



# 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](#)
- [Displaying the Guard Zones](#)
- [Using Counters to Analyze Traffic](#)
- [Displaying the Zone Status](#)
- [Managing Guard Logs](#)
- [Monitoring Network Traffic and Extracting Attack Signatures](#)
- [Displaying General Diagnostic Data](#)
- [Managing Disk Space](#)
- [Displaying Memory Consumption](#)
- [Displaying the CPU Utilization](#)
- [Monitoring System Resources](#)
- [Managing the ARP Cache](#)
- [Displaying Network Statistics](#)
- [Using Traceroute](#)
- [Verifying Connectivity](#)
- [Obtaining Debug Information](#)
- [Displaying the Guard Self-Protection Configuration](#)
- [Understanding the Flex-Content Filter Default Configurations](#)

## 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
<b>all</b>	Displays configuration files of all Guard functions (Guard, zones, interfaces, router, and self-protection).
<b>Guard</b>	Displays the Guard configuration file.
<b>interfaces</b> <i>interface-name</i>	Displays the configuration file of the Guard interfaces. Enter the interface name.
<b>router</b>	Displays the router configuration.
<b>self-protection</b>	Displays the Guard self-protection configuration.
<b>zones</b>	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 details**—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 <b>zone</b> 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-scanner# 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-daemon/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 <b>warning</b> , 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
<b>zone</b> <i>zone-name</i>	(Optional) Specifies the <i>zone name</i> . Exports the <i>zone log file</i> . The default is to export the Guard log file.
<b>log</b>	Exports the log file.
<b>ftp</b>	Specifies FTP.
<b>sftp</b>	Specifies SFTP.
<b>scp</b>	Specifies SCP.
<i>server</i>	IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).
<i>full-file-name</i>	Complete name of the file. If you do not specify a path, the server saves the file in your home directory.
<i>login</i>	(Optional) Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
<i>password</i>	(Optional) Password for the remote FTP server. If you do not enter the password, the 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](#)
- [Activating the Guard to Manually Record Traffic](#)
- [Stopping the Guard from Manually Recording Traffic](#)
- [Managing Packet-Dump Capture Files Disk Space](#)
- [Displaying Manual Packet-Dump Settings](#)
- [Displaying Automatic Packet-Dump Settings](#)
- [Exporting Packet-Dump Capture Files Automatically](#)
- [Exporting Packet-Dump Capture Files Manually](#)
- [Importing Packet-Dump Capture Files](#)
- [Displaying Packet-Dump Capture Files](#)
- [Generating Attack Signatures from Packet-Dump Capture Files](#)
- [Copying Packet-Dump Capture Files](#)
- [Deleting Packet-Dump Capture Files](#)

## 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: <ul style="list-style-type: none"> <li>• <b>protect</b>—The Guard recorded the traffic during zone protection.</li> <li>• <b>learn</b>—The Guard recorded the traffic during the zone learning process or the protect and learning process.</li> </ul>
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: <ul style="list-style-type: none"> <li>• <b>forwarded</b>—The Guard identified traffic as legitimate and forwarded it to the zone.</li> <li>• <b>dropped</b>—The Guard identified traffic as malicious and dropped it.</li> <li>• <b>replied</b>—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.</li> </ul>

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-scanner# 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                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>view</b>               | (Optional) Displays the traffic that the Guard is recording in real time.                                                                                                                                                                                                                                                                                                                                   |
| <i>capture-name</i>       | 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.                                                                                                                                                                                                                                                   |
| <i>pdump-rate</i>         | Sample rate in packets per second (pps). Enter a value from 1 to 10000.<br><br><b>Note</b> The Guard supports a maximum accumulated packet-dump capture rate of 10000 pps for all concurrent manual captures.<br><br>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. |
| <i>pdump-count</i>        | 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.                                                                                                                                                                                                                  |
| <b>all</b>                | Captures all traffic.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>dropped</b>            | Captures only traffic that the Guard dropped.                                                                                                                                                                                                                                                                                                                                                               |
| <b>forwarded</b>          | Captures only legitimate traffic that the Guard forwarded to the zone.                                                                                                                                                                                                                                                                                                                                      |
| <b>replied</b>            | Captures only the traffic that the Guard anti-spoofing and anti-zombie functions sent back to the source in a verification attempt.                                                                                                                                                                                                                                                                         |
| <i>tcpdump-expression</i> | (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 <a href="#">“Configuring the tcpdump-expression Syntax”</a> 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-scanner# 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-scanner# 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](http://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                                                                                                                                                                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>zone</b> <i>zone-name</i> | Specifies the name of an existing zone.                                                                                                                                                                                                                                                                       |
| <b>packet-dump captures</b>  | Exports packet-dump capture files.                                                                                                                                                                                                                                                                            |
| <i>capture-name</i>          | (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 “ <a href="#">Displaying Packet-Dump Capture Files</a> ” section on <a href="#">page 12-17</a> for more information. |
| <b>ftp</b>                   | Specifies FTP.                                                                                                                                                                                                                                                                                                |
| <b>sftp</b>                  | Specifies SFTP.                                                                                                                                                                                                                                                                                               |
| <b>scp</b>                   | Specifies SCP.                                                                                                                                                                                                                                                                                                |
| <i>server</i>                | IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).                                                                                                                                                                                          |
| <i>remote-path</i>           | Complete name of the path where the Guard saves the packet-dump capture files.                                                                                                                                                                                                                                |
| <i>login</i>                 | (Optional) Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.                                                                                      |

