Cisco Traffic Anomaly Detector Module
Web-Based Manager Configuration Guide
for the Catalyst 6500 Series Switch and Cisco 7600 Series Router

Software Release 6.1 and 6.1-XG
February 2008
CONTENTS

Preface ix
Audience ix
Organization ix
Symbols and Conventions x
Obtaining Documentation, Obtaining Support, and Security Guidelines xi

CHAPTER 1

Product Overview 1-1
User Interface Requirements 1-2
Minimum Requirements 1-2
Installing Java 2 Runtime Environment 1-2
Detector Module Requirements for WBM Operation 1-2
Understanding the Detector Module 1-3
Understanding DDoS Attacks 1-3
Understanding Spoofed Attacks 1-4
Understanding Nonspoofed Attacks 1-4
Understanding Zones and Zone Policies 1-4
Understanding the WBM Interface 1-5
Understanding the WBM Browser Window 1-5
Understanding Zone Status Icons 1-7
Understanding WBM Navigation Maps 1-7

CHAPTER 2

Launching and Customizing the WBM 2-1
Configuring Network Access for the WBM 2-1
Launching the WBM 2-2
Configuring the Login Banner 2-3
Configuring the WBM Logo 2-3

CHAPTER 3

Managing User Access 3-1
Understanding User Authentication and Authorization Methods 3-2
Using Preconfigured System User Profiles 3-2
Displaying the Users List 3-3
Creating a User Profile 3-3
Deleting a User Profile 3-4
Changing Your Password       3-5
Changing the Password of Another User       3-5
Moving Between User Privilege Levels       3-6
Configuring User Profiles on a TACACS+ Server       3-6
Managing the WBM Portal to Restrict User Access to Specific Zones       3-6
Managing Authorization to Specific WBM Commands       3-7

CHAPTER 4
Creating and Configuring Zones       4-1
Understanding Zones       4-1
Configuring Guard Zones       4-2
Displaying the Configuration of Guard Zones       4-2
Understanding the Protection Characteristics       4-3
Understanding the Protection Activation Methods       4-3
Understanding the Extent of Zone Protection       4-4
Creating a Zone       4-4
Creating a Zone from a Zone Template       4-4
Creating a Zone from an Existing Zone       4-11
Configuring the Zone IP Address Range       4-11
Adding an IP Address to the Zone IP Address Range       4-11
Deleting an IP Address from the Zone IP Address Range       4-12
Updating the Zone Policies       4-12
Viewing and Modifying a Zone Configuration       4-12
Deleting a Zone       4-14

CHAPTER 5
Configuring Zone Filters       5-1
Understanding Zone Filters       5-1
Managing Bypass Filters       5-2
Adding a Bypass Filter       5-2
Deleting a Bypass Filter       5-3
Managing Flex-Content Filters       5-4
Understanding the Flex-Content Expression Syntax       5-4
Understanding the Flex-Content Filter Pattern Syntax       5-7
Adding a Flex-Content Filter       5-7
Deleting a Flex-Content Filter       5-9
Managing User Filters for GUARD Zones       5-9
Adding a User Filter       5-10
Deleting a User Filter       5-12
Contents

Adding an IP Address and Threshold 8-9
Deleting an IP Address and Threshold 8-9
Adding or Deleting a Service 8-10
Adding a Service 8-10
Deleting a Service 8-11
Backing Up the Zone Policies 8-13

CHAPTER 9

Activating Anomaly Detection 9-1
Understanding the Anomaly Detection Activation Options 9-2
Detect, Detect and Learn 9-2
Automatic and Interactive Operation Modes 9-2
Managing Anomaly Detection 9-3
Activating Anomaly Detection 9-3
Verifying Traffic Anomaly Detection 9-3
Deactivating Anomaly Detection 9-3
Managing Dynamic Filters 9-5
Displaying the Dynamic Filters List 9-5
Displaying Dynamic Filter Details 9-6
Adding Dynamic Filters 9-7
Deleting Dynamic Filters 9-8
Preventing the Creation of Unwanted Dynamic Filters 9-8
Activating Automatic or Interactive Detect Mode 9-9
Activating Automatic Detect Mode 9-9
Activating Interactive Detect Mode 9-9
Taking Action When the Number of Pending Dynamic Filters Exceeds 1000 9-10
Managing Detector Module Recommendations for Dynamic Filters 9-11
Viewing Recommendations 9-11
Managing Recommendations 9-12
Viewing the Pending Dynamic Filters of a Recommendation 9-13
Viewing Pending Dynamic Filter Details 9-14
Accepting a Pending Dynamic Filter 9-15

CHAPTER 10

Monitoring Detector Module and Zone Operations 10-1
Viewing the Detector Summary Screen 10-1
Using the Detector Module Global Diagnostic Tools 10-3
Displaying the Global Counters 10-3
Clearing the Detector Module Counters 10-4
Viewing the Global Received Counter in Real Time 10-4
Viewing the Event Log | 10-5
Monitoring Device Resources | 10-6

Viewing the Zone Status Screen | 10-7
  Understanding the Zone Status Bar | 10-9
  Understanding the Zone Traffic Rate Graph | 10-9
  Understanding the Zone Status Table | 10-9
  Understanding the Zone Recent Events Table | 10-10

Using the Zone Diagnostic Tools | 10-10
  Viewing the Zone Counters | 10-10
  Using Zone Counters to Analyze Traffic Flow | 10-11
  Clearing the Zone Counters | 10-11
  Viewing the Zone Counters in Real Time | 10-12
  Viewing the Zone Event Log | 10-12
  Viewing the Attacks Summary Report | 10-13
  Viewing Details of an Attack Report | 10-15
  Understanding Attack Report Details | 10-15
    General Attack Information | 10-16
    Attack Statistics | 10-16
    Detected Anomalies | 10-16
    Viewing Details of Detected Anomalies | 10-18
  Exporting Attack Reports | 10-19
  Deleting Attack Reports | 10-19
  Viewing the Policy Statistics Table | 10-20

**CHAPTER 11**

**Monitoring Network Traffic and Extracting Attack Signatures** | 11-1

Understanding Packet-Dump Capture | 11-1
Enabling Automatic Packet-Dump Capture | 11-2
Disabling Automatic Packet-Dump Capture | 11-3
Activating Manual Packet-Dump Captures | 11-4
  Starting a Manual Packet-Dump Capture | 11-4
  Stopping a Manual Packet-Dump Capture | 11-5
Viewing Packet-Dump Captures | 11-5
  Viewing the Packet-Dump Capture List | 11-6
  Viewing the Packet-Dump Capture Details | 11-7
  Changing the Packet-Dump Capture Details Screen View | 11-9
  Comparing Two Packet-Dump Captures | 11-10
Managing Packet-Dump Capture Files | 11-11
  Renaming a Manual Packet-Dump Capture File | 11-11
  Copying a Packet-Dump Capture File | 11-12
Preface

This guide describes how to use the Web-Based Manager (WBM) graphical user interface to operate the Detector module remotely and to monitor the Detector module activity, status, and statistics.

