



CHAPTER 11

Using Attack Reports

This chapter describes the attack reports that the Cisco Guard (Guard) produces and contains the following sections:

- [Understanding the Report Layout](#)
- [Understanding the Report Parameters](#)
- [Displaying Attack Reports](#)
- [Exporting Attack Reports](#)
- [Deleting Attack Reports](#)

Understanding the Report Layout

The Guard provides an attack report for each zone to help you form a comprehensive view of the attack. An attack begins when the Guard produces the first dynamic filter and ends when no dynamic filter is in use and no new dynamic filters are added. Reports include details of the attacks that are organized into sections that describe different characteristics of the traffic flow during an attack. You can display reports of previous attacks and ongoing attacks, and you can export reports to a network server using File Transfer Protocol (FTP), Secure FTP (SFTP), or Secure Copy Protocol (SCP).

This section contains the following topics:

- [General Details](#)
- [Attack Statistics](#)
- [Malicious Packet Statistics](#)
- [Detected Anomalies](#)
- [Mitigated Attacks](#)
- [Zombies](#)

General Details

The general details section of the attack report includes general information about an attack.

Table 11-1 describes the fields in this section of the report.

Table 11-1 *Field Descriptions in General Details Section of Attack Report*

Field	Description
Report ID	Identification number of the report. A value of current indicates that there is an ongoing attack.
Attack Start	Date and time that the attack started.
Attack End	Date and time that the attack ended. A value of Attack in progress indicates that there is an ongoing attack.
Attack Duration	Duration of the attack.

Attack Statistics

The attack statistics' section provides a general analysis of the zone traffic flow for various packets. Table 11-2 describes the packet types.

Table 11-2 *Packet Types*

Type	Description
Received	Total amount of the diverted traffic.
Forwarded	Legitimate traffic that the Guard forwarded on to the zone.
Replied	Traffic that the Guard anti-spoofing and anti-zombie mechanisms sent back to the source in a verification attempt.
Dropped	Traffic that the Guard dropped.

Malicious Packet Statistics

The malicious packets statistics' section of the attack report analyzes the packets that the Guard dropped and sent back to the source in a verification attempt (replied). The report classifies the packets by their type (spoofed or malformed) and by the Guard function that handled them (filter types or the rate limiter).

Table 11-3 describes the different types of malicious packets.

Table 11-3 *Types of Malicious Packets*

Type	Description
Rate Limiter	Packets that were dropped because they exceeded the rate of traffic defined by the rate limit parameter of the user filters and the zone rate-limit command as allowed to be injected to the zone.
Flex-Content Filters	Packets that were dropped by the flex-content filters.
User Filters	Packets that were dropped by the user filters.
Dynamic Filters	Packets that were dropped by the dynamic filters.

Table 11-3 *Types of Malicious Packets (continued)*

Type	Description
Spoofed	Packets that were identified by the Guard as spoofed packets or packets originated by zombies and not injected to the zone. Spoofed packets are replied (bounced) packets to which no replies were received.
Malformed	Packets that were analyzed as malformed because of their malformed structure or due to the Guard anti-spoofing functions.

Detected Anomalies

The detected anomalies' section of the attack report provides details of the traffic anomalies that the Guard detected in the zone traffic. A flow is classified as being an anomaly when it requires the production of a dynamic filter. These anomalies can occur infrequently or can turn into systematic Distributed Denial of Service (DDoS) attacks. The Guard clusters anomalies with the same type and flow parameters (such as source IP address and destination port) under one anomaly type.

Table 11-4 describes the different types of detected anomalies.

