protocol. Use an asterisk (*****) to specify any protocol. Review possible protocol numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/protocol-numbers
dest-port	Traffic that is destined to a specific destination port. Use an asterisk (*****) to specify any destination port. Review possible port numbers at the Internet Assigned Numbers Authority (IANA) website: http://www.iana.org/assignments/port-numbers
fragments-type	(Optional) Traffic type that the filter acts on. The three fragmented types are as follows: • **no-fragments**—nonfragmented traffic • **fragments**—fragmented traffic • **any-fragments**—fragmented and nonfragmented traffic The default is **no-fragments**.

The following example shows how to add a dynamic filter that directs the traffic to the user filters with an expiration time of 600 seconds:

```
admin@GUARD-conf-zone-scannet# dynamic-filter to-user-filters 600 192.128.30.45
255.255.255.252 6 88 no-fragments
```

Deleting Dynamic Filters

When you delete dynamic filters, the deletion is effective for a limited period of time because the Guard continues to configure new dynamic filters when zone protection is enabled. See the "Preventing the Production of Dynamic Filters" section on page 6-23 for information on how to prevent the Guard from producing a dynamic filter.

To delete a dynamic filter, use the following command in zone configuration mode:

no dynamic-filter *dynamic-filter-id*

The *dynamic-filter-id* argument specifies the dynamic filter ID. To display the list of dynamic filters and identify the ID of the dynamic filter to delete, use the **show dynamic-filters** command (see the "Displaying Dynamic Filters" section on page 6-19). To delete all zone dynamic filters, enter an asterisk (*****) for the dynamic filter identifier.

The following example shows how to delete a dynamic filter:

```
user@GUARD-conf-zone-scannet# no dynamic-filter 876
```

Preventing the Production of Dynamic Filters

To prevent the Guard from producing unwanted dynamic filters, perform one of the following actions:

- Deactivate the policy that produces the dynamic filters (see the "Changing the Policy State" section on page 7-13 for more information). To determine which policy produced the unwanted dynamic filters, see the "Displaying Dynamic Filters" section on page 6-19.
- Configure a bypass filter for the desired traffic flow (see the "Configuring Bypass Filters" section on page 6-11).
- Increase the threshold of the policy that produces the undesired dynamic filter (see the "Configuring the Policy Threshold" section on page 7-13).

Deactivating Dynamic Filters

When the dynamic filter timeout expires, the Guard determines whether or not the dynamic filter should be deactivated based on current traffic conditions. If the Guard determines that the dynamic filter should not be deactivated, the filter remains active for another time span.

Dynamic filters are deactivated if one of the following conditions applies:

- The total zone malicious traffic rate, which equals the sum of the spoofed and dropped traffic, is less than or equal to the zone-malicious-rate termination threshold. See the following commands in this section.
- The dynamic filter measures the traffic rate (the filter rate counter does not display N/A) and the filter-rate termination threshold (see the following commands in this section) is equal to or greater than both of the following:
  - The dynamic filter current traffic rate.
  - The dynamic filter average traffic rate during a user-configured time span. This time span is defined by the policy timeout parameter. See the "Configuring the Policy Timeout" section on page 7-18 for more information.

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

To configure the zone malicious traffic threshold, use the following command in zone configuration mode:

filter-termination zone-malicious-rate *threshold*

The *threshold* argument specifies the zone malicious traffic threshold for a zone in packets per second (pps). This traffic consists of the sum of the spoofed and the dropped traffic. The default value is 50 pps.

To configure the dynamic filter-rate termination threshold, use the following command in zone configuration mode:

filter-termination filter-rate *threshold*

The *threshold* argument specifies the dynamic filter traffic threshold in pps units. The default value is 2 pps.

The following example shows how to configure the dynamic filter termination rates:

```
user@GUARD-conf-zone-scannet# filter-termination zone-malicious-rate 200
user@GUARD-conf-zone-scannet# filter-termination filter-rate 50
```

CHAPTER 7

Configuring Policy Templates and Policies

This chapter describes the Cisco Guard (Guard) zone policies, policy structure, and policy templates, and it describes how to configure the zone policy and the policy template parameters.

This chapter contains the following sections:

Understanding Zone Policies

The zone policies enable the Guard to perform a statistical analysis of the zone traffic flow. The zone policies are configured to take action against a particular traffic flow if they identify that flow as malicious or abnormal, which occurs when the flow exceeds the policy threshold, and configure filters (dynamic filters) dynamically to protect the traffic flow according to the severity of the attack.

Every zone configuration contains a set of policies. When you create a new zone using a policy template, the Guard configures the new zone with policies associated with the template. When you create a new zone by copying an existing zone, the Guard configures the new zone with the policies of the existing zone.

To create zone-specific policies and tune their thresholds to recognize normal zone traffic, the Guard learns the zone traffic in a two-phase learning process (see "Understanding the Learning Process" section on page 1-4). The Guard uses predefined policy templates to construct the policies and then learns the policy thresholds as determined by the zone traffic. The Guard uses each policy template to create policies that the Guard requires to protect the zone against a specific Distributed Denial of Service (DDoS) threat. After the Guard creates and tunes the zone policies, you can add and delete policies or change policy parameters.

Policies have cross dependencies and priorities. If two different policies define the same traffic flow, the Guard analyzes the flow using the policy that is more specific. For example, policies relating to TCP services exclude the HTTP services that are handled by the HTTP-related policies.

You can configure the policy operational aspects, which define the policy triggers and the action that the policy takes once it is activated.

Understanding and Configuring Policy Templates

A policy template is a collection of policy construction rules that the Guard uses during the policy construction phase to create the zone policies. At the end of the policy construction phase, the Guard has a set of zone-specific policies that it created using the policy templates. The name of the policy template is derived from the characteristics that are common to all the policies that it creates and can be a protocol (such as DNS), an application (such as HTTP), or the objective (such as ip_scan). For example, the policy template *tcp_connections* produces policies that relate to connections, such as the number of concurrent connections. When you create a new zone, the Guard includes a set of policy templates in the zone configuration.

Table 7-1 describes the Guard policy templates. The Guard includes these policy templates when you create a new zone using the GUARD_DEFAULT zone template.

Table 7-1 Policy Templates

Policy Template	Constructs a Group of Policies Relating To
dns_tcp	DNS-TCP protocol traffic.
dns_udp	DNS-UDP protocol traffic.
fragments	Fragmented traffic.
http	HTTP traffic that flows, by default, through port 80 (or other user-configured ports).
ip_scan	IP scanning. A situation in which a client from a specific source IP address tries to access many destination IP addresses in the zone. This policy template is designed primarily for zones in which the IP address definition is a subnet. By default, this policy template is disabled. The default action for this policy template is notify. **Note** The policies that are produced from this policy template consume system resources and can affect the performance of the Guard.
other_protocols	Non-TCP and non-UDP protocols.
port_scan	Port scanning. A situation in which a client from a specific source IP address tries to access many ports in the zone. By default, this policy template is disabled. The default action for this policy template is notify. **Note** The policies that are produced from this policy template consume system resources and can affect the performance of the Guard.
tcp_connections	TCP connection characteristics.
tcp_not_auth	TCP connections that have not been authenticated by the Guard anti-spoofing functions.
tcp_outgoing	TCP connections initiated by the zone.
tcp_ratio	Ratios between different types of TCP packets, for example, the number of SYN packets compared to the number of FIN/RST packets.
tcp_services	TCP services on ports other than HTTP related, such as ports 80 and 8080.

Table 7-1 Policy Templates (continued)

Policy Template	Constructs a Group of Policies Relating To
tcp_services_ns	TCP services. By default, the policies created from this policy template monitor IRC ports (666X), SSH, and Telnet. This policy template does not create policies with actions that require the Guard to apply the strong protection level to the traffic flow. See the "Understanding the Protection Cycle" section on page 1-6 for more information about the strong protection level.
udp_services	UDP services.

The Guard includes additional policy templates for zones that were created from zone templates that are designed for specific types of attacks or specific services. Table 7-2 details the policy templates that the Guard adds to a zone configuration based on a specific zone template.

Table 7-2 Additional Policy Templates

Zone Template	Policy Template
GUARD_VOIP	sip_udp—Constructs a group of policies that monitor VoIP[1] applications that use SIP[2] over UDP to establish the VoIP sessions and RTP/RTCP[3] to transmit voice data between the SIP end points after sessions are established.

[1] VoIP = Voice over IP

[2] SIP = Session Initiation Protocol

[3] RTP/RTCP = Real-Time Transport Protocol/Real-Time Control Protocol

Note The Guard looks for indicators of TCP traffic first on dedicated ports 6660 to 6670 and 21 to 23 as follows:

- If traffic is traced on these ports, the tcp_services_ns policy template constructs a group of policies, and the tcp_services policy template monitors TCP services on other ports.
- If no traffic is traced on these ports, the tcp_services_ns policy template is not used.

You can add services to policies that were created from the tcp_services_ns policy template.

The Guard includes additional policy templates that protect zones for which you do not want to use the TCP proxy anti-spoofing functions in which the Guard serves as a proxy. You can use these policy templates if the zone is controlled based on the IP addresses, such as an Internet Relay Chat (IRC) server-type zone, or if you do not know the type of services that are running on the zone.

If you define a zone with the GUARD_TCP_NO_PROXY zone template, the Guard uses the policy templates described in Table 7-3. The Guard replaces the policy templates http, tcp_connections, and tcp_outgoing with the policy templates http_ns, tcp_connections_ns, and tcp_outgoing_ns policies. The http_ns, tcp_connections_ns, and tcp_outgoing_ns policy templates do not create policies with actions that require the Guard to apply the strong protection level to the traffic flow.

Table 7-3 details the Guard policy templates for GUARD_TCP_NO_PROXY.

Table 7-3 GUARD_TCP_NO_PROXY Policy Templates

Policy Template	Replaces Policy Template	Constructs a group of policies relating to
tcp_connections_ns	tcp_connections	TCP connection characteristics.
tcp_outgoing_ns	tcp_outgoing	TCP connections initiated by the zone.
http_ns	http	HTTP traffic flowing, by default, through port 80 (or other user-configured ports).

To view a list of all policy templates, use the **policy-template** command in zone configuration mode and press **Tab** twice.

During the learning process, zone traffic flows transparently through the Guard. Each active policy template produces a group of policies based on the policy definitions and the zone traffic characteristics. The Guard ranks the services (protocol and port numbers) that the policy template monitors by the level of traffic volume. The Guard then selects the services that have the highest traffic volume and that have exceeded the defined minimum threshold, and it creates a policy for each service. Some policy templates create an additional policy to handle all traffic flows for which a specific policy was not added with a service of **any.**

You can configure the following policy template parameters:

- Maximum Number of Services—Defines the maximum number of services that the Guard picks up for the policy template to create specific policies.
- Minimum Threshold—Defines the minimum threshold that must be exceeded for the Guard to rank the service.
- Policy Template State—Defines whether or not the Guard produces policies from the policy template.

To configure the policy template parameters, enter the policy template configuration mode by entering the following command in zone configuration mode:

policy-template *policy-template-name*

The *policy-template-name* argument specifies the name of the policy template. See Table 7-1 for more information.

The following example shows how to enter http policy template configuration mode:

```
user@GUARD-conf-zone-scannet# policy-template http
user@GUARD-conf-zone-scannet-policy_template-http#
```

To display the parameters of a specific policy template, use the **show** command in policy template configuration mode.

This section contains the following topics:

- Configuring the Maximum Number of Services
- Configuring the Minimum Threshold
- Configuring Policy Template States
- Configuring All Policy Template Parameters Simultaneously

Configuring the Maximum Number of Services

The maximum number of services parameter defines the maximum number of services (protocol numbers or port numbers) for which the policy template selects and creates policies. The Guard ranks the services that the policy template relates to by the level of traffic volume for each service. The Guard then selects the services that have the highest traffic volume and that have exceeded the defined minimum threshold (as defined by the *min-threshold* parameter), and it creates policies for each service. The Guard may add an additional policy with a service of **any** to handle all other traffic flows with the characteristics of the policy template.

Note The higher the maximum number of services, the more Guard memory the zone requires.

You can only define the maximum number of services parameter for policy templates that detect services: tcp_services, tcp_services_ns, udp_services, and other protocols. You cannot configure it for policy templates that monitor a specific service, such as *dns_tcp,* which monitors service 53, or for policy templates that relate to a specific traffic characteristic, such as *fragments*.

The Guard measures the traffic rate of the service based on the policy traffic characteristics. The traffic characteristic can be the source IP addresses or the destination IP addresses. A policy that monitors the service **any** measures the rate of source IP addresses on all services that are not handled by a specific policy.

By limiting the service number, you can configure the Guard policies to your preferred traffic flow requirements.

To configure the maximum number of services, use the following command in policy template configuration mode:

max-services *max-services*

The *max-services* argument is an integer greater than 1 that defines the maximum number of services that the Guard selects. We recommend that you do not exceed the maximum of 10 services.

The following example shows how to configure the maximum number of services that the Guard monitors to 5:

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# max-services 5
```

Configuring the Minimum Threshold

The minimum threshold parameter defines the minimum traffic volume for a service. When the threshold is exceeded, the Guard constructs policies that relate to the service traffic according to the particular traffic flow that exceeded the threshold. By setting the threshold, you can adapt the protection operation to the traffic volume of the zone services.

You cannot configure the minimum threshold parameter for policy templates that are essential for proper zone protection and that always construct a policy such as the following policy templates: tcp_services, tcp_services_ns, udp_services, other_protocols, http, and fragments.

To configure the minimum threshold, use the following command in policy template configuration mode:

min-threshold *min-threshold*

The *min-threshold* argument is a real number (a floating point number with two decimal places), equal to or greater than 0, that defines the minimum threshold rate in packets per second (pps). When measuring concurrent connections and the SYN/FIN ratio, the threshold is an integer that defines the total number of connections.

The following example shows how to configure the minimum threshold of the policy template http:

```
user@GUARD-conf-zone-scannet-policy_template-http# min-threshold 12.3
```

Configuring Policy Template States

The policy template state parameter defines whether the policy template is enabled or disabled. If you disable a policy template, it is prevented from producing policies when the Guard is in the policy construction phase.

⚠ **Caution** Disabling a policy template may seriously compromise zone protection. If you disable a policy template, the Guard cannot protect the zone from the traffic to which the policy template relates. For example, disabling the dns_udp policy template prevents the Guard from creating zone policies that manage DNS (UDP) attacks.

To disable a policy template, use the **disable** command in policy template configuration mode.

To enable a policy template, use the **enable** command in policy template configuration mode.

The following example shows how to disable the policy template http:

```
user@GUARD-conf-zone-scannet-policy_template-http# disable
```

Configuring All Policy Template Parameters Simultaneously

You can configure all policy template operational parameters with a single command by entering the following command in zone configuration mode:

policy-template *policy-template-name max-services min-threshold* {**disabled** | **enabled**}

Table 7-4 provides the arguments and keywords for the **policy-template** command.

Table 7-4 Arguments and Keywords for the policy-template Command

Parameter	Description
policy-template-name	Policy template name. See Table 7-5 for more information.
max-services	Maximum number of services for which the Guard selects and constructs policies from the specific policy template. To prevent the Guard from changing the current value, enter a value of –1. See the "Configuring the Maximum Number of Services" section on page 7-5 for more information.
min-threshold	Minimum threshold that must be exceeded for the Guard to rank the service. To prevent the Guard from changing the current value, enter a value of –1. See the "Configuring the Minimum Threshold" section on page 7-5 for more information.

Table 7-4 Arguments and Keywords for the policy-template Command (continued)

Parameter	Description
disabled	Disables the policy template from producing policies. See the "Configuring Policy Template States" section on page 7-6 for more information.
enabled	Enables the policy template. See the "Configuring Policy Template States" section on page 7-6 for more information**.**

The following example shows how to set the parameters of the tcp_services policy template. The maximum number of services is set to 3, the policy state is set to **enabled**, and the minimum threshold is unchanged (–1).

```
user@GUARD-conf-zone-scannet# policy-template tcp_services 3 -1 enabled
```

Understanding the Policy Path

The name of the policy is composed of sections that describe the traffic characteristic that it measures. For example, the policy http/80/analysis/syns/src_ip measures traffic flows of HTTP SYN packets destined to port 80 that were authenticated by the Guard analysis protection level functions and aggregated according to source IP addresses.

Figure 7-1 provides an example of a zone policy name.

Figure 7-1 Policy Name

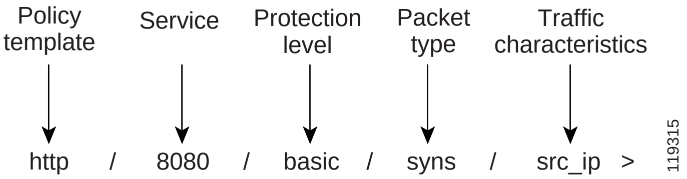


Table 7-5 describes the policy name sections.

Table 7-5 Policy Name Sections

Section	Description
Policy template	Policy template that was used to construct the policy. Each policy template deals with the characteristics that the Guard requires to protect against a specific DDoS threat. See the "Understanding and Configuring Policy Templates" section on page 7-2 for more information.
Service	Port number or protocol number in the traffic flow that the policy monitors. You can add or delete services from the policies.
Protection level	Protection level that the Guard applies to the traffic flow. Protection levels have a static configuration and cannot be configured manually.
Packets type	Packet types that the Guard monitors.
Traffic characteristics	Traffic characteristics that the Guard uses to aggregate the policy.

The first four sections of the policy name (policy template, service, protection level, and packet type) define the type of traffic that is analyzed. The last section of the policy path (traffic characteristics) defines how to analyze the flow.

This section describes each of the policy path sections as follows:

- Understanding and Managing the Policy Services
- Understanding the Guard Protection Levels
- Understanding the Packet Types that the Guard Monitors
- Understanding the Traffic Characteristics that the Guard Monitors

Understanding and Managing the Policy Services

The service section defines the zone application port or protocol to which each policy relates. Policies have cross dependencies and priorities. If two different policies define the same traffic flow, the Guard analyzes the flow using the policy that is more specific. The service **any** relates to all traffic that does not specifically match other services created from the same policy template.

We recommend that you define specific policies for the zone main services to obtain protection that is most suited to your individual needs.

⚠ **Caution** Do not add the same service (port number) to more than one policy because it may decrease the performance of the Guard.

When you add or delete a service from the zone policies, the Guard marks the zone policies as untuned. If you enabled zone protection and the learning process, the Guard cannot detect anomalies in the zone traffic until you perform one of the following actions:

- Perform the threshold tuning phase of the learning process and accept the results (see the "Activating the Threshold Tuning Phase" section on page 8-6).
- Mark the zone policies tuned (see the "Marking the Policies as Tuned" section on page 8-10).

This section contains the following topics:

- Adding a Service
- Deleting a Service

Adding a Service

You can add services to all policies that were created from a specific policy template. The new service is an addition to the services that were discovered during the policy construction phase and is defined with default values. You can define the threshold manually, but we recommend that you run the threshold tuning phase of the learning process to tune the policies to the zone traffic. See the "Activating the Threshold Tuning Phase" section on page 8-6 for more information.

You can add a new service to policies that were created from the following policy templates:

- tcp_services, udp_services, or tcp_services_ns

  The service designates a port number.
- other_protocols

  The service designates a protocol number.

Note If you activate the policy construction phase after adding a service, new services might override the manually added service.

Unless you enable the policy construction phase, you may need to add a service manually in the following situations:

- A new application or service was added to the zone network.
- The policy construction phase was activated for a short period, so it does not reflect all the network services (for instance, if there are known applications or services that are active only once a week or during the night).

To add a service, use one of the following commands:

- **add-service** *service-num* (in policy template configuration mode)
- **policy-template** *policy-template-name* **add-service** *service-num (*zone configuration mode)

Table 7-6 provides the arguments for the **add-service** command.

Table 7-6 Arguments for the add-service Command

Parameter	Description
service-num	Protocol or port number.
policy-template-name	Policy template name. See Table 7-1 for more information.

The following example shows how to add a service to all the policies that were created from the policy template tcp_services:

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# add-service 25
```

Deleting a Service

You can delete a specific service for any policy template. The Guard will delete the service from all policies that were created from the specific policy template.

To delete a service, use one of the following commands:

- **remove-service** *service-num* (in policy template configuration mode)
- **policy-template** *policy-template-name* **remove-service** *service-num* (in zone configuration mode)

Table 7-7 provides the arguments for the **remove-service** command.

Table 7-7 Arguments for the remove-service Command

Parameter	Description
service-num	Protocol or port number to remove.
policy-template-name	Policy template name. See Table 7-1 for more information.

Caution If you delete a service, the Guard policies cannot monitor the traffic of that service, which may compromise zone protection.

You can remove services from the following policy templates:

- tcp_services, udp_services, or tcp_services_ns

  The service is a port number.
- other_protocols

  The service is a protocol number.

If you do not activate the policy construction phase of the learning process, you may need to remove a service manually in the following situations:

- An application or service was removed from the network.
- An application or service that you do not want to enable (because it is uncommon for the network environment) but was identified during the policy construction phase.

Note If you activate the policy construction phase after removing a service, the Guard may add the same service to the zone configuration.

The following example shows how to delete a service from all policies that were created from the policy template tcp_services:

```
user@GUARD-conf-zone-scannet-policy_template-tcp_services# remove-service 25
```

Understanding the Guard Protection Levels

The Guard applies three protection levels in which it applies different processes to the traffic flow. The Guard has the following three protection levels:

- Analysis protection level—The Guard allows the traffic to flow monitored, but unhindered, during zone protection, as long as no anomalies are traced. Once the Guard traces anomalies, it directs the traffic to the appropriate protection level.
- Basic protection level—The Guard activates anti-spoofing and anti-zombie functions to authenticate the traffic by inspecting the suspicious traffic flow to verify its source. The Guard performs authentication for each host. The authentication is valid for a predefined period of time only. When the time expires, the Guard authenticates the host again.
- Strong protection level—The Guard activates severe anti-spoofing functions that inspect the traffic flow packets to verify the flow legitimacy.

The Guard performs authentication for each connection.

After activating a protection function, the Guard continues to analyze the traffic. If the Guard can still spot traffic abnormalities in traffic destined to the zone, it applies a stronger protection level.

Note Protection levels have a static configuration and cannot be configured manually.

Understanding the Packet Types that the Guard Monitors

The Guard monitors packet characteristics, which can be one of the following:

- Packet type (for example, TCP-SYN packets)

- Packet analysis (for example, authenticated packets, which are packets that the Guard has verified their connection by performing a TCP handshake)
- Packet direction (for example, incoming connections)

Table 7-8 describes the packet types that the Guard monitors.

Table 7-8 Packet Types

Packet Type	Description
auth_pkts	Packets for which either a TCP handshake or UDP authentication was performed.
auth_tcp_pkts	Packets for which a TCP handshake was performed.
auth_udp_pkts	Packets for which UDP authentication was performed.
in_nodata_conns	Incoming zone connections that have no data transfer on the connection (packets without a data payload).
in_conns	Incoming zone connections.
in_pkts	Incoming zone DNS query packets.
in_unauth_pkts	Incoming zone unauthenticated DNS queries.
num_sources	Packets that have TCP source IP addresses that are destined to the zone and that have been authenticated by the Guard anti-spoofing functions.
out_pkts	Incoming zone DNS reply packets.
reqs	Request packets with a data payload.
syns	Synchronization packets (TCP SYN flagged packets).
syn_by_fin	SYN and FIN flagged packets. The Guard verifies the ratio between the number of SYN flagged packets and the number of FIN flagged packets.
unauth_pkts	Packets that did not undergo a TCP handshake.
pkts	All packet types that do not fall under any other category in the same protection level.

Understanding the Traffic Characteristics that the Guard Monitors

Traffic characteristics define how to analyze the traffic flow and what characteristics were used to aggregate the policies. Different policies can analyze the same traffic flow but measure the rate based on different characteristics, as shown in this example:

dns_tcp/53/analysis/pkts/dst_ip and dns_tcp/53/analysis/pkts/src_ip.

Table 7-9 describes the traffic characteristics that the Guard monitors.

Table 7-9 Traffic Characteristics

Traffic Characteristic	Description
dst_ip	Traffic destined to a zone IP address.
dst_ip_ratio	Ratio of SYN and FIN flagged packets destined to a specific IP address.
dst_port	Traffic destined to a specific zone port.
dst_port_ratio	Ratio of SYN and FIN flagged packets destined to a specific port.

Table 7-9 Traffic Characteristics (continued)

Traffic Characteristic	Description
global	Summation of all traffic flow as defined by the other policy sections.
protocol	Traffic destined to the zone aggregated based on the protocol.
src_ip	Traffic destined to the zone aggregated according to the source IP address.
src_ip_many_dst_ips	Traffic from a single IP address that probes a large number of zone IP addresses on the same port. This key is used for IP scanning.
src_ip_many_ports	Traffic from a single IP address that probes a large number of ports on a zone destination IP address. This key is used for port scanning.

Configuring Policy Parameters

After completing the learning process, you can display specific policy parameters (policy state, policy threshold, policy timeout, policy action, and policy interactive status) to determine if the policy parameters suit the zone traffic. You can configure the policy parameters of a single policy or a group of policies to adapt to zone traffic requirements.

To display the configuration of the policy parameters, use the **show** command in policy configuration mode.

To enter policy configuration mode, use the following command in zone configuration mode:

policy *policy-path*

The *policy-path* argument specifies the policy path sections. The path can be a partial path that includes only part of the policy sections. See the "Understanding Zone Policies" section on page 7-1 for more information.

Note To move up one level in the policy path hierarchy, enter **policy ..** at the policy path prompt.

The following example shows how to enter the dns_tcp/53/analysis/syns/global policy configuration mode:

```
user@GUARD-conf-zone-scannet# policy dns_tcp/53/analysis/syns/global
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global#
```

You can change the policy *action*, *timeout*, *threshold*, and learning parameters at every section of the policy path. However, more policies are affected if you change these parameters at the higher-level policy sections (such as policy template or service sections). If you configure these parameters at a high-level policy path hierarchy, these parameters change in all the subpolicy paths.

You can use an asterisk (*) as a wildcard character in each policy path section. If you do not specify a policy path section, the Guard relates to the unspecified section as a wildcard (*). For example, the tcp_services//analysis//global policy uses a wildcard for the service and the packet type.

This section contains the following topics:

- Changing the Policy State
- Configuring the Policy Threshold
- Configuring the Policy Timeout
- Configuring the Policy Action

- Configuring the Policy Interactive Status

Changing the Policy State

The zone policies have three possible states as follows:

- Active—The policy monitors the traffic and performs an action once the threshold is exceeded.
- Inactive—The policy monitors the traffic and obtains the threshold, but it takes no action when a threshold is exceeded. You can inactivate a policy to avoid reactivating the threshold-tuning phase of the learning process.
- Disabled—The policy does not monitor the traffic flow, so no threshold is obtained.

Note We recommend that you activate the threshold tuning phase of the learning process to ensure that the Guard monitors the correct thresholds for the other policies.

Caution When you disable a policy, the active zone policies assume responsibility for the traffic that would normally be monitored by the disabled policy. To adjust the thresholds of the active policies, we recommend that you activate the threshold tuning phase before you activate zone protection.

To change the policy state, use the following command in policy configuration mode:

state {**active** | **disabled** | **inactive**}

The following example shows how to set the policy state:

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns# state disabled
```

The following example shows how to set the state of all global policies:

```
user@GUARD-conf-zone-scannet-policy-/*/*/*/global# state inactive
```

Caution If you deactivate or disable a zone policy, the active zone policies may not assume the protection capabilities that the deactivated policy provided, which may compromise zone protection.

If you activate the policy construction phase after disabling a zone policy, all zone policies are reconfigured according to the current traffic flow and the policy may be reactivated.

Configuring the Policy Threshold

The policy threshold defines the threshold traffic rate for a specific policy and is adjusted by the threshold tuning phase. The threshold is set, by default, to a value that is appropriate for on-demand protection. When this threshold is exceeded, the policy takes action to protect the zone.

The threshold is measured in packets per second except for policies that are constructed from the following policy templates:

- num_soruces—The threshold is measured in the number of IP addresses or ports.
- tcp_connections—The threshold is measured in the number of connections.

- tcp_ratio—The threshold is measured as the ratio number.

You can configure the policy threshold in the following ways:

- Set the threshold—You can set the value of the policy threshold. See the "Setting the Policy Threshold" section on page 7-14.
- Multiply the threshold—The Guard multiplies the current policy thresholds by a factor. The new value may change in subsequent threshold tuning phases if you do not set it as fixed. See the "Multiplying a Threshold by a Factor" section on page 7-16.
- Configure specific IP thresholds—The Guard sets thresholds for specific IP source addresses within the zone address range. See the "Configuring Specific IP Thresholds" section on page 7-17.
- Configure a proxy threshold—The Guard sets a threshold for traffic of clients that connect to the zone in HTTP through proxies. See the "Configuring the Proxy Threshold" section on page 7-18.

The policy threshold may change if you perform additional threshold tuning phases. You can modify how a threshold may change in subsequent threshold tuning phases in the following ways:

- Set the threshold as fixed—The Guard will not change the value of the policy threshold, proxy-threshold, and threshold-list in subsequent threshold tuning phases. See the "Setting the Threshold as Fixed" section on page 7-14.
- Set a fixed multiplier for the policy threshold—The Guard calculates the policy threshold in subsequent threshold tuning phases based on the current policy threshold, the learned threshold, and the fixed multiplier. See the "Configuring a Threshold Multiplier" section on page 7-15.

This section contains the following topics:

Setting the Policy Threshold

To configure the policy threshold, use the following command in policy configuration mode:

threshold *threshold*

The *threshold* argument is a positive number that specifies the policy threshold.

The following example shows how to set the threshold value of the policy dns_tcp/53/analysis/syns/global to 300:

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/
global# threshold 300
```

Setting the Threshold as Fixed

You can set a policy threshold, proxy-threshold, and threshold-list as fixed. The Guard ignores new thresholds in the threshold tuning phase of the learning process and maintains the current thresholds. Setting a threshold as fixed enables you to configure the thresholds of a policy but continue learning the thresholds of other policies.

To set a policy threshold as fixed, use the following command in policy configuration mode:

learning-params fixed-threshold

The following example shows how to set the threshold of the policy dns_tcp/53/analysis/syns/global as fixed:

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/
global# learning-params fixed-threshold
```

You can set the threshold of several policies as fixed in a single command by entering the command in zone configuration mode. To set a policy threshold as fixed while in zone configuration mode, use the following command:

policy *policy-path* **learning-params fixed-threshold**

The *policy-path* argument specifies the policy path. The path can be a partial path that includes only part of the policy sections. See the "Understanding Zone Policies" section on page 7-1 for more information.

The following example shows how to set the thresholds of all policies that were created from the dns_tcp policy template as fixed:

```
user@GUARD-conf-zone-scannet# policy dns_tcp learning-params fixed-threshold
```

To display the policy learning parameters, use the **show learning-params** command in policy configuration mode, or use the **show policies** *policy-path* **learning-params** command in zone configuration mode.

Configuring a Threshold Multiplier

You can set a multiplier for a policy threshold. The Guard calculates a new policy threshold by multiplying the learned threshold by the specified multiplier before accepting the result of subsequent threshold tuning phases. The Guard accepts the results of the threshold tuning phase using the configured threshold selection method. See the "Configuring the Threshold Selection Method" section on page 8-9.

To set a multiplier for the policy threshold, use the following command in zone configuration mode:

policy *policy-path* **learning-params threshold-multiplier** *threshold-multiplier*

Table 7-10 provides the arguments and keywords for the **policy learning-params threshold-multiplier** command.

Table 7-10 Arguments and Keywords for the policy learning-params threshold-multiplier Command

Parameter	Description
policy-path	Policy path for which to multiply the thresholds. The path can be a partial path that includes only part of the policy sections. See the "Understanding Zone Policies" section on page 7-1 for more information.
learning-params	Configures the learning parameters.
threshold-multiplier *threshold-multiplier*	Multiplies the policy threshold. The *threshold-multiplier* is a real positive number (a floating point number with two decimal places) by which the policy threshold is multiplied. Enter a number less than 1 to decrease the policy threshold.

To set a multiplier for the policy threshold in policy configuration mode, use the **learning-params threshold-multiplier** *threshold-multiplier* command.

The following example shows how to configure a threshold multiplier so that the Guard decreases the thresholds of policies that were created from the policy template dns_tcp by half in subsequent threshold tuning phases:

```
user@GUARD-conf-zone-scannet# policy dns_tcp learning-params threshold-multiplier 0.5
```

To display the policy learning parameters, use the **show learning-params** command in policy configuration mode, or use the **show policies** *policy-path* **learning-params** command in zone configuration mode.

Multiplying a Threshold by a Factor

You can multiply the thresholds of a policy or a group of policies by a factor, which enables you to increase or decrease the threshold of a policy or a group of policies if the traffic volume does not represent the zone traffic. You can enable the Guard to multiply the policy thresholds, the proxy thresholds, and the thresholds that were defined by the **policy threshold-list** command.

To multiply policy thresholds by a factor, use the following command in zone configuration mode:

policy *policy-path* **thresh-mult** *threshold-multiply-factor*

Table 7-11 provides the arguments and keywords for the **policy thresh-mult** command.

Table 7-11 Arguments and Keywords for the policy thresh-mult Command

Parameter	Description
policy-path	Policy template name. See Table 7-1 for more information.
thresh-mult *threshold-multiply-factor*	*Specifies a real positive number* (a floating point number with 4 decimal places) by which *to multiply the threshold.* Enter a number less than 1 to decrease the policy threshold.

The following example shows how to decrease the thresholds of policies that were created from the policy template dns_tcp by half:

```
user@GUARD-conf-zone-scannet# policy */*/*/*/src_ip thresh-mult 0.5
```

Note The Guard may change the threshold value in subsequent threshold tuning phases. To prevent the Guard from changing the threshold value, set the threshold value as fixed. See the "Setting the Threshold as Fixed" section on page 7-14.

To display the policy learning parameters, use the **show learning-params** command in policy configuration mode, or use the **show policies** *policy-path* **learning-params** command in zone configuration mode.

Configuring Specific IP Thresholds

You can avoid false attack detections by the Guard when traffic increases on a known high traffic source or destination IP address by configuring a policy with a threshold for traffic that is associated with that IP address.

You should consider configuring a specific IP threshold if one of the following situations occurs:

- When there is known high-volume traffic from a source IP address, you can configure a threshold to apply to traffic that originates from the specific source IP address.
- When there is a nonhomogeneous zone (a zone that has more than a single IP address defined) and there is known high-volume traffic flowing to part of the zone only, you can configure a threshold to apply to traffic that targets the specific destination IP address within the zone.

You can configure specific IP thresholds only for the following policies:

- Policies with traffic characteristic of destination IP (dst_ip).
- Policies with traffic characteristics of source IP address (src_ip) where the default policy action is drop. The default policy action is the action that the Guard applies to the policy when you create a new zone. You can configure the threshold list for such policies even if you change the policy action.

To configure a specific IP threshold, use one of the following commands:

- **policy** *policy-path* **threshold-list** *ip threshold* [*ip threshold* ...] (in zone configuration mode)
- **threshold-list** *ip threshold* [*ip threshold* ...] (in policy configuration mode)

Table 7-12 provides the arguments for the **threshold-list** command.

Table 7-12 Arguments for the policy threshold-list Command

Parameter	Description
policy-path	Policy template name. See Table 7-1 for more information.
ip	Specific IP address.
threshold	Threshold traffic rate in packets per second, except for policies that measure concurrent connections and SYN-by-FIN ratio, where the threshold is the number of connections.

You can add a maximum of 10 specific IP thresholds for each policy. You can enter all specific IP thresholds in a single command.

The Guard might change the policy thresholds in subsequent threshold tuning phases if the threshold selection method is set to new-thresholds. See the "Configuring the Threshold Selection Method" section on page 8-9 for more information.

The following example shows how to set specific IP thresholds for IP addresses 10.10.10.2 and 10.10.15.2 for the policy http/80/analysis/syns/src_ip:

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# threshold-list
10.10.10.2 500 10.10.15.2 500
```

Configuring the Proxy Threshold

The proxy threshold parameter defines the traffic rate for clients that connect to the zone in HTTP through proxies and enables the Guard to adapt the policy to traffic volumes that come from different sources. The Guard uses the proxy thresholds to block traffic only, so you can configure them only for policies in the DEFAULT zone template with a strong protection level and for policies in the TCP_NO_PROXY zone template with a basic protection level.