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

This preface contains the following sections:

- Audience
- Organization
- Symbols and Conventions
- Obtaining Documentation, Obtaining Support, and Security Guidelines

Audience

The *Cisco Traffic Anomaly Detector Module Web-Based Manager Configuration Guide* is intended primarily for the following audiences:

- Network administrators
- Engineers
- Operators
- Network security professionals

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

Organization

This user guide is divided into the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Product Overview”</td>
<td>Provides information on system requirements and an overview of the Detector module and the WBM.</td>
</tr>
<tr>
<td>Chapter 2, “Launching and Customizing the WBM”</td>
<td>Provides an overview of the basic WBM procedures and explains how to set up and connect to the Detector module WBM.</td>
</tr>
</tbody>
</table>
Symbols and Conventions

This guide uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface font</td>
<td>Boldface text indicates commands and keywords that you enter exactly as shown.</td>
</tr>
<tr>
<td>Italic font</td>
<td>Italic font indicates arguments for which you supply the values.</td>
</tr>
<tr>
<td>Screen font</td>
<td>Screen font indicates information that the Detector module displays on the screen.</td>
</tr>
<tr>
<td>Braces ( {</td>
<td>)</td>
</tr>
<tr>
<td>Square brackets ([</td>
<td>])</td>
</tr>
<tr>
<td>admin@DETECTOR#</td>
<td>Default CLI prompt.</td>
</tr>
</tbody>
</table>
This guide uses the following symbols and conventions to identify different types of information:

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

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

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

### Obtaining Documentation, Obtaining Support, and Security Guidelines

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

Product Overview

This chapter provides an overview of the Cisco Traffic Anomaly Detector Module (Detector module) Web-Based Manager (WBM) that you can use to remotely operate and monitor the Detector module. The WBM is a graphical user interface that communicates with the Detector module by translating its HTML pages into Detector module commands. Some features of the Detector module, mostly related to the initial installation and configuration of the Detector module, can only be configured using the CLI and cannot be configured using the WBM. See the Cisco Traffic Anomaly Detector Module Configuration Guide for information about using the CLI.

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- User Interface Requirements
- Detector Module Requirements for WBM Operation
- Understanding the Detector Module
- Understanding DDoS Attacks
- Understanding Zones and Zone Policies
- Understanding the WBM Interface
User Interface Requirements

This section describes the minimum requirements for the WBM client and contains the following topics:

- Minimum Requirements
- Installing Java 2 Runtime Environment

Minimum Requirements

The minimum requirements to access and use the WBM on the Detector module are as follows:

- MS Internet Explorer 5.5 (or higher)—Must support HTML, tables, cookies, Javascript, and frames.
- Sun Microsystems Java 2 Runtime Environment (JRE) Standard Edition (SE) version 5.0 or higher—JRE is required to view the real-time counters (see the “Installing Java 2 Runtime Environment” section).
- Monitor resolution—We recommend that your monitor has a minimum resolution of 1024 x 768 pixels.

Installing Java 2 Runtime Environment

You must install Java 2 JRE to view the real-time counters. To download and install JRE from the Sun Microsystems website, perform the following steps:

Step 1
Open the following URL in your web browser: www.sun.com. The Sun Microsystems home page displays.

Step 2
Navigate to the Downloads > Java SE page and choose Java Runtime Environment (JRE) 5.0 Update 11 or higher.

Step 3
Accept the license agreement and download Java Runtime Environment (JRE) 5.0 Update 11 or higher.

Step 4
Run the file that you just downloaded and follow the online installation instructions that Sun Microsystems provides.

Detector Module Requirements for WBM Operation

Before using the WBM, ensure that the Detector module is properly installed as described in the Cisco Traffic Anomaly Detector Module Configuration Guide. You must perform the initial configuration process using the CLI. Verify that you have configured the following features on the Detector module to ensure proper operation of the WBM:

- Configure the network interfaces—Configures the Detector module network interfaces. You cannot connect to the Detector module until you configure the Detector module interfaces for operation in your networking environment.
- Enable the WBM service and permit access—Enables the WBM service on the Detector module and permits access to the Detector module from the WBM client. The CLI procedures to configure this operation are also included in this guide (see the “Configuring Network Access for the WBM” section).
Understanding the Detector Module

The Detector module monitors a copy of the network traffic, continuously looking for indications of a Distributed Denial of Service (DDoS) attack against a network element, or zone, such as a server, firewall interface, or router interface.

The Detector module can operate as an independent DDoS detection and alarm component; however, it works optimally with the Guard, the companion product of the Detector module.

You can install the Detector module in one of the following products:

- Catalyst 6500 series switch
- Cisco 7600 series router

You must configure the switch to capture the traffic sent to the zone and pass a copy of it to the Detector module.

The Detector module uses a set of zone policies to analyze a copy of all inbound zone traffic. The zone policies enable the Detector module to identify traffic anomalies that indicate an attack on the zone. When the Detector module identifies a traffic anomaly, it can issue a syslog message to notify you of the attack or it can activate a Guard to mitigate the attack.

The Detector module performs the following tasks:

- Traffic learning—Learns the characteristics (services and traffic rates) of normal zone traffic using an algorithm-based process. During the learning process, the Detector module modifies the default zone traffic policies and policy thresholds to match the characteristics of normal zone traffic. The traffic policies and thresholds define the reference points that the Detector module uses to determine when the zone traffic is normal or abnormal (indicating and attack on the zone).
- Traffic anomaly detection—Detects anomalies in zone traffic based on normal traffic characteristics.

Understanding DDoS Attacks

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

This section contains the following topics:

- Understanding Spoofed Attacks
- Understanding Nonspoofed Attacks
Understanding Spoofed Attacks

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

Understanding Nonspoofed Attacks

Nonspoofed attacks (or client attacks) are mostly TCP-based with real TCP connections that can overwhelm the application level on the server rather than the network link or operating system. Client attacks from a large number of clients (or zombies) may overwhelm the server application even without any of the individual clients creating an anomaly. The zombie programs try to imitate legitimate browsers that access the target site.

Understanding Zones and Zone Policies

A zone that the Detector module monitors for traffic anomalies can be one of the following elements:

- A network server, client, or router
- A network link, subnet, or an entire network
- An individual Internet user or a company
- An Internet Service Provider (ISP)
- Any combination of these elements

When you create a new zone, you assign a name to it and configure the zone with network addresses. The Detector module configures the zone with a default set of policies and policy thresholds to detect anomalies in the zone traffic. For more information, see the “Understanding Policy Templates” section in Chapter 6, “Configuring Policy Templates” and the “Understanding Zone Policies” section in Chapter 8, “Managing Zone Policies”.