**Table 12-11 Arguments and Keywords for the copy zone packet-dump Command (continued)**

| Parameters              | Description                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>password</i>         | (Optional) Password for the remote FTP server. If you do not enter the password, the Guard prompts you for one.                                                                                                                                                                                                                                   |
| <i>file-server-name</i> | Name of a network server. You must configure the network server using the <b>file-server</b> command.<br><br>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.<br><br>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                                                                                  |
|-----------------------------|----------------------------------------------------------------------------------------------|
| <b>ftp</b>                  | Specifies FTP.                                                                               |
| <b>sftp</b>                 | Specifies SFTP.                                                                              |
| <b>scp</b>                  | Specifies SCP.                                                                               |
| <b>zone zone-name</b>       | Specifies the name of an existing zone for which the packet-dump capture files are imported. |
| <b>packet-dump captures</b> | Imports packet-dump capture files.                                                           |

**Table 12-12 Arguments and Keywords for the copy zone packet-dump Command (continued)**

| Parameter               | Description                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>server</i>           | IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).                                                                                                                                                                                                                              |
| <i>full-file-name</i>   | Complete 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.<br><br><b>Note</b> Do not specify the file extension because it will cause the import process to fail.                                                                        |
| <i>login</i>            | Server login name. The <i>login</i> argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.                                                                                                                                     |
| <i>password</i>         | (Optional) Password for the FTP server. If you do not enter the password, the Guard prompts you for one.                                                                                                                                                                                                                                          |
| <i>file-server-name</i> | Name of a network server. You must configure the network server using the <b>file-server</b> command.<br><br>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.<br><br>See the “Exporting Files Automatically” section on page 13-5 for more information. |
| <i>capture-name</i>     | 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 <b>file-server</b> 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                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>capture-name</i>       | (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.<br><br>If you specify the name of a packet-dump capture file, the Guard displays the file in TCPDump format.                                |
| <i>tcpdump-expression</i> | (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 “ <a href="#">Configuring the tcpdump-expression Syntax</a> ” 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-scanner# 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 “ <a href="#">Configuring the tcpdump-expression Syntax</a> ” 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                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>capture-name</i>           | Name of an existing packet-dump capture file from which to generate an attack signature.                                                                                                                                |
| <i>reference-capture-name</i> | (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 <i>start-offset</i> 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 <i>end-offset</i> 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 <a href="#">“Configuring the pattern-expression Syntax” section on page 6-8</a> 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                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>zone</b> zone-name           | Specifies the name of an existing zone.                                                                                                                                                                                                                                                                                                                                               |
| <b>packet-dump</b>              | Copies the packet-dump capture file.                                                                                                                                                                                                                                                                                                                                                  |
| <b>captures</b><br>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 <a href="#">“Configuring the tcpdump-expression Syntax” section on page 6-6</a> for more information. |
| new-name                        | Name of the new packet-dump capture file.<br><br>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                                     |
|------------------------------|-------------------------------------------------|
| <b>zone</b> <i>zone-name</i> | Specifies the name of an existing zone.         |
| <b>packet-dump captures</b>  | Deletes packet-dump capture files.              |
| *                            | Erases all packet-dump capture files.           |
| <i>name</i>                  | 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                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>logs</b>        | Sets the history parameters for the Guard and zone logs.                                                                                                                                                                                                                                                                                                                                                         |
| <b>reports</b>     | Sets the history parameters for the zone attack reports.                                                                                                                                                                                                                                                                                                                                                         |
| <i>days</i>        | Length of history time. The logs history time range is 1 to 7 days. The report history time range is 1 to 60 days.<br>The default history time is 7 days for the logs and 30 days for the reports.                                                                                                                                                                                                               |
| <b>enforce-now</b> | (Optional) Adopts and if necessary, erases the recorded log and report history recording capacity to the current command parameters.                                                                                                                                                                                                                                                                             |
|                    |  <p><b>Note</b> If you configure the history reporting to a shorter period, use the <b>enforce-now</b> keyword to reduce the log file and report file sizes to the newly configured size. You can also use the <b>disk-clean</b> command to erase the stored logs and reports to match the newly configured history size.</p> |