A proxy threshold is available for the http, http_ns, tcp_connections, and tcp_connections_ns policies only and is effective for tcp_connections or tcp_connections_ns policy templates if the zone has active http or http_ns policies only.

To configure the proxy-threshold, use the following command in policy configuration mode:

proxy-threshold *proxy-threshold*

The *proxy-threshold* argument specifies the proxy-threshold traffic rate in packets per second for http and http_ns policies. It specifies the proxy-threshold in the number of connections for tcp_connections and tcp_connections_ns policies.

Because proxy servers handle much more traffic than network clients that are part of the zone, we recommend that when you configure a proxy threshold, you configure the *proxy-threshold* argument with a higher value than the *threshold* argument.

The following example shows how to set the proxy threshold for the *http/80/strong/syns/src_ip* policy to 20:

```
user@GUARD-conf-zone-scannet-policy-/http/80/strong/syns/src_ip# proxy-threshold 20
```

Configuring the Policy Timeout

The timeout parameter defines the minimum time for dynamic filters that are produced by the policy to apply their action. When the timeout expires, the Guard determines whether or not to deactivate the dynamic filters that were produced by the policy. If the Guard decides not to deactivate the dynamic filters, the filter activation timeout resumes for another time span. To change the criteria for dynamic filter deactivation, use the **filter-termination** command. See the "Deactivating Dynamic Filters" section on page 6-23 for more information.

To configure the policy timeout, use the following command in policy configuration mode:

timeout {**forever** | *timeout*}

Table 7-13 provides the arguments and keywords for the **timeout** command.

Table 7-13 Arguments and Keywords for the timeout Command

Parameter	Description
forever	Specifies an indefinite time span.
timeout	Integer from 1 to 3,000,000 that specifies the minimum time in seconds that the dynamic filters, which are produced by the policy, are active.

The following example shows how to set the timeout of the policy http/80/analysis/syns/src_ip to 100 seconds:

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# timeout 100
```

To change the timeout of a group of policies simultaneously, use the **policy set-timeout** command in zone configuration mode.

The following example shows how to set the timeout of all policies that were produced from the HTTP policy template and measure source IP addresses to 100:

```
user@GUARD-conf-zone-scannet# policy http/*/*/*/src_ip set-timeout 100
```

Configuring the Policy Action

The action parameter defines the type of action that the policy takes once its threshold is exceeded.

Configure the policy action so that it enhances the protection that the policy defines. For example, configure the policy action to to-user-filters for policies with a protection level of analysis, or configure the policy action to filter/drop for policies with a protection level of strong. Do not configure the policy action so that it reduces the protection level that the policy defines. For example, do not configure the policy action to to-user-filters for policies with a protection level of basic or strong.

To configure the policy action, use the following command in policy configuration mode:

action *policy-action*

Table 7-14 describes the policy actions.

Table 7-14 Policy Actions

Policy Action	Description
block-unauthenticated	Adds a filter that blocks traffic that was not authenticated by the anti-spoofing functions, such as an ACK with no prior handshake. Configure this policy action for policies with a packet type of in_unauth_pkts and unauth_pkts only.
filter/strong	Adds a filter that applies the strong protection level to the traffic flow. Configure this policy action for policies with a protection level of analysis and basic. We recommend that you use this policy action on TCP (incoming) policies with traffic characteristics of src_ip only and do not use it on policies with traffic characteristics of global because it may cause network problems in networks that use a load balancer or an ACL[1] to manage traffic.
to-user-filters	Adds a filter directing the traffic to the user filters. Configure this policy action for policies with a protection level of analysis.
filter/drop	Adds a filter that directs the Guard to drop the specified traffic. Configure this policy action for policies that monitor traffic after the Guard has applied the anti-spoofing functions (policies with a protection level of basic and strong). We do not recommend that you use this action for policies with a protection level of analysis because this might cause the Guard to deplete all the Guard filters when mitigating a spoofed attack.

Table 7-14 Policy Actions (continued)

Policy Action	Description
redirect/zombie	Adds a filter that enhances authentication for all user filters with an action of redirect. This policy action applies to the tcp_connections/any/basic/num_sources/global policy only.
notify	Notifies you when its threshold is exceeded.

[1] ACL = Access Control List

The following example shows how to set the action of the policy http/80/analysis/syns/src_ip:

```
user@GUARD-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip# action drop
```

To change the action of a group of policies simultaneously, use the **policy set-action** command in zone configuration mode.

Note Not all actions are valid for all policies. If you modify the policy action to an action that is not valid for the specific policy, the Guard displays an error message.

The following example shows how to set the action of all dns_tcp policies:

```
user@GUARD-conf-zone-scannet# policy dns_tcp/ set-action filter/drop
set action of dns_tcp/ to filter/drop:
16 policy actions set.
```

Configuring the Policy Interactive Status

The interactive status parameter defines the interactive status that the pending dynamic filters, which are created by the zone policy, will assume. The interactive status applies only to zones if you enable zone protection, and the zone is in interactive protect mode. See Chapter 10, “Using Interactive Protect Mode,” for more information.

To modify the status of the pending dynamic filters that a policy produces after you have set the interactive status of a recommendation to **always-accept** or **always-ignore,** use the **interactive-status** command.

For example, if you have defined the status of a recommendation to **always-accept**, the recommendation and the pending dynamic filters of the recommendation are no longer displayed. To ignore the recommendation or the pending dynamic filters that the recommendation produces, change the policy interactive status to **interactive** or **always-accept**.

To configure the policy interactive status, use the following command in policy configuration mode:

interactive-status {**always-accept** | **always-ignore** | **interactive**}

Table 7-15 provides the keywords for the **interactive-status** command.

Table 7-15 Keywords for the interactive-status Command

Parameter	Description
always-accept	Accepts the dynamic filters that the policy produces automatically. The action applies automatically whenever the policy produces new recommendations. The Guard does not display **these** recommendations.
always-ignore	Ignores the dynamic filters that the policy produces automatically. The policy does not produce recommendations when its threshold is exceeded. The Guard does not display **these** recommendations.
interactive	Waits for you to accept or ignore the dynamic filters that the policy produces. The Guard displays these dynamic filters as part of the recommendations.

The following example shows how to configure the interactive status of policy dns_tcp/53/analysis/pkts/src_ip to always-accept:

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/pkts/
src_ip# interactive-status always-accept
```

Monitoring Policies

You can monitor the policies to see how well they are suited to the zone traffic volume and services.

This section describes the following topics:

- Displaying Policies
- Displaying Policy Statistics

Displaying Policies

You can display the zone policies to verify that they are adapted to the zone traffic characteristics. You might want to view the zone-constructed policies to verify that these policies are customized for the traffic characteristics of the zone. You can configure only policies that appear in this list.

The Guard displays only current zone policies. If a policy template was disabled during the policy construction phase, the Guard does not create policies from that policy template, and you do not see these policies when you enter the **show policies** command.

To display the zone policies, use the following command in zone configuration mode:

show policies *policy-path*

The *policy-path* argument specifies a group of policies. You can use an asterisk (*) as a wildcard character in each policy path section. If you do not specify a policy path section, the Guard considers the unspecified section to be a wildcard (*). For example, the policy tcp_services//analysis//global uses wildcards for the service and the packet type sections.

To display the statistics of all policies, enter an asterisk (*) for the policy path.

See the "Understanding Zone Policies" section on page 7-1 for more information about the policy path sections.

The following example shows how to display all the zone policies:

```
user@GUARD-conf-zone-scannet# show policies *
```

The following example shows how to display all policies that monitor DNS-over-TCP synchronization packets on port 53:

```
user@GUARD-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

Table 7-16 describes the fields in the **show policies** command output.

Table 7-16 Field Descriptions of the show policies Command Output

Field	Description
Policy	Policy name. See the "Understanding Zone Policies" section on page 7-1 for more information about the policy path sections.
State	Policy state. See the "Changing the Policy State" section on page 7-13 for more information. act = active, inact = inactive, disab= disabled
IStatus	Policy interactive status. See the "Configuring the Policy Interactive Status" section on page 7-20 for more information. a-accept = always-accept, a-ignor = always-ignore, interac = interactive
Threshold	Policy threshold. When this threshold is exceeded, the Guard takes action to protect the zone. See the "Configuring the Policy Threshold" section on page 7-13 for more information.
Proxy	Policy proxy-threshold. See the "Configuring the Proxy Threshold" section on page 7-18 for more information.
List	Number of specific IP thresholds defined for the policy. See the "Configuring Specific IP Thresholds" section on page 7-17 for more information.
Action	Action that the policy takes when the threshold is exceeded. See the "Configuring the Policy Action" section on page 7-19 for more information.
Timeout	Minimum time span that the policy action is valid. The Guard determines, according to the filter-termination thresholds, whether or not the dynamic filter that was produced by the policy is to be inactivated. See the "Configuring the Policy Timeout" section on page 7-18 for more information.

Displaying Policy Statistics

You can display the rate of the traffic flowing through a zone policy or a group of zone policies, and you can determine whether the type of services and volume represent the zone traffic. The Guard displays the traffic flows forwarded to the zone with the highest rates as measured by the policies. The rate is calculated based on traffic samples.

To display the policy statistics, use the following command in zone configuration mode:

show policies *policy-path* **statistics** [*num-entries*]

Table 7-17 provides the arguments for the **show policies statistics** command output.

Table 7-17 Arguments for the show policies statistics Command

Parameter	Description
policy-path	Group of policies for which to display statistics. You can use an asterisk (*) as a wildcard character in each policy path section. If you do not specify a policy path section, the Guard relates to the unspecified section as a wildcard (*). For example, the policy tcp_services//analysis//global uses wildcards for the service and the packet type sections. To display the statistics of all policies, enter an asterisk (*) for the policy-path. See the "Understanding Zone Policies" section on page 7-1 for more information about the policy path sections.
num-entries	(Optional) Number of entries to display. Enter a number from 1 to 100. The Guard displays the policies with the highest values.

The following example shows how to display the statistics of all the zone policies:

```
user@GUARD-conf-zone-scannet# show policies * statistics
```

The following example shows how to display the statistics of all policies that monitor DNS-over-TCP synchronization packets on port 53:

```
user@GUARD-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

The following example shows how to display the statistics of the zone global traffic:

```
user@GUARD-conf-zone-scannet# show policies */*/*/*/global statistics
```

The Guard displays the information in three tables. The information in each table is sorted by value, with the highest values appearing at the top of the table.

Table 7-18 displays the fields in the tables in the **show policies statistics** command output.

Table 7-18 Field Descriptions of the show policies statistics Command Output Tables

Column	Description
Fields in all output tables	
Key	Key that is the traffic characteristic used to aggregate the policies. For example, in the tcp_services/any/analysis/syns/dst_ip policy, the key is the destination IP address (dst_ip). If the traffic characteristic that was used to aggregate the policies is global, the key displays N/A. See Table 7-8 for more information.
Policy	Policy name. See the "Understanding Zone Policies" section on page 7-1 for more information.
Fields in one of the output tables	
Rate	Rate of the traffic that flows through the policy and is measured in packets per second (pps). The rate is calculated based on traffic samples.

Table 7-18 Field Descriptions of the show policies statistics Command Output Tables (continued)

Column	Description
Connection	Number of concurrent connections. This information is available for tcp_connections policies and for the following packet types: • in_conns—For the strong protection level • in_nodata_conns—For the analysis protection level
Ratio	Ratio between the number of SYN flagged packets and the number of FIN/RST flagged packets. This information is available for syn_by_fin policies only.

Note The Guard does not display tables that contain no data.

Backing Up the Policy Configuration

You can back up the current zone policies at any time by using the **snapshot threshold-selection cur-thresholds** command in zone configuration mode.

The following example shows how to create a snapshot to back up the current policy configuration:

```
user@GUARD-conf-zone-scannet# snapshot threshold-selection cur-thresholds
```

CHAPTER 8

Learning the Zone Traffic Characteristics

This chapter describes how to use the Cisco Guard (Guard) learning process to analyze zone traffic characteristics to create and tune the policies that the Guard uses for zone protection.

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 the Learning Process and Related Options
- Activating the Policy Construction Phase
- Activating the Threshold Tuning Phase
- Configuring Learning Parameters
- Enabling the Protect and Learn Function
- Using Snapshots to Verify the Results of the Learning Process
- Backing Up the Zone Policies

Understanding the Learning Process and Related Options

The learning process allows the Guard to analyze normal zone traffic conditions to establish a baseline for determining when traffic is normal and when traffic contains anomalies that indicate an attack on the zone. During the learning process, the Guard creates new zone policies and modifies the policy thresholds based on the normal traffic patterns to produce the reference baseline.

To learn the zone traffic characteristics, the Guard analyzes zone traffic that is diverted from its normal network path to Guard. As the Guard analyzes the traffic, it injects the traffic back into the network. You must configure traffic diversion before initiating the learning process or divert the zone traffic to the Guard manually using an external device. You can configure zone traffic diversion using the routing configuration of the Guard. See Chapter 4, “Configuring Traffic Diversion” for more information.

Note During the learning process, the Guard drops packets if one of the following fields in the packet equals zero: source IP address, protocol number, UDP source or destination port, and TCP source or destination port.

If there is an attack on the zone before the learning process has been completed, use on-demand protection to protect the zone if one of the following conditions apply:

- The Guard is in the process of learning the zone traffic.
- You enabled the protect and learn function but the Guard has not learned the zone traffic characteristics (see the "Understanding the Protect and Learn Function" section on page 1-5).
- You have accepted policy thresholds that no longer represent the zone traffic.

For more information about on-demand protection, see the "Activating On-Demand Protection" section on page 9-2.

You can enter **learning**-related commands for several zones at the same time. Enter the command in global mode and use an asterisk (*) as a wildcard. For example, to initiate the policy construction phase for all zones, enter the **learning policy-construction *** command in global mode. To accept the results of the policy construction phase for all Guard zones with names that begin with *scan* (such as scannet and scanserver), enter the **no learning** *scan* *** accept** command in global mode.

This section contains the following topics:

- Understanding the Phases of the Learning Process
- Verifying the Results of the Learning Process
- Understanding the Protect and Learn Function
- Synchronizing the Zone Learning Process Results with a Detector

Understanding the Phases of the Learning Process

The learning process consists of these two phases:

- Policy Construction—The Guard uses the zone configuration's policy templates to create new policies for the services that it detects in the zone traffic. The new policies override the existing policies.

  The policy templates define the types of zone policies that the Guard creates, the maximum number of services that the Guard monitors closely, and the minimum threshold that triggers the Guard to create new policies. To change the rules for constructing zone policies, you must change the policy template parameters before you initiate the policy construction phase. See Chapter 7, "Configuring Policy Templates and Policies," for more information.

  Note You cannot perform the policy construction phase for zones that you created using the GUARD_LINK zone templates.

  For more information about using the policy construction phase, see the "Activating the Policy Construction Phase" section on page 8-4.

- Threshold Tuning—The Guard tunes the thresholds of the zone policies to the traffic rates of the zone services. The new thresholds override the existing thresholds.

  You can activate the threshold tuning phase and zone protection simultaneously (the protect and learn function) to prevent the Guard from learning malicious traffic thresholds. You can set the Guard to constantly tune the zone policies and define the intervals in which the Guard updates the policy thresholds.

Note When you activate the protect and learn function, the Guard constantly diverts the zone traffic to itself.

For more information about using the threshold tuning phase, see the "Activating the Threshold Tuning Phase" section on page 8-6.

During both phases of the learning process, the Guard does not modify the current zone policies until the results of a learning phase are accepted as follows:

- Manually—You accept the results of a learning phase.
- Automatically—You configure the Guard to automatically accept the learning phase results.

After the policies are created, you can add and delete policies or change policy parameters such as thresholds, services, timeouts, and actions.

Verifying the Results of the Learning Process

You can save the current results of either learning phase at any stage during the learning process and review it later by using the **snapshot** command. Taking a snapshot of the learning process allows you to view the policy information that the Guard has created up to the point of the snapshot and decide whether or not to accept the results of the learning process. Saving the results of the learning phase in a snapshot does not affect the zone configuration. You can update the zone configuration with the policy information in a snapshot.

For more information about using the **snapshot** command, see the "Creating Snapshots" section on page 8-13.

Understanding the Protect and Learn Function

After the Guard has performed the policy construction phase, you can activate the threshold tuning phase of the learning process and enable zone protection simultaneously using the protect and learn function. The Guard tunes the policy thresholds while monitoring the traffic for anomalies using the last saved policy thresholds. The protect and learn function enables the Guard to protect the zone, constantly update the policy thresholds based on the zone traffic characteristics, and prevents the Guard from learning malicious traffic thresholds.

Before you activate the protect and learn function, you can configure when and how the Guard accepts the results of the threshold tuning phase by configuring the learning parameters.

See the "Enabling the Protect and Learn Function" section on page 8-11 for more information.

Synchronizing the Zone Learning Process Results with a Detector

You can configure a Detector to perform threshold tuning and to update the corresponding zone configuration on the Guard using a process called *zone synchronization*, For example, when you enable the detect and learn function on the Detector and it detects an anomaly, it stops the learning process, updates the Guard with the latest zone configuration using zone synchronization, and then activates the Guard's attack mitigation services. Zone synchronization enables you to use the Detector to continuously adjust the zone policy thresholds to changes in the traffic for both the Detector and the Guard. Because the Detector analyzes a copy of the zone traffic, you avoid having to constantly divert the zone traffic to the Guard for the learning process.

Note You configure zone synchronization on the Detector only. See the *Cisco Traffic Anomaly Detector Configuration Guide* or the *Cisco Traffic Anomaly Detector Configuration Guide* for more information.

To synchronize the Detector learning process results with the Guard, you must perform the following tasks:

1. Add the Guard to a remote Guard list on the Detector and define the communication method as Secure Sockets Layer (SSL).
2. Establish an SSL communication channel with the Detector. See the "Configuring the SSL Communication Channel Parameters" section on page 3-18.

Create the zone on the Detector using a Guard zone template.You can synchronize the zone configuration with the Detector manually or configure the Detector to synchronize the zone configuration with the Guard automatically. See the "Synchronizing Zone Configurations with a Detector" section on page 5-8 for more information.

Activating the Policy Construction Phase

Use the policy construction phase of the learning process after creating a new zone or any time that the zone configuration needs updating with new service policies. When you enable the policy construction phase, the Guard diverts the zone traffic from the traffic's normal network path so that the traffic flows through the Guard, enabling it to discover the main services (ports and protocols) that the zone uses. The Guard creates the zone policies using the rules established by the policy templates.

Note You can reconfigure the policy construction rules by modifying the policy templates before you initiate the policy construction phase. For example, you can prevent the Guard from creating policies of a certain type by disabling the relevant policy template. You can also modify the default values for the policy parameters (timeout, action, and threshold). See Chapter 7, "Configuring Policy Templates and Policies" for information.

The new policies that the Guard creates during the policy construction phase replace the existing policies when you accept the results of the phase.

Note You cannot perform the policy construction phase of the learning process for zones that are based on these bandwidth-limited link zone templates: GUARD_LINK_128K, GUARD_LINK_1M, GUARD_LINK_4M, and GUARD_LINK_512K.

Caution Before you activate the policy construction phase, make sure that no attack on the zone is in progress so that the Guard does not construct the policies based on the traffic characteristics of a Distributed Denial of Service (DDoS) attack. If you allow the Guard to learn the traffic characteristics of a DDoS attack and save the results of the attack as a baseline, you may prevent the Guard from detecting future attacks because the Guard may view the attacks as normal traffic conditions.

To activate the policy construction phase of the learning process, perform the following steps:

Step 1 Enable the policy construction phase by entering the following command in zone configuration mode:

```
learning policy-construction
```

Step 2 Check that the Guard is diverting the zone traffic.

Wait at least 10 seconds after initiating policy construction or threshold tuning and enter the **show rates details** command. Verify that the value of the *Received traffic* rate is greater than zero. A value of zero indicates a diversion problem.

Step 3 (Optional) Display the policies that the Guard is constructing.

You can save a snapshot of the learning parameters (services, thresholds, and other policy-related data) by using the **snapshot** command at any stage during the policy construction phase, and review it later. You can save a single snapshot or save a periodic snapshot at specified intervals.

For more information, see the "Backing Up the Policy Configuration" section on page 7-24.

Step 4 (Optional) After you have run the policy construction phase long enough for the Guard to analyze a complete sample of the network traffic, you can accept the policies that the Guard suggested without stopping the policy construction phase. You can accept the policies once, or define that the Guard automatically accept the suggested policies at specified intervals. You can ensure that the zone has the most updated policies and continues to learn the zone traffic.

To accept the policies that the Guard suggested and continue the policy construction phase, use the following command:

```
learning accept
```

To automatically accept the policies that the Guard suggests at specified intervals, use the following command:

```
learning-params periodic-action auto-accept learn_params_days learn_params_hours
learn_params_minutes
```

See the "Configuring Learning Parameters" section on page 8-8 for more information.

Use the **no learning-params periodic-action** command to terminate the periodic action.

Step 5 After allowing the Guard enough time to analyze a complete sample of the network traffic, terminate the policy construction phase and accept or reject the current suggested policies.

Note We recommend that you allow the policy construction phase to continue for at least 2 hours before terminating it. This time interval allows the Guard to discover the main services (ports and protocols) that the zone uses.

You can perform one of the following actions:

- Accept the suggested policies—Terminate the policy construction phase and accept the policies that the Guard suggests by entering the following command in zone configuration mode:

  ```
  no learning accept
  ```

  The Guard erases previously learned policies and thresholds.

  After accepting the newly constructed policies, you can manually add or remove policies. See Chapter 7, "Configuring Policy Templates and Policies," for more information.

- Reject the suggested policies—Terminate the policy construction phase and reject the policies that the Guard suggests by entering the following command in zone configuration mode:

  ```
  no learning reject
  ```

  The Guard stops the policy construction phase and makes no changes to the current policies. The policies of the zone are the policies that the Guard had prior to initiating the learning process or prior to the last time that you accepted the results of the policy construction phase.

After performing the policy construction phase, enable the threshold tuning phase to tune the thresholds of each policy (see the "Activating the Threshold Tuning Phase" section on page 8-6).

The following example shows how to initiate the policy construction phase and accept the suggested policies at 12-hour intervals. The example also shows how to stop the policy construction phase and accept the suggested policies.

```
user@GUARD-conf-zone-scannet# learning policy-construction
user@GUARD-conf-zone-scannet# learning-params periodic-action auto-accept 0 12 0
user@GUARD-conf-zone-scannet# no learning accept
```

Activating the Threshold Tuning Phase

Use the threshold tuning phase to enable the Guard to analyze the zone traffic and define thresholds for the zone policies. We recommend that you run the threshold tuning phase during peak traffic time (the busiest part of the day) for a minimum of 24 hours to allow the Guard enough time to properly tune the policy thresholds. However, if the Guard is constantly diverting the zone traffic, you should keep the protect and learn function active and do not terminate the threshold tuning phase.

Note The following procedure includes the command for enabling the protect and learn function which enables the Guard to perform threshold tuning and zone protection simultaneously. We recommend that you enable the protect and learn function when you need to perform the threshold tuning phase (see the "Understanding the Protect and Learn Function" section on page 8-3).

To activate the threshold tuning phase of the learning process, perform the following steps:

Step 1 Initiate the threshold tuning phase by entering one of the following commands in zone configuration mode:

- **learning threshold-tuning**—Enables the threshold tuning phase only.
- **protect learning**—Enables the protect and learn function in which the threshold tuning phase and zone protection perform simultaneously. You can also activate the protect and learn function by entering the **learning threshold-tuning** command and the **protect** command (the order is not important).

Note If you activate the protect and learn function when traffic to the zone is moderate, the Guard may consider the traffic during peak time as an attack. In this case, you can perform one of the following tasks:

- Set the state of the zone policy thresholds to untuned by entering the **no learning-params threshold-tuned** command in zone configuration mode. See the "Marking the Policies as Tuned" section on page 8-10 for more information.

- Deactivate zone protection and continue to learn the zone policy thresholds by entering the **no protect** command in zone configuration mode.

Step 2 Verify that the Guard is diverting the zone traffic. Wait at least 10 seconds after initiating the policy construction phase and enter the **show rates details** command. Verify that the value of the *Received traffic* rate is greater than zero. A value of zero indicates a diversion problem.

Step 3 (Optional) Display the zone policies that the Guard is tuning by using the **snapshot** command (see the "Using Snapshots to Verify the Results of the Learning Process" section on page 8-12).

Step 4 Accept the suggested thresholds. You can accept the thresholds that the Guard suggested and continue the threshold tuning phase, or configure the Guard automatically accept the suggested policies at specified intervals to ensure that the zone has the most updated policies and continues to learn the zone traffic.

To accept the thresholds that the Guard suggested and continue the threshold tuning phase, use the following command:

```
learning accept [threshold-selection {new-thresholds | max-thresholds | weighted weight}]
```

See Table 8-2 on page 8-10 for a description of the threshold-selection arguments and keywords.

To automatically accept the thresholds that the Guard suggests at specified intervals, use the following command:

```
learning-params periodic-action auto-accept learn_params_days learn_params_hours
learn_params_minutes
```

See the "Configuring Learning Parameters" section on page 8-8 for more information.

Use the **no learning-params periodic-action** command to terminate the periodic action.

Step 5 Terminate the threshold tuning phase and accept or reject the current suggested thresholds after allowing the Guard enough time to properly tune the policy thresholds.

Note If you have the protect and learn function enabled, we recommend that you do not terminate the threshold tuning phase.

Perform one of the following actions:

- Accept the current suggested thresholds—Terminate the learning process and accept the policy thresholds that the Guard suggests by entering the following command in zone configuration mode:

  ```
  no learning accept [threshold-selection {new-thresholds | max-thresholds | weighted
  weight}]
  ```

  See Table 8-2 for a description of the threshold-selection arguments and keywords.

  The Guard replaces the previously learned thresholds with the new thresholds. After accepting the newly tuned policies, you can manually change the policy parameters. See Chapter 7, "Configuring Policy Templates and Policies," for more information.

- Reject the current suggested thresholds—Terminate the learning process and reject the policy thresholds that the Guard suggests by entering one of the the following commands in zone configuration mode:
  - `no learning reject`

The Guard stops tuning the thresholds and makes no changes to the current thresholds. This process may result in a situation in which new zone policies have thresholds that were obtained based on past traffic characteristics. We recommend that you enable the threshold tuning phase at a later time or that you configure the thresholds manually.

– `deactivate`

If you have the protect and learn function enabled, use the **deactivate** command to terminate zone protection and the threshold tuning phase without saving the current suggested thresholds.

The following example shows how to initiate the threshold tuning phase and accept the suggested policies at 1-hour intervals. The Guard then stops the threshold tuning phase and accepts the suggested policies if the threshold values are higher than the current values (the max-thresholds method).

```
user@GUARD-conf-zone-scannet# learning threshold-tuning
user@GUARD-conf-zone-scannet# learning-params periodic-action auto-accept 0 1 0
user@GUARD-conf-zone-scannet# no learning accept threshold-selection max-thresholds
```

After performing the threshold tuning phase, you can perform the following tasks:

- Display the learning process results—Use the **show policies statistics** command to view the results of the threshold tuning phase. See the "Displaying Policies" section on page 7-21.
- Modify the learning process results—Change policy parameter values that may not accurately represent normal traffic characteristics. See the "Configuring Policy Parameters" section on page 7-12 for more information.
- Set the policy threshold as fixed—The next time you enable the threshold tuning phase, the Guard ignores new thresholds and maintains the current ones. See the "Setting the Threshold as Fixed" section on page 7-14 for more information.
- Set a fixed multiplier for the policy—The next time you enable the threshold tuning phase, the Guard calculates new policy thresholds by multiplying the learned threshold by the specified multiplier and then applying the threshold selection method on the result. See the "Configuring a Threshold Multiplier" section on page 7-15 for more information.

Configuring Learning Parameters

This section shows how to configure the learning parameters to manage the following functions that affect all of the zone policies:

- Period Guard actions—Configure the Guard to automatically accept the zone policies and save a snapshot of the zone policies at specified intervals.
- Threshold selection method—Configure the default method that the Guard uses to generate new policy thresholds after it accepts the results of the threshold tuning phase.
- Tuned state of the zone policies—Set the state of the current zone polices to tuned or untuned.

To display the current configuration of the learning parameters, use the **show learning-params** command in zone configuration mode.

This section contains the following topics:

- Configuring Periodic Actions
- Configuring the Threshold Selection Method
- Marking the Policies as Tuned

Configuring Periodic Actions

You can configure the Guard to perform one of the following actions at specified intervals:

- Automatically accept the zone policies and save a snapshot of the policies
- Save a snapshot of the zone policies only

See the "Verifying the Results of the Learning Process" section on page 8-3 for more information about snapshots.

To set the periodic action that the Guard performs, use the following command in zone configuration mode:

learning-params periodic-action {**auto-accept** | **snapshot-only**} *learn_params_days learn_params_hours learn_params_minutes*

Table 8-1 provides the arguments and keywords for the **learning-params** command.

Table 8-1 Arguments and Keywords for the learning-params periodic-action Command

Parameter	Description
auto-accept	Accepts the policies that the Guard suggested at the specified interval. The Guard saves a snapshot of the zone policies after accepting the newly suggested ones.
snapshot-only	Saves a snapshot of the policies at the specified interval. The Guard does not accept the new policies and does not modify the policy thresholds.
learn_params_days	Interval in days. Enter an integer from 0 to 1000.
learn_params_hours	Interval in hours. Enter an integer from 0 to 1000.
learn_params_minutes	Interval in minutes. Enter an integer from 0 to 1000.

The value of the interval is the sum of the *learn_params_days* value, the *learn_params_hours* value, and the *learn_params_minutes* value.

The following example shows how to set the Guard to accept the policies at 1-hour intervals:

```
user@GUARD-conf-zone-scannet# learning-params periodic-action auto-accept 0 1 0
```

Configuring the Threshold Selection Method

You can define the default method that the Guard uses to generate new thresholds to accept during the threshold tuning phase. You can accept the results of the threshold tuning phase manually, or configure the Guard to automatically accept the results of the threshold tuning phase at specified intervals.

To configure the threshold selection method, use the following command in zone configuration mode:

learning-params threshold-selection {**new-thresholds** | **max-thresholds** | **weighted** *weight*}

Table 8-2 provides the arguments and keywords for the **learning-params threshold-selection** command.

Table 8-2 Arguments and Keywords for the learning-params threshold-selection Command

Parameter	Description
new-thresholds	Saves the results of the leaning process to the zone configuration.
max-thresholds	Compares the current policy threshold to the learned threshold and saves the higher threshold to the zone configuration. This method is the default.
weighted *weight*	Calculates the policy thresholds to save based on the following formula: new-threshold = (learned-threshold * *weight* + current-threshold * (100 – *weight*)) / 100

This example shows how to configure the Guard to accept the suggested policies if the learned threshold values are higher than the current policy threshold values:

```
user@GUARD-conf-zone-scannet# learning-params threshold-selection max-thresholds
```

Marking the Policies as Tuned

The Guard marks the policy threshold status that defines if the policy thresholds are tuned or not and relates to this status when you enable the protect and learn function. The policy threshold status specifies if the Guard identifies an attack on the zone when the policy threshold is exceeded.

When a new zone is created, or after you accept the policy construction phase results for a zone, the Guard marks the zone policy thresholds as untuned. The default thresholds of the zone templates are tuned so that the Guard activates the anti-spoofing functions quickly if it identifies traffic anomalies in the zone traffic. When you enable the protect and learn function, the learning process might stop if the current zone traffic is higher than the current policy threshold values. To avoid such situations, if the zone policies are not tuned, the Guard does not detect attacks in the zone traffic when you enable the protect and learn function until the zone policy thresholds are accepted once.