The Detector module can monitor the traffic of multiple zones simultaneously if the network address ranges do not overlap.
Understanding the WBM Interface

The WBM is a browser-based graphical user interface (GUI) that provides access to Detector module configuration and management functions. Providing a subset of the CLI functionality, the WMB allows you to create and modify zone configurations, manage zone protection, and monitor Detector module and zone operations. Some features of the Detector module, mostly related to the initial installation and configuration of the Detector module, can only be configured using the CLI and cannot be configured using the WBM. See the Cisco Traffic Anomaly Detector Module Configuration Guide for information about using the CLI.

This section contains the following topics:

- Understanding the WBM Browser Window
- Understanding Zone Status Icons
- Understanding WBM Navigation Maps

Understanding the WBM Browser Window

Figure 1-1 and Table 1-1 describe the sections of the WBM window.

Figure 1-1  WBM Screen Sections
### Table 1-1  
**WBM Window Sections**

<table>
<thead>
<tr>
<th>Section</th>
<th>Function</th>
</tr>
</thead>
</table>
| 1       | Main Menu Bar—Displays the main menu for the link that is selected in the navigation pane. The WBM displays one of the following two menu bars in this section:  
  - Detector Summary menu—Provides access to the following Detector module statistical and configuration options:  
    - Detector module status and diagnostic tools  
    - List of defined zones  
    - User profile manager  
  - Zone main menu—Provides access to detailed zone information and configuration options.  
  
  To view the Detector module summary menu, click **Detector Summary** in the navigation pane (3).  
  - Zone main menu—Provides access to detailed zone information and configuration options.  
  
  To view the zone-specific menu, click on a zone that is listed in the navigation area (3). |
| 2       | Navigation Path—Displays the path to the location of the screen that is displayed in the work area (5). To navigate to a specific section of the path, click the desired section of the path. |
| 3       | Navigation Area—Displays the list of links to the Detector module summary screen and the zone status screens. Click a link from the list to display the relevant status information in the work area (5). The selected navigation area link is highlighted with a white frame.  
  
  To resize the navigation area, drag the frame bar between the navigation and the display areas. |
| 4       | Information Area—Displays information on the username and privilege level of the current user and provides the following links:  
  - Home—Returns you to the Detector summary screen.  
  - Enable—Moves you between user privilege levels.  
  - Logout—Closes the WBM session (the System Login screen appears).  
  - About—Displays WBM software information, which includes the software version number, system serial number, and software licensing agreement.  
  - Cisco Systems icon—Provides a link to the homepage of the Detector module on cisco.com. |
| 5       | Work Area—Displays the information that you select. To resize the work area, drag the frame bar between the navigation and work areas. |
Understanding Zone Status Icons

The WBM uses icons to represent the current status of a zone. The status icons appear in the navigation area and in the zone status bar. Table 1-2 describes what each of the status icons represents.

Table 1-2 Zone Status Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Circle]</td>
<td>Zone is inactive. The Detector module is not learning zone traffic or monitoring zone traffic for anomalies.</td>
</tr>
<tr>
<td>![Blue Circle]</td>
<td>Zone is active and in a phase of the learning process. The Detector module is performing either the policy construction phase or the threshold tuning phase of the learning process.</td>
</tr>
<tr>
<td>![Yellow Circle]</td>
<td>Zone is active. The Detector module is either monitoring zone traffic for anomalies or it is monitoring zone traffic for anomalies and learning the zone traffic at the same time.</td>
</tr>
<tr>
<td>![Red Circle]</td>
<td>Zone is active. The Detector module is monitoring an attack on the zone and new zone protection recommendations are available that require your attention.</td>
</tr>
</tbody>
</table>

Understanding WBM Navigation Maps

You can navigate in the screen hierarchy by using either the menus or the navigation path (see section 2 in Table 1-1). Selection items in the menus have a drop-down list. Selection items that are not available in the current view are grayed out.

The tables in this section map the links that are available from the two WBM menu bars:

- Detector Summary menu—Provides access to general Detector module statistical and configuration tools. To view the Detector Summary menu, click Detector Summary in the navigation area or click Home in the Information area. Table 1-2 provides a map of the Detector Summary menu levels.

Table 1-3 Detector Summary Menu

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Counters</td>
<td>Device counters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Real-time counters</td>
</tr>
<tr>
<td></td>
<td>Event log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device Resources</td>
<td></td>
</tr>
<tr>
<td>Zones</td>
<td>Zone list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Template list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compare zone policies</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>User list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change password</td>
<td></td>
</tr>
</tbody>
</table>
- Zone menu—Provides access to zone-specific statistical and configuration tools. To view the zone menu, click on the desired zone listed in the navigation area. Table 1-4 provides a map of the zone menu levels.

<table>
<thead>
<tr>
<th>Table 1-4</th>
<th>Zone Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong></td>
<td><strong>Level 2</strong></td>
</tr>
<tr>
<td>Main</td>
<td>Summary</td>
</tr>
<tr>
<td></td>
<td>Create zone</td>
</tr>
<tr>
<td></td>
<td>Save as . . .</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Counters</td>
</tr>
<tr>
<td></td>
<td>Event log</td>
</tr>
<tr>
<td></td>
<td>Attack log</td>
</tr>
<tr>
<td></td>
<td>Attack reports</td>
</tr>
<tr>
<td>Statistics</td>
<td>Policy statistics</td>
</tr>
<tr>
<td></td>
<td>Drop Statistics</td>
</tr>
<tr>
<td>Packet-Dump</td>
<td>Start Packet-Dump</td>
</tr>
<tr>
<td></td>
<td>Stop Packet-Dump</td>
</tr>
<tr>
<td></td>
<td>Packet-Dump List</td>
</tr>
<tr>
<td>Detection</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td>Deactivate</td>
</tr>
<tr>
<td></td>
<td>Dynamic Filters</td>
</tr>
<tr>
<td></td>
<td>Recommendations</td>
</tr>
<tr>
<td>Learning</td>
<td>Construct Policies</td>
</tr>
<tr>
<td></td>
<td>Tune Thresholds</td>
</tr>
<tr>
<td></td>
<td>Deactivate</td>
</tr>
<tr>
<td></td>
<td>Stop Learning</td>
</tr>
<tr>
<td></td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>Snapshot</td>
</tr>
<tr>
<td></td>
<td>Snapshot List</td>
</tr>
</tbody>
</table>
### Table 1-4  Zone Menu (continued)

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Filters</td>
<td>User Filters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bypass Filters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flex-Content Filters</td>
<td></td>
</tr>
<tr>
<td>Policy Templates</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remove Service</td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compare Policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Learning Parameters</td>
<td></td>
</tr>
</tbody>
</table>
Launching and Customizing the WBM

This chapter describes how to launch and customize the Cisco Traffic Anomaly Detector Module (Detector module) WBM. To access the Detector module WBM, you must first use the CLI to configure network access for the WBM.