## 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                     | <p>Percentage of the allocated disk space that the Guard is using.</p> <p>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.</p> <p><b>Note</b> 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.</p> <p>If the disk space usage reaches 80 percent, follow the guidelines described in the “<a href="#">Managing Disk Space</a>” section on page 12-22.</p>                                                    |
| Accelerator card memory usage        | <p>Percentage of memory that the accelerator card is using.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| Accelerator card CPU utilization     | <p>Percentage of the accelerator card CPU utilization.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| Anomaly detection engine used memory | <p>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.</p> <p>If the anomaly detection engine memory usage is higher than 95 percent, we strongly recommend that you lower the number of active zones.</p>                                                                                                                                                                                                               |
| Dynamic filters used                 | <p>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.</p> <p>A high value may indicate that the Guard is monitoring a high traffic volume of a DDoS attack.</p> |

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 <b>pub</b> 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 <b>temp</b> 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 ifa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table 12-21 Arguments and Keywords for the arp Command (continued)

| Abbreviated Parameter Name | Parameter Full Name    | Description                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-e</b>                  |                        | Displays the entries in default style.                                                                                                                                                                                                                                                                                                                         |
| <b>-f filename</b>         | <b>--file filename</b> | Creates an ARP address mapping entry. The information is taken from the <i>filename</i> 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: <ul style="list-style-type: none"> <li>[--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]]</li> <li>[--unix -x] [--inet --ip] [--ax25] [--ipx] [--netrom]</li> <li>[--ddp]</li> </ul> |
| <b>-r</b>                  | <b>--route</b>           | Displays the Guard routing tables.                                                                                                                                                                                                                      |
| <b>-g</b>                  | <b>--groups</b>          | Displays multicast group membership information for IPv4 and IPv6.                                                                                                                                                                                      |
| <b>-i iface</b>            | <b>--interface iface</b> | Displays a table of all network interfaces or of the optional <i>iface</i> value.                                                                                                                                                                       |
| <b>-M</b>                  | <b>--masquerade</b>      | Displays a list of masqueraded connections for which Network Address Translation (NAT) was used.                                                                                                                                                        |
| <b>-s</b>                  | <b>--statistics</b>      | Displays summary statistics for each protocol.                                                                                                                                                                                                          |
| <b>-v</b>                  | <b>--verbose</b>         | (Optional) Displays the output in verbose.                                                                                                                                                                                                              |
| <b>-n</b>                  | <b>--numeric</b>         | (Optional) Displays numerical addresses.                                                                                                                                                                                                                |
|                            | <b>--numeric-hosts</b>   | (Optional) Displays numerical host addresses but does not affect the resolution of port or usernames.                                                                                                                                                   |
|                            | <b>--numeric-ports</b>   | (Optional) Displays numerical port numbers but does not affect the resolution of host or usernames.                                                                                                                                                     |
|                            | <b>--numeric-users</b>   | (Optional) Displays numerical user IDs but does not affect the resolution of host or port names.                                                                                                                                                        |
| <b>-c</b>                  | <b>--continuous</b>      | (Optional) Displays the selected information every second on a continuous basis.                                                                                                                                                                        |
| <b>-e</b>                  | <b>--extend</b>          | (Optional) Displays additional information. Use this option twice for maximum detail.                                                                                                                                                                   |
| <b>-o</b>                  | <b>--timers</b>          | (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                                                                       |
|----------------------------|---------------------|-----------------------------------------------------------------------------------|
| <b>-p</b>                  | <b>--program</b>    | (Optional) Displays the PID and name of the program to which each socket belongs. |
| <b>-l</b>                  | <b>--listening</b>  | (Optional) Displays only listening sockets. These sockets are omitted by default. |
| <b>-a</b>                  | <b>--all</b>        | (Optional) Displays both listening and nonlistening sockets.                      |
| <b>delay</b>               |                     | (Optional) Netstat cycles printing through statistics every <i>delay</i> 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 **tracert** command.