Table 11-4 *Types of Detected Anomalies*

Type	Description
dns (tcp)	Attacking DNS-TCP protocol flow.
dns (udp)	Attacking DNS-UDP protocol flow.
fragments	Detected flow with an unusual amount of fragmented traffic.
http	Unusual HTTP traffic flow.
ip_scan	Detected flow initiated from a source IP address that tried to access many zone destination IP addresses.
other_protocols	Non-TCP and non-UDP attacking protocol flow.
port_scan	Detected flow initiated from a source IP address that tried to access many zone ports.
tcp_connections	Detected flow with an unusual number of TCP concurrent connections, with or without data.
tcp_incoming	Detected flow that attacks a TCP service when the zone is a server.
tcp_outgoing	Detected flow that consists of a SYN-ACK flood or other packet attacks on connections initiated by the zone when the zone is the client.
tcp_ratio	Detected flow with an unusual ratio between different types of TCP packets, such as a high ratio of SYN packets to FIN/RST packets.
udp	Attacking UDP protocol flow.
unauthenticated_tcp	Detected flow that the Guard anti-spoofing functions have not succeeded in authenticating, such as an ACK flood, FIN flood, or any other flood of unauthenticated packets.
user	Anomaly flow that was detected by user definitions.
sip_udp	Detected VoIP ¹ anomaly flow that uses SIP ² over UDP to establish the VoIP sessions.

1. VoIP = Voice over IP

2. SIP = Session Initiation Protocol

Mitigated Attacks

The mitigated attacks' section of the attack report details the steps that the Guard took to mitigate the attacks. The report provides details of the timing of the mitigation and the type of mitigated attack. The Guard defines the mitigation type according to the functions that the Guard used to mitigate the attack. These functions indicate the attack type and subtype.

For example, if the Guard uses a basic anti-spoofing function to mitigate an attacking flow of syn packets, the mitigated attack appears as spoofed/tcp_syn_basic where spoofed indicates the attack type and tcp_syn_basic indicates the attack subtype.

This section describes the five types of mitigated attacks in the following topics:

- [Spoofed Attacks](#)
- [Zombie Attacks](#)
- [Client Attacks](#)
- [User-Defined Attacks](#)
- [Malformed Packets](#)

Spoofed Attacks

Spoofed attacks include all traffic anomalies identified as a DDoS attack that come from a spoofed source. [Table 11-5](#) describes the different types of spoofed attacks.

Table 11-5 *Types of Spoofed Attacks*

Attack Type	Description
spoofed/tcp_syn (basic)	Flood of SYN packets that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_syn (strong)	Flood of SYN packets that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_syn_ack (basic)	Flood of syn_ack packets that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_syn_ack (strong)	Flood of syn_ack packets that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_incoming (basic)	Flood of traffic that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_incoming (strong)	Flood of traffic that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_outgoing (strong)	Flood of traffic from zone-initiated connections that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/udp (basic)	Flood of UDP traffic that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/udp (strong)	Flood of UDP traffic that the strong anti-spoofing functions have not succeeded in authenticating.

Table 11-5 *Types of Spoofed Attacks (continued)*

Attack Type	Description
spoofed/other_protocols	Flood of other than TCP and UDP traffic that the Guard anti-spoofing functions have not succeeded in authenticating.
spoofed/tcp_fragments	Flood of TCP fragmented packets that the Guard anti-spoofing functions have not succeeded in authenticating.
spoofed/udp_fragments	Flood of UDP fragmented packets that the Guard anti-spoofing mechanisms have not succeeded in authenticating.
spoofed/other_protocols_fragments	Flood of other than TCP and UDP fragmented packets that the Guard anti-spoofing mechanisms have not succeeded in authenticating.
spoofed/dns_queries (strong)	Flood of DNS query packets that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/dns_replies (basic)	Flood of DNS packets from zone-initiated connections that the basic anti-spoofing functions have not succeeded in authenticating.
spoofed/dns_replies (strong)	Flood of DNS packets from zone-initiated connections that the strong anti-spoofing functions have not succeeded in authenticating.
spoofed/sip	Flood of SIP over UDP packets that the basic anti-spoofing functions have not succeeded in authenticating.

Zombie Attacks

Zombie attacks include traffic anomalies identified as a DDoS attack originated by zombies. [Table 11-6](#) describes the different types of zombie attacks.

Table 11-6 *Types of Zombie Attacks*

Attack Type	Description
zombie/http	Flood of HTTP traffic from many sources that were identified as nonspoofed, but the Guard anti-zombie functions have not succeeded in authenticating.

Client Attacks

Client attacks include all nonspoofed traffic anomalies. [Table 11-7](#) describes the different types of client attacks.