This chapter contains the following sections:

- Configuring Network Access for the WBM
- Launching the WBM
- Configuring the Login Banner
- Configuring the WBM Logo

### Configuring Network Access for the WBM

You must use the Detector module CLI to enable the WBM service and to permit network access to the Detector module through the WBM. You must log on as a user with either administration or configuration user privilege level rights to make the necessary configuration changes. For information about accessing and using the Detector module CLI, see the Cisco Traffic Anomaly Detector Module Configuration Guide.

To configure network access for the WBM, perform the following steps using the Detector module CLI:

#### Step 1
Log on to the Detector module CLI using a console or a Secure Shell (SSH) connection.

#### Step 2
Enter configuration mode by entering the following command in global mode:

```
admin@DETECTOR# configure
```

#### Step 3
Enable the WBM service by entering the following command:

```
admin@DETECTOR-conf# service wbm
```

#### Step 4
Permit access to the Detector module from the WBM by entering the following command:

```
admin@DETECTOR-conf# permit wbm ip-addr [ip-mask] [if-service]
```

The `ip-addr` and `ip-mask` arguments define the IP address of the client device that you will use to connect to the WBM.

The optional `if-service` argument specifies the management port designator that restricts user access to the management interface only. The default is all interfaces. Enter `mng`. 
The following example shows how to configure network access for the WBM that connects from IP address 192.168.30.32:

```
admin@DETECTOR# configure
admin@DETECTOR-conf# service wbm
admin@DETECTOR-conf# permit wbm 192.168.30.32
```

After you finish configuring network access for the WBM on the Detector module, you may exit the CLI and launch the WBM using a web browser.

### Launching the WBM

To launch the WBM, perform the following steps:

---

**Step 1**
Open a web browser and enter the Detector module IP address using Secure HTTP (HTTPS):

`https://Detector module-ip-address/`

The `Detector module-ip-address` argument is the management IP address of the Detector module.

The Detector module WBM login window appears.

**Step 2**
Enter your username and password and click **OK**. The WBM home page appears.

---

**Note**

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

Use the Detector module CLI to configure the user authentication methods. For information about accessing and using the Detector module CLI, see the *Cisco Traffic Anomaly Detector Module Configuration Guide*.

---

If you fail to connect to the Detector module, check the following troubleshooting tips:

- Verify that you have entered a valid username and password.
- Verify that you have entered the correct Detector module management IP address and are specifying HTTPS in the URL.
- Check the network connections of both the WBM client and the Detector module.
- Ensure that you can connect to the Detector module from the WBM client using SSH.

**Note** Connecting using SSH will validate the network connection between the WBM and the Detector module.
• Ensure that you have enabled the WBM service and permitted access to the Detector module from the IP address of the WBM client (see the “Configuring Network Access for the WBM” section for more information).

Configuring the Login Banner

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

The login banner appears in the following locations:
• CLI—Before the password login prompt.
• WBM—On the right side of the Detector module login window.

You must access the Detector module CLI and use the `login-banner` command in configuration mode to configure the login banner. You must log on as a user with either administration or configuration user privilege level rights to make the necessary configuration changes. For information about using the CLI to configure and import a login banner, see the *Cisco Traffic Anomaly Detector Module Configuration Guide*.

Configuring the WBM Logo

You can customize the WBM interface by adding a company logo or any customized logo to the WBM web pages.

The new logo appears in the following places:
• On the Detector module Login page under the Cisco Systems logo.
• On all WBM pages on the right side of the Cisco Systems logo.

You must use the Detector module CLI and use the `copy {ftp | sftp | scp} wbm-logo` command in global mode or configuration mode to configure the WBM logo. You must log on as a user with either administration or configuration user privilege level rights to make the necessary configuration changes. For information about using the CLI to import the WBM logo, see the *Cisco Traffic Anomaly Detector Module Configuration Guide*. 
Managing User Access

This chapter describes how to control access to the Cisco Traffic Anomaly Detector Module (Detector module) by creating user profiles. When a user attempts to log on to the WBM, the Detector module authenticates the login username and password against a user profile database.

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding User Authentication and Authorization Methods
- Using Preconfigured System User Profiles
- Displaying the Users List
- Creating a User Profile
- Deleting a User Profile
- Changing Your Password
- Changing the Password of Another User
- Moving Between User Privilege Levels
- Configuring User Profiles on a TACACS+ Server
Understanding User Authentication and Authorization Methods

Depending on how you configure the Detector module using the CLI, the Detector module performs user authentication and authorization using one or both of the following methods:

- **Local**—Authenticates the username and password against its own internal database. You can configure each username with a user privilege level that allows the user to execute a predefined set of commands.

  The local authentication and authorization method is the default. You configure local user authentication and authorization using the WBM.

- **AAA (authentication, authorization, and accounting)**—Authenticates the username and password against an external database that resides on one or more Terminal Access Controller Access Control System Plus (TACACS+) servers. AAA authorization enables you to specify access rights for each command. In addition to configuring user authentication and authorization, AAA services allow you to configure accounting, which enables you to track device events. For example, you can track user-initiated events, such as Detector module configuration changes.

  You must use the CLI to enable AAA services and to define the TACACS+ servers on the Detector module.

Using Preconfigured System User Profiles

The Detector module is preconfigured with the following two system user profiles on the local database:

- **admin**—Use this default username to initially access the CLI on the Detector module. You assign a password to the admin user profile when you log into the Detector module for the first time. If you log on as an administrator, you have full access to the CLI commands and the WBM windows. Use the admin user profile to configure the Detector module and to create other user profiles.

- **riverhead**—The Detector module uses the riverhead username to initially access the Guard and establish the communication channel between them. You assign a password to the riverhead user profile when you log into the Detector module for the first time. After the initial communication link has been established between the Guard and the Detector module, the two devices use a private-public key pair to establish future communication links, eliminating the need for user intervention. The riverhead system user profile is configured with the dynamic user privilege level.

  You can change the password of a system user, but you cannot delete a system user from the Detector module database.

Note: We recommend that you create new user accounts and avoid using the system user accounts after initial configuration so that you can monitor user actions.
Displaying the Users List

The WBM allows you to display a list of the users that are defined in the local user database. From the user list, you can add or delete a user profile. The user list is divided into two categories as follows:

- **System users**—User profiles that are predefined by Cisco and cannot be deleted (see the “Using Preconfigured System User Profiles” section).
- **Users**—User profiles that you define.

To view the list of users that are defined in the local user database, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the navigation pane, click Detector Summary. The Detector module summary menu appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Detector module summary menu, choose Users &gt; Users list. The Users list appears.</td>
</tr>
</tbody>
</table>

Creating a User Profile

To create a user profile on the local database, you must have administration access rights.

**Note**

If the Detector module is configured to authenticate users using local and AAA services for authentication (or just AAA services), you must also configure the user profile information on each TACACS+ server that is used for authentication purposes (see the “Configuring User Profiles on a TACACS+ Server” section).

