CHAPTER 11

Using Attack Reports

This chapter describes the attack reports that the Cisco Traffic Anomaly Detector Module (Detector module) produces and contains the following sections:

Understanding the Report Layout

The Detector module provides an attack report for each zone to help you form a comprehensive view of the attack. An attack begins when the Detector module 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

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 received traffic flow.

Detected Anomalies

The detected anomalies' section of the attack report provides details of the traffic anomalies that the Detector module 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 Detector module clusters anomalies with the same type and flow parameters (such as a source IP address and destination port) under one anomaly type.

Table 11-2 describes the different types of detected anomalies.

Table 11-2 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 attacking a TCP service.
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.

Table 11-2 Types of Detected Anomalies (continued)

Type	Description
udp	Attacking UDP protocol flow.
unauthenticated_tcp	Detected flow that the Detector 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.
worm_tcp	Worm attack over the TCP/IP protocol.

Understanding the Report Parameters

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

Table 11-3 describes the fields for Attack Statistics.

Table 11-3 Field Descriptions for Attack Statistics

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

Table 11-4 describes the flow statistics for Detected Anomalies.

Table 11-4 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.
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. The characteristics include the protocol number, source IP address, source port, destination IP address, and destination port. This field 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 Detector module may display a value of notify on the right side of the flow description. A value of notify indicates that the Detector module produces a notification for the type of traffic that the row describes. The Detector module 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 [**current** | *report-id*] [**details**]

Table 11-5 provides the arguments and keywords for the **show reports** command.

Table 11-5 Arguments and Keywords for the show reports Command

Parameter	Description
current	(Optional) Displays the report of the attack that is in progress. The number of bits and packets is not displayed for an ongoing attack. In reports of an attack in progress, the packets and bits fields have a value of zero (0).
report-id	(Optional) Identification number of the report.
details	(Optional) Displays the details of the flows.

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

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

Table 11-6 describes the fields in the **show reports** command output.

Table 11-6 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	The duration of the attack.

Table 11-6 Field Descriptions for the show reports Command Output (continued)

Field	Description
Attack Type	Type of detected attack. Possible values are as follows: • **tcp_connections**—Detected flow with an unusual number of TCP concurrent connections, with or without data. • **http**—Unusual HTTP traffic flow. • **tcp_incoming**—Detected flow attacking a TCP service. • **tcp_outgoing**—Detected attack flow in which the client seems to be the zone, such as SYN-ACK attacks on connections initiated by the zone when the zone is the client. • **unauthenticated_tcp**—Detected flow that the Detector module anti-spoofing functions have not succeeded in authenticating. For example, an ACK flood, a FIN flood, or any other flood of unauthenticated packets. • **dns (udp)**—Attacking DNS-UDP protocol flow. • **dns (tcp)**—Attacking DNS-TCP protocol flow. • **udp**—Attacking UDP protocol flow. • **other_protocols**—Non-TCP and non-UDP attacking protocol flow. • **fragments**—Detected flow with an unusual quantity of fragmented traffic. • **hybrid**—Attack composed of several attacks with different characteristics. • **ip_scan**—Detected flow initiated from a source IP address that tried to access many zone destination IP addresses. • **port_scan**—Detected flow initiated from a source IP address that tried to access many zone ports.
Attack Type (continued)	• **user_detected**—Anomaly flow detected by user definitions. • **worm_tcp**—Worm attack over the TCP/IP protocol.
Peak Malicious Traffic	This field is relevant to the Guard only and is not applicable to the Detector module.

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

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

The attack report displays the following output. For more information about the different sections, see the "Understanding the Report Layout" section on page 11-1.

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


Attack Statistics:
```

```
                Total       Average    Average      Max pps    Max bps
                Packets     pps        bps
Received        95878       186.53     110977.74    1455.44    914428.24    N/A

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

To display a more detailed report on the flow of detected anomalies, use the **details** option.

Table 11-7 describes the flow fields in the detailed report.

Table 11-7 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.

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 Detector module to export attack reports in XML format. The Detector module 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 Detector module 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 FTP (SFTP) or Secure Copy (SCP), you must configure the SSH key that the Detector module uses for SFTP and SCP communication. See the "Exporting Files Automatically to a Network Server" section on page 13-6 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@DETECTOR-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**] *file-server-name dest-file-name*

Table 11-8 provides the arguments and keywords for the **copy reports** command.

Table 11-8 Arguments and Keywords for the copy reports Command

Parameter	Description
details	(Optional) Exports details of flow and attacking source IP addresses.
xml	(Optional) Exports the report in XML format. See the xsd file released with the version for a description of the XML schema (you can download the xsd files that accompany the version from www.cisco.com). By default, reports are exported in text format.
ftp	Exports the attack reports to a network server using FTP.
server	IP address of the network server.
full-file-name	Full name of the file. If you do not specify a path, the server saves the file in your home directory.
login	(Optional) Server login name. The *login* argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
password	(Optional) Password for the remote FTP server.
file-server-name	Name of a network server that you defined by using the **file-server** command. The network server must be an FTP server. You cannot export attack reports to a network server using SFTP or SCP. See the "Exporting Files Automatically to a Network Server" section on page 13-6 for more information.
dest-file-name	Name of the file. The Detector module 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 Detector module (in text format) to an FTP server at IP address 10.0.0.191 by using login name user1 and password password1:

```
user@DETECTOR# copy reports ftp 10.0.0.191 admreports.txt user1 password1
```

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

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

Exporting Zone Reports

You can copy the attack reports of a specific zone to an FTP 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**] *file-server-name dest-file-name*

Table 11-9 describes the arguments and keywords for the **copy zone reports** command.

Table 11-9 Arguments and Keywords for the copy zone reports Command

Parameter	Description
zone *zone-name*	Specifies the name of an existing zone.
current	(Optional) Exports an ongoing attack report (if applicable). The default is to export all zone reports.
report-id	(Optional) Identifier of an existing report. The Detector module 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	Exports the attack reports to a network server using FTP.
server	IP address of the server and complete path of the directory where the files are saved.
login	(Optional) Server login name. The *login* argument is optional when you define an FTP server. When you do not enter a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
password	(Optional) Password for the remote FTP server.

Table 11-9 Arguments and Keywords for the copy zone reports Command (continued)

Parameter	Description
file-server-name	Name of a network server. You must configure the network server using the **file-server** command. The network server must be an FTP server. You cannot export reports to a network server using SFTP or SCP. See the "Exporting Files Automatically to a Network Server" section on page 13-6 for more information.
dest-file-name	Name of the file. The Detector module 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@DETECTOR# 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@DETECTOR# 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@DETECTOR-conf-zone-scannet# no reports *
```