Table 11-7 *Types of Client Attacks*

Attack Type	Description
client_attack/tcp_connections	Flow with an unusual number of TCP concurrent connections with or without data.
client_attack/http	Flood of HTTP traffic flow.
client_attack/tcp_incoming	Flood that attacks a TCP service when the zone is a server.
client_attack/tcp_outgoing	Flood from an attacking authenticated IP connection that the zone initiated.

Table 11-7 *Types of Client Attacks (continued)*

Attack Type	Description
client_attack/unauthenticated_tcp	Flood of ACKs, FINs, any other packets without a TCP handshake, or TCP connections that the Guard anti-spoofing functions have not succeeded in authenticating.
client_attack/dns (udp)	Flood from an attacking DNS-UDP protocol flow.
client_attack/dns (tcp)	Flood from an attacking DNS-TCP protocol flow.
client_attack/udp	Flood from an attacking UDP protocol flow.
client_attack/other_protocols	Flood from a non-TCP/UDP attacking protocol flow.
client_attack/fragments	Flood of fragmented traffic.
client_attack/user	Flood that a user-defined dynamic filter identified.

User-Defined Attacks

User-defined attacks include all anomalies handled by the user filters. The user filters can either function by default or you can configure them manually. See [Chapter 7, “Configuring Policy Templates and Policies”](#) for more information. [Table 11-8](#) describes the different types of user-defined attacks.

Table 11-8 *Types of User-Defined Attacks*

Attack Type	Description
user_defined/user_filter_rate_limit	Flood that was dropped because it exceeded the rate limit defined for a user filter.
user_defined/user_drop_filters	Flood that was dropped by user filters.
user_defined/rate_limit	Flood that was dropped due to one of the following: <ul style="list-style-type: none"> The flood exceeded the rate limit defined for a user filter. The flood exceeded the rate limit defined by the zone rate-limit command. The flood exceeded the internal rate limit defined for unauthenticated TCP RST packets or unauthenticated DNS zone transfer packets.
user_defined/flex_content_filter	Flood that was dropped by the flex-content filters.

Malformed Packets

Malformed packets include all traffic anomalies identified as consisting of maliciously malformed packets. [Table 11-9](#) describes the different types of malformed packets.

Table 11-9 *Types of Malformed Packets*

Attack Type	Description
malformed_packets /packets_to_proxy_ip	Flood that attacks a Guard proxy IP address.
malformed_packets /dns_anti_spoofing_algo	Flood of malformed packets due to the operation of the Guard DNS anti-spoofing functions.
malformed_packets /dns (queries)	Flood of malformed DNS packets.
malformed_packets /dns (short_queries)	Flood of short DNS queries.
malformed_packets /dns (replies)	Flood of malformed DNS replies.
malformed_packets /src_ip_equals_dst_ip	Flood of packets with the zone IP address as their source and destination.
malformed_packets /zero_header_field	Flood of packets in which the destination port, source port, protocol, or source IP address field in the header illegally equals zero.
malformed_packets /sip_bad_header	Flood of SIP over UDP packets with a malformed header.

Zombies

Zombie attacks include traffic anomalies identified as a DDoS attack originated by zombies. The Guard attack report displays a table listing zombies that are currently attacking the zone. Use the **show reports details** and **show zombies** commands to display the list of currently attacking zombies.



Note

This report section is available only when you enter the **show reports details** and **show zombies** commands

See [Table 11-15 on page 11-11](#) for information about the fields in the **show zombies** command output.

Understanding the Report Parameters

This section describes the aspects of the traffic flow that relate to each section of the report.

[Table 11-10](#) describes the fields for [Attack Statistics](#) and [Malicious Packet Statistics](#).

Table 11-10 *Field Descriptions for Attack Statistics*

Field	Description
Total Packets	Total number of attack packets.
Average pps	Average traffic rate in packets per second.
Average bps	Average traffic rate in bits per second.
Max. pps	Maximum traffic rate measured in packets per second.

Table 11-10 *Field Descriptions for Attack Statistics (continued)*

Field	Description
Max. bps	Maximum traffic rate measured in bits per second.
Percentage	Number of forwarded, replied, and dropped packets as a percentage of the total received packets.