To create a new user profile, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the navigation pane, click Detector Summary. The Detector module summary menu appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Use one of the following methods to display the Create User screen:</td>
</tr>
<tr>
<td></td>
<td>• From the Detector module summary menu, choose Users &gt; Create user.</td>
</tr>
<tr>
<td></td>
<td>• From the Detector module summary menu, choose Users &gt; Users list (the Users list appears) and then click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Define the user profile parameters as described in Table 3-1.</td>
</tr>
</tbody>
</table>

**Table 3-1  User Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the user profile. Enter a case-sensitive alphanumeric string from 1 to 63 characters that starts with an alphabetic character. The string cannot contain spaces but can contain underscores.</td>
</tr>
<tr>
<td>Initial password</td>
<td>User password. Enter a case-sensitive 6- to 24-character string with no spaces.</td>
</tr>
</tbody>
</table>
Deleting a User Profile

When you delete a user profile, the associated user can no longer access the Detector module if authentication is performed using the local user database only.

To delete a user profile, perform the following steps:

Step 1 In the navigation pane, click **Detector Summary**. The Detector module summary menu appears.

Step 2 From the Detector module summary menu, choose **Users > Users list**. The Users list appears.

Step 3 Check the check box next to the username that you want to delete, and then click **Delete**. To delete all the usernames listed, check the User check box, and then click **Delete**. The delete validation message appears.

Step 4 Choose one of the following options:

- **OK**—Deletes the user profile from the local database. The Users list appears.
- **Cancel**—Ignores the delete user request. The Users list appears.
Changing Your Password

You can change your own password. Administrators can change their own password and the passwords of other users (see the “Changing the Password of Another User” section).

To change your own password, perform the following steps:

Step 1  In the navigation pane, click Detector Summary. The Detector module summary menu appears.
Step 2  From the Detector module summary menu, choose Users > Change Password. The Change Password screen appears.
Step 3  In the Old Password field, enter your current password.
Step 4  In the New Password field, enter a new password. The password must be a case-sensitive 6- to 24-character string with no spaces.
Step 5  In the Confirm New Password field, reenter the new password.
Step 6  Choose one of the following options:
   •  OK—Saves the new password to the user profile on the Detector module database. The Detector module summary screen appears.
   •  Cancel—Exits the Change Password screen without saving any information. The Detector module summary screen appears.

If you enter an invalid current password, the Detector module displays an error message because it cannot verify the new password. Click Go Back to repeat the procedure.

Changing the Password of Another User

Users with an administration user privilege level can change passwords of other users.

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

Step 1  In the navigation pane, click Detector Summary. The Detector module summary menu appears.
Step 2  From the Detector module summary menu, choose Users > Change Password. The Change Password screen appears.
Step 3  Click on a username. The user details screen appears.
Step 4  Click Config. The Config User screen appears.
Step 5  Enter the new password. The password must be a case-sensitive 6- to 24-character string with no spaces.
Step 6  Click OK to save the new password to the user profile on the local database.
Moving Between User Privilege Levels

You can move between user privilege levels.

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

**Step 1**
From the information area, click **Enable**.
The Enable Authentication window appears.

**Step 2**
From the Level drop-down list, choose a user privilege level to which you want to move. The privilege level can be one of the following:
- **admin**—Permits full access to all WBM functions.
- **config**—Permits full access to all WBM functions except for user profile management.
- **dynamic**—Permits access to monitoring and diagnostic operations, protection, and learning-related operations. Users with Dynamic privileges can also configure the flex-content and dynamic filters.

**Step 3**
In the Password field, enter the privilege level password.

**Step 4**
To apply the change, click **OK**.

Configuring User Profiles on a TACACS+ Server

The information in this section is intended for administrators who must configure the WBM user profile information on a TACACS+ server. To manage user access to the WBM using a TACACS+ server and AAA services, you must use the Detector module CLI to enable the AAA services and to define the TACACS+ servers on the Detector module (see the *Cisco Traffic Anomaly Detector Module Configuration Guide*).

**Note**
When you enable TACACS+ accounting, each recorded event is assigned a task identification (task_id) number. For WBM events, the task_id numbering sequence begins at 40000.

You can configure user authorization on a TACACS+ server to restrict user access to specific zones and WBM functions.

**Note**
All commands are case sensitive.

This section contains the following topics:
- Managing the WBM Portal to Restrict User Access to Specific Zones
- Managing Authorization to Specific WBM Commands

Managing the WBM Portal to Restrict User Access to Specific Zones

You can customize the WBM portal to limit the zones that a user can view and access by configuring the TACACS+ server with the command `showZonePortal` command and the `zone_name` attribute.
The following commands, which provide basic WBM navigation, are mandatory and must always be configured to permit: `ShowGuardPortal` and `ShowZonesList`.

For example, in the following TACACS+ server configuration, user ABC is granted permission to access zones ABC_1 and ABC_2 only, regardless of how many zones you have configured on the device.

```plaintext
user = ABC {
    default service=permit
    login=cleartext 123456

cmd = ShowZonePortal {
    permit "zone_name_ABC_1"
    permit "zone_name_ABC_2"
    deny .*
}

cmd = ShowDetectorPortal {
    permit .*
}

cmd = ShowZonesList {
    permit .*
}
}
```

Managing Authorization to Specific WBM Commands

Every WBM menu item and function button is mapped to a command that allows you to control whether or not a user is authorized to access specific menu items or function buttons. Table 3-2 displays the WBM commands that you can configure on a TACACS+ server to manage user access to WBM functionality.

<table>
<thead>
<tr>
<th>Privilege Level</th>
<th>Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>User management</td>
<td>ShowUserList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddUser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteUser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowUserDetails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigUser</td>
</tr>
<tr>
<td>Config</td>
<td>Create/Add</td>
<td>CreateBypassFilter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateZone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateZoneTemplate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddZoneIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddPolicyThreshold</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AddService</td>
</tr>
</tbody>
</table>
### Table 3-2 WBM Operations Supported by TACACS+ (continued)

<table>
<thead>
<tr>
<th>Privilege Level</th>
<th>Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config (continued)</td>
<td>Delete</td>
<td>DeleteZones</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteZoneIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteZoneTemplate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteReports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteBypassFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeletePacketDump</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteSnapshot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeletePolicyThreshold</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RemoveService</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ClearCounters</td>
</tr>
<tr>
<td>Export</td>
<td>Export</td>
<td>ExportReports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SetFtpServer</td>
</tr>
<tr>
<td>Learn</td>
<td>Start Detect &amp; Learn</td>
<td>StartDetect&amp;Learn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StartPolicyConstruction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StopPolicyConstruction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StartThresholdTuning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StopThresholdTuning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AcceptPolicyConstruction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AcceptThresholdTuning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateSnapshot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteSnapshot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RejectResults</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NoLearningAccept</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NoLearningReject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SavePoliciesRecommendations</td>
</tr>
</tbody>
</table>
### Table 3-2  
**WBM Operations Supported by TACACS+ (continued)**