**Table 12-23 Arguments and Keywords for the tracert Command**

| Parameter                  | Description                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>          | IP address to which the route will be traced.                                                                                                                      |
| <b>-F</b>                  | (Optional) Sets the <i>don't fragment</i> bit.                                                                                                                     |
| <b>-f</b> <i>first_ttl</i> | (Optional) Sets the initial time-to-live (TTL) used in the first outgoing probe packet.                                                                            |
| <b>-g</b> <i>gateway</i>   | (Optional) Specifies a loose source route gateway. You can specify more than one gateway by using <b>-g</b> for each gateway. The maximum number of gateways is 8. |
| <b>-i</b> <i>iface</i>     | (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.            |
| <b>-m</b> <i>max_ttl</i>   | (Optional) Sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops.                                          |
| <b>-p</b> <i>port</i>      | (Optional) Sets the base UDP port number used in probes. The default is 33434.                                                                                     |
| <b>-q</b> <i>nqueries</i>  | (Optional) Sets the number of probes that are defined for the ttl value. The default is 3.                                                                         |
| <b>-s</b> <i>src_addr</i>  | (Optional) Sets the <i>src_addr</i> IP address as the source IP address in outgoing probe packets.                                                                 |
| <b>-t</b> <i>tos</i>       | (Optional) Sets the type-of-service in probe packets to the <i>tos</i> value. The default is zero.                                                                 |
| <b>-w</b> <i>waittime</i>  | (Optional) Sets the time in seconds to wait for a response for a probe. The default is 5 seconds.                                                                  |
| <i>packetlen</i>           | (Optional) Packet length of the probe.                                                                                                                             |

The following example shows how to trace the route to IP address 10.10.10.34:

```
user@GUARD# tracert 10.10.10.34
tracert 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] [-I 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                                                                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-address</i>                 | Destination IP address.                                                                                                                                                              |
| <b>-c</b> <i>count</i>            | (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. |
| <b>-i</b> <i>interval</i>         | (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.                                        |
| <b>-l</b> <i>preload</i>          | (Optional) Sends preload packets without waiting for a reply.                                                                                                                        |
| <b>-s</b> <i>packetsize</i>       | (Optional) Specifies the number of data bytes to send. The default is 56.                                                                                                            |
| <b>-t</b> <i>tll</i>              | (Optional) Sets the IP TTL.                                                                                                                                                          |
| <b>-w</b> <i>deadline</i>         | (Optional) Specifies the timeout in seconds before ping exits, regardless of how many packets have been sent or received.                                                            |
| <b>-F</b> <i>flow label</i>       | (Optional) Allocates and sets a 20-bit flow label on echo request packets. If the value is zero, a random flow label is used.                                                        |
| <b>-I</b> <i>interface</i>        | (Optional) Sets the source IP address to the specified interface address.                                                                                                            |
| <b>-Q</b> <i>tos</i>              | (Optional) Sets Type of Service (ToS)-related bits in ICMP datagrams.                                                                                                                |
| <b>-T</b> <i>timestamp option</i> | (Optional) Sets special IP time-stamp options.                                                                                                                                       |
| <b>-W</b> <i>timeout</i>          | (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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>time</i>           | Time of the event that triggers the need for debug information. The time string uses the format <i>MMDDhhmm</i> [[ <i>CC</i> ] <i>YY</i> ][ <i>.ss</i> ] as follows: <ul style="list-style-type: none"> <li><i>MM</i>—The month in numeric figures</li> <li><i>DD</i>—The day of the month</li> <li><i>hh</i>—The hour in a 24-hour clock</li> <li><i>mm</i>—The minutes</li> <li><i>CC</i>—(Optional) The first two digits of the year (for example, <b>2005</b>)</li> <li><i>YY</i>—(Optional) The last two digits of the year (for example, <b>2005</b>)</li> <li><i>.ss</i>—(Optional) The seconds (the decimal point must be present)</li> </ul> |
| <b>ftp</b>            | Specifies FTP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>scp</b>            | Specifies SCP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>sftp</b>           | Specifies SFTP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <i>server</i>         | IP address of the network server. Enter the IP address in dotted-decimal notation (for example, enter 192.168.10.2).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <i>full-file-name</i> | Full name of the version file. If you do not specify a path, the server saves the file in your home directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <i>login</i>          | (Optional) Server login name. The server assumes an anonymous login when you do not enter a login name. The server does not prompt you for a password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>password</i>       | (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.