Table 11-11 describes the flow statistics for [Detected Anomalies](#) and [Mitigated Attacks](#).

Table 11-11 *Field Descriptions for Flow Statistics*

Field	Description
ID	Identifier of the detected anomaly.
Start time	Date and time that the anomaly was detected.
Duration	Duration of the anomaly in hours, minutes, and seconds.
Type	Type of anomaly or mitigated attack.
Triggering rate	Anomaly traffic rate that exceeded the policy threshold.
% Threshold	Percentage by which the triggering rate is above the policy threshold.
Flow	Anomaly flow and mitigated attack flow. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. It indicates whether or not the traffic is fragmented. A value of any indicates that there is both fragmented and nonfragmented traffic.

An asterisk (*), which is used as a wildcard, for one of the parameters indicates one of the following:

- The value is undetermined.
- More than one value was measured for the anomaly parameter.

A number sign (#) followed by a number for any of the parameters indicates the number of values measured for that parameter.

The Guard may display a value of **notify** on the right side of the flow description. A value of **notify** indicates that the Guard produces a notification for the type of traffic that the row describes. The Guard does not take an action if the value is **notify**.

Displaying Attack Reports

You can display a list of attack reports for any specific zone or a more detailed report for a specific attack by using the following command in zone configuration mode:

```
show reports [sub-zone-name] [current | report-id] [details]
```

Table 11-12 provides the arguments and keywords for the **show reports** command.

Table 11-12 Arguments and Keywords for the show reports Command

Parameter	Description
<i>sub-zone-name</i>	(Optional) Name of a subzone that was created from the zone. See the “Understanding Subzones” section on page 9-7 for more information.
current	(Optional) Displays the report of the attack that is in progress. The number of bits and packets is not displayed for an ongoing attack. In reports of an attack in progress, the packets and bits fields have a value of zero (0).
<i>report-id</i>	(Optional) Identification number of the report.
details	(Optional) Displays the details of the flows and attacking zombies.

The following example shows how to view a list of all attacks on the zone:

```
user@GUARD-conf-zone-scannet# show reports
```

Table 11-13 describes the fields in the **show reports** command output.

Table 11-13 Field Descriptions for the show reports Command Output

Field	Description
Report ID	Report identification number. A value of current indicates that there is an ongoing attack.
Attack Start	Date and time that the attack started.
Attack End	Date and time that the attack ended. A value of Attack in progress indicates that there is an ongoing attack.
Attack Duration	Duration of the attack.
Attack Type	Type of mitigated attack. Possible values are as follows: <ul style="list-style-type: none"> • client_attack—All nonspoofed traffic anomalies. • malformed_packets—All traffic anomalies identified as consisting of maliciously malformed packets. • spoofed—Traffic anomalies identified as a DDoS attack coming from a spoofed source. • user_defined—All anomalies handled by the user filters. The user filters can either function by default or be user configured. • zombie—Traffic anomalies identified as having been originated by zombies. • hybrid—An attack made up of several attacks with different characteristics. • traffic_anomaly—An anomaly that was only detected for a short period of time and did not require mitigation.
Peak Malicious Traffic	Sum of the number of the following types of packets: <ul style="list-style-type: none"> • Packets that the Guard identified as part of an attack and dropped. • Packets to which the Guard sent replies to the initiating client in order to verify whether they are part of authentic traffic or part of an attack.

The following example shows how to display the report of the current attack on the zone:

```
user@GUARD-conf-zone-scannet# show reports current
```

The attack report displays the following output. For more information about the different sections, see the [“Understanding the Report Layout”](#) section on page 11-1.

```
Report ID       : current
Attack Start    : Feb 26 2004 09:58:54
Attack End      : Attack in progress
Attack Duration : 00:08:34
```

Attack Statistics:

	Total Packets	Average pps	Average bps	Max pps	Max bps	Percentage
Received	95878	186.53	110977.74	1455.44	914428.24	N/A
Forwarded	53827	104.72	64278.54	1430.85	899196.24	56.14
Replied	1870	3.64	2172.89	23.03	14433.88	1.95
Dropped	40181	78.17	44526.32	96.82	55010.13	41.91