<table>
<thead>
<tr>
<th>Privilege Level</th>
<th>Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config (continued)</td>
<td>Configure</td>
<td>ConfigExtendedFlexFilter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigWormSrcIPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigPolicies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigPolicyTemplate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigZone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigLearn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigPolicy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigPolicyGroup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ConfigPolicyThreshold</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ChangePolicyState</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RecommendationAcceptForever</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SaveAsZone</td>
</tr>
<tr>
<td>Dynamic</td>
<td>Create/Add/Delete</td>
<td>CreateExtendedFlexFilter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteExtendedFlexFilter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateDynamicFilter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteAllDynamicFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteDynamicFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RecommendationIgnore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RecommendationAccept</td>
</tr>
<tr>
<td>Victim Activation</td>
<td>StartDetection</td>
<td>StartDetection</td>
</tr>
<tr>
<td></td>
<td>StopDetection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ActivatePolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DeactivatePolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AcceptPendingDynFilter</td>
<td></td>
</tr>
<tr>
<td>Packet-dump</td>
<td>StartPacketDump</td>
<td>StartPacketDump</td>
</tr>
<tr>
<td></td>
<td>StopPacketDump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SavePacketDump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RenamePacketDump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CopyPacketDump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ExportPacketDump</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ImportPacketDump</td>
<td></td>
</tr>
<tr>
<td>Show</td>
<td>Password/Login/Logout</td>
<td>UserLogin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UserLogout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EnableUser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ChangePassword</td>
</tr>
</tbody>
</table>
### WBM Operations Supported by TACACS+ (continued)

<table>
<thead>
<tr>
<th>Privilege Level</th>
<th>Function</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show (continued)</td>
<td>Show</td>
<td>ShowGuardPortal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowGuardCounters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowGuardRealtimeCounters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowGuardLog</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowZoneList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowTemplateList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPolicyComparison</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowZonePortal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowZoneCounters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowRealtimeCounters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowZoneLog</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowAttacksSummary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowAttack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowAttackDetails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowZombiesAttack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPolicyStatistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPacketDumpList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowCaptureAnalysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowDynamicFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowDynamicFilterDetails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPendingRecommendations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPendingFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowSnapshotList</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowGeneralConfiguration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowUserFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowBypassFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowFlexContentFilters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPolicyTemplate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPolicies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPolicyDetails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowLearningParams</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowPolicyComparison</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowSignatureExtraction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ShowVersion</td>
</tr>
</tbody>
</table>
The following TACACS+ server example shows how to configure Customer A user with authorization to access the following zones and functionality:

- Zones A1 and A2 only.
- All WBM functions except for the following diagnostic functions:
  - Guard counters
  - Real time counters
  - Show logs

```
key = 12345
default authentication = file /etc/passwd
accounting file = /var/log/tacacs.log
default authorization = permit

user = Customer_A {
  default service=permit
  service=connection {}
  login=cleartext 1234

  cmd = ShowZonePortal {
    permit "zone_name_zone_A1"
    permit "zone_name_zone_A2"
    deny .*
  }

  cmd = ShowGuardCounters {
    deny .*
  }

  cmd = ShowGuardRealtimeCounters {
    deny .*
  }

  cmd = ShowGuardLog {
    deny .*
  }
}
```
Creating and Configuring Zones

This chapter describes how to create and manage zones on the Cisco Traffic Anomaly Detector Module (Detector module).

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding Zones
- Configuring Guard Zones
- Creating a Zone
- Configuring the Zone IP Address Range
- Viewing and Modifying a Zone Configuration
- Deleting a Zone

Understanding Zones

A zone is a network element that you define and that the Detector module monitors for Distributed Denial of Service (DDoS) attacks. A zone can be any combination of the following elements:

- A network server, client, or router
- A network link, subnet, or an entire network
- An individual Internet user or a company
- An Internet Service Provider (ISP)

When the Detector module identifies a DDoS attack, it can activate a Guard automatically to protect the zone against the attack or it can notify you to activate the Guard manually. The Detector module can analyze the traffic of different zones simultaneously if their network address ranges do not overlap.
The zone configuration includes the following attributes:

- Zone description—Defines the zone name and description.
- Zone network definition—Defines the zone network attributes that include the zone network IP address and subnet mask.
- Policy templates—Define the types of policies that the Detector module creates when performing the learning process.
- Policies—Analyze zone traffic and execute an action when the Detector module identifies an anomaly in the zone traffic. The zone policies can be the default policies that came with the zone template or zone-specific policies that the Detector module created during the learning process.
- Zone Filters—Direct the zone traffic to the required protection level and define how the Detector module handles specific traffic flows.

You can create a zone by using one of the following methods:

- Use a predefined zone template—Create a new zone using one of the predefined zone templates, which configures the zone with a set of default policies and filters.
  After you create a new zone, you must configure the zone attributes.
- Use an existing zone as a template—Create a zone by making a copy of an existing zone. Use this method if the new zone has traffic patterns that are similar to those of an existing zone.

### Configuring Guard Zones

You can create a zone using a Guard zone template and synchronizing the zone configuration with a Guard. A zone that you create using a Guard zone template has two sets of definitions; one for the Detector module, and one for the Guard. The zone configuration contains additional parameters that affect the Guard only.

This section contains the following topics:

- Displaying the Configuration of Guard Zones
- Understanding the Protection Characteristics
- Understanding the Protection Activation Methods
- Understanding the Extent of Zone Protection

### Displaying the Configuration of Guard Zones

You can display both sets of definitions of the zone configurations, one for the Detector module, and one for the Guard. A toggle filter appears at the top of the screen enabling you to toggle between the display of the two sets of definitions as follows:

- To display the configuration of the zone on the Detector module, click View Guard. The toggle button displays “View Detector” to indicate that the Detector module configuration is displayed.
- To display the configuration of the zone on the Guard, click View Detector. The toggle button displays “View Guard” to indicate that the Guard module configuration is displayed.
Understanding the Protection Characteristics

You can define how the Guard activates zone protection. You must ensure that the zone configuration is synchronized to the Guard before you activate zone protection for the configuration to take effect. You can define the following protection characteristics:

- **Operation mode**—You can configure how the Guard performs zone protection and define whether the Guard applies measures to protect the zone automatically or in an interactive manner in which you must determine the protection measures that the Guard applies.

- **Activation method**—You can define whether to activate the zone according to the zone name, the zone address range, or the received traffic. See the “Understanding the Protection Activation Methods” section for more information.

- **Activation extent**—You can define whether to activate zone protection for the entire zone address range or only for a specific IP address within the zone. The activation extent applies to zones where zone protection is activated by an external device, such as a Detector module. See the “Understanding the Extent of Zone Protection” section for more information.

- **Protection termination timeout**—You can define the timeout after which the Guard terminates zone protection.

Understanding the Protection Activation Methods

The protection activation method defines how the Guard identifies the zone for which it activates zone protection when it receives an external indication. This indication can be a command from an external device, such as an external device, or traffic packets that are destined to the zone.