If the zone policies are untuned, the Guard activates only a threshold selection method of accept-new and ignores previous threshold values when accepting the new policies. If the Guard accepts the threshold tuning phase results of the learning process for a zone with a threshold selection method other than accept-new, bad policy threshold values may result. See the "Configuring the Threshold Selection Method" section on page 8-9 for more information about the threshold selection method.

The Guard marks the zone policies as untuned in the following situations:

- When creating a new zone
- After accepting the policy construction phase results
- After removing a service or adding a new service to the zone policies

The Guard marks the zone policies as tuned after accepting the threshold tuning phase results.

You can modify the settings of the zone policies. To mark the zone policies as tuned, use the following command in zone configuration mode:

learning-params threshold-tuned

To mark the zone policies as untuned, use the **no** form of this command.

You may want to change the status of the zone policies to tuned when one of the following applies:

- The new zone was duplicated from an existing zone or snapshot that has similar traffic characteristics.
- You have manually configured all policy thresholds.

You may want to change the status of the zone policies to untuned when one of the following applies:

- A major change was made in the zone network.
- The zone IP address or subnet was modified.
- You have not initiated the protect and learn function during the peak traffic time. Change the status of the zone policies to untuned to prevent the Guard from identifying the traffic during the peak time as an attack.

When the zone policies are marked as untuned, the Guard does not monitor the current policy thresholds and does not detect attacks on the zone if the policy thresholds are exceeded.

⚠

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

The following example shows how to mark the status of the zone policies as tuned:

```
user@GUARD-conf-zone-scannet# learning-params threshold-tuned
```

Enabling the Protect and Learn Function

You can enable the threshold tuning phase of the learning process and zone protection simultaneously by using the protect and learn function. The Guard continuously tunes the policy thresholds and at the same time monitors the traffic for anomalies using the last saved policy thresholds. If the Guard detects an attack on the zone, it stops the learning process to prevent it from learning malicious traffic thresholds and begins mitigating the attack. After the attack ends, the Guard resumes the threshold tuning phase along with zone protection.

Perform the following actions before you activate the protect and learn function:

- Activate the policy construction phase of the learning process to construct zone-specific policies (see the "Activating the Policy Construction Phase" section on page 8-4)
- Display the current tuned state of the zone policies by using the **show learning-params** command in zone configuration mode. If the policies are tuned, then the Guard is ready to perform the protect and learn operation.

⚠

Caution If the zone policies are untuned when you enable the protect and learn function, the Guard is unable to provide zone protection until the first time that you accept the results of the threshold tuning phase.

If the policies are untuned when you enable the protect and learn function, the Guard operates as follows:

- Performs the threshold tuning phase of the learning process only. The Guard does not perform zone protection because it does not monitor the traffic for policy threshold violations. After the first time that you accept the results of the threshold tuning phase, the Guard marks the policies as tuned and performs zone protection.

- The Guard activates a threshold selection method of **accept-new** even if you have the threshold selection method configured for **max-threshold** or **weighted** (see the "Configuring the Threshold Selection Method" section on page 8-9). After the first time that you accept the results of the threshold tuning phase, the Guard uses the threshold selection method that you have configured.

See the "Marking the Policies as Tuned" section on page 8-10 for more information.

You can accept the results of the threshold tuning phase manually or configure the Guard to accept the results automatically. You can also configure when and how the Guard accepts the results of the learning process (see the "Configuring Learning Parameters" section on page 8-8).

To activate the learning process and zone protection simultaneously, use the **protect learning** command or enter both the **learning threshold-tuning** command and the **protect** command (the order is not important).

For more information about the threshold tuning phase, see the "Activating the Threshold Tuning Phase" section on page 8-6. For more information about enabling zone protection, see Chapter 9, "Protecting Zones."

Using Snapshots to Verify the Results of the Learning Process

The snapshot function allows you to save a copy of the learning parameters (services, thresholds, and other policy-related data) at any stage of the learning process. You can use snapshots to perform the following tasks:

- Compare the learning parameters of two zones.
- Compare two of the zone snapshots to verify the outcome of the learning process and trace the differences in policies, services, and thresholds.
- Use the policies of a snapshot taken during normal traffic conditions to provide zone protection if an attack occurs during the learning process.
- Copy zone policies from a snapshot to configure the zone according to previous learning results.

We recommend that you save a snapshot every few hours during the learning process. You can take the snapshot manually or configure the Guard to automatically take a snapshot at specified intervals. The Guard can save up to 100 snapshots for each zone. New snapshots replace the previous ones.

This section contains the following topics:

- Creating Snapshots
- Comparing Learning Results
- Displaying Snapshots
- Deleting Snapshots
- Copying Policies to the Zone Configuration

Creating Snapshots

You can save a single snapshot of the zone learning parameters or configure the Guard to automatically take a snapshot at specified intervals. The Guard continues the learning process while taking the snapshot.

To configure the Guard to automatically take a snapshot at specified intervals, see the "Configuring Periodic Actions" section on page 8-9 for more information.

To save a single snapshot of the zone learning parameters, use the following command in zone configuration mode:

snapshot [**threshold-selection** {**cur-thresholds** | **max-thresholds** | **new-thresholds** | **weighted** *calc-weight*}]

Table 8-3 provides the arguments and keywords for the **snapshot** command.

Table 8-3 Arguments and Keywords for the snapshot Command

Parameter	Description
threshold-selection	(Optional) Specifies the method that the Guard uses to calculate the snapshot thresholds. By default, the Guard uses the zone threshold-selection method that is defined by the **learning-params threshold-selection** command. The default zone threshold-selection method is **max-thresholds.**
cur-thresholds	Ignores the new thresholds of the learning process and saves the current policy thresholds to the snapshot. You can use this method to create a backup of the current zone policies and policy thresholds.
max-thresholds	Compares the current policy threshold to the learned threshold and saves the higher threshold to the zone configuration. This is the default method.
new-thresholds	Saves the results of the leaning process to the zone configuration.
weighted *calc-weight*	Calculates the policy thresholds to save based on the following formula: threshold = (new-threshold * *calc-weight* + current-threshold * (100 – *calc-weight*)) / 100

The following example shows how to create a snapshot in which the thresholds are the highest value between the current policy threshold and the new threshold of the learning process:

```
user@GUARD-conf-zone-scannet# snapshot threshold-selection max-thresholds
```

To save a single snapshot in global mode, use the following command:

snapshot *zone-name* [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *weight*}]

Comparing Learning Results

You can compare the learning results of two snapshots or two zones to trace the differences in policies, services, and thresholds.

This section contains the following topics:

- Comparing Snapshots
- Comparing Zones

Comparing Snapshots

To compare two snapshots, use the following command in zone configuration mode:

diff snapshots *snapshot-id1 snapshot-id2* [*percent*]

Table 8-4 provides the arguments for the **diff** command.

Table 8-4 Arguments for the diff Command

Parameter	Description
snapshot-id1	Identifier of the first snapshot to compare. To display a list of the zone snapshots, use the **show snapshots** command.
snapshot-id2	Identifier of the second snapshot to compare.
percent	(Optional) Percentage of difference. The Guard compares the two snapshots and displays only the differences in policy thresholds that are greater than the specified value. The default percentage is 100%, which means that the Guard displays all the differences between the two snapshots.

The following example shows how to display the zone snapshots and compare the two most recent snapshots:

```
user@GUARD-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
3    Feb 10 11:01:50
user@GUARD-conf-zone-scannet# diff 2 3
```

To compare snapshots in global mode, use the following command:

diff *zone-name* **snapshots** *snapshot-id1 snapshot-id2* [*percent*]

Comparing Zones

You can compare the learning parameters of two zones by using the following command in global mode or in configuration mode:

diff *zone-name1 zone-name2* [*percent*]

Table 8-5 provides the arguments for the **diff** command.

Table 8-5 Arguments for the diff Command

Parameter	Description
zone-name1	Name of the first zone with learning parameters to compare.

Table 8-5 Arguments for the diff Command (continued)

Parameter	Description
zone-name2	Name of the second zone with learning parameters to compare.
percent	(Optional) Percentage of difference. The Guard compares the two zones and displays only differences in policy thresholds that are higher than the specified value. The default percentage is 100%, which means that the Guard displays all differences between the two zones.

The following example shows how to compare the learning parameters of two zones:

```
user@GUARD# diff scannet scannet-mailserver
```

Displaying Snapshots

You can display a list of the zone snapshots or the snapshot parameters to get a comprehensive view of the zone learning results by entering the following command in zone configuration mode:

show snapshots [*snapshot-id* [**policies** *policy-path*]]

Table 8-6 provides the arguments and keywords for the **show snapshots** command.

Table 8-6 Arguments and Keywords for the show snapshots Command

Parameter	Description
snapshot-id	(Optional) Identifier of the snapshot to display. If you do not specify policies, the default is to display a list of all the zone snapshots. To view the snapshot ID, use this command with no arguments.
policies *policy-path*	(Optional) Specifies a group of policies to display. See the "Understanding Zone Policies" section on page 7-1 for more information.

To compare snapshots in global mode, use the the following command:

show zone *zone-name* **snapshots** [*snapshot-id* [**policies** *policy-path*]]

The fields of the **show zone** *zone-name* **snapshots** *snapshot-id* **policies** *policy-path* command output are identical to the fields in the output of the **show policies** command. See the "Displaying Policies" section on page 7-21 for more information.

Table 8-7 describes the fields in the **show snapshots** command output.

Table 8-7 Field Descriptions for show snapshots Command Output

Field	Description
ID	Snapshot identifier.
Time	Date and time that the snapshot was taken.

The following example shows how to display a list of the zone snapshots and the policies that are related to dns_tcp in snapshot 2:

```
user@GUARD-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@GUARD-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

Deleting Snapshots

You can delete old snapshots to free disk space by using the following command in zone configuration mode:

no snapshot *snapshot-id*

The *snapshot-id* argument specifies the identifier of an existing snapshot. Enter an asterisk (*) to delete all the zone snapshots. To view the details of a snapshot, use the **show snapshots** command.

The following example shows how to delete all the zone snapshots:

```
user@GUARD-conf-zone-scannet# no snapshot *
```

Copying Policies to the Zone Configuration

You can copy a complete policy configuration or a partial configuration to the current zone.

You can copy the following information:

- Copy services—You can copy services from a source zone to the zone, which allows you to configure the zone policies without applying the policy construction phase to discover these services. Before you copy services to the zone, verify that the zones have similar traffic patterns.
- Copy policy parameters—You can replace the zone policy parameters with the policy parameters of one of the zone snapshots, which allows you to revert to prior learning results. The Guard copies parameters of existing policies only.

To copy the zone policies, use the following command in zone configuration mode:

copy-policies {*snapshot-id* | *src-zone-name* [*service-path*]}

Table 8-8 provides the arguments for the **copy-policies** command.

Table 8-8 Arguments for the copy-policies Command

Parameter	Description
snapshot-id	Identifier of the snapshot from which the policies are copied. To view the snapshot ID, use the **show snapshots** command.
src-zone-name	Name of the zone for which service policies are copied.
service-path	(Optional) Service to be copied. A service path can have one of the following formats: • policy-template—Copies all policies that relate to the policy template. • policy-template/service-num—Copies all policies that relate to the policy template and the specified service. The default is to copy all policies and services.

The following example shows how to copy all services that relate to the policy template tcp_connections from the zone webnet to the current zone, scannet:

```
user@GUARD-conf-zone-scannet# copy-policies webnet tcp_connections/
```

The following example shows how to display a list of the zone snapshots and then copy the policies from the snapshot with ID 2:

```
user@GUARD-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@GUARD-conf-zone-scannet# copy-policies 2
```

Backing Up the Zone Policies

You can create a backup the current zone policies at any time by using the following command in zone configuration mode:

snapshot threshold-selection cur-thresholds

The following example shows how to back up the current zone policies:

```
user@GUARD-conf-zone-scannet# snapshot threshold-selection cur-thresholds
```

CHAPTER 9

Protecting Zones

This chapter describes how to configure and activate the Cisco Guard (Guard) to protect a zone. These procedures are required to enable zone protection.

Note The Guard can protect several zones at the same time providing their IP address ranges do not overlap.

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 Zone Protection Requirements and Options
- Activating On-Demand Protection
- Configuring the Zone Protection Mode of Operation
- Configuring the Protection Activation Method
- Configuring the Activation Sensitivity for Zone Protection
- Configuring the Protection Activation Extent
- Understanding Subzones
- Configuring the Protection Inactivity Timeout
- Activating Zone Protection
- Deactivating Zone Protection

Understanding Zone Protection Requirements and Options

Before you activate zone protection, observe the following requirements and recommendations:

- Configure traffic diversion—You must configure traffic diversion to enable the Guard to hijack zone traffic from its normal network path for analysis and attack mitigation and then to inject the legitimate traffic only back into the network. See Chapter 4, “Configuring Traffic Diversion” for more information.

- Update the zone configuration—We recommend that you use one of the following methods to ensure that the zone configuration is up to date, enabling the Guard to accurately discern between normal traffic conditions and attack traffic:
  - Learning process—The Guard creates a set of zone-specific policies and poly thresholds based on the zone traffic characteristics. See Chapter 8, "Learning the Zone Traffic Characteristics" for more information.
  - Zone synchronization—The Detector learns the zone traffic for the Guard and synchronizes the zone configuration with the Guard (automatically or manually). See the "Synchronizing Zone Configurations with a Detector" section on page 5-8 for more information.
- Activate the protect and learn function—The Guard monitors the zone traffic for anomalies (attacks) while performing the threshold tuning phase of the learning process. If the Guard detects an attack, it suspends the threshold tuning phase while it mitigates the attack.

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

  See the "Enabling the Protect and Learn Function" section on page 8-11for more information.
- Define the protection characteristics—You can configure the following optional protection characteristics:
  - Operation mode—Configure how the Guard performs zone protection and define whether the Guard applies measures to protect the zone automatically or in an interactive manner (see the "Configuring the Zone Protection Mode of Operation" section on page 9-3).
  - Activation method—Define whether to activate the zone according to the zone name, the zone address range, or the received traffic (see the "Configuring the Protection Activation Method" section on page 9-4). You should configure the activation method if zone protection is activated by an external device, such as a Detector.
  - Activation extent—Define whether to activate zone protection for the entire zone address range or only for a specific IP address within the zone (see the "Configuring the Protection Activation Extent" section on page 9-6). The activation extent applies to zones where zone protection is activated by an external device, such as a Detector only.
  - Protection termination timeout—Define the timeout after which the Guard terminates zone protection (see the "Configuring the Protection Inactivity Timeout" section on page 9-8).

Activating On-Demand Protection

On-demand protection is the act of using one of the predefined zone templates to mitigate an attack on a zone that occurs before the Guard has learned the specifics of the zone traffic. Each policy template contains a set of predefined policies and filters that provide immediate zone protection. The default thresholds of these zone policies are tuned so that the Guard activates the anti-spoofing functions quickly if it identifies traffic anomalies in the zone traffic.

The default thresholds used to block (drop) source IP addresses are set to high values and because they are not tuned specifically to the zone traffic, on-demand protection requires that you monitor the mitigation process for nonspoofed attacks. You must monitor the zone legitimate rate, malicious traffic rate, and the Guard mitigation actions.

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

- The Guard is currently learning the zone traffic.
- You have enabled the protect and learn function and the Guard has not had enough time to learn the zone traffic.
- The current policy thresholds of the zone configuration do not accurately represent normal zone traffic.

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

Step 1 Create a new zone by entering the following command:

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

See the "Creating a New Zone from a Zone Template" section on page 5-4 for more information.

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

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

See the "Configuring Zone Attributes" section on page 5-5 for more information.

Step 3 Activate zone protection by entering the following command:

```
protect
```

See the "Activating Zone Protection" section on page 9-9 for more information.

Step 4 Analyze the zone traffic patterns. See Chapter 14, "Analyzing Guard Mitigation" for more information.

Configuring the Zone Protection Mode of Operation

During an attack on a zone, the Guard creates dynamic filters that determine how the Guard mitigates the attack. You can configure the Guard to execute the mitigation 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 mitigation actions, you configure the Guard to perform zone protection in one of the following modes:

- Automatic protect mode—The Guard activates the dynamic filter actions as soon as the Guard creates the filter. This operation mode is the default.
- Interactive protect mode—The Guard 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 protect mode, use the following command in zone configuration mode:

interactive

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

no interactive

See Chapter 10, “Using Interactive Protect 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 the Protection Activation Method

The protection activation method defines how the Guard identifies the zone requiring protection when it receives an external indication, which can be a command from an external device, such as a Detector, or traffic that is destined to the zone as determined by the packet IP address.

You can configure the Guard to use one of the following methods to activate protection:

- IP address—Activates zone protection when it receives a command from an external device, such as a Detector, that consists of an IP address or subnet that is part of the zone.
- Packet—Activates zone protection when it receives traffic that is destined to the zone.
- Packet or IP address—Activates zone protection when it receives traffic (a packet) that is destined to the zone or when it receives a command from an external device, such as the Detector, that consists of an IP address or subnet that is part of the zone address range.
- Zone name only—Activates zone protection based on the zone name.

Perform the following tasks when you configure zones with a protection activation method of packet, or packet or IP address:

- Manually divert the zone traffic to the Guard using an external device so the Guard can monitor the zone traffic.
- Ensure that you do not configure multiple zones with the same IP address range or zone protection may not function properly.
- (Optional) Configure the minimum received traffic rate that is required for the Guard to activate zone protection by entering the **protect-packet activation-sensitivity** command (see the “Configuring the Activation Sensitivity for Zone Protection” section on page 9-6 for more information).

The Guard activates the entire zone or a specific IP address range according to the zone activation extent unless the protection activation method is zone name only, in which case the Guard activates the entire zone (see the “Configuring the Protection Activation Extent” section on page 9-6 for more information).

To configure the protection activation method, use the following command in zone configuration mode:

activation-interface {**ip-address** | **packet** [**divert**] | **packet-or-ip-address** [**divert**] | **zone-name-only**}

The default is **zone-name-only**. If you create a zone by duplicating an existing zone, the protection activation method is set to the **zone-name-only**, regardless of the configuration of the source zone (see the “Creating a New Zone by Duplicating an Existing Zone” section on page 5-5 for more information).

Table 9-1 provides the keywords for the **activation-interface** command.

Table 9-1 Keywords for the activation-interface Command

Parameter	Description
ip-address	Activates zone protection when it receives a command from an external device, such as a Detector, that consists of an IP address or subnet that is part of the zone. The Guard scans the zone database and activates the zone that has an address range that includes the received IP address or subnet. If you have configured several zones with an address range that includes the received IP address, the Guard activates the zone with the longest prefix match (the zone that has the most specific address range that includes the received IP address). The received IP address or subnet must be completely included in the zone IP address range.
packet	Activates zone protection when it receives traffic for the zone as determined by the packet IP address. The Guard scans the zone database and activates the zone that has an address range that includes the received packet IP address. If you have configured several zones with an address range that includes the received packet IP address, the 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. **Note** When you configure a zone with a protection activation method of **packet**, the Guard changes the way that it handles traffic that is not destined to an active zone. If you have configured injection for that traffic, the Guard forwards the traffic instead of dropping it.
divert	(Optional) Sends a BGP[1] announcement to the adjacent router to divert the zone traffic from the original path to the Guard. Use the **divert** keyword when a Detector activates zone protection on the Guard using BGP. See the *Cisco Traffic Anomaly Detector Configuration Guide* for more information.
packet-or-ip-address	Activates zone protection when it receives traffic (a packet) that is destined to the zone or when it receives a command from an external device, such as the Detector, that consists of an IP address or subnet that is part of the zone address range. See the ip-address and packet protection activation methods in this table for more information.
zone-name-only	Activates zone protection based on the zone name. The Guard activates zone protection for the zone called out in the command that the Guard receives from an external device such as a Detector. This activation method is the default.

[1] BGP = Border Gateway Protocol

The following example shows how to configure the protection activation method so that the Guard activates protection when it receives a packet that is within the zone IP address range:

```
user@GUARD-conf-zone-scannet# activation-interface packet
```

Note If the activation extent is **ip-address-only** (see the "Configuring the Protection Activation Extent" section on page 9-6) and the protection 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 using the

protection-end-timer command (see the "Configuring the Protection Inactivity Timeout" section on page 9-8). If you enter the **protection-end-timer forever** command, the Guard does not terminate zone protection when the attack ends and does not delete the subzone that it has created to protect the specific IP address.

You can create a default zone for the Guard to protect if the received IP address or packet is not part of any other zone. You can define a default zone only if the network is homogenous and can use the same zone template. You cannot perform the learning process with a default zone. Create the default zone with the following required parameters:

- Configure the default zone with the following two IP addresses:
  - 0.0.0.0 128.0.0.0
  - 128.0.0.0 128.0.0.0
- Define the activation extent as ip-address (see the "Configuring the Protection Activation Extent" section on page 9-6). To display the zone activation method, use the **show running-config** command in zone configuration mode.

Configuring the Activation Sensitivity for Zone Protection

You can configure the activation sensitivity parameter that determines when the Guard activates zone protection based on the traffic rate to a single IP address. The Guard activates zone protection only if the received traffic rate to a single IP address is higher than the activation sensitivity value that you define. The Guard applies the activation sensitivity parameter to all of the zones that you configure with a protection activation method of **packet** or **packet-or-ip-address** (see the "Configuring the Protection Activation Method" section on page 9-4).

To define the minimum packet rate that is required to activate zone protection, use the following command in configuration mode:

protect-packet activation-sensitivity *min-rate*

The *min-rate* argument defines the minimum packet rate that is destined to a single zone destination IP address that causes the Guard to activate zone protection. The default is 1 packet per second (pps).

The following example shows how to configure the activation sensitivity to 10 pps:

```
user@GUARD-conf# protect-packet activation-sensitivity 10
```

Configuring the Protection Activation Extent

The protection activation extent defines whether the Guard activates zone protection for the entire zone or for a partial zone when it receives an external indication from an external device, such as the Detector, or traffic that is destined to the zone as determined by the packet IP address.

The Guard supports the following activation extent methods:

- Entire zone—Activates zone protection for the entire zone. The Guard activates zone protection when it receives traffic that is destined to the zone or when it receives an external indication that consists of an IP address or subnet that is part of the zone.

- IP Address only—Activates zone protection only for the specified IP address or subnet. When the Guard receives traffic that is destined to the zone or when it receives a command from an external device, such as the Detector, which consists of an IP address or subnet that is part of the zone, the Guard creates a new zone (subzone). This activation extent is the default. See the "Understanding Subzones" section on page 9-7 for more information.

To configure the activation extent, use the following command in zone configuration mode:

activation-extent {**entire-zone** | **ip-address-only**}

Table 9-2 provides the keywords for the **activation-extent** command.

Table 9-2 Keywords for the activation-extent Command

Parameter	Description
entire-zone	Activates zone protection for the entire zone.
ip-address-only	Activates zone protection only for the specified IP address or subnet. This activation extent is the default.

The following example shows how to use the **activation-extent** command to configure the activation extent of zone protection for the entire zone:

```
user@GUARD-conf-zone-scannet# activation-extent entire-zone
```

To display the zone activation extent, use the **show running-config** command.

Understanding Subzones

The Guard creates a subzone when it activates zone protection for a partial zone (a zone that does not include the complete IP address range of the source zone). The IP address range of the subzone is included in the address range of the source zone.

The subzone configuration is similar to the configuration of the source zone except that the IP address and zone name are different. The name of the subzone consists of the first 30 characters of the name of the source zone, the IP address, and the subnet, concatenated with underscores. If the subzone consists of a single IP address, the subnet is not added. For example, if the name of the source zone is *scannet* with an address range of *10.10.10.0* and a subnet of *255.255.255.0* and the Guard activates zone protection for an internal range of IP address *10.10.10.192* and subnet *255.255.255.252*, the name of the subzone is *scannet_10.10.10.192_255.255.255.252*.

The IP address and subnet of the subzone are the IP address and subnet that the Guard received with the external command or the IP address of the packet that triggered the Guard to activate zone protection.

The Guard deletes subzones when it terminates zone protection. The Guard terminates zone protection for a subzone according to how you configure the source zone's activation method and the protection termination timeout. The Guard does not delete a subzone if you manually terminate zone protection by using the **no protect** command or the **deactivate** command.

Note If you configure the timer that the Guard uses to determine when an attack on the zone has ended by using the **protection-end-timer forever** command, the Guard does not terminate zone protection when the attack ends and does not delete the subzone.

When the Guard deletes a subzone, it does not erase the logs and attack reports of the subzone. To display the subzone logs and reports after the Guard deletes the subzone, use the following commands:

- **show log** *sub-zone-name*—See the "Displaying the Guard Configuration" section on page 12-1 for more information.
- **show reports** *sub-zone-name* [*report-id* | **current**] [**details**]—See the "Displaying Attack Reports" section on page 11-8 for more information.

You can display the list of the subzones that the Guard created from the zone by entering the **show log** or **show reports** commands without specifying a subzone name.

The following example shows how to display the logs of a subzone that was erased:

```
user@GUARD-conf-zone-scannet# show logs scannet_10.10.10.192
```

Configuring the Protection Inactivity Timeout

You can configure the Guard to automatically stop zone protection when a specified period of inactivity passes. The Guard measures the inactivity period based on the dynamic filter inactivity and the dropped traffic. If for a specified span of time, no dynamic filters are in use and both the following conditions apply, the Guard assumes the attack on the zone has ended:

- No new dynamic filters are added—See the "Deactivating Dynamic Filters" section on page 6-23 for information about how the Guard decides when to remove dynamic filters.
- The rate of the zone traffic that is being dropped is lower than the defined threshold—The Guard drops zone packets that the dynamic filters, user filters, and flex-content filters have identified as part of an attack, and the Guard drops traffic that has exceeded the rate limit that was defined for the zone when you use the **rate-limit** command. The Guard counts the dropped packets using the zone dropped counter (see the "Using Counters to Analyze Traffic" section on page 12-3 for more information). The default threshold is 1 pps. To change the drop counter threshold, use the following command in zone configuration mode:

  attack-detection zone-malicious-rate *threshold*

  The *threshold* argument defines the minimum rate of dropped zone packets. If the rate goes lower than this threshold, the Guard may end zone protection. If the rate exceeds this threshold, the Guard identifies an attack on the zone and creates an attack report.

If the zone activation method is Packet, the Guard checks for inactivity based on the received traffic before deactivating a zone. The Guard deactivates protection only if the previous conditions apply, and no packet to the zone was received.

To define the inactivity timeout, use the following command in zone configuration mode:

protection-end-timer {*time-seconds* | **forever**}

Table 9-3 provides the arguments and keywords for the **protection-end-timer** command.

Table 9-3 Arguments and Keywords for the protection-end-timer Command

Parameter	Description
time-seconds	Timeout in seconds. Enter an integer greater than 60.
forever	Sets an indefinite timeout.

The default is **forever**. If you do not change the default value, you must deactivate zone protection manually.

The following example shows how to configure the protection inactivity timeout:

```
user@GUARD-conf-zone-scannet# protection-end-timer 300
```

Activating Zone Protection

You can configure the Guard to activate zone protection when it receives a command from an external device (such as a Detector) or you can activate zone protection manually at any time after you configure the zone. If the zone is under attack before the Guard has learned the zone traffic characteristics, use on-demand protection to protect the zone. The Guard default policy thresholds for a new zone enable effective on-demand protection. See the "Activating On-Demand Protection" section on page 9-2 for more information.

Note You must manually divert the zone traffic to the Guard using an external device if you configure the activation extent to **packet** by using the **activation-interface packet** command or the Guard cannot monitor the zone traffic (see the "Configuring the Protection Activation Extent" section on page 9-6).

You can verify that the Guard is receiving the zone traffic after you activate zone protection by waiting at least 10 seconds after activating zone protection and then entering the **show rates** command. Verify that the value of at least one of the rates is greater than zero. If the value of all rates equals zero, a diversion problem could exist. See Chapter 4, "Configuring Traffic Diversion" and Appendix B, "Troubleshooting Diversion," for more information.

You can activate zone protection for the entire zone or for only a portion of the zone as described in the following sections:

- Protecting the Entire Zone
- Protecting an IP Zone that is Part of the Zone Address Range
- Protecting an IP Address when the Zone Name is Not Known

Protecting the Entire Zone

You can protect the entire zone by entering the following command in zone configuration mode:

protect [**learning**]

The optional **learning** keyword enables the Guard to protect the zone and tune the policy thresholds using the protect and learn function (see the "Enabling the Protect and Learn Function" section on page 8-11 for more information).

The following example shows how to activate zone protection:

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

Protecting an IP Zone that is Part of the Zone Address Range

You can protect an IP-specific zone that is a part of the zone address range. In this case, the Guard creates a new zone. The name of the new zone consists of the first 30 characters of the major zone and the specific IP address concatenated by an underscore. If a zone by the same name already exists, the Guard activates zone protection for the existing zone instead of creating another zone by the same name.

To activate zone protection for an IP-specific zone, use the following command in global mode:

protect *zone-name ip-address-general*

Table 9-4 provides the arguments for the **protect** command.

Table 9-4 Arguments for the Zone Configuration Mode protect Command

Parameter	Description
zone-name	Name of the zone.
ip-address-general	Specific IP address within the zone address range. Enter the IP address in dotted-decimal notation. For example, enter 192.168.5.6.

To remove this zone, use the **no** form of the **zone** command.

The following example shows how to activate zone protection for IP address 192.168.5.6 that is included in the IP address range of the zone scannet:

```
user@GUARD# protect scannet 192.168.5.6
creating zone scannet_192.168.5.6
user@GUARD#
```

Protecting an IP Address when the Zone Name is Not Known

You can protect a specific IP address within a zone’s range of IP addresses even if you do not know the name of the zone by entering the following command in global mode:

protect *ip-address-general* [*subnet-mask*]

Table 9-5 provides the arguments for the **protect** command.

Table 9-5 Arguments for the Global Mode protect Command

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

The Guard activates zone protection for the zone that the IP address is included in its IP address range based on the IP address activation method. See the *“Configuring the Protection Activation Extent” section on page 9-6* for more information.

The following example shows how to activate zone protection for IP address 192.168.5.6:

```
user@GUARD# protect 192.168.5.6
```

Note You can enter the **protect**-related commands for several zones at the same time. Enter the command in global mode and use an asterisk (*) as a wildcard. For example, to activate zone protection for all zones, enter the **protect *** command in global mode. To activate zone protection for all zones with names that begin with *scan* (such as scannet and scanserver), enter the **protect** *scan****** command in global mode.

Deactivating Zone Protection

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

To deactivate zone protection, use one of the following commands in zone configuration mode:

- **no protect**—Ends zone protection. If you enabled the protect and learn function, the Guard continues to learn the policy thresholds.

  Note You can enter the **protect**-related commands for several zones at the same time by entering the command in global mode and using an asterisk (*) as a wildcard. For example, to stop zone protection for all zones, enter the **no protect *** command in global mode. To stop zone protection for all zones with names that begin with *scan* (such as scannet and scanserver), enter the **no protect** *scan****** command in global mode.

- **deactivate**—Ends both zone protection and the threshold tuning phase of the learning process.

The following example show how to deactivate zone protection and the learning process:

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

CHAPTER 10

Using Interactive Protect Mode

You can activate the Cisco Guard (Guard) to perform zone protection in either one of the following modes of operation:

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

This chapter describes the interactive protect mode and how to switch between the two modes of operation.

This chapter includes the following sections:

- Understanding Interactive Protect Mode
- Activating Interactive Protect Mode and Zone Protection
- Configuring the Zone for Interactive Protect Mode
- Displaying Recommendations
- Managing Recommendations
- Deactivating Interactive Protect Mode

Understanding Interactive Protect Mode

When a Distributed Denial of Service (DDoS) attack on a zone begins, the zone policies create dynamic filters to mitigate the attack. If you configure the zone to operate in interactive protect mode, the Guard does not activate the dynamic filters automatically, but waits for you to decide on what action to take. The filters that await your decision are called *pending dynamic filters*. The Guard groups the pending dynamic filters according to the policy that produced them and presents the groups to you as Guard *recommendations*, which provide the following information:

- A summary of the pending filters, including information about the name of the policy that caused the creation of the pending dynamic filters.
- The data on the traffic anomaly that resulted in the policy activation.
- The number of pending dynamic filters.
- The recommended action.

When you enable interactive protect mode in a zone configuration, you take control over which actions the Guard executes to mitigate an attack in progress. You decide which pending dynamic filters to accept, ignore, or direct to automatic activation. You can configure the zone to operate in interactive protect mode when you define the zone, before you activate zone protection, or after you activate zone protection.

The Guard continues to produce pending dynamic filters as long as it is in interactive protect mode. You can enable the interactive protect mode at any time during zone protection.

The Guard can manage up to 1000 pending dynamic filters and when the number of pending dynamic filters reaches this limit, the Guard performs the following actions:

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

You can switch from the interactive protect mode to the automatic protect mode at any time during zone protection, even when the zone is under attack. When you switch to automatic protect mode during an attack, the Guard performs the following actions:

- Retains the dynamic filters that were added as a result of you accepting a recommendation.
- Accepts the pending dynamic filters associated with any recommendations that you did not act upon prior to switching to automatic protect mode.
- Accepts any new dynamic filters automatically as the policies produce them.

Activating Interactive Protect Mode and Zone Protection

This section provides a quick overview of the steps that you need to take to activate the Guard in interactive protect mode. Each step includes the CLI command required to complete the task.

To activate interactive protect mode, perform the following steps:

Step 1 Configure a new or existing zone to operate in interactive protect mode by using the appropriate command as follows:

- New zone—Enter the **zone** *new-zone-name* **interactive** command in zone configuration mode.

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

- Existing zone—Enter the **interactive** command in zone configuration mode.

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

See the "Configuring the Zone for Interactive Protect Mode" section on page 10-3 for more information.

Step 2 (Optional) Configure the Guard to display a notification when new recommendations are available by using the **event monitor** command.