Malicious Packets Statistics:

	Total Packets	Average pps	Average bps	Max pps	Max bps	Percentage
Rate Limiter	0	0	0	0	0	0
Flex-Content Filter	0	0	0	0	0	0
User Filters	0	0	0	0	0	0
Dynamic Filters 40128	78.07	44473.53	96.82	55010.13	99.84	
Spoofed	12	0.02	11.95	0.15	75.29	0.03
Malformed	53	0.1	52.79	1.56	798.12	0.13

Detected Anomalies:

ID	Start Time	Duration	Type	Triggering Rate	%Threshold
1	Feb 26 09:58:54	00:08:34	HTTP	997.44	897.44
	Flow: 6 *	*	92.168.100.34	80	no fragments

Mitigated Attacks:

ID	Start Time	Duration	Type	Triggering Rate	%Threshold
1	Feb 26 09:59:40	00:07:59	client_attack/ tcp_connections	38	280
	Flow: 6 (#52)	*	92.168.200.254	80	no fragments

To display a more detailed report on flows of the detected anomalies and the mitigated attacks, and to display a list of zombies attacks, use the **details** option.

Table 11-14 describes the flow fields in the detailed report.

Table 11-14 *Field Descriptions of Flows in Detailed Report*

Field	Description
Detected Flow	Flow that caused the production of the dynamic filter. The detected flow may indicate a specific source port for a specific source IP address. The flow characteristics include the protocol number, source IP address, source port, destination IP address, destination port, and an indication of whether the traffic is fragmented or not. A value of any indicates that there is both fragmented and nonfragmented traffic.
Action Flow	Flow that was addressed by the dynamic filter. The action flow may indicate all source ports for the specified source IP address. The action flow may have a wider range than the detected flow. The flow characteristics include the protocol number, source IP address, source port, destination IP address, destination port, and an indication of whether the traffic is fragmented or not. A value of any indicates that there is both fragmented and nonfragmented traffic.

Table 11-15 describes the fields in the detailed report about zombie attacks.

Table 11-15 *Field Descriptions for Zombie Attacks Table*

Field	Description
IP	Zombie IP address.
Start Time	Date and time that the zombie connection was initially identified.
Duration	Duration of the zombie attack.
#Requests	Number of HTTP get requests sent by the zombie.



Note

If there are no zombie attacks, the “Report doesn’t exist” message appears under the Zombies heading in the report.

Exporting Attack Reports

You can export attack reports to a network server for monitoring and diagnostic capabilities. You can export attack reports in text format or in Extensible Markup Language (XML) format.

This section contains the following topics:

- [Exporting Attack Reports Automatically](#)
- [Exporting Attack Reports of All Zones](#)
- [Exporting Zone Reports](#)

Exporting Attack Reports Automatically

You can configure the Guard to export attack reports in XML format. The Guard exports the reports of any one of the zones when an attack on the zone ends. The XML schema is described in the `ExportedReports.xsd` file which you can download from the Software Center at <http://www.cisco.com/public/sw-center/>.

To configure the Guard to export attack reports automatically, use the following command in configuration mode:

```
export reports file-server-name
```

The *file-server-name* argument specifies the name of a network server to which you export the files that you configure by using the **file-server** command. If you configure the network server for Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP), you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the “Exporting Files Automatically” section on page 13-5 for more information.

The following example shows how to automatically export reports (in XML format) at the end of an attack to a network server:

```
user@GUARD-conf# export reports Corp-FTP-Server
```

Exporting Attack Reports of All Zones

You can export the attack reports of all zones in text or XML format by entering one of the following commands in global mode:

- **copy reports** [details] [xml] **ftp** *server full-file-name* [login] [password]
- **copy reports** [details] [xml] {**sftp** | **scp**} *server full-file-name login*
- **copy reports** [details] [xml] *file-server-name dest-file-name*

Because SFTP and SCP rely on SSH for secure communication, if you do not configure the key that the Guard uses before you enter the **copy** command with the **sftp** or **scp** option, the Guard prompts you for the password.