The method that the Guard uses to activate protection can be one of the following:

- **IP Address**—Activates zone protection when it receives a command from an external device, such as a Detector module, that consists of an IP address or subnet that is part of the zone.

- **Packet**—Activates zone protection when it receives traffic that is destined to the zone.

- **Packet or IP Address**—Activates zone protection when it receives traffic (a packet) that is destined to the zone or when it receives a command from an external device, such as the Detector module, that consists of an IP address or subnet that is part of the zone address range.

- **Zone Name Only**—Activates zone protection based on the zone name.

The following rules apply when you configure a zone with a protection activation method of Packet or Packet or IP Address:

- You must manually divert the zone traffic to the Guard using an external device. Otherwise, the Guard cannot monitor the zone traffic.

- You can configure the minimum received traffic rate that is required for the Guard to activate zone protection by using the `protect-packet activation-sensitivity` CLI command. You can only configure the activation sensitivity using the Guard CLI. See the Cisco Guard Configuration Guide or the Cisco Anomaly Guard Module Configuration Guide for more information.

- Do not configure more than one zone with the same address range or zone protection may not function properly.
Understanding the Extent of Zone Protection

The activation extent defines whether to activate zone protection for the entire zone or for a partial zone when the Guard receives an external indication. This indication can be a command from an external device, such as the Detector module, or traffic packets that are destined to the zone.

The Guard supports the following activation extents:

- **Entire zone**—Activates protection for the entire zone. The Guard activates protection when it receives traffic that is destined to the zone or when it receives an external indication that consists of an IP address or subnet that is part of the zone.

- **IP Address only**—Activates zone protection only for the specified IP address or subnet. When the Guard receives traffic that is destined to the zone or when it receives a command from an external device, such as the Detector module that consists of an IP address or subnet that is part of the zone, the Guard creates a new zone (subzone). This activation extent is the default.

Creating a Zone

You can create a zone and configure the zone name, description, network address, operation definitions, and networking definitions.

You can create a new zone in two ways:

- Use a predefined zone template—Create a new zone using one of the predefined zone templates. Use this method to create a new zone with the default policies and filters.

  **Note** When you create a zone using a zone template containing PPH policies for monitoring low-rate zombie attacks, the PPH policies by default are set to the disabled state because they may increase the amount of memory used by the zone and also affect Guard module performance. To enable the zone PPH policies, you must change the policy states to active (see the “Modifying Policy Parameters” section in Chapter 8, “Managing Zone Policies”).

- Use an existing zone configuration as a template—Create a new zone by duplicating an existing zone. Use this method if the new zone has traffic patterns that are similar to those of an existing zone.

See the “Configuring the Zone IP Address Range” section for information about how to modify the zone configuration settings.

This section contains the following topics:

- Creating a Zone from a Zone Template
- Creating a Zone from an Existing Zone

Creating a Zone from a Zone Template

To create a new zone using a zone template, perform the following steps:

**Step 1** From the navigation pane, click Detector Summary. The Detector summary menu appears.

**Step 2** From the Detector main menu, choose Zones > Create Zone. The Zone Definition Form appears.
To display the Zone Definition Form, you can also choose Zones > Zone list and then click Add or choose Main > Create Zone from the zone main menu.

**Step 3** Define the first set of zone configuration parameters. Table 4-1 describes the fields in the Zone Definition Form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the new zone. The name is an alphanumeric string from 1 to 63 characters. The string must start with a letter, can contain underscores, but cannot contain any spaces.</td>
</tr>
<tr>
<td>Description</td>
<td>Text describing the zone. Enter an alphanumeric string from 1 to 80 characters.</td>
</tr>
<tr>
<td>Zone Template</td>
<td>Zone template that defines the policies used in the zone configuration. The Detector module contains two sets of zone templates with the following prefixes:</td>
</tr>
<tr>
<td></td>
<td>• DETECTOR_—Zone templates for Detector module use only. Select the DETECTOR_ version of the zone template when you are not going to share the zone configuration with a Guard.</td>
</tr>
<tr>
<td></td>
<td>• GUARD_—Zone templates for use on the Detector module and the Guard. You can configure both Detector module and Guard attributes for zones that were created from these templates, and copy the zone configuration to the Guard. Select the GUARD_ version of the zone template when you plan to synchronize the zone configuration with a Guard.</td>
</tr>
<tr>
<td></td>
<td>Choose one of the following zone templates:</td>
</tr>
<tr>
<td></td>
<td>• DETECTOR_DEFAULT—Default zone template. You can use this zone template to protect a Voice-over-IP server. If you create a zone using this zone template, you cannot detect TCP worm attacks on the zone.</td>
</tr>
<tr>
<td></td>
<td>• DETECTOR_WORM—Zone template that allows the Detector module to detect TCP worm attacks on the zone. Zones that are created from the DETECTOR_WORM zone template contain policies that are produced from the worm_tcp policy template.</td>
</tr>
<tr>
<td></td>
<td>• DETECTOR_LINK templates—Zone templates that allow the Detector module to detect large subnets segmented according to zones with a known bandwidth. You can activate zone detection for zones defined by these zone templates without undergoing the learning process. To enable the Detector module to activate zone protection on a Guard for the attacked IP address or subnet only, configure the Protect-IP State parameter to Only Dst IP. See the Protect-IP State parameter in this table for more information. The following bandwidth-limited link zone templates are available for 128-Kb, 1-Mb, 4-Mb, and 512-Kb links: DETECTOR_LINK_128K, DETECTOR_LINK_1M, DETECTOR_LINK_4M, and DETECTOR_LINK_512K.</td>
</tr>
<tr>
<td></td>
<td>You cannot perform the policy construction phase of the learning process for zones that were created from these templates (see “Understanding the Learning Process” section in Chapter 7, “Learning Zone Traffic”).</td>
</tr>
</tbody>
</table>
Creating a Zone

Zone Template (continued)

- GUARD_DEFAULT—Guard default zone template. The Guard may change the packet source IP address to the Guard TCP-proxy IP address. You can use this zone template if you do not use access-control lists, access policies, or load-balancing policies that are based on the incoming IP address for the zone network.

- GUARD_VOIP—Zone template designed for a zone that contains a Voice-over-IP (VoIP) server that uses Session Initiation Protocol (SIP) over UDP to establish VoIP sessions and the Real-Time Transport Protocol/Real-Time Control Protocol (RTP/RTCP) to transmit voice data between SIP endpoints after sessions are established.

Zones that are created from the GUARD_VOIP zone template contain specific policies to handle VoIP traffic that are produced from the sip_udp policy template.

- GUARD_LINK templates—Zone templates for zones with a known bandwidth. The following templates are available for 128-Kb, 1-Mb, 4-Mb, and 512-Kb links: GUARD_LINK_128K, GUARD_LINK_1M, GUARD_LINK_4M, and GUARD_LINK_512K.

You cannot perform policy construction for zones that were created from these templates. You can activate zone detection for zones that were created from the GUARD_LINK zone templates without undergoing the threshold tuning phase.