```
user@GUARD# event monitor
```

You can also use an external syslog server to receive notification of new pending dynamic filters or manually display the status of the zone by using the **show** command in zone configuration mode.

Step 3 Activate the Guard to learn the zone traffic patterns by using the **learning** command.

If you have created the zone for on-demand protection, you can skip this step (see the "Activating On-Demand Protection" section on page 9-2 for more information about on-demand protection).

See Chapter 8, "Learning the Zone Traffic Characteristics," for more information on the learning process.

Step 4 Activate zone protection by using the **protect** command.

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

See Chapter 9, "Protecting Zones," for more information.

Step 5 Display new recommendations and their pending dynamic filters by using the **show recommendations** command.

```
user@GUARD-conf-zone-scannet# show recommendations
user@GUARD-conf-zone-scannet# show recommendations 135 pending-filters
```

See the "Displaying Recommendations" section on page 10-4 for more information.

Step 6 Decide how to manage the new recommendations by using the **recommendation** command. You can decide to accept, ignore, or have the Guard automatically activate the new recommendations.

```
user@GUARD-conf-zone-scannet# recommendation 135 accept
```

See the "Managing Recommendations" section on page 10-5 for more information.

Step 7 You can deactivate interactive protect mode at any time by using the **no interactive** command. The Guard activates new dynamic filters automatically.

```
user@GUARD-conf-zone-scannet# no interactive
```

See the "Deactivating Interactive Protect Mode" section on page 10-7 for more information.

Configuring the Zone for Interactive Protect Mode

You can activate interactive protect mode for an existing zone by using the **interactive** command in zone configuration mode.

The following example shows how to activate interactive protect mode for an existing zone:

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

To create a new zone configured for interactive protect mode, use the following command in configuration mode:

zone *new-zone-name* **interactive**

The *new-zone-name* argument specifies the name of the new zone. The zone name is an alphanumeric string that must start with a letter, cannot include any spaces, and can have a maximum of 63 characters.

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

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

The new zone is created with a default zone template that is configured for interactive protect mode. See the "Creating a New Zone" section on page 5-3 for more information.

Displaying Recommendations

You can display a list of all recommendations, a list of pending dynamic filters, or a specific recommendation for a zone by entering the following command in zone configuration mode:

show recommendations [*recommendation-id*] [**pending-filters**]

Table 10-1 provides the keywords and arguments for the **show recommendations** command.

Table 10-1 Keywords and Arguments for the show recommendations Command

Parameter	Description
recommendation-id	(Optional) ID for a specific recommendation.
pending-filters	(Optional) Displays a list of the pending filters for a specific recommendation.

The following example shows how to display a list of all recommendations:

```
user@GUARD-conf-zone-scannet# show recommendations
```

Table 10-2 describes the fields in the **show recommendations** command output.

Table 10-2 Field Descriptions for the show recommendations Command Output

Field	Description
ID	Recommendation identification number.
Policy	Policy that created the recommendation.
Threshold	Policy threshold that was exceeded.
Detection date	Date and time that the recommendation was created.
Attack flow	Characteristics of the attack flow. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. They indicate whether or not the traffic is fragmented. A value of **any** indicates that there is both fragmented and nonfragmented traffic.
Min current rate	Minimum attack rate measured in packets per second (pps). For recommendations that have several pending dynamic filters, the rate of the lowest pending dynamic filter is displayed.
Max current rate	Maximum attack rate measured in packets per second (pps). For recommendations that have several pending dynamic filters, the rate of the highest pending dynamic filter is displayed.
No. of pending-filters	Number of pending dynamic filters that were created because the policy threshold was exceeded.
Recommended action	Recommended action. This action is taken if you accept the recommendation.

To display a list of all recommendations with recommendation IDs before displaying pending filters for a specific recommendation, use the **show recommendations** command.

Table 10-3 describes the fields in the **show recommendations pending-filters** command output.

Table 10-3 Field Descriptions for the show recommendations pending-filters Command

Field	Description
ID	Recommendation identification number.
Policy	Policy that created the recommendation.
Threshold	Policy threshold, in packets per second (pps), that was exceeded.
Pending-filter-id	Pending dynamic filter identification number.
Detection date	Date and time that the recommendation was created.
Attack flow	Flow characteristics of the attack. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. They indicate whether or not the traffic is fragmented. A value of **any** indicates that there is both fragmented and nonfragmented traffic.
Triggering rate	Attack rate, in packets per second (pps), that triggered the creation of the pending dynamic filter.
Current rate	Current attack rate in packets per second (pps).
Recommended action	Recommended action. This action is taken if you accept the recommendation.
Action flow	Resulting characteristics of the traffic flow to the zone if you accept the pending dynamic filter. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. They indicate whether or not the traffic is fragmented. A value of **any** indicates that there is both fragmented and nonfragmented traffic.

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

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

Note You can display recommendations and their pending dynamic filters only if the Guard is in interactive protect mode and a DDoS attack on the zone is in progress.

The following example shows how to display the pending dynamic filters of recommendation 135:

```
user@GUARD-conf-zone-scannet# show recommendations 135 pending-filters
```

Managing Recommendations

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

You can instruct the Guard to automatically activate the pending dynamic filters of a specific policy. You can also instruct the Guard to prevent policies from producing recommendations. The Guard policies continue to produce recommendations if the zone is in interactive protect mode and a DDoS attack is in progress. We recommend that you display the zone status when you manage recommendations in order to verify the zone status and determine whether or not additional actions are required.

Note When you accept a recommendation, you also accept the additional recommendations that contain the same or partial flow with the same action and timeout as the accepted recommendation. The Guard deletes any duplicate recommendations.

To decide on recommendations for a zone, use the following command in zone configuration mode:

recommendation *recommendation-id* [**pending-filters** *pending-filter-id*] *decision* [*timeout*]

Table 10-4 provides the arguments and keywords for the **recommendation** command.

Table 10-4 Arguments and Keywords for the recommendation Command

Parameter	Description
recommendation-id	Identification number of the recommendation. An asterisk (*****) is a wildcard, indicating all recommendations.
pending-filters *pending-filter-id*	(Optional) Specifies the ID of a specific pending dynamic filter.
decision	Action for the recommendation. The following are possible values: • **accept**—Accepts the specific recommendation. The pending dynamic filters become active dynamic filters. • **always-accept**—Accepts the specific recommendation. The decision applies automatically whenever the recommendation policy produces new recommendations. Pending dynamic filters automatically become active dynamic filters. If you take this action, the Guard no longer displays such recommendations. • **always-ignore**—Ignores the specific recommendation. No dynamic filter or pending dynamic filters are produced. The decision automatically applies to all future recommendations produced by the policy. If you decide to always ignore a recommendation, the Guard no longer displays it.
timeout	(Optional) Length of time that the decision applies. The following are possible values: • **forever**—Activates the dynamic filters produced by the recommendations for as long as protection is in effect. This timeout is the default. See the “Configuring Dynamic Filters” section on page 6-18 for more information. • ***new-timeout***—Activates the dynamic filters produced by the policies for a period of time that you define. This time is measured in seconds. See the “Configuring Dynamic Filters” section on page 6-18 for more information.

The following example shows how to accept recommendation 135:

```
user@GUARD-conf-zone-scannet# recommendation 135 accept
```

You can configure the interactive status for a specific policy, or any part of it, and decide whether or not that part of the policy should produce recommendations and pending dynamic filters. Configuring the interactive status of a policy gives you control and enables you to improve how policies adapt to traffic flows. See the "Configuring the Policy Interactive Status" section on page 7-20 for more information.

The Guard does not display **always-accept** or **always-ignore** recommendations. When you decide to always ignore or accept a recommendation, your decision becomes part of the interactive status of the policy that created the recommendation.

You can disable or inactivate a policy to prevent the policy from producing recommendations and their pending dynamic filters. Use the **state** command to disable or inactivate a policy. See the "Changing the Policy State" section on page 7-13 for more information.

The following example configures the interactive status for dns_tcp/53/analysis to **always-accept**:

```
user@GUARD-conf-zone-scannet-policy-/dns_tcp/53/analysis/# interactive-status
always-accept
```

Deactivating Interactive Protect Mode

To deactivate the interactive protect mode, use the **no interactive** command in zone configuration mode. When you deactivate the interactive protect mode, the Guard activates all new dynamic filters automatically and configures the interactive status of the policies to **always-accept** (see the "Displaying Policies" section on page 7-21 for information on displaying the zone policies).

The following example shows how to deactivate interactive protect mode for the zone scannet:

```
user@GUARD-conf-zone-scannet# no interactive
```

CHAPTER 11

Using Attack Reports

This chapter describes the attack reports that the Cisco Guard (Guard) produces and contains the following sections:

- Understanding the Report Layout
- Understanding the Report Parameters
- Displaying Attack Reports
- Exporting Attack Reports
- Deleting Attack Reports

Understanding the Report Layout

The Guard provides an attack report for each zone to help you form a comprehensive view of the attack. An attack begins when the Guard produces the first dynamic filter and ends when no dynamic filter is in use and no new dynamic filters are added. Reports include details of the attacks that are organized into sections that describe different characteristics of the traffic flow during an attack. You can display reports of previous attacks and ongoing attacks, and you can export reports to a network server using File Transfer Protocol (FTP), Secure FTP (SFTP), or Secure Copy Protocol (SCP).

This section contains the following topics:

- General Details
- Attack Statistics
- Malicious Packet Statistics
- Detected Anomalies
- Mitigated Attacks
- Zombies

General Details

The general details section of the attack report includes general information about an attack.

Table 11-1 describes the fields in this section of the report.

Table 11-1 Field Descriptions in General Details Section of Attack Report

Field	Description
Report ID	Identification number of the report. A value of **current** indicates that there is an ongoing attack.
Attack Start	Date and time that the attack started.
Attack End	Date and time that the attack ended. A value of **Attack in progress** indicates that there is an ongoing attack.
Attack Duration	Duration of the attack.

Attack Statistics

The attack statistics' section provides a general analysis of the zone traffic flow for various packets. Table 11-2 describes the packet types.

Table 11-2 Packet Types

Type	Description
Received	Total amount of the diverted traffic.
Forwarded	Legitimate traffic that the Guard forwarded on to the zone.
Replied	Traffic that the Guard anti-spoofing and anti-zombie mechanisms sent back to the source in a verification attempt.
Dropped	Traffic that the Guard dropped.

Malicious Packet Statistics

The malicious packets statistics' section of the attack report analyzes the packets that the Guard dropped and sent back to the source in a verification attempt (replied). The report classifies the packets by their type (spoofed or malformed) and by the Guard function that handled them (filter types or the rate limiter).

Table 11-3 describes the different types of malicious packets.

Table 11-3 Types of Malicious Packets

Type	Description
Rate Limiter	Packets that were dropped because they exceeded the rate of traffic defined by the rate limit parameter of the user filters and the zone **rate-limit** command as allowed to be injected to the zone.
Flex-Content Filters	Packets that were dropped by the flex-content filters.
User Filters	Packets that were dropped by the user filters.
Dynamic Filters	Packets that were dropped by the dynamic filters.

Table 11-3 Types of Malicious Packets (continued)

Type	Description
Spoofed	Packets that were identified by the Guard as spoofed packets or packets originated by zombies and not injected to the zone. Spoofed packets are replied (bounced) packets to which no replies were received.
Malformed	Packets that were analyzed as malformed because of their malformed structure or due to the Guard anti-spoofing functions.

Detected Anomalies

The detected anomalies' section of the attack report provides details of the traffic anomalies that the Guard detected in the zone traffic. A flow is classified as being an anomaly when it requires the production of a dynamic filter. These anomalies can occur infrequently or can turn into systematic Distributed Denial of Service (DDoS) attacks. The Guard clusters anomalies with the same type and flow parameters (such as source IP address and destination port) under one anomaly type.

Table 11-4 describes the different types of detected anomalies.

Table 11-4 Types of Detected Anomalies

Type	Description
dns (tcp)	Attacking DNS-TCP protocol flow.
dns (udp)	Attacking DNS-UDP protocol flow.
fragments	Detected flow with an unusual amount of fragmented traffic.
http	Unusual HTTP traffic flow.
ip_scan	Detected flow initiated from a source IP address that tried to access many zone destination IP addresses.
other_protocols	Non-TCP and non-UDP attacking protocol flow.
port_scan	Detected flow initiated from a source IP address that tried to access many zone ports.
tcp_connections	Detected flow with an unusual number of TCP concurrent connections, with or without data.
tcp_incoming	Detected flow that attacks a TCP service when the zone is a server.
tcp_outgoing	Detected flow that consists of a SYN-ACK flood or other packet attacks on connections initiated by the zone when the zone is the client.
tcp_ratio	Detected flow with an unusual ratio between different types of TCP packets, such as a high ratio of SYN packets to FIN/RST packets.
udp	Attacking UDP protocol flow.
unauthenticated_tcp	Detected flow that the Guard anti-spoofing functions have not succeeded in authenticating, such as an ACK flood, FIN flood, or any other flood of unauthenticated packets.
user	Anomaly flow that was detected by user definitions.
sip_udp	Detected VoIP[1] anomaly flow that uses SIP[2] over UDP to establish the VoIP sessions.

[1] VoIP = Voice over IP

2. SIP = Session Initiation Protocol

Mitigated Attacks

The mitigated attacks' section of the attack report details the steps that the Guard took to mitigate the attacks. The report provides details of the timing of the mitigation and the type of mitigated attack. The Guard defines the mitigation type according to the functions that the Guard used to mitigate the attack. These functions indicate the attack type and subtype.

For example, if the Guard uses a basic anti-spoofing function to mitigate an attacking flow of syn packets, the mitigated attack appears as spoofed/tcp_syn_basic where spoofed indicates the attack type and tcp_syn_basic indicates the attack subtype.

This section describes the five types of mitigated attacks in the following topics:

- Spoofed Attacks
- Zombie Attacks
- Client Attacks
- User-Defined Attacks
- Malformed Packets

Spoofed Attacks

Spoofed attacks include all traffic anomalies identified as a DDoS attack that come from a spoofed source. Table 11-5 describes the different types of spoofed attacks.

Table 11-5 Types of Spoofed Attacks

Attack Type	Description
spoofed/tcp_syn (basic)	Flood of SYN packets that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_syn (strong)	Flood of SYN packets that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_syn_ack (basic)	Flood of syn_ack packets that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_syn_ack (strong)	Flood of syn_ack packets that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_incoming (basic)	Flood of traffic that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_incoming (strong)	Flood of traffic that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_outgoing (strong)	Flood of traffic from zone-initiated connections that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/udp (basic)	Flood of UDP traffic that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/udp (strong)	Flood of UDP traffic that the strong anti-spoofing functions have not succeeded in authenticating.

Table 11-5 Types of Spoofed Attacks (continued)

Attack Type	Description
spoofed/other_protocols	Flood of other than TCP and UDP traffic that the Guard anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_fragments	Flood of TCP fragmented packets that the Guard anti-spoofing functions have not succeeded in authenticating.
spoofed/udp_fragments	Flood of UDP fragmented packets that the Guard anti-spoofing mechanisms have not succeeded in authenticating.
spoofed /other_protocols_fragments	Flood of other than TCP and UDP fragmented packets that the Guard anti-spoofing mechanisms have not succeeded in authenticating.
spoofed/dns_queries (strong)	Flood of DNS query packets that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/dns_replies (basic)	Flood of DNS packets from zone-initiated connections that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/dns_replies (strong)	Flood of DNS packets from zone-initiated connections that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/sip	Flood of SIP over UDP packets that the basic anti-spoofing functions have not succeeded in authenticating.

Zombie Attacks

Zombie attacks include traffic anomalies identified as a DDoS attack originated by zombies. Table 11-6 describes the different types of zombie attacks.

Table 11-6 Types of Zombie Attacks

Attack Type	Description
zombie/http	Flood of HTTP traffic from many sources that were identified as nonspoofed, but the Guard anti-zombie functions have not succeeded in authenticating.

Client Attacks

Client attacks include all nonspoofed traffic anomalies. Table 11-7 describes the different types of client attacks.

Table 11-7 Types of Client Attacks

Attack Type	Description
client_attack/tcp_connections	Flow with an unusual number of TCP concurrent connections with or without data.
client_attack/http	Flood of HTTP traffic flow.
client_attack/tcp_ incoming	Flood that attacks a TCP service when the zone is a server.
client_attack/tcp_outgoing	Flood from an attacking authenticated IP connection that the zone initiated.

Table 11-7 Types of Client Attacks (continued)

Attack Type	Description
client_attack /unauthenticated_tcp	Flood of ACKs, FINs, any other packets without a TCP handshake, or TCP connections that the Guard anti-spoofing functions have not succeeded in authenticating.
client_attack/dns (udp)	Flood from an attacking DNS-UDP protocol flow.
client_attack/dns (tcp)	Flood from an attacking DNS-TCP protocol flow.
client_attack/udp	Flood from an attacking UDP protocol flow.
client_attack/other_protocols	Flood from a non-TCP/UDP attacking protocol flow.
client_attack/fragments	Flood of fragmented traffic.
client_attack/user	Flood that a user-defined dynamic filter identified.

User-Defined Attacks

User-defined attacks include all anomalies handled by the user filters. The user filters can either function by default or you can configure them manually. See Chapter 7, "Configuring Policy Templates and Policies" for more information. Table 11-8 describes the different types of user-defined attacks.

Table 11-8 Types of User-Defined Attacks

Attack Type	Description
user_defined/ user_filter_rate_limit	Flood that was dropped because it exceeded the rate limit defined for a user filter.
user_defined/ user_drop_filters	Flood that was dropped by user filters.
user_defined/rate_limit	Flood that was dropped due to one of the following: • The flood exceeded the rate limit defined for a user filter. • The flood exceeded the rate limit defined by the zone **rate-limit** command. • The flood exceeded the internal rate limit defined for unauthenticated TCP RST packets or unauthenticated DNS zone transfer packets.
user_defined/ flex_content_filter	Flood that was dropped by the flex-content filters.

Malformed Packets

Malformed packets include all traffic anomalies identified as consisting of maliciously malformed packets. Table 11-9 describes the different types of malformed packets.

Table 11-9 Types of Malformed Packets

Attack Type	Description
malformed_packets /packets_to_proxy_ip	Flood that attacks a Guard proxy IP address.
malformed_packets /dns_anti_spoofing_algo	Flood of malformed packets due to the operation of the Guard DNS anti-spoofing functions.
malformed_packets /dns (queries)	Flood of malformed DNS packets.
malformed_packets /dns (short_queries)	Flood of short DNS queries.
malformed_packets /dns (replies)	Flood of malformed DNS replies.
malformed_packets /src_ip_equals_dst_ip	Flood of packets with the zone IP address as their source and destination.
malformed_packets /zero_header_field	Flood of packets in which the destination port, source port, protocol, or source IP address field in the header illegally equals zero.
malformed_packets /sip_bad_header	Flood of SIP over UDP packets with a malformed header.

Zombies

Zombie attacks include traffic anomalies identified as a DDoS attack originated by zombies. The Guard attack report displays a table listing zombies that are currently attacking the zone. Use the **show reports details** and **show zombies** commands to display the list of currently attacking zombies.

Note This report section is available only when you enter the **show reports details** and **show zombies** commands

See Table 11-15 on page 11-11 for information about the fields in the **show zombies** command output.

Understanding the Report Parameters

This section describes the aspects of the traffic flow that relate to each section of the report.

Table 11-10 describes the fields for Attack Statistics and Malicious Packet Statistics.

Table 11-10 Field Descriptions for Attack Statistics

Field	Description
Total Packets	Total number of attack packets.
Average pps	Average traffic rate in packets per second.
Average bps	Average traffic rate in bits per second.
Max. pps	Maximum traffic rate measured in packets per second.

Table 11-10 Field Descriptions for Attack Statistics (continued)

Field	Description
Max. bps	Maximum traffic rate measured in bits per second.
Percentage	Number of forwarded, replied, and dropped packets as a percentage of the total received packets.

Table 11-11 describes the flow statistics for Detected Anomalies and Mitigated Attacks.

Table 11-11 Field Descriptions for Flow Statistics

Field	Description
ID	Identifier of the detected anomaly.
Start time	Date and time that the anomaly was detected.
Duration	Duration of the anomaly in hours, minutes, and seconds.
Type	Type of anomaly or mitigated attack.
Triggering rate	Anomaly traffic rate that exceeded the policy threshold.
% Threshold	Percentage by which the triggering rate is above the policy threshold.
Flow	Anomaly flow and mitigated attack flow. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. It indicates whether or not the traffic is fragmented. A value of **any** indicates that there is both fragmented and nonfragmented traffic.

An asterisk (*),which is used as a wildcard, for one of the parameters indicates one of the following:

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

A number sign (#) followed by a number for any of the parameters indicates the number of values measured for that parameter.

The Guard may display a value of **notify** on the right side of the flow description. A value of **notify** indicates that the Guard produces a notification for the type of traffic that the row describes. The Guard does not take an action if the value is **notify**.

Displaying Attack Reports

You can display a list of attack reports for any specific zone or a more detailed report for a specific attack by using the following command in zone configuration mode:

show reports [*sub-zone-name*] [**current** | *report-id*] [**details**]

Table 11-12 provides the arguments and keywords for the **show reports** command.

Table 11-12 Arguments and Keywords for the show reports Command

Parameter	Description
sub-zone-name	(Optional) Name of a subzone that was created from the zone. See the "Understanding Subzones" section on page 9-7 for more information.
current	(Optional) Displays the report of the attack that is in progress. The number of bits and packets is not displayed for an ongoing attack. In reports of an attack in progress, the packets and bits fields have a value of zero (0).
report-id	(Optional) Identification number of the report.
details	(Optional) Displays the details of the flows and attacking zombies.

The following example shows how to view a list of all attacks on the zone:

```
user@GUARD-conf-zone-scannet# show reports
```

Table 11-13 describes the fields in the **show reports** command output.

Table 11-13 Field Descriptions for the show reports Command Output

Field	Description
Report ID	Report identification number. A value of **current** indicates that there is an ongoing attack.
Attack Start	Date and time that the attack started.
Attack End	Date and time that the attack ended. A value of **Attack in progress** indicates that there is an ongoing attack.
Attack Duration	Duration of the attack.
Attack Type	Type of mitigated attack. Possible values are as follows: • **client_attack**—All nonspoofed traffic anomalies. • **malformed_packets**—All traffic anomalies identified as consisting of maliciously malformed packets. • **spoofed**—Traffic anomalies identified as a DDoS attack coming from a spoofed source. • **user_defined**—All anomalies handled by the user filters. The user filters can either function by default or be user configured. • **zombie**—Traffic anomalies identified as having been originated by zombies. • **hybrid**—An attack made up of several attacks with different characteristics. • **traffic_anomaly**—An anomaly that was only detected for a short period of time and did not require mitigation.
Peak Malicious Traffic	Sum of the number of the following types of packets: • Packets that the Guard identified as part of an attack and dropped. • Packets to which the Guard sent replies to the initiating client in order to verify whether they are part of authentic traffic or part of an attack.

The following example shows how to display the report of the current attack on the zone:

```
user@GUARD-conf-zone-scannet# show reports current
```

The attack report displays the following output. For more information about the different sections, see the "Understanding the Report Layout" section on page 11-1.

```
Report ID        :   current
Attack Start     :   Feb 26 2004 09:58:54
Attack End       :   Attack in progress
Attack Duration  :   00:08:34

Attack Statistics:
                 Total     Average   Average     Max pps   Max bps      Percentage
                 Packets   pps       bps
Received         95878     186.53    110977.74   1455.44   914428.24    N/A
Forwarded        53827     104.72    64278.54    1430.85   899196.24    56.14
Replied          1870      3.64      2172.89     23.03     14433.88     1.95
Dropped          40181     78.17     44526.32    96.82     55010.13     41.91

Malicious Packets Statistics:
                 Total     Average   Average     Max pps   Max bps      Percentage
                 Packets   pps       bps
Rate Limiter     0         0         0           0         0            0
Flex-Content     0         0         0           0         0            0
Filter
User Filters     0         0         0           0         0            0
Dynamic Filters  78.07     44473.53  96.82       55010.13  99.84
40128
Spoofed          12        0.02      11.95       0.15      75.29        0.03
Malformed        53        0.1       52.79       1.56      798.12       0.13

Detected Anomalies:
ID          Start Time          Duration     Type                 Triggering   %Threshold
                                                                  Rate
1          Feb 26 09:58:54     00:08:34     HTTP                 997.44       897.44
           Flow: 6 *           *            92.168.100.34   80   no fragments

Mitigated Attacks:
ID         Start Time         Duration     Type                      Triggering   %Threshold
                                                                     Rate
1         Feb 26 09:59:40     00:07:59    client_attack/              38           280
                                          tcp_connections
          Flow: 6 (#52)      *            92.168.200.254 80         no fragments
```

To display a more detailed report on flows of the detected anomalies and the mitigated attacks, and to display a list of zombies attacks, use the **details** option.

Table 11-14 describes the flow fields in the detailed report.

Table 11-14 Field Descriptions of Flows in Detailed Report

Field	Description
Detected Flow	Flow that caused the production of the dynamic filter. The detected flow may indicate a specific source port for a specific source IP address. The flow characteristics include the protocol number, source IP address, source port, destination IP address, destination port, and an indication of whether the traffic is fragmented or not. A value of **any** indicates that there is both fragmented and nonfragmented traffic.
Action Flow	Flow that was addressed by the dynamic filter. The action flow may indicate all source ports for the specified source IP address. The action flow may have a wider range than the detected flow. The flow characteristics include the protocol number, source IP address, source port, destination IP address, destination port, and an indication of whether the traffic is fragmented or not. A value of **any** indicates that there is both fragmented and nonfragmented traffic.

Table 11-15 describes the fields in the detailed report about zombie attacks.

Table 11-15 Field Descriptions for Zombie Attacks Table

Field	Description
IP	Zombie IP address.
Start Time	Date and time that the zombie connection was initially identified.
Duration	Duration of the zombie attack.
#Requests	Number of HTTP get requests sent by the zombie.

Note If there are no zombie attacks, the “Report doesn’t exist” message appears under the Zombies heading in the report.

Exporting Attack Reports

You can export attack reports to a network server for monitoring and diagnostic capabilities. You can export attack reports in text format or in Extensible Markup Language (XML) format.

This section contains the following topics:

- Exporting Attack Reports Automatically
- Exporting Attack Reports of All Zones
- Exporting Zone Reports

Exporting Attack Reports Automatically

You can configure the Guard to export attack reports in XML format. The Guard exports the reports of any one of the zones when an attack on the zone ends. The XML schema is described in the ExportedReports.xsd file which you can download from the Software Center at http://www.cisco.com/public/sw-center/.

To configure the Guard to export attack reports automatically, use the following command in configuration mode:

export reports *file-server-name*

The *file-server-name* argument specifies the name of a network server to which you export the files that you configure by using the **file-server** command. If you configure the network server for Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP), you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the "Exporting Files Automatically" section on page 13-5 for more information.

The following example shows how to automatically export reports (in XML format) at the end of an attack to a network server:

```
user@GUARD-conf# export reports Corp-FTP-Server
```

Exporting Attack Reports of All Zones

You can export the attack reports of all zones in text or XML format by entering one of the following commands in global mode:

- **copy reports** [**details**] [**xml**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy reports** [**details**] [**xml**] {**sftp** | **scp**} *server full-file-name login*
- **copy reports** [**details**] [**xml**] *file-server-name dest-file-name*

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password.

See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information about how to configure the key that the Guard uses for secure communication.

Table 11-16 provides the arguments and keywords for the **copy reports** command.

Table 11-16 Arguments and Keywords for the copy reports Command

Parameter	Description
details	(Optional) Exports details of flow and attacking source IP addresses.
xml	(Optional) Exports the report in XML format. See the xsd file released with the version for a description of the XML schema (you can download the xsd files that accompany the version from www.cisco.com). By default, reports are exported in text format.
ftp	Specifies FTP.

Table 11-16 Arguments and Keywords for the copy reports Command (continued)

Parameter	Description
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server.
full-file-name	Full name of the file. If you do not specify a path, the server saves the file in your home directory.
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server.
file-server-name	Name of a network server that you defined by using the **file-server** command. If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the "Exporting Files Automatically" section on page 13-5 for more information.
dest-file-name	Name of the file. The Guard appends the name of the file to the path that you defined for the network server by using the **file-server** command.

The following example shows how to copy a list of all attacks handled by the Guard (in text format) to an FTP server at IP address 10.0.0.191 by using login name user1 and password password1:

```
user@GUARD# copy reports ftp 10.0.0.191 agmreports.txt user1 password1
```

The following example shows how to copy a list of all attacks handled by the Guard (in text format) to a network server that was defined by using the **file-server** command:

```
user@GUARD# copy reports Corp-FTP-Server AttackReports.txt
```

Exporting Zone Reports

You can copy the attack reports of a specific zone to a network server by using one of the following commands in global mode:

- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] {**sftp** | **scp**} *server full-file-name login*
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] *file-server-name dest-file-name*

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information about how to configure the key that the Guard uses for secure communication.

Table 11-17 describes the arguments and keywords for the **copy zone reports** command.

Table 11-17 Arguments and Keywords for the copy zone reports Command

Parameter	Description
zone *zone-name*	Specifies the name of an existing zone.
current	(Optional) Exports an ongoing attack report (if applicable). The default is to export all zone reports.
report-id	(Optional) ID of an existing report. The Guard exports the report with the specified ID number. To view the details of the zone attack reports, use the **show zone reports** command. The default is to export all zone reports.
xml	(Optional) Exports the report in XML format. See the xsd file that was released with the version for a description of the XML schema (you can download the xsd files that accompany the version from www.cisco.com). The default is to export reports in text format.
details	(Optional) Exports details about the flow and attacking source IP addresses.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the server.
login	Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server.
file-server-name	Name of a network server. 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 Guard uses for SFTP and SCP communication. See the "Exporting Files Automatically" section on page 13-5 for more information.
dest-file-name	Name of the file. The Guard appends the name of the file to the path that you defined for the network server by using the **file-server** command.

The following example shows how to copy all attack reports of the zone to an FTP server at IP address 10.0.0.191 by using login name user1 and password password1:

```
user@GUARD# copy zone scannet reports ftp 10.0.0.191 ScannetCurrentReport.txt user1
password1
```

The following example shows how to copy the current attack report (in XML format) to a network server that was defined by using the **file-server** command:

```
user@GUARD# copy zone scannet reports current xml Corp-FTP-Server AttackReport-5-10-05.txt
```

Deleting Attack Reports

You can delete old attack reports to free disk space.

To delete attack reports, use the following command in zone configuration mode:

no reports *report-id*

The *report-id* argument specifies the ID of an existing report. Enter an asterisk (*) to delete all attack reports. To view the details of the zone attack reports, use the **show zone reports** command.

Note You cannot delete the attack report of an ongoing attack.

The following example shows how to delete all the zone attack reports:

```
user@GUARD-conf-zone-scannet# no reports *
```

CHAPTER 12

Using Guard Diagnostic Tools

This chapter describes how to display statistics and diagnostics on the Cisco Guard (Guard) and contains the following sections:

Displaying the Guard Configuration

You can display the Guard configuration file, which includes information about the Guard configuration, such as interface IP addresses, default gateway addresses, and configured zones.

To display the Guard configuration file, use the following command:

show running-config [all | Guard | interfaces *interface-name* **| router | self-protection | zones]**

Table 12-1 provides the arguments and keywords for the **show running-config** command.

Table 12-1 Arguments and Keywords for the show running-config Command

Parameter	Description
all	Displays configuration files of all Guard functions (Guard, zones, interfaces, router, and self-protection).
Guard	Displays the Guard configuration file.
interfaces *interface-name*	Displays the configuration file of the Guard interfaces. Enter the interface name.
router	Displays the router configuration.
self-protection	Displays the Guard self-protection configuration.
zones	Displays the configuration files of all zones.

The following example shows how to display the Guard configuration file:

```
user@GUARD# show running-config guard
```

The configuration file consists of the commands that you enter to configure the Guard with the current settings. You can export the Guard configuration file to a remote File Transfer Protocol (FTP) server for backup purposes or for implementing the Guard configuration parameters on another Guard. See the "Displaying the Guard Zones" section on page 12-2 for more information.

Displaying the Guard Zones

You can display an overview of the zones to see which zones are active and what their current status is by entering the **show** command in global mode.

Table 12-2 describes the different zone statuses.

Table 12-2 Zone Status

Status	Description
Auto protect mode	Zone protection is enabled and the dynamic filters are activated without user intervention. The Guard displays (+learning) next to the zone name if zone protection is enabled and the Guard is learning zone traffic characteristics for policy threshold tuning.
Interactive protect mode	Zone is in interactive protect mode and the dynamic filters are activated manually.
Threshold Tuning phase	Zone is in the threshold tuning phase. The Guard analyzes the zone traffic and defines thresholds for the policies that were constructed during the policy construction phase of the learning process.
Policy Construction phase	Zone is in the policy construction phase and the zone policies are created.
Standby	Zone is not active.

The following example shows how to display an overview of the Guard zones:

```
user@GUARD# show
```

Using Counters to Analyze Traffic

You can display Guard and zone counters to display information about the current traffic that the Guard is handling, analyze zone traffic, and perform monitoring tasks.

This section contains the following topics:

- Displaying Counters and Average Traffic Rates
- Clearing Guard and Zone Counters

Displaying Counters and Average Traffic Rates

To display the zone counters, use one of the following commands:

- **show** [**zone** *zone-name*] **rates**—Displays the average traffic rates of the malicious and the legitimate counters.
- **show** [**zone** *zone-name*] **rates deta**ils—Displays the average traffic rates for all Guard counters.
- **show** [**zone** *zone-name*] **rates** history—Displays the average traffic rates of the malicious and the legitimate counters for every minute in the past 24 hours.
- show [**zone** *zone-name*] counters—Displays the Guard malicious and legitimate counters.
- show [**zone** *zone-name*] counters details—Displays all Guard counters.
- show [**zone** *zone-name*] counters history—Displays the values of the malicious and the legitimate counters for every minute in the past hour.

To display the Guard counters, use the command in global or configuration mode.

To display the zone counters, use the command in one of the following command modes:

- Zone configuration mode—Do not use the **zone** *zone-name* keyword and argument because you are in the specific zone configuration mode already.
- Global or configuration mode—Enter the **zone** keyword and the *zone-name* argument to specify the zone name.

The rate units are in bits per second (bps) and in packets per second (pps).

Note Zone rates are available only when you enable zone protection or activate the learning process.

The counter units are in packets and in kilobits. The counters are set to zero when you activate zone protection.

Table 12-3 displays the Guard counters.

Table 12-3 Guard Counters

Counter	Description
Malicious	Malicious traffic destined to the zone. Malicious traffic is the sum of the dropped counter and the spoofed counter (which also include the zombie packets).
Legitimate	Legitimate traffic forwarded by the Guard to the zones.
Received	Packets received and handled by the Guard. The Received counter is the sum of the legitimate counter and the malicious counter.
Forwarded	Legitimate traffic forwarded by the Guard to the zones.
Dropped	Packets that were identified by the Guard protection functions (dynamic filters, flex-content filters, and rate limiter) as part of an attack and dropped.
Replied	Packets to which replies were sent to the initiating client as part of the anti-spoofing or anti-zombie functions to verify whether they are part of authentic traffic or part of an attack.
Spoofed	Packets that were identified by the Guard as spoofed packets and not forwarded to the zone. Spoofed packets are replied packets (see the Replied counter in this table for more information) for which no replies were received. Zombie packets are also included in the spoofed packets counter.
Invalid zone	Traffic that is not destined to any one of the zones for which protection is enabled. This information is available for Guard counters only (if you enter the command in global or configuration mode without using the **zone** keyword).

The following example shows how to display the Guard average traffic rates:

```
admin@GUARD-conf-zone-scannet# show rates
```

Clearing Guard and Zone Counters

You can clear the Guard or zone counters if you are going to perform testing and want to be sure that the counters include information from the testing session only. The Guard clears the counters and the average traffic rates.

To clear the Guard counters, use the following command in global or configuration mode:

clear counters

The following example shows how to clear the Guard counters:

```
user@GUARD-conf# clear counters
```

To clear the zone counters, use one of the following commands:

- **clear counters**—In zone configuration mode.
- **clear zone** *zone-name* **counters**—In global or configuration mode. The *zone-name* argument specifies the name of the zone.

The following example shows how to clear the zone counters:

```
user@GUARD-conf-zone-scannet# clear counters
```

Displaying the Zone Status

To display an overview of the zone and its current status, use the **show** command in zone configuration mode. The overview includes the following information:

- Zone status—Indicates the operation state. The operation state can be one of the following: protect mode, protect and learning mode, threshold tuning mode, policy construction mode, or inactive.
- Zone basic configuration—Describes the basic zone configuration, such as automatic or interactive protect mode, thresholds, timers, and IP addresses.

  See the "Configuring Zone Attributes" section on page 5-5 for more information.
- Zone filters—Includes the flex-content filter configuration, the user filter configuration, and the number of active dynamic filters. If the zone is in interactive protect mode, the overview displays the number of recommendations.

  See the "Configuring Flex-Content Filters" section on page 6-3 and the "Configuring User Filters" section on page 6-13 for more information.
- Zone traffic rates—Displays the zone legitimate and malicious traffic rates.

  See the "Using Counters to Analyze Traffic" section on page 12-3 for more information.

The following example shows how to display the zone status:

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

Managing Guard Logs

The Guard automatically logs the system activity and events. You can display the Guard logs to review and track the Guard activity.

Table 12-4 displays the event log levels.

Table 12-4 Event Log Levels

Event Level	Numeric Code	Description
Emergencies	0	System is unusable.
Alerts	1	Immediate action required.
Critical	2	Critical condition.
Errors	3	Error condition.
Warnings	4	Warning condition.
Notifications	5	Normal but significant condition.
Informational	6	Informational messages.
Debugging	7	Debugging messages.

The log file displays all log levels (emergencies, alerts, critical, errors, warnings, notification, informational, and debugging). The Guard log file includes zone events with severity levels: emergencies, alerts, critical, errors, warnings, and notifications.

You can display the event log locally or from a remote server. This section contains the following topics:

- Managing Online Event Logs
- Managing the Log File

Managing Online Event Logs

This section describes how to manage the Guard real-time logging of events and contains the following topics:

- Displaying Online Event Logs
- Exporting Online Event Logs

Displaying Online Event Logs

You can activate the Guard monitoring feature and display a real-time event log, which enables you to view the online logging of the Guard events. To display the online event logs, use the following command:

event monitor

The following example shows how to activate monitoring:

```
user@GUARD# event monitor
```

The screen constantly updates to show new events.

Note To deactivate monitoring, use the **no event monitor** command.

Exporting Online Event Logs

You can export the Guard online event logs to display the Guard operations that are registered in the log file and to display the Guard events from a remote host while they are registered in the Guard log file. The Guard log file is exported using the syslog mechanism. You can export the Guard log file to several syslog servers and specify additional servers so that if one goes offline, another is available to receive messages.

Online Guard log export is applicable with a remote syslog server only. If a remote syslog server is not available, use the **copy log** command to export the Guard log information to a file.

The following is an example of a logging event:

```
Sep 11 16:34:40 10.4.4.4 cm: scannet, 5 threshold-tuning-start: Zone activation completed
successfully.
```

The system log message syntax is as follows:

event-date event-time Guard-IP-address software-deamon/module zone-name event-severity-level event-type event-description

To export online event logs, perform the following steps:

Step 1 (Optional) Configure the logging parameters by entering the following command in configuration mode:

```
logging {facility | trap}
```

Table 12-5 provides the keywords for the **logging** command.

Table 12-5 Keywords for the logging Command

Parameter	Description
facility	Specifies the export syslog facility. The remote syslog server uses logging facilities to filter events. For example, the logging facility allows the remote user to receive the Guard events in one file and use another file for events from other networking devices. The available facilities are local0 through local7. The default is local4.
trap	Specifies the severity level of the syslog traps sent to the remote syslog. When you specify one of the lower severity levels, the event log includes the higher severity levels above it. For example, if the trap level is set to **warning**, then error, critical, alerts, and emergencies are also sent. The available trap levels from the highest to the lowest severity level are emergencies, alerts, critical, errors, warnings, notification, informational, and debugging. The default is notification.

Note To receive events about the addition and removal of dynamic filters, change the trap level to informational.

Step 2 Configure the remote syslog server IP address by entering the following command:

logging host *remote-syslog-server-ip*

The *remote-syslog-server-ip* argument specifies the remote syslog server IP address.

To build a list of syslog servers that receive logging messages, use the **logging host** command more than once.

The following example shows how to configure the Guard to send traps with a severity level that is higher than notification. The Guard sends the traps using the facility local3 to a syslog server with IP address 10.0.0.191:

```
user@GUARD-conf# logging facility local3
user@GUARD-conf# logging trap notifications
user@GUARD-conf# logging host 10.0.0.191
```

To display the configuration that the Guard uses to export online event logs, use the **show logging** command or the **show log export-ip** command.

Managing the Log File

This section describes how to manage the Guard log file and contains the following topics:

- Displaying the Log File
- Exporting the Log File
- Clearing the Log File
- Clearing the BIOS System Log File

Displaying the Log File

You can display the Guard log for diagnostic or monitoring purposes. The Guard log file includes zone events with these severity levels: emergencies, alerts, critical, errors, warnings, and notification.

To display the Guard log, use the following command in global mode:

show log

The following example shows how to display the Guard log:

```
user@GUARD# show log
```

You can display a zone log to display events that relate to the specified zone only.

To display the zone log, use the **show log** [*sub-zone-name*] command in zone configuration mode. The *sub-zone-name* argument specifies the name of a subzone that was created from the zone. See the "Understanding Subzones" section on page 9-7 for more information.

Exporting the Log File

You can export the Guard log file to a network server for monitoring or diagnostics by entering one of the following commands in global mode:

- **copy** [**zone** *zone-name*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log** {**sftp** | **scp**} *server full-file-name login*

Table 12-6 provides the arguments and keywords for the **copy log ftp** command.

Table 12-6 Arguments and Keywords for the copy log ftp Command

Parameter	Description
zone *zone-name*	*(Optional)* Specifies the *zone name. Exports the zone log file*. The default is to export the Guard log file.
log	Exports the log file.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Complete name of the file. If you do not specify a path, the server saves the file in your home directory.
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for it.

Note You can configure the Guard to export event logs automatically by using the **logging host** command. See the "Exporting Online Event Logs" section on page 12-6 for more information.

Because Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP) rely on Secure Shell (SSH) for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information about how to configure the key that the Guard uses for secure communication.

The following example shows how to export the Guard log file to an FTP server:

```
user@GUARD# copy log ftp 10.0.0.191 log.txt <user> <password>
```

Clearing the Log File

You can clear the Guard or zone log file if it is large or if you are going to perform testing and want to be sure that the log file includes information from the testing session only.

To clear the zone log file of all entries, use the following command in zone configuration mode:

clear log

To clear the Guard or zone log file of all entries, use the following command in configuration mode:

clear [**zone** *zone-name*] **log**

The optional **zone** *zone-name* keyword and argument specifies the zone name. The default is to clear the Guard log file.

The following example shows how to clear the Guard log:

```
user@GUARD-conf# clear log
```

Clearing the BIOS System Log File

You can clear the BIOS system log, which contains mostly hardware-related event messages such as the number of times that the device was powered off or restarted.

To clear the BIOS system log, use the following command in configuration mode:

clear log bios

The following example shows how to clear the BIOS log:

```
user@GUARD-conf# clear log bios
```

Monitoring Network Traffic and Extracting Attack Signatures

You can configure the Guard to record traffic directly from the network through nonintrusive taps and create a database from the recorded traffic. By querying the recorded traffic database, you can analyze past events, generate signatures of an attack, or compare current network traffic patterns with traffic patterns that the Guard recorded previously under normal traffic conditions.

You can configure filters so that the Guard records only traffic that meets certain criteria or you can record all traffic data and filter the traffic that the Guard displays.

The Guard records the traffic in Packet Capturing Application Program (PCAP) format, which is compressed and encoded by the gzip (GNU zip) program with an accompanying file in Extensible Markup Language (XML) format that describes the recorded data.

The Guard can analyze the recorded traffic to determine if there are any common patterns or signatures that appear in the payload of the recorded attack packets. The Guard can extract signatures from the recorded traffic. Using the signature, you can configure a flex-content filter to block all traffic containing packet payloads that match the signature.

The Guard can record traffic as follows:

- Automatically—Continuously records traffic data in packet-dump capture files.
- Manually—Records traffic in a packet-dump capture file when you activate a recording session.

  New packet-dump capture files replace previous files. To save the recorded traffic, export the packet-dump capture files to a network server before you activate the Guard to record traffic again.

  You can activate only one manual packet-dump capture at a time for a zone, but you can activate the manual packet-dump capture and the automatic packet-dump capture simultaneously. The Guard can manually record traffic for up to 10 zones simultaneously.

The Guard allocates, by default, 5-GB disk space for the manual packet-dump capture files of all zones and can save up to 50-GB disk space for manual and automatic packet-dump capture files of all zones. You must delete old files to free the disk space for additional packet-dump capture files.

This section contains the following topics:

Configuring the Guard to Automatically Record Traffic

You can activate the Guard to automatically record network traffic for troubleshooting network problems or analyzing attack traffic. You can also record all traffic and apply packet-dump capture filters to the recorded traffic when you view it.

The Guard records traffic in a capture buffer. When the capture buffer size reaches 50 MB, or after 10 minutes have elapsed, the Guard saves the buffered information to a local file in a compressed format, clears the buffer, and then continues recording traffic.

The Guard saves multiple automatic packet-dump capture files. The Guard divides the recorded traffic based on the way that it handled the traffic, so you might have more than one automatic packet-dump capture file from a single time frame. The name of the automatic packet-dump capture file provides information about when the Guard recorded the traffic and how it handled the traffic.

Table 12-7 describes the sections of the automatic packet-dump capture filename.

Table 12-7 Sections of the Automatic Packet-Dump Capture Filename

Section	Description
Function	Type of Guard function performed at the time of the packet-dump capture: • **protect**—The Guard recorded the traffic during zone protection. • **learn**—The Guard recorded the traffic during the zone learning process or the protect and learning process.
Capture start time	Time that the Guard started recording the traffic.
Capture end time	(Optional) Time that the Guard finished recording the traffic. If the Guard is currently recording the traffic to the file, the end time is not displayed.
Dispatch	Method that the Guard used to handle the traffic. This method can be one of the following: • **forwarded**—The Guard identified traffic as legitimate and forwarded it to the zone. • **dropped**—The Guard identified traffic as malicious and dropped it. • **replied**—The Guard sent replies to the initiating client as part of the anti-spoofing or anti-zombie functions in order to verify whether the packets are part of authentic traffic or part of an attack.

When you enable the learning process or the protect and learning function, the Guard saves all of the packet-dump capture files that it creates. When you enable zone protection, the Guard saves one set of past packet-dump capture files only. To save all packet-dump capture files when zone protection is enabled, configure the Guard to automatically export the packet-dump capture files that it creates to a network server.

When you activate zone protection or activate the Guard to automatically record network traffic, the Guard erases all previous packet-dump capture files that it recorded during the protection process and creates new ones.

To configure the Guard to automatically record network traffic, perform the following steps:

Step 1 Configure the Guard to automatically record zone traffic. Enter the following command in zone configuration mode:

```
packet-dump auto-capture
```

Step 2 (Optional) Create a packet-dump capture database by exporting the packet-dump capture files to a network server.

See the "Configuring the Guard to Automatically Record Traffic" section on page 12-10.

The following example shows how to configure the Guard to automatically record zone traffic:

```
user@GUARD-conf-zone-scannet# packet-dump auto-capture
```

To stop the Guard from automatically capturing zone traffic data, use the **no packet-dump auto-capture** command.

To display the current packet-dump settings, use the **show packet-dump** command.

Activating the Guard to Manually Record Traffic

You can activate the Guard to start recording traffic so that you can record traffic during a specific period or change the criteria that the Guard uses to record the traffic.

The Guard stops recording traffic and saves the manual packet-dump capture to a file when the specified number of packets have been recorded or when either the learning process or zone protection have ended.

You can activate only one manual packet-dump capture at a time for a zone, but you can activate the manual packet-dump capture and the automatic packet-dump capture simultaneously. The Guard can record manual packet-dump captures for up to 10 zones simultaneously.

To activate a manual packet-dump capture, use the following command in zone configuration mode:

```
packet-dump capture [view] capture-name pdump-rate pdump-count {all | dropped | forwarded
    | replied} [tcpdump-expression]
```

Note The CLI session halts while the traffic is captured. To continue working while the capture is in process, establish an additional session with the Guard.

Table 12-8 provides the arguments and keywords for the **packet-dump** command.

Table 12-8 Arguments and Keywords for the packet-dump Command

Parameter	Description
view	(Optional) Displays the traffic that the Guard is recording in real time.
capture-name	Name of the packet-dump capture file. Enter an alphanumeric string from 1 to 63 characters. The string can contain underscores but cannot contain spaces.
pdump-rate	Sample rate in packets per second (pps). Enter a value from 1 to 10000. **Note** The Guard supports a maximum accumulated packet-dump capture rate of 10000 pps for all concurrent manual captures. A packet-dump capture configured with a high sample-rate value consumes resources. We recommend that you use high-rate values cautiously because of the potential performance penalty.
pdump-count	Number of packets to record. When the Guard finishes recording the specified number of packets, it saves the manual packet-dump capture buffer to a file. Enter an integer from 1 to 5000.
all	Captures all traffic.
dropped	Captures only traffic that the Guard dropped.
forwarded	Captures only legitimate traffic that the Guard forwarded to the zone.
replied	Captures only the traffic that the Guard anti-spoofing and anti-zombie functions sent back to the source in a verification attempt.
tcpdump-expression	(Optional) Filter that you apply to specify the traffic to record. The Guard captures only traffic that complies with the filter expression. The expression rules are identical to the flex-content filter TCPDump expression rules. See the "Configuring the tcpdump-expression Syntax" section on page 6-6 for more information.

The following example shows how to activate a manual packet-dump capture to record 1000 packets with a sample rate of 10 pps and display the packets that are captured:

```
user@GUARD-conf-zone-scannet# packet-dump capture view 10 1000 all
```

Stopping the Guard from Manually Recording Traffic

The Guard stops a manual packet-dump capture when it records the number of packets that you specified when you activated the capture. However, you can stop a manual packet-dump capture before the Guard records the specified number of packets by performing one of the following actions:

- Press **Ctrl-C** in the open CLI session.
- Open a new CLI session and enter the following command in the zone configuration mode of the desired zone:

  no packet-dump capture *capture-name*

  The *capture-name* argument specifies the name of the capture to stop.

  The Guard saves the packet-dump capture file.

Managing Packet-Dump Capture Files Disk Space

By default, the Guard allocates 2-GB disk space for the zone automatic packet-dump capture files. You can modify the amount of disk space that the Guard allocates for the zone automatic packet-dump capture files by using the following command in zone configuration mode:

packet-dump disk-space *disk-space*

The *disk-space* argument specifies the amount of disk space that the Guard allocates for the zone automatic packet-dump capture files in megabytes. Enter an integer from 1 to 51200.

The following example shows how to configure the amount of disk space that the Guard allocates for the zone automatic packet-dump capture files:

```
user@GUARD-conf-zone-scannet# packet-dump disk-space 500
```

The Guard saves past packet-dump capture files in PCAP format, which is compressed and encoded by the gzip (GNU zip) program.

See the “Displaying Manual Packet-Dump Settings” section on page 12-13 for information about how to view the current amount of allocated disk space.

Displaying Manual Packet-Dump Settings

You can display the current amount of disk space that the Guard allocated for manual packet-dump capture files by using the **show packet-dump** command in configuration mode or in global mode. The Guard allocates a single block of disk space for the manual packet-dump capture files of all zones.

The following example shows how to display the current amount of disk space that the Guard allocated for manual packet-dump capture files:

```
user@GUARD-conf# show packet-dump
```

Table 12-9 describes the fields in the **show packet-dump** command output.

Table 12-9 Field Descriptions for the Manual show packet-dump Command Output

Field	Description
Allocated disk-space	Amount of total disk space that the Guard has allocated for manual packet-dump captures of all zones in megabytes.
Occupied disk-space	Percentage of allocated disk space consumed by manual packet-dump files from all zones.

Displaying Automatic Packet-Dump Settings

You can display the current amount of disk space that is allocated for the zone automatic packet-dump capture files by using the **show packet-dump** command in zone configuration mode.

The following example shows how to display the current amount of disk space that is allocated for the zone automatic packet-dump capture files:

```
user@GUARD-conf-zone-scannet# show packet-dump
```

Table 12-10 describes the fields in the **show packet-dump** command output.

Table 12-10 Field Descriptions for the Automatic show packet-dump Command Output

Field	Description
Automatic-capture	State of the automatic packet-dump capture process.
Allocated disk-space	Amount of disk space that the Guard has allocated for automatic packet-dump captures in megabytes.
Occupied disk-space	Percentage of the allocated disk space that is currently consumed by the automatic packet-dump captures.

Exporting Packet-Dump Capture Files Automatically

You can configure the Guard to automatically export packet-dump capture files to a network server that uses FTP, SFTP, or SCP to transfer files. When you enable the automatic export function, the Guard exports the packet-dump capture files each time that it saves the contents of the packet-dump buffer to a local file. The Guard exports the packet-dump capture files in PCAP format, which is compressed and encoded by the gzip (GNU zip) program, with an accompanying file in XML format that describes the recorded data. The XML schema is described in the Capture.xsd file which you can download from the Software Center at http://www.cisco.com/public/sw-center/.

To configure the Guard to export packet-dump capture files automatically, use the following command in configuration mode:

export packet-dump *file-server-name*

The *file-server-name* argument specifies the name of a network server to which you export the files that you configure by using the **file-server** command. If you configure the network server for SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the "Exporting Files Automatically" section on page 13-5 for more information.

The following example shows how to automatically export packet-dump capture files:

```
user@GUARD-conf# export packet-dump Corp-FTP-Server
```

Exporting Packet-Dump Capture Files Manually

You can manually export packet-dump capture files to a network server that uses FTP, SFTP, or SCP to transfer files. You can export a single packet-dump capture file or all packet-dump capture files of a specific zone. The Guard exports the packet-dump capture files in PCAP format, which is compressed and encoded by the gzip (GNU zip) program with an accompanying file in XML format that describes the recorded data. See the Capture.xsd file that accompanies the version for a description of the XML schema. You can download the xsd files that accompany the version from www.cisco.com.

To manually export packet-dump capture files to a network server, use one of the following commands in global mode:

- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **ftp** *server remote-path [login [password]]*
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] {**sftp** | **scp**} *server remote-path login*
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] *file-server-name*

Table 12-11 provides the arguments and keywords for the **copy zone packet-dump** command.

Table 12-11 Arguments and Keywords for the copy zone packet-dump Command

Parameters	Description
zone *zone-name*	Specifies the name of an existing zone.
packet-dump captures	Exports packet-dump capture files.
capture-name	(Optional) Name of an existing packet-dump capture file. If you do not specify the name of a packet-dump capture file, the Guard exports all the zone packet-dump capture files. See the "Displaying Packet-Dump Capture Files" section on page 12-17 for more information.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
remote-path	Complete name of the path where the Guard saves the packet-dump capture files.
login	(Optional) Server login name. The *login* 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.

Table 12-11 Arguments and Keywords for the copy zone packet-dump Command (continued)

Parameters	Description
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.
file-server-name	Name of a network server. 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 Guard uses for SFTP and SCP communication. See the "Exporting Files Automatically" section on page 13-5 for more information.

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information about how to configure the key that the Guard uses for secure communication.

The following example shows how to manually export the packet-dump capture files of zone scannet to FTP server 10.0.0.191:

```
user@GUARD# copy zone scannet packet-dump captures ftp 10.0.0.191 <user> <password>
```

The following example shows how to manually export the packet-dump capture files of zone scannet to a network server that was defined by using the **file-server** command:

```
user@GUARD# copy zone scannet packet-dump captures cap-5-10-05 Corp-FTP-Server
```

Importing Packet-Dump Capture Files

You can import packet-dump capture files from a network server to the Guard so that you can analyze past events or compare current network traffic patterns with traffic patterns that the Guard previously recorded under normal traffic conditions. The Guard imports the packet-dump capture files in both XML and PCAP formats.

To import a packet-dump capture file, use one of the following commands in global mode:

- **copy ftp zone** *zone-name* **packet-dump captures** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **zone** *zone-name* **packet-dump captures** *server full-file-name login*
- **copy** *file-server-name* **zone** *zone-name* **packet-dump captures** *capture-name*

Table 12-12 provides the arguments and keywords for the **copy zone packet-dump** command.

Table 12-12 Arguments and Keywords for the copy zone packet-dump Command

Parameter	Description
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
zone *zone-name*	Specifies the name of an existing zone for which the packet-dump capture files are imported.
packet-dump captures	Imports packet-dump capture files.

Table 12-12 Arguments and Keywords for the copy zone packet-dump Command (continued)

Parameter	Description
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Complete path and filename, excluding the file extension, of the file to import. If you do not specify a path, the server copies the file from your home directory. **Note** Do not specify the file extension because it will cause the import process to fail.
login	Server login name. The *login* 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.
password	(Optional) Password for the FTP server. If you do not enter the password, the Guard prompts you for one.
file-server-name	Name of a network server. 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 Guard uses for SFTP and SCP communication. See the "Exporting Files Automatically" section on page 13-5 for more information.
capture-name	Name of the file to import. The Guard appends the name of the file to the path that you defined for the network server by using the **file-server** command.

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information about how to configure the key that the Guard uses for secure communication.

The following example shows how to import packet-dump capture files of zone scannet from FTP server 10.0.0.191:

```
user@GUARD# copy ftp zone scannet packet-dump captures 10.0.0.191
/root/scannet/captures/capture-1 <user> <password>
```

The following example shows how to import a packet-dump capture file from a network server:

```
user@GUARD# copy CorpFTP running-config capture-1
```

Displaying Packet-Dump Capture Files

You can display either a list of packet-dump capture files or the contents of a single packet-dump capture file. By default, the Guard displays a list of all zone packet-dump capture files.

To display packet-dump capture files, use the following command in zone configuration mode:

show packet-dump captures [*capture-name* [*tcpdump-expression*]]

Table 12-13 provides the arguments for the **show packet-dump captures** command.

Table 12-13 Arguments for the show packet-dump captures Command

Parameters	Description
capture-name	(Optional) Name of an existing packet-dump capture file. If you do not specify the name of a packet-dump capture file, the Guard displays a list of all zone packet-dump capture files. See Table 12-14 for field descriptions of the command output. If you specify the name of a packet-dump capture file, the Guard displays the file in TCPDump format.
tcpdump-expression	(Optional) Filter that the Guard uses when displaying the packet-dump capture file. The Guard displays only the portion of the packet-dump capture file that matches the filter criteria. The expression rules are identical to the flex-content filter TCPDump expression rules. See the "Configuring the tcpdump-expression Syntax" section on page 6-6 for more information.

The following example shows how to display the list of packet-dump capture files:

```
user@GUARD-conf-zone-scannet# show packet-dump captures
```

Table 12-14 describes the fields in the **show packet-dump captures** command output.

Table 12-14 Field Descriptions for the show packet-dump captures Command Output

Field	Description
Capture-name	Name of the packet-dump capture file. See Table 12-7 for a description of the automatic packet-dump capture filenames.
Size (MB)	Size of the packet-dump capture file in megabytes.
Filter	User-defined filter that the Guard used when recording traffic. The filter is in TCPDump format. The expression rules are identical to the flex-content filter TCPDump expression rules. See the "Configuring the tcpdump-expression Syntax" section on page 6-6 for more information.

Generating Attack Signatures from Packet-Dump Capture Files

An attack signature describes the common pattern that appears in the payload of attack packets. You can activate the Guard to generate the signature of attack traffic and then use this information to quickly identify future attacks of the same type. This feature allows you to detect new DDoS attacks and Internet worms even before signatures are published (for example, from antivirus software companies or mailing lists).

The Guard can generate an attack signature using the flex-content filter pattern expression syntax. You can use the attack signature in the flex-content filter pattern to filter out attack traffic. See the "Configuring Flex-Content Filters" section on page 6-3 for more information.

When you execute the attack signature generating process, you can determine the accuracy of the generated attack signature by specifying a reference packet-dump capture file containing clean (legitimate) traffic. After the Guard generates the attack signature from the packet-dump capture file containing malicious traffic, the Guard runs an analysis to determine how often the attack signature appears in the clean traffic of the reference packet-dump capture file. The Guard displays the results of the analysis as a percentage of the attack signature occurrences in the reference packet-dump capture file to the number of packets in the reference file. A percentage value that is less than 10% indicates that the attack signature is accurate and that you can use the signature to detect malicious traffic.

A percentage value that is greater than 10% indicates that the signature generating process failed. Do not use the signature to detect malicious traffic because it will result in the Guard wrongly identifying clean traffic as malicious traffic. The signature generating process may fail for the following reasons:

- The packet-dump capture file that contains malicious traffic also contains valid traffic. Use a packet-dump capture file that contains malicious traffic only during the signature generating process.
- The Guard's signature generating algorithm is unable to detect a unique signature in the sample of malicious traffic.

To generate a signature of an attack, perform the following steps:

Step 1 Activate the Guard to record traffic during the attack by using the **packet-dump capture** command.

See the "Activating the Guard to Manually Record Traffic" section on page 12-12 for more information.

Step 2 Identify the packet-dump capture file that the Guard recorded during the attack. To display the list of packet-dump capture files, use the **show packet-dump captures** command.

See the "Displaying Packet-Dump Capture Files" section on page 12-17 for more information.

Step 3 Activate the Guard to generate a signature of the attack traffic. Enter the following command in zone configuration mode:

```
show packet-dump signatures capture-name [reference-capture-name]
```

Table 12-15 provides the arguments for the **show packet-dump signatures** command.

Table 12-15 Arguments for the show packet-dump signatures Command

Parameter	Description
capture-name	Name of an existing packet-dump capture file from which to generate an attack signature.
reference-capture-name	(Optional) Name of an existing packet-dump capture file that the Guard recorded during normal traffic conditions. The Guard runs an analysis to determine how often the attack signature appears in the reference file.

Table 12-16 describes the fields in the **show packet-dump signatures** command output.

Table 12-16 Field Descriptions for the show packet-dump signatures Command Output

Field	Description
Start Offset	Offset (in bytes) from the beginning of the packet payload where the pattern begins. If you copy the pattern into the flex-content filter pattern expression, copy this offset into the flex-content filter *start-offset* argument.
End Offset	Offset (in bytes) from the beginning of the packet payload where the pattern ends. If you copy the pattern into the flex-content filter pattern expression, copy this offset into the flex-content filter *end-offset* argument.

Table 12-16 Field Descriptions for the show packet-dump signatures Command Output

Field	Description
Pattern	Signature that the Guard generated. The Guard generates the signature using the flex-content filter pattern expression syntax. See the "Configuring the pattern-expression Syntax" section on page 6-8 for more information. You can copy this pattern into the flex-content filter pattern expression.
Percentage	Percentage of the attack signature occurrences in the reference packet-dump capture file to the number of packets in the reference file.

The following example shows how to generate a signature from a manual packet-dump capture file:

```
user@GUARD-conf-zone-scannet# show packet-dump signatures PDumpCapture
```

Copying Packet-Dump Capture Files

You can copy a packet-dump capture file (or a portion of a file) under a new name. When you copy an automatic packet-dump capture file or a manual packet-dump capture file, the Guard saves them as manual files. If you want to save an existing automatic packet-dump capture file, you need to create a copy of it before the Guard overwrites the automatic packet-dump capture file with a new one.

You must manually delete packet-dump capture files if you need to free disk space. See the "Deleting Packet-Dump Capture Files" section on page 12-21 for more information.

To copy a packet-dump capture file, use the following command in configuration mode:

copy zone *zone-name* **packet-dump captures** *capture-name* [*tcpdump-expression*] *new-name*

Table 12-17 provides the arguments and keywords for the **copy zone packet-dump captures** command.

Table 12-17 Arguments and Keywords for the copy zone packet-dump captures Command

Parameters	Description
zone *zone-name*	Specifies the name of an existing zone.
packet-dump	Copies the packet-dump capture file.
captures *capture-name*	Specifies the name of an existing packet-dump capture file.
tcpdump-expression	(Optional) Filter that the Guard uses to copy the packet-dump capture file. The Guard copies only the portion of the packet-dump capture file that matches the filter criteria. The expression rules are identical to the flex-content filter TCPDump expression rules. See the "Configuring the tcpdump-expression Syntax" section on page 6-6 for more information.
new-name	Name of the new packet-dump capture file. The name is an alphanumeric string from 1 to 63 characters and can contain underscores but cannot contain spaces.

The following example shows how to copy a portion of the packet-dump capture file capture-1 that complies with the capture file under the name capture-2:

```
user@GUARD-conf# copy zone scannet capture-1 "tcp and dst port 80 and not src port 1000"
capture-2
```

Deleting Packet-Dump Capture Files

The Guard allocates by default, 5 GB of disk space for the manual packet-dump capture files of all zones. It can save up to 50 GB of manual and automatic packet-dump capture files of all zones. To free disk space for additional packet-dump capture files, delete the old ones.

You can save only one manual packet-dump capture file per zone and no more than 10 packet-dump capture files on the Guard. You must delete old manual packet-dump capture files to allow space for new files.

To delete automatic or manual packet-dump capture files, use one of the following commands:

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*} (in configuration mode)
- **clear packet-dump captures** {***** | *name*} (in zone configuration mode)

Table 12-18 provides the arguments and keywords for the **clear packet-dump** command.

Table 12-18 Arguments and Keywords for the clear packet-dump Command

Parameter	Description
zone *zone-name*	Specifies the name of an existing zone.
packet-dump captures	Deletes packet-dump capture files.
*****	Erases all packet-dump capture files.
name	Name of the packet-dump capture file to delete.

The following example shows how to delete all manual packet-dump capture files:

```
user@GUARD-conf# clear packet-dump captures *
```

Displaying General Diagnostic Data

You can display a general summary of the diagnostic data by using the following command:

show diagnostic-info [**details**]

The diagnostic data consists of the following information:

- Accelerator card CPU speed—Accelerator card CPU speed.
- Accelerator card revision—Accelerator card revision number.
- Accelerator card serial—Accelerator card serial number.
- CFE version—Common Firmware Environment version number.

Note To change the CFE version, you must install a new flash version by using the **flash-burn** command. See the "Upgrading the Guard Software Version" section on page 13-7 for more information.

- Recognition Average Sample Loss—Calculated average packet sample loss.
- Forward failures (no resources)—Number of packets that were not forwarded due to lack of system resources.

Note A high Recognition Average Sample Loss or a large number of Forward failures indicate that the Guard is overloaded with traffic. We recommend that you install more than one Guard in a load-sharing configuration.

- Fan Speeds—Speed of each fan. The values are a percentage of maximum RPM.
- Maximum Fans—Maximum number of fans that the system supports.
- Installed Fans—Number of fans currently installed in the system.
- Running Fans—List of operational fans.
- The number of system restarts—Number of times that the system has been restarted.
- System UUID—System Universal Unique ID (UUID).
- CPU Temperature—Current CPU temperature in Celsius for each installed CPU.
- DASD Temperature—Current hard disk drive temperature in Celsius.
- Ambient Temperature—Ambient system temperature in Celsius.

The Guard has several LEDs that indicate the inner operation status and are normally off. Lit LEDs indicate a hardware failure and the Guard sends a syslog message and a Simple Network Management Protocol (SNMP) trap to inform the user of the problem.

Managing Disk Space

The Guard maintains activity logs and zone attack reports. If the disk usage is higher than 75 percent or if a large number of zones are defined on the Guard (more than 500), we recommend that you decrease the file history parameters. When the used disk space reaches approximately 80 percent of the disk maximum capacity, the Guard displays a syslog warning message. If the Guard displays this warning message, perform the following tasks to reduce disk usage:

- Export the Guard or zone log to a network server and then clear the log (see the "Exporting the Log File" section on page 12-8 and the "Clearing the Log File" section on page 12-9).
- Export the zone attack reports to a network server and then delete the old attack reports (see the "Exporting Attack Reports" section on page 11-11 and the "Deleting Attack Reports" section on page 11-15).
- Export the packet-dump capture files and then delete the old packet-dump capture files (see the "Exporting Packet-Dump Capture Files Automatically" section on page 12-14. the "Exporting Packet-Dump Capture Files Manually" section on page 12-15, and the "Deleting Packet-Dump Capture Files" section on page 12-21).
- Decrease log file and attack reports history size (see the "Configuring Logs and Reports History" section on page 12-23).
- Decrease the amount of disk space that is allocated for zone automatic packet-dump capture files (see the "Managing Packet-Dump Capture Files Disk Space" section on page 12-13).

Note When the disk usage reaches 80 percent of the disk maximum capacity, the Guard erases information to reduce the used disk space to approximately 75 percent. To avoid a high disk usage condition, periodically store the Guard records on a network server and then clear the logs.

To display the disk used space, use the following command in global mode:

show disk-usage

The following example shows how to display the disk used space:

```
user@GUARD# show disk-usage
2%
```

Configuring Logs and Reports History

You can configure the length of time that the Guard records the logs and the attack reports of both the Guard and its zones. The Guard deletes old logs and reports.

To configure the report and log history, use the following command:

history {**logs** | **reports**} *days* [**enforce-now**]

Table 12-19 provides the arguments and keywords for the **history** command.

Table 12-19 Arguments and Keywords for the history Command

Parameter	Description
logs	Sets the history parameters for the Guard and zone logs.
reports	Sets the history parameters for the zone attack reports.
days	Length of history time. The logs history time range is 1 to 7 days. The report history time range is 1 to 60 days. The default history time is 7 days for the logs and 30 days for the reports.
enforce-now	(Optional) Adopts and if necessary, erases the recorded log and report history recording capacity to the current command parameters. **Note** If you configure the history reporting to a shorter period, use the **enforce-now** keyword to reduce the log file and report file sizes to the newly configured size. You can also use the **disk-clean** command to erase the stored logs and reports to match the newly configured history size.

Displaying Memory Consumption

The Guard displays the following information:

- Memory usage in kilobytes.
- Percentage of memory that the Guard statistical engine uses as the Anomaly Detection Engine Used Memory field.

The anomaly detection engine memory usage is affected by the number of active zones and the number of services that each zone monitors.

Note If the anomaly detection engine memory usage is higher than 95 percent, we strongly recommend that you lower the number of active zones.

To display the Guard memory consumption, use the following command:

show memory

The following example shows how to display the Guard memory consumption:

```
user@GUARD# show memory
              total    used    free    shared   buffers   cached
    In KBytes:  2065188  146260  1918928    0     2360      69232

    Anomaly detection engine used memory: 0.3%
```

Note The total amount of free memory that the Guard has is a sum of the free memory and the cached memory.

Displaying the CPU Utilization

The Guard displays the percentage of CPU time in user mode, system mode, niced tasks (tasks with a nice value representing the priority of a process that is negative), and idle. Niced tasks are counted in both system time and user time so the total CPU utilization can be more than 100 percent.

To display the current percentage of CPU utilization, use the following command:

show cpu

The Guard displays the CPU utilization for both processors.

The following example shows how to display the current percentage of CPU utilization:

```
user@GUARD# show cpu
Host CPU1: 0.0% user, 0.1% system, 0.1% nice, 98.0% idle
Host CPU2: 0.0% user, 7.0% system, 0.0% nice, 92.0% idle
```

Monitoring System Resources

You can display an overview of the resources that the Guard is using to help you analyze and monitor the system status by using the following command in global or configuration mode:

show resources

The following example shows how to display the system resources:

```
user@GUARD# show resources
```

Table 12-20 describes the fields in the **show resources** command output.

Table 12-20 Field Descriptions for the show resources Command Output

Field	Description
Host CPU1	Percentage of CPU time for CPU1 in user mode, system mode, niced tasks, and idle. Niced tasks are also counted in system time and user time so that the total CPU utilization can be more than 100 percent.
Host CPU2	Percentage of CPU time for CPU2 in user mode, system mode, niced tasks, and idle. Niced tasks are also counted in system time and user time so that the total CPU utilization can be more than 100 percent.
Disk space usage	Percentage of the allocated disk space that the Guard is using. When the disk space usage reaches approximately 75 percent of the disk maximum capacity, the Guard displays a syslog warning message and sends a trap. **Note** When the disk usage reaches 80 percent of the disk maximum capacity, the Guard automatically erases information to reduce the used disk space to approximately 75 percent. If the disk space usage reaches 80 percent, follow the guidelines described in the "Managing Disk Space" section on page 12-22.
Accelerator card memory usage	Percentage of memory that the accelerator card is using. If the accelerator card memory usage is higher than 85 percent, the Guard generates an SNMP trap. A high value may indicate that the Guard is monitoring a high volume of traffic.
Accelerator card CPU utilization	Percentage of the accelerator card CPU utilization. If the accelerator card CPU utilization is higher than 85 percent, the Guard generates an SNMP trap. A high value may indicate that the Guard is monitoring a high volume of traffic.
Anomaly detection engine used memory	Percentage of memory that the Guard statistical engine uses. The anomaly detection engine memory usage is affected by the number of active zones, the number of services each of the zones monitors, and the amount of nonspoofed traffic that the Guard is monitoring. If the anomaly detection engine memory usage is higher than 95 percent, we strongly recommend that you lower the number of active zones.
Dynamic filters used	Total number of dynamic filters that are active in all the zones. The Guard displays the number of active dynamic filters and the percentage of dynamic filters that are active out of the total number of dynamic filters that the Guard supports, which is 150,000. If the number of active dynamic filters reaches 150,000, the Guard generates an SNMP trap with a severity level of EMERGENCY. If the number of active dynamic filters reaches 135,000, the Guard generates an SNMP trap with a severity level of WARNING. A high value may indicate that the Guard is monitoring a high traffic volume of a DDoS attack.

For more information about the traps that the Guard generates, see Table 3-15 on page 3-27.

Managing the ARP Cache

You can display or manipulate the Address Resolution Protocol (ARP) cache to clear an address mapping entry or to manually define an address mapping entry. To manage the ARP cache, use one of the following commands:

arp [**-evn**] [**-H** *type*] [**-i** *if*] **-a** [*hostname*]

arp [**-v**] [**-i** *if*] **-d** *hostname* [**pub**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**netmask** *nm*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if*] **-Ds** *hostname ifa* [**netmask** *nm*] **pub**

arp [**-vnD**] [**-H** *type*] [**-i** *if*] **-f** [*filename*]

Note You can enter the complete keyword or an abbreviation of the keyword. The abbreviated keyword is preceded by a dash (-) and the complete keyword is preceded by two dashes (--).

Table 12-21 provides the arguments and keywords for the **arp** command.

Table 12-21 Arguments and Keywords for the arp Command

Abbreviated Parameter Name	Parameter Full Name	Description
-H *type*, **-t** *type*	**--hw-type** *type*	(Optional) Specifies the class of entries for which the Guard checks. The default type value is ether (hardware code 0x01 for IEEE 802.3 10-Mbps Ethernet).
-i *If*	**--device** *If*	(Optional) Specifies an interface. When you dump the ARP cache, only entries that match the specified interface are printed. If you configure a permanent or temporary ARP entry, this interface is associated with the entry. If you do not use this option, the Guard determines the interface based on the routing table. If you use the **pub** keyword, this interface is the interface on which the Guard answers ARP requests and must be different from the interface to which the IP datagrams are routed.
-s *hostname hw_addr*	**--set** *hostname hw_addr*	Creates an ARP address mapping entry for the hostname with the hardware address set to the *hw_addr* class value. If you do not enter the **temp** flag, the entries are stored permanently in the ARP cache.
-a [*hostname*]	**--display** [*hostname*]	Displays the entries of the specified hosts in alternate (BSD) style. The default is to display all entries.
-v	**--verbose**	(Optional) Displays the output in verbose.
-n	**--numeric**	Displays numerical addresses.
-d *hostname*	**--delete** *hostname*	Remove any entry for the specified host.
-D	**--use-device**	Uses the hardware address of interface if*a*.

Table 12-21 Arguments and Keywords for the arp Command (continued)

Abbreviated Parameter Name	Parameter Full Name	Description
-e		Displays the entries in default style.
-f *filename*	**--file** *filename*	Creates an ARP address mapping entry. The information is taken from the *filename* file. The file format is ASCII text lines with a hostname and a hardware address separated by white space. You can also use the pub, temp, and netmask flags. In all places where a hostname is expected, you can also enter an IP address in dotted-decimal notation.

Caution To configure the Guard ARP cache, you must be familiar with the Guard system and the network.

The following example shows how to display the ARP entries in default style:

```
user@GUARD# arp -e

Address         HWtype  HWaddress           Flags Mask  Iface
10.10.1.254     ether   00:02:B3:C0:61:67   C           eth1
10.10.8.11      ether   00:02:B3:45:B9:F1   C           eth1
10.10.8.253     ether   00:D0:B7:46:72:37   C           eth1
10.10.10.54     ether   00:03:47:A6:44:CA   C           eth1
```

Displaying Network Statistics

You can display the host network connections, routing tables, interface statistics, and multicast memberships to debug network problems by entering one of the following commands:

netstat [*address_family_options*] [**--tcp** | **-t**] [**--udp** | **-u**] [**--raw** | **-w**] [**--listening** | **-l**] [**--all** | **-a**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--symbolic** | **-N**] [**--extend** | **-e** [**--extend** | **-e**]] [**--timers** | **-o**] [**--program** | **-p**] [**--verbose** | **-v**] [**--continuous** | **-c**] [*delay*]

netstat {**--route** | **-r**} [*address_family_options*] [**--extend** | **-e** [**--extend** | **-e**]] [**--verbose** | **-v**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--continuous** | **-c**] [*delay*]

netstat {**--interfaces** | **-i**} [*iface*] [**--all** | **-a**] [**--extend** | **-e** [**--extend** | **-e**]] [**--verbose** | **-v**] [**--program** | **-p**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--continuous** | **-c**] [*delay*]

netstat {**--groups** | **-g**} [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--continuous** | **-c**] [*delay*]

netstat {**--masquerade** | **-M**} [**--extend** | **-e**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--continuous** | **-c**] [*delay*]

netstat {**--statistics** | **-s**} [**--tcp** | **-t**] [**--udp** | **-u**] [**--raw** | **-w**] [*delay*]

netstat {**--version** | **-V**}

netstat {**--help** | **-h**}

Note If you do not specify any address families, the Guard displays the active sockets of all configured address families.

Table 12-22 provides arguments and keywords for the **netstat** command.

Note You can enter the complete keyword or an abbreviation of the keyword. The abbreviated keyword is preceded by a dash (-) and the complete keyword is preceded by two dashes (--).

Table 12-22 Arguments and Keywords for the netstat Command

Abbreviated Parameter Name	Parameter Full Name	Description
address_family_ options		(Optional) The address family options can be one of the following: • [--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]] • [--unix|-x] [--inet|--ip] [--ax25] [--ipx] [--netrom] • [--ddp]
-r	**--route**	Displays the Guard routing tables.
-g	**--groups**	Displays multicast group membership information for IPv4 and IPv6.
-i ***iface***	**--interface** ***iface***	Displays a table of all network interfaces or of the optional *iface* value.
-M	**--masquerade**	Displays a list of masqueraded connections for which Network Address Translation (NAT) was used.
-s	**--statistics**	Displays summary statistics for each protocol.
-v	**--verbose**	(Optional) Displays the output in verbose.
-n	**--numeric**	(Optional) Displays numerical addresses.
	--numeric-hosts	(Optional) Displays numerical host addresses but does not affect the resolution of port or usernames.
	--numeric-ports	(Optional) Displays numerical port numbers but does not affect the resolution of host or usernames.
	--numeric-users	(Optional) Displays numerical user IDs but does not affect the resolution of host or port names.
-c	**--continuous**	(Optional) Displays the selected information every second on a continuous basis.
-e	**--extend**	(Optional) Displays additional information. Use this option twice for maximum detail.
-o	**--timers**	(Optional) Displays information related to networking timers.

Table 12-22 Arguments and Keywords for the netstat Command (continued)

Abbreviated Parameter Name	Parameter Full Name	Description
-p	**--program**	(Optional) Displays the PID and name of the program to which each socket belongs.
-l	**--listening**	(Optional) Displays only listening sockets. These sockets are omitted by default.
-a	**--all**	(Optional) Displays both listening and nonlistening sockets.
delay		(Optional) Netstat cycles printing through statistics every *delay* seconds.

Note You can enter a maximum of 13 arguments and keywords in one command.

The following example shows how to display netstat information in verbose:

```
user@GUARD# netstat -v
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address         State
tcp        0      0 localhost:1111  localhost:32777    ESTABLISHED
tcp        0      0 localhost:8200  localhost:32772    ESTABLISHED
.
.
.
tcp        0      0 localhost:33464 localhost:8200     TIME_WAIT
tcp        1      0 localhost:1113  localhost:33194    CLOSE_WAIT
.
.
.
Active UNIX domain sockets (w/o servers)
unix  2      [ ]         STREAM     CONNECTED     928
unix  3      [ ]         STREAM     CONNECTED     890  /tmp/.zserv
.
.
.
user@GUARD#
```

Using Traceroute

You can determine the route that packets take to arrive at a network host to debug network problems by entering the following command:

traceroute *ip-address* [**-F**] [**-f** *first_ttl*] [**-g** *gateway*] [**-i** *iface*]
[**-m** *max_ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] [*packetlen*]

Note The **traceroute** command displays IP addresses only, not names.

Table 12-23 provides the arguments and keywords for the **traceroute** command.

Table 12-23 Arguments and Keywords for the traceroute Command

Parameter	Description
ip-address	IP address to which the route will be traced.
-F	(Optional) Sets the *don't fragment* bit.
-f *first_ttl*	(Optional) Sets the initial time-to-live (TTL) used in the first outgoing probe packet.
-g *gateway*	(Optional) Specifies a loose source route gateway. You can specify more than one gateway by using **-g** for each gateway. The maximum number of gateways is 8.
-i *iface*	(Optional) Specifies a network interface to obtain the source IP address for outgoing probe packets and, in most cases, is useful on a multihomed host.
-m *max_ttl*	(Optional) Sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops.
-p *port*	(Optional) Sets the base UDP port number used in probes. The default is 33434.
-q *nqueries*	(Optional) Sets the number of probes that are defined for the ttl value. The default is 3.
-s *src_addr*	(Optional) Sets the *src_addr* IP address as the source IP address in outgoing probe packets.
-t *tos*	(Optional) Sets the type-of-service in probe packets to the *tos* value. The default is zero.
-w *waittime*	(Optional) Sets the time in seconds to wait for a response for a probe. The default is 5 seconds.
packetlen	(Optional) Packet length of the probe.

The following example shows how to trace the route to IP address 10.10.10.34:

```
user@GUARD# traceroute 10.10.10.34
traceroute to 10.10.10.34 (10.10.10.34), 30 hops max, 38 byte packets
 1 10.10.10.34 (10.10.10.34) 0.577 ms  0.203 ms  0.149 ms
```

Verifying Connectivity

You can send Internet Control Message Protocol (ICMP) ECHO_REQUEST packets to network hosts and verify connectivity by entering the following command:

ping *ip-address* [-**c** *count*] [-**i** *interval*] [-**l** *preload*] [-**s** *packetsize*] [-**t** *ttl*] [-**w** *deadline*] [-**F** *flowlabel*] [-**I** *interface*]
[-**Q** *tos*] [-**T** *timestamp option*] [-**W** *timeout*]

Table 12-24 provides arguments and keywords for the **ping** command.

Table 12-24 Arguments and Keywords for the ping Command

Parameter	Description
ip-address	Destination IP address.
-c *count*	(Optional) Specifies the number of ECHO_REQUEST packets to send. With a deadline option, the command waits for the specified number of ECHO_REPLY packets until the timeout expires.
-i *interval*	(Optional) Specifies the amount of time to wait before sending packets. The interval time is in seconds. The default is to wait for 1 second.
-l *preload*	(Optional) Sends preload packets without waiting for a reply.
-s *packetsize*	(Optional) Specifies the number of data bytes to send. The default is 56.
-t ttl	(Optional) Sets the IP TTL.
-w *deadline*	(Optional) Specifies the timeout in seconds before ping exits, regardless of how many packets have been sent or received.
-F *flow label*	(Optional) Allocates and sets a 20-bit flow label on echo request packets. If the value is zero, a random flow label is used.
-I *interface*	(Optional) Sets the source IP address to the specified interface address.
-Q *tos*	(Optional) Sets Type of Service (ToS)-related bits in ICMP datagrams.
-T *timestamp option*	(Optional) Sets special IP time-stamp options.
-W *timeout*	(Optional) Specifies the time (in seconds) to wait for a response.

You can enter a maximum of 10 arguments and keywords in one command.

The following example shows how to send one ICMP ECHO_REQUEST packet to IP address 10.10.10.30:

```
user@GUARD# ping 10.10.10.30 -n 1
```

Obtaining Debug Information

If the Guard experiences an operational problem, Cisco TAC may request that you send them a copy of the Guard internal debug information. The Guard debug core file contains information for troubleshooting Guard malfunctions. The file output is encrypted and intended for use by Cisco TAC personnel only.

To extract debug information to an FTP, SCP, or SFTP server, perform the following steps:

Step 1 Display the Guard log file.

See the "Displaying the Log File" section on page 12-8 for more information.

Step 2 Identify the first log message that indicates a problem to determine the time from when to extract debug information. The Guard extracts the debug information from the time specified up to the current time.

Step 3 Copy the debug information to an FTP, SCP, or SFTP server by entering the following command in global mode:

```
copy debug-core time {ftp | scp | sftp} server full-file-name [login [password]]
```

Table 12-25 provides the arguments and keywords for the **copy debug-core** command.

Table 12-25 Arguments and Keywords for the copy debug-core Command

Parameter	Description
time	Time of the event that triggers the need for debug information. The time string uses the format *MMDDhhmm*[[*CC*]*YY*][*.ss*] as follows: • *MM*—The month in numeric figures • *DD*—The day of the month • *hh*—The hour in a 24-hour clock • *mm*—The minutes • *CC*—(Optional) The first two digits of the year (for example, **20**05) • *YY*—(Optional) The last two digits of the year (for example, 20**05**) • *.ss*—(Optional) The seconds (the decimal point must be present)
ftp	Specifies FTP.
scp	Specifies SCP.
sftp	Specifies SFTP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Full name of the version file. If you do not specify a path, the server saves the file in your home directory.
login	(Optional) Server login name. The server assumes an anonymous login when you do not enter a login name. The server does not prompt you for a password.
password	(Optional) Server password. If you do not enter the password, the Guard prompts you for one.

The following example shows how to extract debug information from November 9 at 06:45 a.m. of the current year to FTP server 10.0.0.191:

```
user@GUARD# copy debug-core 11090645 ftp 10.0.0.191 /home/debug/debug-file <user>
<password>
```

Displaying the Guard Self-Protection Configuration

The Guard, as a network element that has an independent IP address, is exposed to potential DDoS attacks. The default configuration of the Guard provides protection against such attacks. You can access and modify the self-defense protection configuration.

Caution We strongly advise that you do not change the Guard self-defense protection default configurations. Unnecessary configurations may seriously compromise the ability of the Guard to protect itself.

To enter self-protection configuration mode to modify the Guard self-defense protection configuration, use the following command in configuration mode:

self-protection

The set of commands available for the Guard self-defense protection are identical to the commands for an ordinary zone. See the following chapters for more information:

- Chapter 5, "Configuring Zones"
- Chapter 6, "Configuring Zone Filters"
- Chapter 7, "Configuring Policy Templates and Policies"
- Chapter 10, "Using Interactive Protect Mode"

To display the Guard self-protection configuration file, use the **show running-config** command. See the "Displaying the Guard Configuration" section on page 12-1 for more information.

Understanding the Flex-Content Filter Default Configurations

The Guard flex-content filter is configured, by default, to block (drop) all traffic flows unless explicitly specified.

Table 12-26 displays the flex-content filter default configuration to enable the communication that is required for proper Guard functionality.

Table 12-26 Flex-Content Filter Default Configuration

Service	IP-Proto	Src-port	Dst-port	Allow-SYN
ftp-control	6	21	*	no
ftp-data	6	20	*	yes
tacacs	6	49	*	yes
ssh	6	22	*	no
ssh	6	*	22	yes
https	6	*	443	yes
icmp	1	*	*	—
snmp	17	*	161	—
ssl	6	*	3220	no
ssl	6	3220	*	yes
ntp	17	*	123	—
ntp	17	123	*	—
bgp	6	179	*	no
ospf	89	*	*	—
rip	17	520	*	—
rip	17	*	520	—
gre	47	*	*	—
mdm	6	*	134	yes

The flex-content filter default configuration enables the following features:

- FTP communication, initiated by the Guard, with an FTP server, but blocks incoming FTP control SYN packets with source port 21.
- Terminal Access Controller Access Control System (TACACS) communication with a TACACS+ server for authentication, authorization, and accounting, but block incoming SYN packets from source port 49.
- Incoming and outgoing SSH communication.
- Incoming Hypertext Transfer Protocol Secure (HTTPS) communication.
- ICMP communication.
- SNMP communication.
- Secure Sockets Layer (SSL) communication
- Network Time Protocol (NTP) communication.
- Border Gateway Protocol (BGP) communication, initiated by the Guard, on port 179, but block incoming SYN packets with source port 179. This enables BGP connections initiated by the Guard to the router that the traffic is being diverted from.
- Open Shortest Path First (OSPF) communication.
- Routing Information Protocol (RIP) communication.
- Generic Routing Encapsulation (GRE) communication.

CHAPTER 13

Performing Maintenance Tasks

This chapter describes how to perform tasks used for general care and maintenance of the Cisco Guard (Guard) and contains the following sections:

- Configuring File Servers
- Exporting the Configuration
- Importing and Updating the Configuration
- Exporting Files Automatically
- Reloading the Guard
- Rebooting the Guard and Inactivating Zones
- Shutting Down the Guard
- Upgrading the Guard Software Version
- Burning a New Flash Version to Upgrade the Common Firmware Environment
- Resetting the Linux root or Guard admin User Account Password
- Resetting the Guard Configuration to Factory Defaults

Configuring File Servers

You can define a network server on the Guard for importing and exporting files between the Guard and the server. The Guard allows you to create a network server profile in which you define the network server attributes such as the IP address, the communication method, and the login details. Creating a network server profile allows you to specify just the server name when importing or exporting files

After you configure the network server, you must configure the export or the import commands. For example, use the **export reports** commands to configure the Guard to export attack reports to a network server.

To configure a network server, use one of the following commands in configuration mode:

- **file-server** *file-server-name description* **ftp** *server remote-path login password*
- **file-server** *file-server-name description* [**sftp** | **scp**] *server remote-path login*

Table 13-1 provides the arguments and keywords for the **file-server** command.

Table 13-1 Arguments and Keywords for the file-server Command

Parameter	Description
file-server-name	Name for the network server. Enter an alphanumeric string from 1 to 63 characters. The string can contain underscores but cannot contain any spaces.
description	String to describe the network server. The maximum alphanumeric string length is 80 characters. If you use spaces in the expression, enclose the expression in quotation marks (" ").
ftp	Specifies File Transport Protocol (FTP).
sftp	Specifies Secure File Transport Protocol (SFTP).
scp	Specifies Secure Copy Protocol (SCP).
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
remote-path	Complete path of the directory in which to save the files or from which to import the files.
login	Login name for the network server.
password	Password for the network server. This option is valid only for an FTP server. The Guard authenticates network servers that use SFTP and SCP using a public key.

Note Because SFTP and SCP rely on Secure Shell (SSH) for secure communication, you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information.

The following example shows how to define an FTP server with the IP address 10.0.0.191:

```
user@GUARD-conf# file-server CorpFTP-Server "Corp's primary FTP server" ftp 10.0.0.191
/root/ConfigFiles <user> <password>
```

To delete a network server, use the **no file-server** [*file-server-name* | *] command in configuration mode.

To display the list of network servers, use the **show file-servers** command in global or configuration mode.

Exporting the Configuration

You can export the Guard configuration file or a zone configuration file (running-config) to a network server, which allows you to do the following:

- Implement the Guard configuration parameters on another Guard
- Back up the Guard configuration

To export the Guard configuration file, use one of the following commands in global mode:

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

- **copy** [**zone** ***zone-name***] **running-config** *file-server-name dest-file-name*

Table 13-2 provides the arguments and keywords for the **copy running-config ftp** command.

Table 13-2 Arguments and Keywords for the copy running-config ftp Command

Parameter	Description
zone *zone-name*	*(Optional) Specifies the zone name. If you specify the zone name, the Guard exports the zone configuration file.* The default is to export the Guard *configuration* file.
running-config	Exports the complete Guard configuration or the configuration of the specified zone.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Complete name of the file. If you do not specify a path, the server saves the file in your home directory.
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.
file-server-name	Name of a network server to which to export the configuration file. You must configure the network server using the **file-server** command (see the "Configuring File Servers" section on page 13-1).
dest-file-name	Name of the configuration file on the remote server. The Guard saves the configuration file on the network server using the destination filename in the directory that you defined for the network server by using the **file-server** command.

Note If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. If you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information.

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

```
user@GUARD# copy running-config ftp 10.0.0.191 run-conf.txt <user> <password>
```

The following example shows how to export the Guard configuration file to a network server:

```
user@GUARD# copy running-config CorpFTP Configuration-12-11-05
```

Importing and Updating the Configuration

You can import a Guard or zone configuration file from an FTP server and reconfigure the Guard according to the newly transferred file. Import the configuration to do one of the following tasks:

- Configure the Guard based on an existing Guard configuration file
- Restore the Guard configuration

Zone configuration is a partial Guard configuration. To copy both types of configuration files to the Guard and reconfigure it accordingly, use the **copy ftp running-config** command.

Note The new configuration replaces the existing configuration. You must reload the Guard for the new configuration to take effect.

We recommend that you deactivate all zones before you initiate the import process. The Guard deactivates a zone before importing the zone configuration.

The Guard, by default, ignores older versions of the self-protection configuration. We recommend that you do not overwrite the self-protection configuration with an older configuration because the older configuration may not be compatible with the current version.

To import a Guard configuration file, use one of the following commands in global mode:

- **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 13-3 provides the arguments for the **copy ftp running-config** command.

Table 13-3 Arguments for the copy ftp running-config Command

Parameter	Description
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
full-file-name	Complete name of the file. If you do not specify a path, the server searches for the file in your home directory.
login	(Optional) Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.
file-server-name	Name of a network server. You must configure the network server using the **file-server** command (see the "Configuring File Servers" section on page 13-1).
source-file-name	Name of the file to import. The Guard appends the name of the file to the path that you defined for the network server by using the **file-server** command.

Note If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. If you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information.

The following example shows how to import the Guard configuration file from an FTP server:

```
user@GUARD# copy ftp running-config 10.0.0.191 /root/backup/conf/scannet-conf <user>
<password>
```

The following example shows how to import the Guard configuration file from a network server:

```
user@GUARD# copy CorpFTP running-config scannet-conf
```

When you import a configuration that was exported from an older version, the Guard displays the following message:

```
WARNING: The configuration file includes a self-protection definition that is incompatible
with the current version and will be ignored.
Continue? [yes|no]
```

Enter one of the following options:

- **yes**—Ignores the old self-protection configuration. The Guard performs as follows:
  - Ignores the old self-protection configuration and does not import it
  - Imports all other configurations, such as the zone, interface, and services configuration
- **no**—Enables you to import the old self-protection configuration. The Guard displays the following message:

  ```
  You can abort the import process or import the old self-protection definition as-is.
  WARNING: The self-protection definitions are incompatible with the current version.
  Abort? [yes|no]
  ```

Caution We recommend that you do not overwrite the self-protection configuration with an older configuration because the older configuration may not be compatible with the current software version.

To import the older self-protection configuration, enter **no**.

To abort the import process, enter **yes**.

Exporting Files Automatically

You can configure the Guard to export the following file to a network server automatically:

- Packet-dump capture files—The Guard exports the packet-dump capture files when the capture buffer size reaches 50 MB or after 10 minutes have elapsed. See the "Exporting Packet-Dump Capture Files Automatically" section on page 12-14 for more information.
- Attack reports—The Guard exports the reports of any one of the zones when an attack on the zone ends. See the "Exporting Attack Reports Automatically" section on page 11-12 for more information.

The Guard exports the packet-dump capture files and the attack reports in Extensible Markup Language (XML) format. The software version is accompanied by xsd files that describe the XML schema. You can download the xsd files from www.cisco.com.

To export files automatically to a network server, perform the following steps:

Step 1 Define the network server to which you can export files.

See the "Configuring File Servers" section on page 13-1 for more information.

Step 2 Configure the Guard to export files automatically by entering the following command:

```
export {packet-dump | reports} file-server-name
```

Table 13-4 provides the arguments and keywords for the **export** command.

Table 13-4 Arguments and Keywords for the export Command

Parameter	Description
packet-dump	Exports packet-dump capture files each time that the contents of the packet-dump buffer are saved to a local file. The Guard exports the packet-dump capture files in PCAP format, which is compressed and encoded by the gzip (GNU zip) program, with an accompanying file in XML that describes the recorded data. See the Capture.xsd file that accompanies the version for a description of the XML schema. See the "Monitoring Network Traffic and Extracting Attack Signatures" section on page 12-9 for more information about packet-dump capture files.
reports	Exports attack reports in XML format at the end of an attack. The Guard exports the reports of any one of the zones when an attack on the zone ends. See the ExportedReports.xsd file that accompanies the version for a description of the XML schema. See the "Exporting Attack Reports" section on page 11-11 for more information.
file-server-name	Name of the network server on which you can save files. You must configure the network server using the **file-server** command (see the "Configuring File Servers" section on page 13-1).

The following example shows how to define an FTP server with the IP address 10.0.0.191 and then to configure the Guard to automatically export reports (in XML) at the end of an attack to that server:

```
user@GUARD-conf# file-server CorpFTP-Server "Corp's primary FTP server" ftp 10.0.0.191
/root/ConfigFiles <user> <password>
user@GUARD-conf# export reports CorpFTP-Server
```

To disable the automatic export of files to a network server, use the **no** form of the command.

Reloading the Guard

You can reload the Guard configuration without rebooting the machine by using the **reload** command.

For the following changes to take effect, you must reload the Guard:

- Synchronizing the Guard with an NTP server
- Deactivating or activating a physical interface using the **shutdown** command

- Enabling the giga0 interface using the **no shutdown** command
- Burning a new flash

Rebooting the Guard and Inactivating Zones

You can reboot the Guard by using the following command in global mode:

reboot

By default, the Guard loads all zones in an inactive operation state. The Guard does not enable zone protection or the learning process after reboot, regardless of the zone operation state prior to the reboot.

To allow the Guard to automatically activate zones that were active prior to the reboot process, enter the following command in configuration mode:

boot reactivate-zones

Caution The zone learning phase is restarted after reboot.

Shutting Down the Guard

A clean shutdown enables the Guard to save vital information.

To shut down the Guard, perform the following steps:

Step 1 Enter the following command:

```
poweroff
```

Step 2 Type **yes** at the command prompt to verify the process.

Step 3 Push the Guard power control button to turn the power off. The green power LED turns off.

Caution Pushing the power control button without entering the **poweroff** command may result in critical data loss.

Upgrading the Guard Software Version

To upgrade the Guard software version, perform the following steps:

Step 1 Back up the Guard configuration before initiating the upgrade process by using the **copy running-config** command. Backing up enables you to save your existing configuration so that you can quickly restore the configuration to the current state if needed. See the "Exporting the Configuration" section on page 13-2 for more information.

Step 2 Export files that you want to save. You can export the following files:

- Export attack reports that you want to save by using the **copy reports** command or the **copy zone** *zone-name* **reports** command. See the "Exporting Attack Reports of All Zones" section on page 11-12 and the "Exporting Zone Reports" section on page 11-13 for more information.
- Export logs that you want to save by using the **copy log** command. See the "Exporting the Log File" section on page 12-8 for more information.
- Export the packet-dump capture files that you want to save by using the **copy zone** *zone-name* **packet-dump captures** command. See the "Exporting Packet-Dump Capture Files Manually" section on page 12-15 for more information.

Step 3 Upgrade to the latest software release by locating the software image on www.cisco.com and copy the software image to a remote server that is accessible to FTP, SFTP, or SCP.

Step 4 Copy the software image from the remote server to the Guard software from the network server by entering one of the following commands in global mode:

- **copy ftp new-version** *server full-file-name* [*login* [*password*]]
- **copy** {**scp** | **sftp**} **new-version** *server full-file-name login*

Table 13-5 provides arguments for the **copy new-version** command.

Table 13-5 Arguments for the copy new-version Command

Parameter	Description
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
server	IP address of the server.
full-file-name	Complete name of the file. If you do not specify a path, the server copies the file from your home directory.
login	Server login name. The *login* 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.
password	(Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.

Note Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password. See the "Configuring the Keys for SFTP and SCP Connections" section on page 3-25 for more information.

Step 5 Install the downloaded version by entering the following command:

```
install new-version
```

When you enter the **install new-version** command, the learning and the protection processes are deactivated.

Caution During the upgrade process, you must be sure that there is a stable power supply to the Guard and avoid performing any Guard operations until the Guard displays the following message: "Press Enter to close this CLI session." If you fail to adhere to these restrictions, the upgrade may fail and cause the Guard to become inaccessible.

Step 6 Establish a new session with the Guard and check the software version by entering the **show version** command.

The following example shows how to copy a new software version file to the Guard and then to upgrade the software version:

```
user@GUARD# copy ftp new-version 10.0.0.191 /home/Versions/R3.i386.rpm user <password>
FTP in progress...
user@GUARD# install new-version
.
.
.
Press Enter to close this CLI session.
```

Note When you upgrade the software version, the Guard updates the self-protection configuration. We recommend that you do not overwrite the self-protection configuration with an older configuration because the older configuration may not be compatible with the current version.

Burning a New Flash Version to Upgrade the Common Firmware Environment

You can burn a new flash version only when there is a mismatch between the current Common Firmware Environment (CFE) and the software release. A mismatch condition can occur when you update the Guard software.

When a CFE mismatch is detected, the Guard displays the following message when you enter the **install new-version** command (X denotes the old flash version and Y denotes the new flash version): "Bad CFE version (X). This version requires version Y."

Caution You must be sure that there is a stable power supply to the Guard and avoid performing any Guard operations while you burn a new flash version. If you fail to adhere to these restrictions, the upgrade may fail and cause the Guard to become inaccessible.

To burn a new flash version, perform the following steps:

Step 1 Enter the following command in configuration mode:

```
flash-burn
```

If you try to burn a new flash version when the CFE and the Guard software versions match, the operation fails.

Step 2 Reload the Guard by entering the following command:

```
reload
```

You must enter the **reload** command after burning a new flash version. The Guard is not fully functional until you enter the **reload** command.

The following example shows how to burn a new flash version:

```
user@GUARD-conf# flash-burn
Please note: DON'T PRESS ANY KEY WHILE IN THE PROCESS!
. . .
Burned firmware successfully
SYSTEM IS NOT FULLY OPERATIONAL. Type 'reload' to restart the system
```

Resetting the Linux root or Guard admin User Account Password

You can reset the password associated with the Guard default admin user account using the Linux root user account. This may be necessary if you forget the password for the admin user account and another user with administrative privileges is not available. If another user with administrative privileges is available, see the "Changing the Passwords of Other Users" section on page 3-8.

To log in as the Linux root user, you must know the password associated with this account, which is encrypted and can only be replaced by a new password. This section shows how to reset the Linux root user password (if needed) to allow you to log in as the root user and reset the Guard default admin user password.

This section contains the following topics:

- "Resetting the Linux root User Account Password"
- "Resetting the Guard Default admin User Account Password"

Resetting the Linux root User Account Password

To reset the Linux root user account password, perform the following steps:

Step 1 Attach a keyboard and a monitor to the Guard.

Step 2 Log in as a Guard user with administrative or configuration privileges and enter the **reboot** command. If you have forgotten all passwords associated with user accounts having administrative or configuration privileges, press CTRL-ALT-DEL to reboot the Guard.

Step 3 Press down and hold the **Shift** key while the Guard is powering up.

The Guard displays the following prompt:

```
Lilo:
```

Step 4 Enter the following command to load a single user image:

```
Cisco 1
```

Note If you are running a version previous to 3.0.8, enter **Riverhead 1**. If you do not know which version you are running, press the **Tab** key to see the list of images.

Step 5 Press **Enter** at the password prompt to enter a null password.

The Guard enters the root prompt.

Step 6 Use the **passwd** command to change the root user account password. Enter a new password at the New password prompt. Reenter the new password at the “Retype new password” prompt to verify your choice.

The following example shows how to change the root password:

```
[root@GUARD root]# passwd
    Changing password for user root.
    New password: <new password typed in here>
    Retype new password: <new password typed in here>
    passwd: all authentication tokens updated successfully.
```

Step 7 Restart the Guard in normal operational mode by using the **reboot** command.

If you also need to reset the Guard default admin user account password, see the “Resetting the Guard Default admin User Account Password” section.

Resetting the Guard Default admin User Account Password

To reset the Guard default admin user account password, perform the following steps:

Step 1 Log in to the Guard as the Linux root user. If you have forgotten the password associated with the root user account, see the “Resetting the Linux root User Account Password” section.

Step 2 Switch to the admin username by using the **su - admin** command.

- **username admin admin** *password*—The *password* argument consists of 6 to 24 characters.
- **password admin**—The CLI prompts you to enter a password and reenter it for verification as shown in the following example:

```
@PGuardR3#password admin
New Password:
Retype New Password:
finished successfully
Password was changed successfully
```

The password consists of 6 to 24 characters.

Step 3 Switch back to the root prompt by using the **exit** command.

Step 4 Log out of root using the **exit** command.

Step 5 Log in to the Guard using the **admin** username and the new password.

Step 6 (Optional) Configure the other Guard user account names and passwords if required (see the “Adding a User” section on page 3-6).

Resetting the Guard Configuration to Factory Defaults

You can reset the Guard to the factory-default settings and configure it as a new Guard by using the following command in configuration mode:

clear config all

Resetting the configuration to factory defaults is useful when you want to remove an undesirable configuration in the Guard, if the configuration has become complex, or if you want to move the Guard from one network to another network.

Caution Resetting the Guard configuration deletes all configured user account information, including all usernames and associated passwords. After you reset the Guard configuration, the default user accounts (root, admin, and riverhead) are the only user accounts that remain, requiring you to log on using the procedure in the "Accessing the Guard for the First Time" section on page 2-6.

We recommend that you back up the Guard configuration before you reset it to the factory-default settings by using the **copy running-config** command. See the "Exporting the Configuration" section on page 13-2.

The out-of-band interface configurations for eth0 and eth1 are available until you reboot the Guard.

To reset the Guard to the factory-default configuration, perform the following steps:

Step 1 Enter the **clear config all** command from the configuration mode. The CLI displays a verification prompt that asks you to verify that you want to clear all of the configuration information.

Step 2 Enter **yes**. The CLI displays a prompt stating that a reboot is required and to press the Enter key.

Caution You must reboot the Guard at this time (using the current session) or the Guard will not operate correctly.

Step 3 Press the **Enter** key. The Guard reboots to the factory-default settings.

Step 4 Access the Guard by following the procedure in the "Accessing the Guard for the First Time" section on page 2-6.

Step 5 (Optional) Configure the other Guard user account names and passwords (see the "Adding a User" section on page 3-6).

The following example shows how to reset the Guard to the factory-default settings:

```
user@GUARD-conf# clear config all
Are you sure you want to clear ALL configuration and logging information?
Type 'yes' to clear config, or any other key to cancel
yes

Reboot is required after clear config. Please press Enter to continue
```

CHAPTER 14

Analyzing Guard Mitigation

This chapter describes how to analyze the Cisco Guard (Guard) mitigation and the zone traffic, and it shows how to identify configuration problems. It provides a brief explanation of how to identify the type of attack. This chapter contains the following sections:

- Analyzing Zone Traffic Patterns
- Verifying Attack Mitigation

Analyzing Zone Traffic Patterns

We recommend that once the current attack ends, you allow the Guard to learn the zone traffic patterns if the zone is an on-demand zone configuration using default parameters or if the zone traffic characteristics have changed since the last time the Guard learned the zone traffic.

Use the **show rates** command to display the current zone traffic rates. See the "Using Counters to Analyze Traffic" section on page 12-3 for more information.

View the received traffic rate and follow these guidelines:

- If the received rate is zero, this rate indicates a diversion problem. See the "Recognizing a Traffic Diversion Problem" section on page 14-2 for more information.
- If the received rate is greater than the legitimate rate, this rate indicates that the Guard mitigation is functioning, and the following problems might exist:
  - If the legitimate traffic rate for the zone is a lot higher than the zone traffic rate under normal traffic conditions, see the "Blocking Flows to the Zone Based on Flow Characteristics" section on page 14-2.
  - If the legitimate traffic for the zone is a lot lower than the zone traffic rate under normal traffic conditions, see the "Verifying Traffic Blocking Criteria" section on page 14-3.

This section contains the following topics:

- Recognizing a Traffic Diversion Problem
- Blocking Flows to the Zone Based on Flow Characteristics
- Verifying Traffic Blocking Criteria

Recognizing a Traffic Diversion Problem

If the Guard does not receive any packets, this condition may indicate a traffic diversion problem where the Guard does not receive the traffic that is sent to the zone.

See Chapter 4, "Configuring Traffic Diversion" and Appendix B, "Troubleshooting Diversion," for more information.

Blocking Flows to the Zone Based on Flow Characteristics

If the legitimate traffic rate for the zone is a lot higher than the zone traffic rate under normal traffic conditions, the Guard might not be blocking all attack traffic. A high rate of legitimate traffic can occur if you did not allow the Guard to learn the traffic patterns of a zone, such as when you use an on-demand zone configuration for zone protection (see the "Activating On-Demand Protection" section on page 9-2). If the Guard does not know the zone traffic patterns, the policy thresholds may be too high for the specific zone.

To prevent the Guard from forwarding unwanted flows to the zone, we recommend that you perform the following tasks:

- Lower the threshold of policies that measure traffic according to source IP addresses.
- View the legitimate traffic rate. If the legitimate traffic rate still seems too high, this condition could indicate a sophisticated, large-scale zombie or client attack. Such attacks consist of many flows that do not differ in the rate or in the number of connections from a regular flow. You can configure a flex-content filter to block such anomaly traffic flows. See the "Configuring Flex-Content Filters" section on page 6-3 for more information.

To lower the policy thresholds, perform the following steps:

Step 1 Display the current policy thresholds by entering the following command in zone configuration mode:

```
show policies
```

See the "Displaying Policies" section on page 7-21 for more information about the policies.

Step 2 Examine the zone global traffic by entering the following command in zone configuration mode:

```
show policies */*/*/*/global statistics
```

The Guard displays the traffic flows with the highest rates that are forwarded to the zone, as measured by the protection policies. Determine whether or not the type of services and the volume represent the zone traffic. See the "Displaying Policy Statistics" section on page 7-22 for more information about policy statistics.

Step 3 Examine the traffic of single users that are represented by a source IP address and determine which policies have a high threshold that should be decreased by entering the following command in zone configuration mode:

```
show policies */*/*/*/src_ip statistics
```

The Guard displays the traffic flows with the highest rates forwarded to the zone, as measured by the protection policies. See the "Displaying Policy Statistics" section on page 7-22 for more information about policy statistics.

Step 4 If the traffic volume does not represent the zone traffic, decrease the threshold of the source IP address policies by entering the following command in zone configuration mode:

```
policy */*/*/*/src_ip thresh-mult threshold-multiply-factor
```

The *threshold-multiply-factor* argument specifies the number by which to multiply the policy threshold. Enter a number less than 1 to decrease the policy threshold. For example, enter 0.5 to decrease the threshold by half. See the "Multiplying a Threshold by a Factor" section on page 7-16 for more information.

Verifying Traffic Blocking Criteria

If the legitimate traffic rate seems too low, it could indicate that the Guard is blocking access to the zone by legitimate clients. This condition could occur if the learning process was performed some time ago and the policy thresholds no longer fit the zone traffic pattern. The result is that the policy thresholds are not tuned properly and are set too low for current normal traffic patterns.

To verify and change the Guard blocking criteria, perform the following steps:

Step 1 If you suspect that the Guard is blocking access to the zone by legitimate clients, verify that dynamic filters are not blocking access from these clients by entering the following command in zone configuration mode:

```
show dynamic-filters [details]
```

The dynamic filters provide details on the policy that caused the production of the dynamic filters. See the "Displaying Dynamic Filters" section on page 6-19 for more information.

Step 2 Identify the policies that caused the production of the dynamic filters and display the statistics of these policies. For example, examine the traffic of single users, represented by a source IP address. Determine which policies have a low threshold that should be increased by entering the following command in zone configuration mode:

```
show policies */*/*/*/src_ip statistics
```

The Guard displays the traffic flows with the highest rates forwarded to the zone, as measured by the zone policies. See the "Displaying Policy Statistics" section on page 7-22 for further information about policy statistics.

Step 3 If the traffic volume does not represent the zone traffic, increase the threshold by entering the following command in zone configuration mode:

```
policy */*/*/*/src_ip thresh-mult threshold-multiply-factor
```

The *threshold-multiply-factor* argument specifies the number by which to multiply the policy threshold. Enter a number greater than 1 to increase the policy threshold. For example, enter 2 to increase the threshold by 2. See the "Multiplying a Threshold by a Factor" section on page 7-16 for more information.

Step 4 Display the list of dynamic filters. (See Step 1.) If the list of dynamic filters includes dynamic filters for IP addresses of legitimate clients with an action of drop, remove those dynamic filters by entering the following command in zone configuration mode:

```
no dynamic-filter filter-id
```

See the "Configuring Dynamic Filters" section on page 6-18 for more information about dynamic filters.

Step 5 If the Guard continues to produce drop-action dynamic filters from specific policies, deactivate these policies by entering the following command in policy configuration mode:

```
state inactive
```

See the "Changing the Policy State" section on page 7-13 for more information.

Tip If several policies that are part of the same policy branch produce drop-action dynamic filters, you can deactivate the policy branch by changing the policy state at the higher-level policy sections (such as policy template or service sections).

Step 6 Configure known client IP addresses that are crucial to proper zone functioning to bypass the Guard protection functions so that the Guard forwards these traffic flows directly to the zone. Create a bypass filter with the IP address of these clients by entering the following command in zone configuration mode:

```
bypass-filter row-num ip-address protocol dest-port fragments-flag
```

See the "Configuring Bypass Filters" section on page 6-11 for more information.

Verifying Attack Mitigation

After you identify an attack on the zone, you can verify that the Guard is mitigating the attack. This action is especially important if you are not familiar with the zone traffic patterns or if the zone is using an on-demand protection configuration (see the "Activating On-Demand Protection" section on page 9-2) and the Guard did not learn the zone traffic patterns.

To verify attack mitigation, perform the following actions:

- Display the zone current attack report to analyze the attack statistical information. See the "Displaying the Zone Current Attack Report" section on page 14-4 for more information.
- View the Guard filters, counters, and statistics.

This section contains the following topics:

- Displaying the Zone Current Attack Report
- Displaying the Guard Advanced Statistics
- Displaying Dropped Traffic Statistics

Displaying the Zone Current Attack Report

You can display the report of an ongoing attack to learn more about the attack characteristics and the measures that the Guard took to mitigate the attack by entering the **show reports current** command. See the "Displaying Attack Reports" section on page 11-8 for more information.

The report provides you with details about the attack. The information includes when the attack started, a general analysis of the zone traffic flow, an analysis of the packets that were dropped and replied, details of the traffic anomalies that the Guard detected in the zone traffic, and the steps that the Guard took to mitigate the attack. See the "Understanding the Report Layout" section on page 11-1 for more information.

The report provides you with details about the two main classes of DDoS attack classifications as follows:

- Bandwidth depletion—Attacks designed to flood the zone with unwanted traffic that prevents legitimate traffic from reaching the zone. These attacks include spoofed attacks and malformed packets.
- Resource depletion—Attacks that are designed to tie up the resources of the zone.

See the "Mitigated Attacks" section on page 11-4 for more information about the types of mitigated attack.

Displaying the Guard Advanced Statistics

You can view the Guard filters, counters, and diagnostics to learn about the attack characteristics and the measures that the Guard is taking to mitigate the attack. The Guard advanced statistics include the following information:

- Dynamic filters—Provides details about how the Guard is handling the attack. To view the dynamic filters, use the **show dynamic-filters command. See the "Displaying Dynamic Filters" section on page 6-19 for more information.**
- User filters—Defines how to handle traffic flows that are suspected as DDoS attacks. The zone configuration includes a default set of user filters. You can add or delete user filters. To display the user filters, use the **show** command or the **show running-config** command. The Guard displays the current traffic rate measured for each user filter. See the "Displaying User Filters" section on page 6-17 for more information.
- Statistics on dropped packets—Provides a list that details the distribution of dropped packets for the ongoing attack. To display the statistics about dropped packets, use the **show drop-statistics** command. See the "Displaying Dropped Traffic Statistics" section on page 14-5 for more information.
- Zone rate history—Provides the rate that the Guard measured for each counter in the past 24 hours and the details about the attack evolvement. To display the zone rate history, use the **show rates history** command. See the "Using Counters to Analyze Traffic" section on page 12-3 for more information.
- Zone counters—Provides the number of packets that the Guard measured for each counter and enables you to analyze how the Guard has handled the zone traffic since the attack was initiated. See the "Using Counters to Analyze Traffic" section on page 12-3 for more information.

Displaying Dropped Traffic Statistics

You can view the distribution of dropped packets for an ongoing attack by entering the following command in configuration mode:

```
show drop-statistics
```

The Guard displays the packets dropped by its protection functions by rate, packet, and bit units.

Table 14-1 provides the drop statistics.

Table 14-1 Drop Statistics

Drop Statistics	Description
Total dropped	Total amount of dropped traffic.
Dynamic filters	Amount of traffic dropped by the dynamic filters.
User filters	Amount of traffic dropped by the user filters.
Flex-Content filters	Amount of traffic dropped by the flex-content filters.
Rate limit	Packets that are defined by the rate limit parameter of the user filters and the zone **rate-limit** command that were dropped.
Incoming TCP unauthenticated basic	Traffic that the TCP basic anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
Incoming TCP unauthenticated-strong	Traffic that the TCP strong anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
Outgoing TCP unauthenticated	Zone-initiated-connections traffic that the TCP anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
UDP unauthenticated-basic	UDP traffic that the basic anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
UDP unauthenticated-strong	UDP traffic that the strong anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
Other protocols unauthenticated	Non-TCP and non-UDP traffic that the Guard anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
TCP fragments unauthenticated	TCP fragmented packets that the Guard anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
UDP fragments unauthenticated	UDP fragmented packets that the Guard anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
Other protocols fragments unauthenticated	Non-TCP and non-UDP fragmented packets that the Guard anti-spoofing functions could not authenticate and dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
DNS malformed replies	Malformed DNS replies that the Guard protection functions dropped. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.

Table 14-1 Drop Statistics (continued)

Drop Statistics	Description
DNS spoofed replies	DNS packets that are in response to zone-initiated connections that the Guard anti-spoofing functions dropped. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
DNS short queries	Short (malformed) DNS queries that the Guard protection functions dropped. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.
Non DNS packets to/from DNS port	Non-DNS traffic destined to a DNS port or from a DNS port that the Guard protection functions dropped. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.
Bad packets to proxy addresses	Malformed traffic destined to the Guard proxy IP address that the Guard protection functions dropped.
TCP anti-spoofing features related pkts	Number of dropped packets due to side operations that the Guard TCP anti-spoofing functions performed. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.
DNS anti-spoofing features related pkts	Number of dropped packets due to side operations that the Guard DNS anti-spoofing functions performed. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.
Anti-spoofing internal errors	Number of packets dropped due to the Guard anti-spoofing function errors. In the attack reports, these packets are counted under the Packets table.
SIP anti-spoofing features related pkts	Number of SIP[1] over UDP packets that the Guard dropped due to side operations. In the attack reports, these packets are counted under the spoofed packets in the Malicious Packets Statistics table.
SIP malformed packets	SIP over UDP packets that the Guard protection functions dropped because they were malformed. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.
Land attack	Number of packets dropped because they had identical source and destination IP addresses. In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.
Malformed packets	Number of packets dropped due to a malformed header in which the port, protocol or IP field in the header equals zero (0). In the attack reports, these packets are counted under the malformed packets in the Malicious Packets Statistics table.

[1] SIP = Session Initiation Protocol

The following example shows how to display the drop statistics:

```
user@GUARD-conf-zone-scannet# show drop-statistics
```

APPENDIX A

Understanding Zone Traffic Diversion

This chapter describes traffic diversion and provides detailed information about the traffic diversion methods that the Cisco Guard (Guard) uses in Layer 2 and Layer 3 topologies. The chapter also describes the long diversion and next-hop discovery methods.

This appendix contains the following major sections:

- Understanding the Router Functions in Traffic Diversion
- Understanding IP Traffic Diversion
- Understanding the Traffic Forwarding Methods
- Understanding the Layer 2 Forwarding Method
- Understanding the Layer 3 Forwarding Methods
- Injecting Traffic to the Zone
- Next-Hop Discovery

Understanding the Router Functions in Traffic Diversion

You place the Guard next to key routers in the network and when you activate the Guard to learn zone traffic or protect the zone, it diverts the traffic addressed to the zone from the routers to the Guard. When protecting a zone, the Guard analyzes and filters the zone traffic, removing the malicious packets from the diverted stream and forwarding the cleaned traffic to the main data path for delivery to the zone. The act of diverting traffic from the router is known as *hijacking*. The act of returning legitimate traffic to the network is known as *injecting*. The entire cycle (hijacking and injecting) is called the traffic diversion process. The following terminology is used in this appendix to describe the different functions of a router in the network:

- Divert-from router—Router from which the Guard diverts the destination zone traffic.
- Inject-to router—Router to which the Guard forwards the clean destination zone traffic.
- Next-hop router—Router that is the next hop to the zone according to the routing table on the divert-from router before the Guard activated traffic diversion.
- Possible next-hop routers—Group of routers, each of which is a legitimate next-hop router. A next-hop router may be changed due to routing changes in a network.

Note A router may perform more than one function in the traffic diversion process.

Understanding IP Traffic Diversion

IP traffic diversion consist of the following two tasks:

1. The Guard hijacks (diverts) the traffic of one or more zones to itself without obstructing the network traffic flow.
2. The Guard injects (forwards) the clean traffic to the original data path and on to the zone.

The Guard filtering arrays do not reside on the critical path. The Guard redirects the affected zone traffic only for processing and filtering. The Guard attack filtering capabilities are used to filter only the attacked sites within the zone while the legitimate traffic is allowed to flow directly to the zone.

This section contains the following topics:

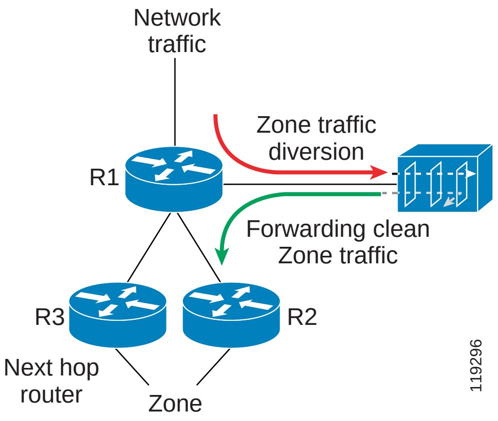
- Traffic Diversion Process
- Layer 3 Topology
- Layer 2 Topology
- Long Diversion
- BGP Diverting Method

Traffic Diversion Process

Traffic diversion (see Figure A-1) consists of the following two tasks:

1. The Guard hijacks the zone traffic from the network to itself—This task is usually performed using the Border Gateway Protocol (BGP). When the Guard is activated to provide protection for a specific zone, the Guard issues a BGP announcement to the divert-from router. The divert-from router modifies its routing table based on the BGP announcement. The routing table lists the Guard as the best next hop to the specified zone. The BGP announcement appears in the divert-from router's routing table and the router directs zone traffic to the Guard.

Figure A-1 Diversion Process



2. The Guard forwards the zone traffic to the zone—The Guard injects the cleaned traffic into the network to the next-hop router through the divert-from router's interface (the method is different in Layer 2 topology—see the "Layer 2 Topology" section).

Note The Guard does not forward the clean traffic using the regular routing table at the divert-from router. The router returns the cleaned traffic to the Guard, which is the preferred next hop for that IP address because of the diversion BGP announcement. The Guard then sends the traffic back to the router, creating a loop.

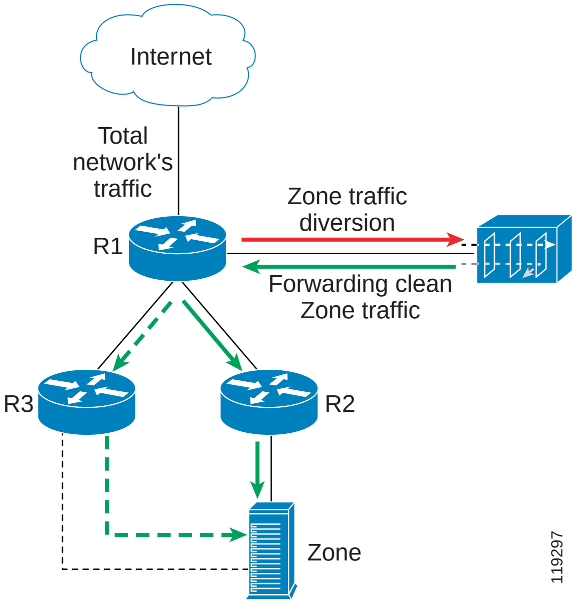
When multiple next-hop routers forward the traffic, the Guard determines which next-hop router to use to forward the traffic to the zone by a process called the next-hop discovery. Figure A-1 shows the traffic diversion process. The next-hop router to the zone could be either R2 or R3. The Guard performs the next-hop discovery process and learns which router to use (R2 in the figure).

When there is a single next-hop router only, the Guard chooses that router as the next-hop router. Due to routing changes, the current next-hop router to the zone may dynamically change. The Guard then selects the next-hop router by duplicating R1's selection of a next-hop router. The Guard acquires R1's next-hop router selection through the next-hop discovery process.

Layer 3 Topology

In a Layer 3 topology, the Guard is directly connected to the divert-from router R1 (see Figure A-2). The Guard receives the diverted traffic from R1, cleans it, and is ready to return the traffic back to R1 to forward the clean traffic to the zone. At this point, there is a danger of a closed loop between R1 and the Guard because R1 has the Guard as the addressee for any zone traffic. To avoid this loop, you must use a routing policy technique such as Policy Based Routing (PBR) or VPN Routing Forwarding (VRF) to enable the traffic to bypass R1's main routing table when R1 receives the traffic from the Guard. These routing policy techniques operate in a Layer 3 topology environment and are referred to as Layer 3 Forwarding (L3F) methods.

Figure A-2 Layer 3 Topology

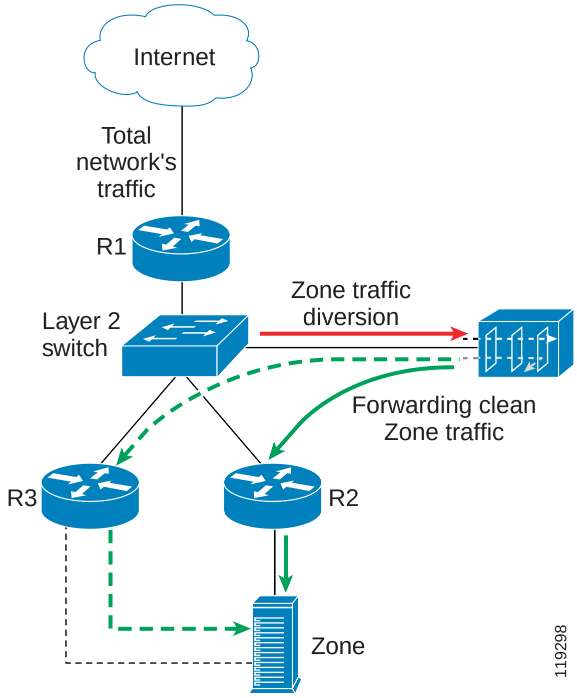


The solid line indicates that R2 is the preferred next hop to the zone; however, the zone can also be accessed through R3. R1 functions as both a divert-from router and an inject-to router. R2 functions as a next-hop router while R3 also functions as the possible next-hop router.

Layer 2 Topology

In a Layer 2 topology, the Guard is connected to a Layer 2 switch so that the divert-from router (R1), the next-hop router (R2) to the zone, and the Guard are located on the same LAN (see Figure A-3). The Guard locates the next-hop router (R2) by sending an Address Resolution Protocol (ARP) query to R2 IP address and forwards the clean zone's traffic directly to the router. The router forwards the traffic to the zone.

Figure A-3 Layer 2 Topology



The straight solid line to router R2 indicates the preferred next hop; however, it is also possible to reach the zone through R3.

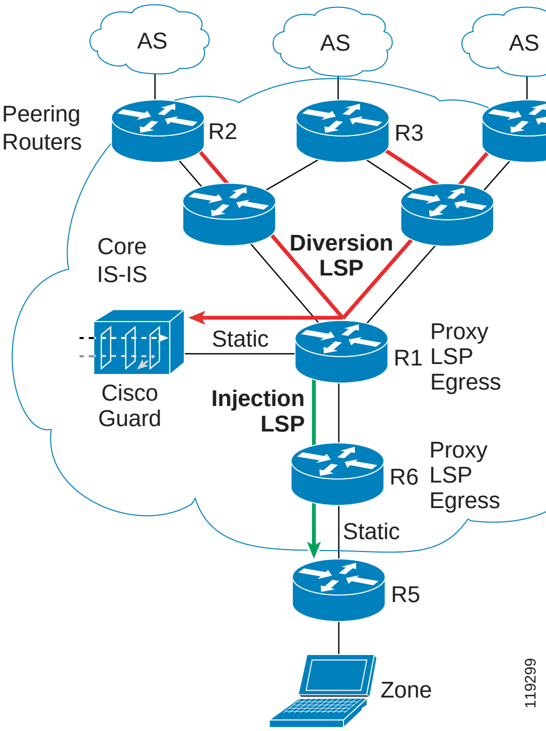
In a Layer 2 topology, the inject-to router is the same as the next-hop router. Also in a Layer 2 topology, the divert-from router, next-hop router, and the Guard are in the same LAN.

Note In some networks, a zone may be directly connected to the Layer 2 switch. A zone may be connected to the same IP subnet as the Guard. In this case, the inject-to router is configured as the zone (R2 = zone).

Long Diversion

Unlike standard diversion techniques where the Guard diverts traffic from an adjacent router only, the long diversion method diverts traffic from remotely located peering routers that may reside several hops away from the Guard. Figure A-4 shows an overview of the long diversion method in a Multiprotocol Label Switching (MPLS) network.

Figure A-4 Using the Guard for Long Diversion



BGP Diverting Method

The Guard sends a BGP announcement to the divert-from router informing the router that the next hop to the zone is the Guard. The BGP announcement can be an external Boarder Gateway Protocol (eBGP) or an internal Boarder Gateway Protocol (iBGP) announcement. In order for the announcement to take precedence over any previous routing decision regarding the zone, the Guard sends the announcement with a longer, more specific prefix than the prefix that represents the zone in the divert-from router routing table.

To ensure that the announcement reaches the Guard's adjacent router only, the BGP announcement is sent with the no-advertise and no-export BGP community strings. Only the Guard's adjacent router receives the announcement. If a packet destined to the zone reaches a next-hop router, the router forwards that packet to the zone and not back to the Guard.

The Guard also adds a special string to the BGP announcement that specifies the Guard as the originator of the announcement. The Guard uses a community that is combined from the following two autonomous system (AS) numbers: AS-number-ISP and AS-number-guard, where the AS-number-guard is a private AS number.

One advantage of using BGP for the Guard's routing announcements is that the traffic diversion to the Guard stops automatically if the router loses communication with the Guard. Because the BGP keep-alive process automatically withdraws the prefixes from the router if the peer (Guard) has not responded to several keepalive messages for a certain amount of time.

Understanding the Traffic Forwarding Methods

This section describes how to forward the clean traffic from the Guard to the next-hop router. The methods vary according to the two main network topology scenarios: Layer 2 and Layer 3 topologies.

This section contains the following topics:

- Layer 2 Topology for Traffic Forwarding
- Layer 3 Topology for Traffic Forwarding

Layer 2 Topology for Traffic Forwarding

In a Layer 2 topology, the Guard, divert-from router, and next-hop router are on the same VLAN. In a Layer 2 topology, a divert-from router and an inject-to router are two different devices. The next-hop router and the inject-to router are the same device.

Layer 3 Topology for Traffic Forwarding

In a Layer 3 topology, the divert-from and inject-to routers are the same router (referred to as the router in this chapter). The Guard sends a BGP announcement that modifies the router's routing table to divert the zone traffic to the Guard. The Guard cleans the traffic and returns the cleaned traffic to the same router. The divert-from router then sends the traffic to the router that appears as the best path to the zone. This process may result in a malicious routing loop. You can avoid this loop by associating routing rules that override the router's routing table with the traffic that the Guard returns to the router. Use the following techniques to forward the packet without using the routing table and avoid traffic loops:

- Policy-Based Routing (PBR)—Describes a rule that overrides any former routing table decision.
- Using VPN Routing Forwarding (VFR)/Routing Instance—Creates another forwarding table in the router that routes packets that the Guard returns to the router. This forwarding table contains information about how to forward the packets to the correct next hop only. The forwarding table does not contain the Guard BGP announcement that is responsible for diverting the traffic to the Guard.
- Tunnel—Uses a tunnel that is configured between the Guard and the next-hop router to forward clean traffic. The inject-to router does not perform routing decisions according to the zone address and forwards the packets to the next-hop router.

Note In long diversion cases, the peering router's main routing table is adjusted so that the zone traffic is tunneled to the Guard. The Guard forwards the cleaned traffic to the adjacent router. The adjacent router's main routing table is not changed throughout the diversion process.

The following three diversion methods depend on the next-hop router configuration; however, the next-hop router may be static for each zone or dynamically change:

- Static Next Hop Diversion methods—The next-hop router is configured in the inject-to router. These diversion methods are applicable only when the next-hop router is static for each zone.

- Dynamic Next Hop Diversion methods—These diversion methods are applicable when the next-hop router dynamically changes. You can use any dynamic diversion method as a static diversion method. Most forwarding techniques require the Guard to learn the current next-hop router described in the "Next-Hop Discovery" section, the Guard learns about the change in the next-hop router. Table A-1 summarizes the diversion methods and their characteristics.

Table A-1 Traffic Diversion Methods Summary

Method	Topology	Static/Dynamic
Layer 2 Forwarding (L2F)	Layer 2	Dynamic using Next-Hop Discovery
Policy-Based Routing Destination (PBR-DST)	Layer 3	Static
VPN (Virtual Private Network) Routing Forwarding Destination (VRF-DST)	Layer 3	Static
Policy-Based Routing VLAN (PBR-VLAN)	Layer 3	Dynamic using Next-Hop Discovery
VPN Routing Forwarding VLAN (VRF-VLAN)	Layer 3	Dynamic using Next-Hop Discovery
TUNNELS	Layer 3	Dynamic using Next-Hop Discovery

Understanding the Layer 2 Forwarding Method

The L2F method is used in a network topology where the Guard, divert-from router, and next-hop router are on the same VLAN (see Figure A-3). In a Layer 2 topology, a divert-from router and an inject-to router are two different devices. The next-hop router and the inject-to router are the same device.

In the L2F method, the Guard resolves the MAC address of the inject-to/next-hop router and then forwards the traffic to that address. To resolve the MAC address, the Guard issues a standard ARP query for the IP address of the inject-to/next-hop router. When using the L2F method, no configuration on the routers is required.

Depending on a particular network configuration, a zone can be directly connected to a Layer 2 switch, which means that the zone is connected to the same LAN as the Guard. The Guard forwards the traffic directly to the zone because the zone IP address is configured as the inject-to router. If the traffic is sent to the protected zone through an IP forwarding device, the IP forwarding device must be defined as the Guard's next-hop device. See the "Layer-2 Forwarding Method" section on page 4-7 for more information.

Understanding the Layer 3 Forwarding Methods

This section describes the traffic forwarding methods that the Guard uses in a Layer 3 network topology.

This section contains the following topics:

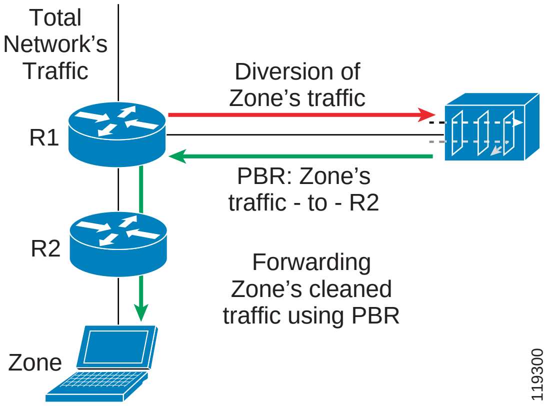
- Policy-Based Routing-Destination
- VPN Routing Forwarding-Destination
- Policy-Based Routing VLAN

- VPN Routing Forwarding VLAN
- Using Tunnel Diversion to Forward Traffic
- Long Diversion Method
- Diverting Traffic to the Guard
- BGP Announcements
- MPLS LSP

Policy-Based Routing-Destination

The Policy-Based Routing-Destination (PBR-DST) method allow you to configure routing rules that are different from the rules configured in the router's routing table. You configure the PBR-DST rules only on the router's interface that faces the Guard. You perform the configuration once. A configured rule specifies that all traffic from the Guard to a zone is forwarded to the corresponding next-hop router. This process is a static next-hop discovery method. See the "PBR Destination Configuration Guidelines" section on page 4-9 for more information.

Figure A-5 PBR Forwarding Method



In Figure A-5, the PBR-DST method is applied to R1's interface facing the Guard to define a rule that specifies that all the zone traffic coming from the Guard is forwarded to R2.

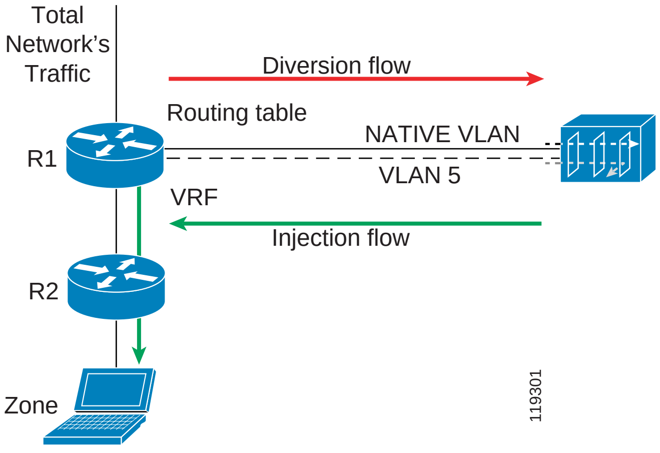
VPN Routing Forwarding-Destination

The VPN Routing Forwarding-Destination (VRF-DST) method (see Figure A-6) allows you to configure another routing and forwarding table (the VRF table) in addition to the main routing and forwarding tables.

The additional routing table is used only to route traffic that comes into the router's interface that faces the Guard. You configure two separate interfaces on the router's physical interface that faces the Guard. The first interface (the NATIVE VLAN) diverts traffic from the router to the Guard. Traffic on this VLAN is forwarded according to the global routing table. On this VLAN, the Guard sends the BGP announcements that divert the traffic to the Guard.

The second VLAN diverts the returned traffic from the Guard to the router. You configure a VRF table on the second VLAN. This table contains a static routing rule to forward all the zone traffic to a specific next-hop router. The VRF-DST method is also a static next-hop diversion method. Dynamic next hop diversion methods using VRF and PBR are described in the "Next-Hop Discovery" section on page A-15. See the "Policy-Based Routing Destination Forwarding Method" section on page 4-9 for more information.

Figure A-6 VRF-DST Forwarding Method



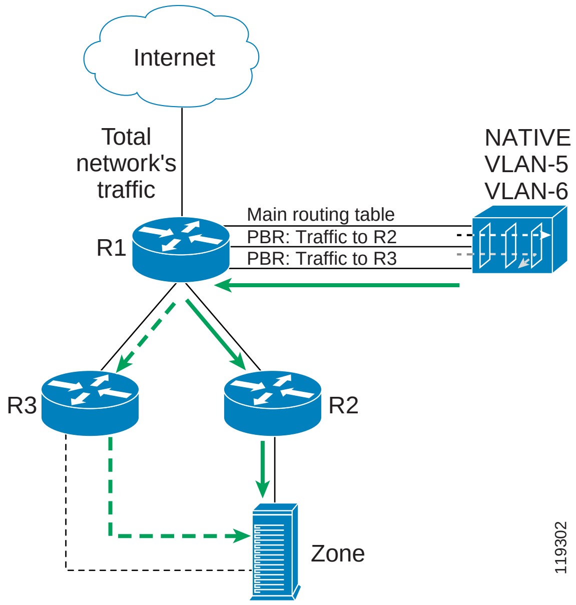
The VRF-DST method is applied on the router interface that faces the Guard. You define a VRF table on this interface to contain a rule that routes all the zone's traffic coming from the Guard to R2.

Note The VRF-DST method is applicable only when the next-hop router is static for each zone.

Policy-Based Routing VLAN

In the PBR VLAN method, you can configure a multiple VLAN (Virtual LAN, 802.1Q) trunk between the Guard and router R1 (see Figure A-7). You associate each VLAN in the trunk with a different possible next-hop router. In addition, you configure a PBR on each of the VLAN logical interfaces in the router side. Each PBR forwards all the traffic from a specific VLAN to its corresponding next-hop router. The Guard then forwards packets to a particular next-hop router by transmitting the packets over the appropriate VLAN to allow the Guard to change the next-hop router of a zone by changing the VLAN on which the packets are forwarded. In the figure, the NATIVE VLAN is used for the diversion of traffic (the Guard sends the BGP announcements on this interface to the router).

Figure A-7 PBR VLAN Forwarding Method

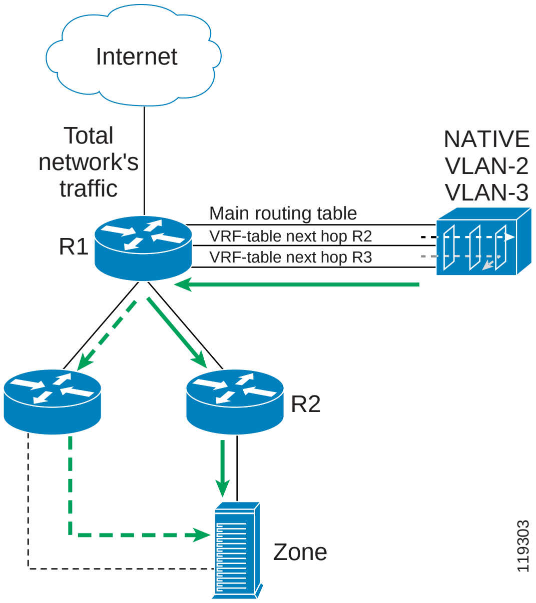


In Figure A-7, the PBR VLAN method is applied on R1's interface that faces the Guard. The traffic that comes over VLAN-5 is forwarded to R2 and the zone's traffic coming from the Guard over VLAN-6 is forwarded to R3. See the "Policy-Based Routing VLAN Forwarding Method" section on page 4-14 for more information.

VPN Routing Forwarding VLAN

The VPN Routing Forwarding (VRF) VLAN method is the same as the PBR VLAN (see the "Policy-Based Routing VLAN" section on page A-9) method except that you can associate a VRF table with each VLAN in the inject-to router instead of a PBR table. Each VRF table contains the rule that directs all the traffic that arrives on it to the corresponding next-hop router. The Guard then forwards packets to a particular next-hop router by transmitting the packets over the appropriate VLAN to allow the Guard to change the zone next-hop router by changing the VLAN that forwards the packets. In Figure A-8, the native VLAN is used for traffic diversion (on this interface, the Guard sends the BGP announcement). See Chapter 4, "Configuring Traffic Diversion" for more information.

Figure A-8 VRF-VLAN Forwarding Method

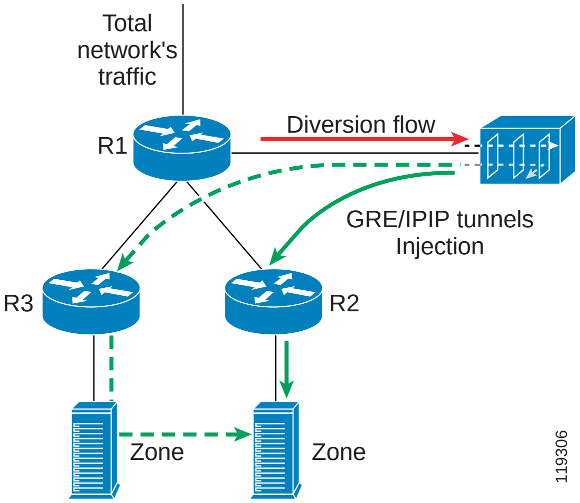


In Figure A-8, the VRF-VLAN method is applied on R1's interface that faces the Guard. Traffic that flows over VLAN-2 is forwarded to R2 and traffic that flows over VLAN-3 is forwarded to R3.

Using Tunnel Diversion to Forward Traffic

In the tunnel diversion method, you configure a tunnel between the Guard and each of the next-hop routers (see Figure A-9). The Guard sends the traffic over the tunnel that ends in the next-hop router of the destined zone. Because the returned traffic goes over a tunnel, the inject-to router performs a routing decision on the end point of the tunnel interface only, not on the zone's address.

Figure A-9 Tunnel Diversion



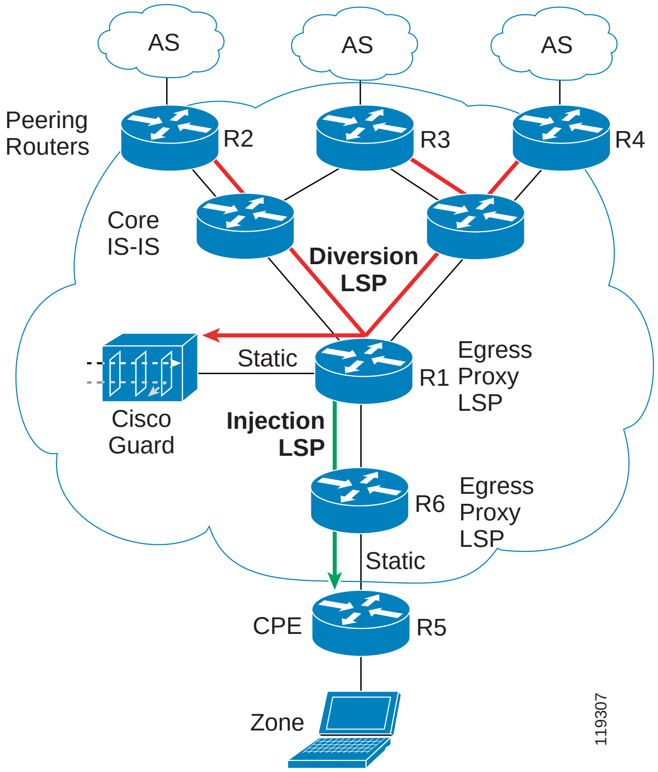
See the "Tunnel Diversion Forwarding Method" section on page 4-20 for more information.

Long Diversion Method

Unlike standard diversion techniques where the Guard diverts traffic only from a directly connected adjacent router, the long diversion method diverts traffic from remotely located peering routers that may reside several hops away from the Guard. The traffic to the zone is diverted from the peering points to the Guard over a tunnel such as GRE/IPIP or MPLS LSP. The regular forwarding method can inject the clean traffic back onto the network because the forwarding tables of R1 (attached to the Guard) and the other backbone routers are untouched.

Figure A-10 shows how a diversion is implemented in an ISP backbone that implements MPLS. In the figure, R2, R3, and R4 are peering routers, while R1 is the router adjacent to the Guard.

Figure A-10 Guard Long Diversion



The long diversion process is divided into three parts:

- Diversion—The Guard diverts the zone's traffic from the peering routers (R2, R3, R4) to itself.
- Cleaning—The Guard removes malicious packets and forwards clean packets.
- Injection—The Guard returns clean traffic back to the network.

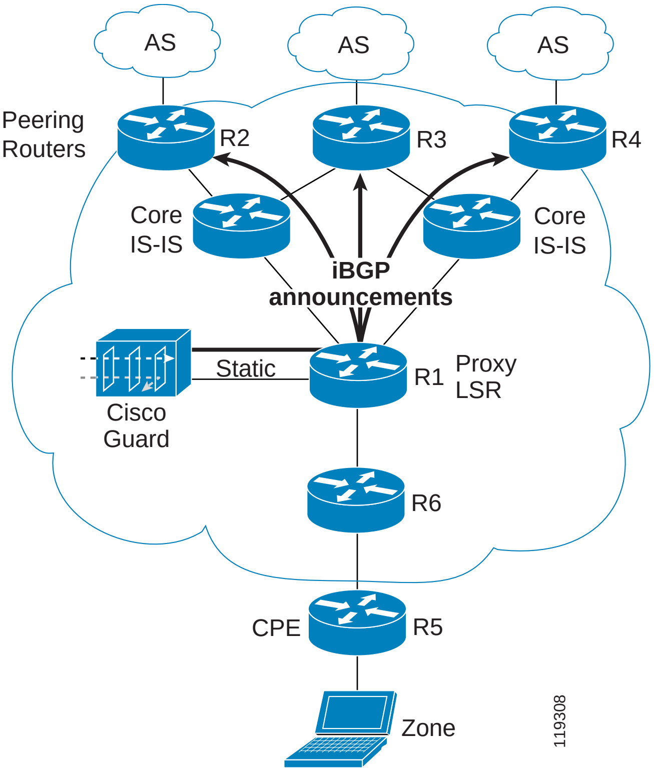
Diverting Traffic to the Guard

Once an attack has been launched against a specific zone, the Guard sends out an iBGP announcement stating that in order to reach the zone, the traffic should route to the Layered Service Provider (LSP) that ends in the Guard's loopback address/interface. To ensure that the BGP announcements do not propagate into all the backbone routers' routing tables, the Guard attaches **no-advertise** and **no-export** BGP community strings to the BGP announcements. Only R2, R3, and R4 get the BGP announcement about the zone's (with a longer prefix) next hop that corresponds to the Guard's loopback interface.

BGP Announcements

In the BGP announcement method, the Guard sends an iBGP announcement (with **no-advertise** and **no-export**) to routers R2, R3, and R4 informing them that the next hop to the zone is the Guard loopback interface. You set the next-hop attribute in the BGP announcement (using the **route-map** command in Cisco IOS software). The announcement uses a longer prefix then the original announcement of the zone and gets priority over the original BGP announcement.

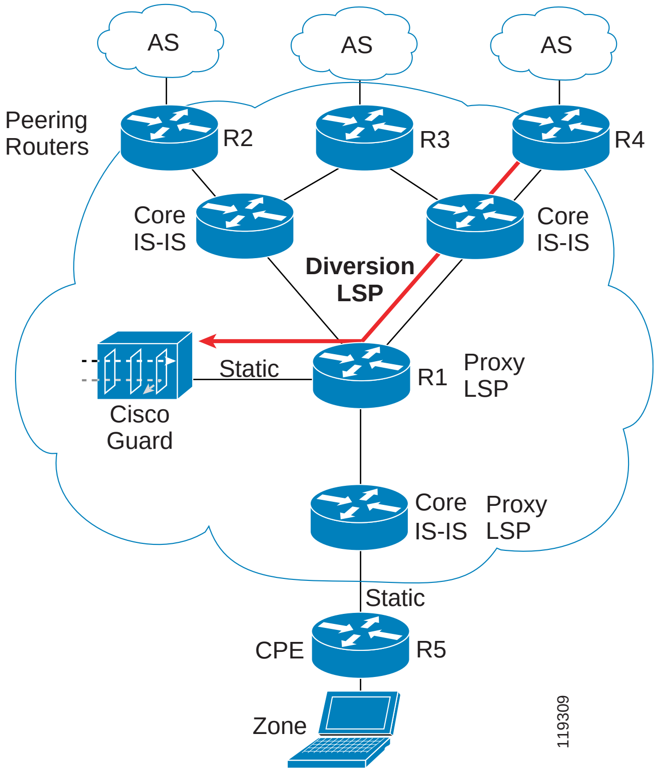
Figure A-11 iBGP Announcement to the Peering Routers



MPLS LSP

In the MPLS LSP method, after the iBGP announcement reaches the peering routers, the routers reroute the zone traffic to the LSP that extends from the peering points to the Guard loopback interface (see Figure A-12).

Figure A-12 MPLS LSP from the Peering Routers (R2, R3, R4) to the Guard



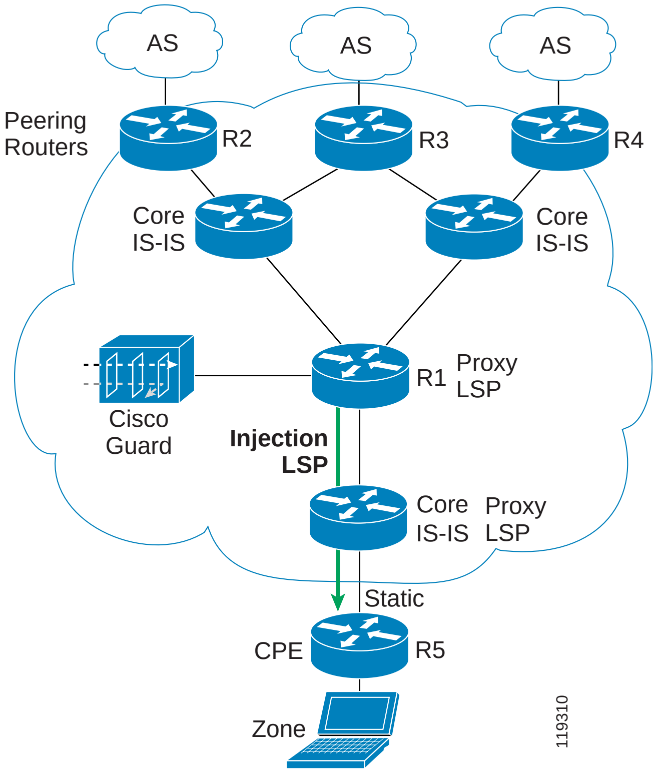
While the Guard is at the end of the LSP, the Guard does not have to support MPLS; it only receives pure IP (IP packets without an MPLS label) because R1 is the egress proxy LSP for the Guard. In other words, R1 performs one hop before the last-hop popping (removal of the MPLS label) on the MPLS packets that arrive at the Guard's loopback interface and delivers them directly to the Guard over the static route.

You should route the Guard's loopback address through IGP in the entire network by configuring R1 with a static route to the loopback address of the Guard. This process redistributes this static route with the IGP protocol (IS-IS in the example). The Guard does not run IS-IS.

Injecting Traffic to the Zone

After the Guard cleans the traffic, it injects the traffic back to R1 (see Figure A-13). In this scenario, it is assumed that R1 stores all routes to all the possible zones as if it was a peering router. R1 forwards the traffic to the zone using the suitable LSP.

Figure A-13 Injecting the Traffic to the Zone



The caveats and limitations for long diversion are as follows:

- Router (R1) connected to the Guard—When injecting clean traffic back into the network, the Guard forwards the traffic to R1, which then performs IP lookup. R1 should have routes to all the possible zones. R1 should not be a peering router (if R1 is a peering router and a divert-from router, then you should use a different method to inject the clean traffic). A regular core router does not have to have all the routes to the potential zones because a core router can store routes to all the loopback interfaces of the routers in the network.
- Backbone Capacity—The ISP backbone infrastructure must be able to handle the volume of the attacked traffic.
- MPLS Enabled—MPLS needs to be implemented on the backbone infrastructure. Several other tunnel techniques can also be implemented (for example, GRE).
- Topology Assumption—If an LSP from R1 to the zone ends at an edge router (for instance, R6), and R6 does not implement egress proxy LSP, then the Guard cannot divert traffic from that router (that is, R6 cannot also be a peering router). If the LSP from R1 to the zone ends in the customer premises equipment (CPE), then the Guard can divert traffic from R6 (R6 can be also a peering router). An LSP may end in a CPE, even if the CPE does not support MPLS, by using R6 as an egress proxy LSP. See the "Long Diversion Method" section on page 4-22 for more information.

Next-Hop Discovery

When forwarding the traffic to the zone, the Guard should know which router is the next-hop router as determined by the divert-from router. Next-hop discovery is the process that the Guard runs in order to learn which router is the next-hop router. Because the next-hop router is the next hop to the zone (according to the divert-from router before diversion), the Guard should have the same view of the routing information that the divert-from router does. This routing information may include IGP and/or BGP information. The Guard should have the same neighbors that the divert-from router does. The Guard should receive all the routing protocols that the divert-from router runs in order to find the route to the zone. In some cases it would be enough to run only the IGP routing protocols, and in some cases it would require receiving the IGP and the BGP protocols. This solution applies only if the divert-from router uses a routing protocol to make its decision on how to route to the zone, instead of using static routes to the zones. If a static route is used, then the next hop route cannot be determined from the routing protocol (you should consider using a discovery by Telnet solution).

To receive the same IGP information as the divert-from router, you should connect the Guard by tunnels (GRE/IPIP) to the possible next-hop routers of the divert-from router.

To receive BGP information, the Guard need only be an iBGP neighbor of the divert-from router because with iBGP, the divert-from router announces its routing information to the Guard.

Caution Make sure that you do allow the Guard to be visible to the network because it will receive traffic other than the zone traffic.

This section contains the following topics:

- Using IGP to Determine the Next-Hop Router
- Using IGP and BGP to Determine the Next-Hop Router

Using IGP to Determine the Next-Hop Router

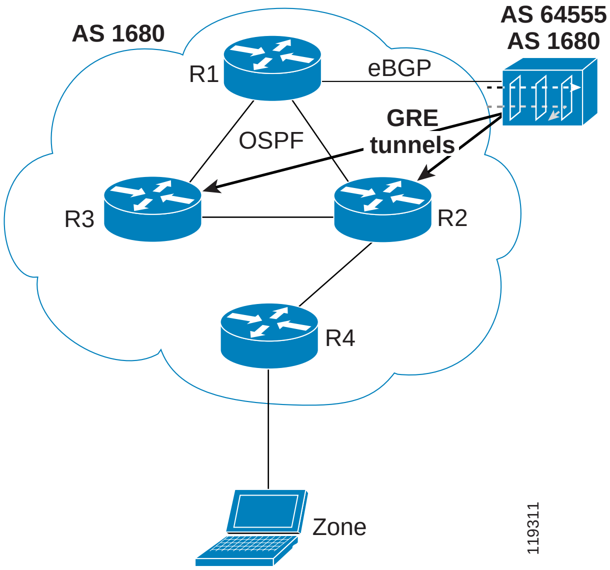
The Guard learns the next-hop router only by receiving the IGP routing information in these situations:

- The zone belongs to the same Autonomous System (AS) as the divert-from router. The routing is done using the IGP information protocol (OSPF/IS-IS/EIGRP).
- The zone and the divert-from router do not belong to the same AS. The route to the zone is learned by BGP, and the routes are redistributed to the IGP protocols.

The Guard supports only OSPF and RIP, because the Guard uses the Zebra routing-protocols software that supports only the above IGP protocols.

Figure A-14 shows how to receive IGP information.

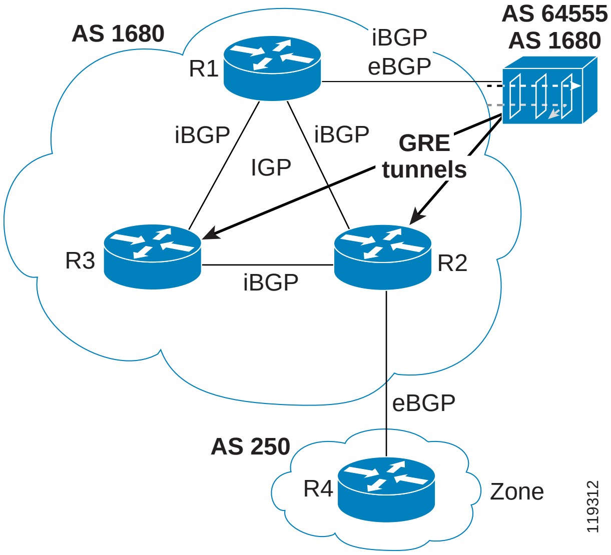
Figure A-14 Next-hop Discovery Leaning by IGP



Using IGP and BGP to Determine the Next-Hop Router

When the zone is in a different AS than the divert-from router, and BGP information is not redistributed to IGP, then the next-hop information to that zone is determined from both the IGP and BGP routing information. The divert-from router decides on the next hop in two phases. First, it learns the next BGP hop to the zone using BGP, and then it learns the actual next-hop router (interface) that leads to that next BGP peer from IGP (see Figure A-15).

Figure A-15 Next-hop Discovery Learning by IGP+BGP



To receive the BGP information of the divert-from router, the Guard receives the iBGP announcement from the divert-from router. The next-hop attribute is unaltered (the original next-hop is saved) in iBGP.

In this method, the two BGP daemons act as peers with the divert-from router. The first, the eBGP daemon (used for traffic diversion), and the second, the iBGP daemon (used for the next-hop discovery process).

To receive the same IGP information as the divert-from router, a third daemon which is the IGP daemon, is connected by tunnels to the possible next-hop routers of the divert-from router.

The Guard performs the same two-phase process as the divert-from router to establish the next hop to a zone. First, the Guard learns the next BGP hop router to the zone from BGP, and then it uses IGP to discover the route to the next-hop BGP router. In the figure, the Guard learns that the next hop to the zone is R4 and the IGP route to this interface.

Blocking the Guard from Announcing Traffic/Updates

The Guard participates in IGP and IBGP only to learn the next-hop router and it must not announce any routing information or receive any traffic in addition to the routing updates over the tunnel. To block the Guard from announcing traffic updates, follow these steps:

Step 1 Configure the Guard not to redistribute any information learned by IBGP.

Step 2 Configure tunnels so that no regular traffic is routed from the network to the Guard using the tunnel. You can configure the OSPF tunnel links to the Guard with the highest weight by using the **ip ospf cost 65535** command.

Step 3 Verify that the Guard is not selected as the DR/BDR by using the **ip ospf priority 0** command.

APPENDIX B

Troubleshooting Diversion

This appendix describes troubleshooting procedures designed to overcome traffic diversion problems related to the Guard divert-from routers.

This chapter contains the following topics:

- Configuring a BGP Session on the Guard and the Divert-From Router
- Verifying the Guard to Divert-From Router BGP Session Configuration
- Verifying the Divert-From Router Records

Configuring a BGP Session on the Guard and the Divert-From Router

This section describes how to configure Border Gateway Protocol (BGP) on the Guard and the Cisco divert-from router.

This section contains the following topics:

- Configuring a BGP Session on the Guard
- Configuring a BGP Session on the Cisco Divert-from Router

Configuring a BGP Session on the Guard

This section describes how to configure BGP on the Guard.

Switch to the Zebra application and configure BGP from the global command group level by entering the following commands:

```
admin@GUARD-conf# router
router> enable
router# config terminal
router(config)# router bgp 7000
router(config-router)# redistribute guard
router(config-router)# bgp router-id 192.168.3.12
router(config-router)# neighbor 192.168.3.1 remote-as 5000
router(config-router)# neighbor 192.168.3.1 description C2948
router(config-router)# neighbor 192.168.3.1 soft-reconfiguration inbound
router(config-router)# neighbor 192.168.3.1 route-map filter-out out
router(config-router)# exit
router(config)# route-map filter-out permit 10
router(config-route-map)# set community no-advertise no-export
```

Configuring a BGP Session on the Cisco Divert-from Router

From the Cisco divert-from router prompt line, enter the following commands:

```
router bgp 5000
 bgp log-neighbor-changes
 neighbor 192.168.3.12 remote-as 7000
 neighbor 192.168.3.12 description "Guard"
 neighbor 192.168.3.12 soft-reconfiguration inbound
 neighbor 192.168.3.12 route-map Guard-in in
!
ip classless
ip route 192.168.4.0 255.255.255.0 192.168.3.2
ip bgp-community new-format
ip community-list 10 permit no-export no-advertise
route-map Guard-in permit 10
 match community 10 exact-match
```

Verifying the Guard to Divert-From Router BGP Session Configuration

This procedure describes how to check the status of the BGP session as established between the Guard and the Guard’s neighboring router (the divert-from router). In this procedure, entering the **show ip bgp summary** command from the Guard and from the divert-from router allows you to scan the summary reports for indications of a problem and check that the BGP connection is alive.

To check the Guard to divert-from router BGP session status, perform the following steps:

Step 1 Switch to the Zebra application by entering the following command from the configuration command group level:

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

The system enters the Zebra application. The router> prompt appears, indicating that the system is in the Zebra non- privileged mode. At each command level of the Zebra application, press the question mark (?) key to display the list of commands available at this mode.

Step 2 Display the BGP summary report by entering the following command:

```
router> show ip bgp summary
```

The following example shows that there is no problem indicated on the Guard to router path. The State/PfxRcd column contains a digit (0), indicating that no problems exist with the BGP session.

Note A nondigit signifier (such as idle, active, or connect) at the State/PfxRcd column indicates a BGP session problem.

```
router> show ip bgp summary
BGP router identifier 192.168.3.12, local AS number 7000
0 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.3.1	4	5000	9	12	0	0	0	00:05:32	0

```
Total number of neighbors 1
router>
```

Step 3 Verify the BGP session on the Cisco Router-to-Guard path by entering the following command from the Cisco divert-from router prompt line:

```
7513# show ip bgp summary
```

In the following example, the zero (Ø) and Active indicators in the State/PfxRcd column indicate a BGP session problem.

Note A zero (0) or Active state displayed in the State/PfxRcd column indicates a BGP session problem. A zero (0) state should display only when the Guard uses the BGP session for hijacking traffic only (not for injecting traffic).

A correlation should exist between the Guard BGP router IP address and the IP address indicated at the router's end (192.168.3.12 in the sample screen). See the above sample screen.

```
7513# show ip bgp summary
BGP router identifier 192.168.77.1, local AS number 5000
BGP table version is 81, main routing table version 81
5 network entries and 5 paths using 605 bytes of memory
2 BGP path attribute entries using 244 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP route-map cache entries using 16 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 51/46 prefixes, 67/62 paths, scan interval 60 secs

Neighbor       V    AS     MsgRcvd MsgSent TblVer  InQ OutQ    Up/Down State/PfxRcd
192.168.3.3    4    6000    6030    5961   81      0   0       2d03h    0
192.168.3.12   4    7000   30030   30002   81      0   0       6d03h    1
192.168.3.21   4    8000   11829   11834   81      0   0       1w1d     0
192.168.3.88   4    9000       0       0    0      0   0       never   Active
192.168.3.99   4   64555       0       0    0      0   0       never   Active
... ... ...
```

Verifying the Guard Routing Table Records and Advertising

This procedure describes how to check that the zone IP mask is correctly inserted in the Guard routing tables and that the Guard properly advertises the route to the divert-from router.

To verify the route to the divert-from router, perform the following steps:

Step 1 Switch to the Zebra application by entering the following command from the configuration command group level:

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

The system enters the Zebra application. The router> prompt appears indicating that the system is in the Zebra non- privileged mode.

Step 2 Switch to the privilege mode by entering the **enable** command. The following prompt appears:

```
router#
```

Step 3 Verify that the Guard has inserted the IP mask information into the routing table by entering the following command:

```
router# show ip route
```

The following example indicates that the Guard has inserted a line (marked with G>) into the Zebra routing tables that contains the zone IP mask:

```
router# show ip route
C>* 10.0.0.0/8 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, l0
C>* 192.168.3.0/24 is directly connected, giga1
C>* 192.168.3.13/32 is directly connected, giga1
C>* 192.168.3.14/32 is directly connected, giga1
G>* 192.168.4.2/32 is directly connected, l0
S>* 192.168.4.2/32 [1/0] via 192.168.3.2, giga1
router#
```

Step 4 Verify that the Guard has advertised the route to the Cisco divert-from router by entering the following command from the Guard's router configuration level:

```
router> show ip bgp neighbors 192.168.3.1 advertised-routes
```

The following example verifies that the Guard advertised the route to the neighboring router (marked in *>) :

```
router> show ip bgp neighbors 192.168.3.1 advertised-routes
BGP table version is 4, local router ID is 192.168.3.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop       Metric LocPrf Weight Path
*> 192.168.4.2/32   192.168.3.12     0           32768  ?
Total number of prefixes 1
router>
```

Verifying the Divert-From Router Records

You can verify the following divert-from router information:

- The Guard has inserted the advertised route into the divert-from router's routing table.
- The route was inserted with a longer prefix.
- The route was received through a BGP update.

Verify the divert-from router information by typing the following from the Cisco divert-from router prompt line:

```
7513(config)# show ip route
```

The following example shows that the Guard has inserted the route into the divert-from router's routing table. The route has a longer prefix (…/32) and it was received through a BGP update.

```
7513(config)# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set

  192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
S 192.168.4.0/24 [1/0] via 192.168.3.2
B 192.168.4.2/32 [20/0] via 192.168.3.12, 00:00:00
C 10.0.0.0/8 is directly connected, FastEthernet0/1
C 192.168.1.0/24 is directly connected, FastEthernet5/0
... ... ...
```

INDEX