See the “Configuring the Keys for SFTP and SCP Connections” section on page 3-25 for more information about how to configure the key that the Guard uses for secure communication.

Table 11-16 provides the arguments and keywords for the **copy reports** command.

Table 11-16 Arguments and Keywords for the copy reports Command

Parameter	Description
details	(Optional) Exports details of flow and attacking source IP addresses.
xml	(Optional) Exports the report in XML format. See the <code>xsd</code> file released with the version for a description of the XML schema (you can download the <code>xsd</code> files that accompany the version from www.cisco.com). By default, reports are exported in text format.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.

Table 11-16 Arguments and Keywords for the copy reports Command (continued)

Parameter	Description
<i>server</i>	IP address of the network server.
<i>full-file-name</i>	Full 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.
<i>file-server-name</i>	Name of a network server that you defined by using the file-server command. If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the “Exporting Files Automatically” section on page 13-5 for more information.
<i>dest-file-name</i>	Name of the file. The Guard appends the name of the file to the path that you defined for the network server by using the file-server command.

The following example shows how to copy a list of all attacks handled by the Guard (in text format) to an FTP server at IP address 10.0.0.191 by using login name user1 and password password1:

```
user@GUARD# copy reports ftp 10.0.0.191 agmreports.txt user1 password1
```

The following example shows how to copy a list of all attacks handled by the Guard (in text format) to a network server that was defined by using the **file-server** command:

```
user@GUARD# copy reports Corp-FTP-Server AttackReports.txt
```

Exporting Zone Reports

You can copy the attack reports of a specific zone to a network server by using one of the following commands in global mode:

- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **ftp** *server* *full-file-name* [*login*] [*password*]
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] {**sftp** | **scp**} *server* *full-file-name* *login*
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] *file-server-name* *dest-file-name*

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

Table 11-17 describes the arguments and keywords for the **copy zone reports** command.

Table 11-17 Arguments and Keywords for the copy zone reports Command

Parameter	Description
zone <i>zone-name</i>	Specifies the name of an existing zone.
current	(Optional) Exports an ongoing attack report (if applicable). The default is to export all zone reports.
<i>report-id</i>	(Optional) ID of an existing report. The Guard exports the report with the specified ID number. To view the details of the zone attack reports, use the show zone reports command. The default is to export all zone reports.
xml	(Optional) Exports the report in XML format. See the xsd file that was released with the version for a description of the XML schema (you can download the xsd files that accompany the version from www.cisco.com). The default is to export reports in text format.
details	(Optional) Exports details about the flow and attacking source IP addresses.
ftp	Specifies FTP.
sftp	Specifies SFTP.
scp	Specifies SCP.
<i>server</i>	IP address of the server.
<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 remote FTP server.
<i>file-server-name</i>	Name of a network server. You must configure the network server using the file-server command. If you configured the network server using SFTP or SCP, you must configure the SSH key that the Guard uses for SFTP and SCP communication. See the “Exporting Files Automatically” section on page 13-5 for more information.
<i>dest-file-name</i>	Name of the file. The Guard appends the name of the file to the path that you defined for the network server by using the file-server command.

The following example shows how to copy all attack reports of the zone to an FTP server at IP address 10.0.0.191 by using login name user1 and password password1:

```
user@GUARD# copy zone scannet reports ftp 10.0.0.191 ScannetCurrentReport.txt user1
password1
```

The following example shows how to copy the current attack report (in XML format) to a network server that was defined by using the **file-server** command:

```
user@GUARD# copy zone scannet reports current xml Corp-FTP-Server AttackReport-5-10-05.txt
```

Deleting Attack Reports

You can delete old attack reports to free disk space.

To delete attack reports, use the following command in zone configuration mode:

```
no reports report-id
```

The *report-id* argument specifies the ID of an existing report. Enter an asterisk (*) to delete all attack reports. To view the details of the zone attack reports, use the **show zone reports** command.

**Note**

You cannot delete the attack report of an ongoing attack.

The following example shows how to delete all the zone attack reports:

```
user@GUARD-conf-zone-scanner# no reports *
```