To enable the Detector module to activate zone protection on a Guard for the attacked IP address or subnet only, configure the Protect-IP State parameter to Only Dst IP. See the Protect-IP State parameter in this table for more information.

- GUARD_TCP_NO_PROXY—Zone template for a zone for which no TCP proxy is to be used. You can use this zone template if the zone is controlled based on IP addresses, such as an Internet Relay Chat (IRC) server-type zone, or if you do not know the type of services running on the zone.

Operation mode

Mode in which the Detector module performs zone protection. The operation mode can be one of the following:

- Automatic—The Detector module automatically activates all dynamic filters as it creates them during an attack.

- Interactive—The Detector module displays the dynamic filters that the policies create as recommendations. You must decide whether or not to activate each dynamic filter.

See the “Activating Automatic or Interactive Detect Mode” section in Chapter 9, “Activating Anomaly Detection” for information about zone operation modes.

IP address

Zone IP address. After you create the zone, you can modify the IP address or add additional IP addresses (see the “Configuring the Zone IP Address Range” section).

IP Mask

Zone address mask. Choose the address mask from the Mask drop-down list. After you create the zone, you can modify the address mask (see the “Configuring the Zone IP Address Range” section).

IP List

Additional zone IP addresses. Create a list of zone IP addresses, space delimited, in dotted-decimal notation (use format a.b.c.d/x, where /x specifies the subnet mask).
**Step 4** Click **OK**. The Zone Configuration Form appears, displaying the second set of zone configuration parameters. This form contains the default parameter values associated with the zone template you selected in the previous step.

**Step 5** Define the second set of zone configuration parameters. Table 4-2 describes the fields in the Zone Configuration Form.

<table>
<thead>
<tr>
<th>Table 4-2 Zone Configuration Form Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>General Parameters</strong></td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>
| Operation mode | Mode in which the Detector module performs zone protection. The operation mode can be one of the following:
- Automatic—The Detector module automatically activates all dynamic filters as it creates them during an attack.
- Interactive—The Detector module displays the dynamic filters that the policies create as recommendations. You must decide whether or not to activate each dynamic filter.
See the “Activating Automatic or Interactive Detect Mode” section in Chapter 9, “Activating Anomaly Detection” for information about zone operation modes. |
| Protect-IP state | Guard-protection method that the Detector module uses to activate remote Guard modules. The Guard-protection method that you select can save Guard resources by allowing the Guard to focus on specific zone protection requirements. The states from the Protect-IP state drop-down list are as follows:
- Entire Zone—Activates a Guard to protect the entire zone when it detects an anomaly in the zone traffic. This method saves Guard resources because it reduces the number of active zones that the Guard protects. We recommend that you use this strategy when the zone consists of related subzones.
- Only Dst IP—Activates a Guard to protect a particular IP address when it detects an anomaly in the zone traffic that is destined to that IP address. You can activate a Guard to protect the attacked IP address but avoid diverting the traffic of the entire zone to the Guard. If the Detector module cannot associate the traffic anomaly with a particular IP address, it does not activate a Guard module to protect the zone.
We recommend that you use this strategy when the zone consists of unrelated subzones. |
Creating a Zone

Protect-IP state (continued)

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

We recommend that you use this strategy when the zone consists of related subzones so that you can avoid a situation in which a targeted zone may cause damage to the entire zone.

- Only Dst IP by address—Activates a Guard to protect a particular IP address when it detects an anomaly in the zone traffic that is destined to that IP address. The IP address must be in the address range of one of the zones that you have defined on the Guard. However, the name of the zone on the Detector module does not have to be identical to the zone name on the Guard module. Selecting Only Dst IP by address is equivalent protecting an IP address when the zone name is not known by choosing Main > Protect IP from the Guard main menu. We recommend that you use this strategy when the zone names on the Detector module are not identical to the zone names on the Guard, or when the zone consists of unrelated subzones.

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

Rate (GUARD_ templates only) Amount of traffic that the Guard is allowed to inject back into the network. Set the bandwidth value to the highest bandwidth measured entering the zone. If the highest bandwidth value is not known, leave the Rate and Burst fields blank and choose unlimited units (unlimit) from the drop-down list.

Enter an integer for the maximum rate and then choose one of the following units of measurement from the drop-down list:

- unlimit—Use this default setting if you do not want to limit the rate of the traffic that the Guard injects back into the network. When you choose unlimit, do not enter a maximum rate value.
- mbps—Megabits per second.
- kbps—Kilobits per second.
- bps—Bits per second.
- kpp—Kilopackets per second.
- pps—Packets per second.

Burst (GUARD_ templates only) Highest traffic peak that the Guard is allowed to pass to the zone. Enter an integer for the burst size rate. The units are bits, kilobits, kilopackets, megabits, and packets that correspond to the rate units that are specified by the rate (Rate) unit of measurement.

Table 4-2 Zone Configuration Form Fields (continued)
### Table 4-2 Zone Configuration Form Fields (continued)

<table>
<thead>
<tr>
<th>Attack detection/termination parameters (GUARD_templates only)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection-end Timer</td>
<td>Inactivity timeout that the Guard uses to terminate zone protection when there is no attack on the zone. The Guard measures the inactivity based on the dynamic filter inactivity and dropped traffic. Enter a value from seconds to an infinite amount of time.</td>
</tr>
<tr>
<td>Malicious-rate detection threshold</td>
<td>Minimum rate of zone packets that are dropped. If the rate goes lower than this threshold, the Guard may end zone protection. If the rate exceeds this threshold, the Guard identifies an attack on the zone and creates an attack report. The default Malicious-rate detection threshold is 10 packets per second (pps).</td>
</tr>
<tr>
<td>Filter-rate termination threshold</td>
<td>Threshold value that together with the malicious-rate termination threshold, specifies when the Guard can deactivate dynamic filters. Define this threshold in packets per second (pps). See the “Managing Dynamic Filters” section in Chapter 9, “Activating Anomaly Detection” for more information.</td>
</tr>
<tr>
<td>Filter-rate-pph termination threshold</td>
<td>Threshold value that, together with the malicious-rate termination threshold, specifies when the Guard can deactivate dynamic filters. Define this threshold in packets per hour (pph). See the “Managing Dynamic Filters” section in Chapter 9, “Activating Anomaly Detection” for more information.</td>
</tr>
<tr>
<td>Malicious-rate termination threshold</td>
<td>Threshold value, that together with the Filter-rate termination threshold, specifies when the Guard can deactivate dynamic filters. Define this threshold in packets per second (pps). See the “Managing Dynamic Filters” section in Chapter 9, “Activating Anomaly Detection” for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activation parameters (GUARD_templates only)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation interface</td>
<td>Protection activation method that defines how the Guard identifies the zone for which it activates zone protection when it receives an external indication. This indication can be a command from an external device, such as a Detector, or traffic that is destined to the zone (packet). The activation method can be one of the following:</td>
</tr>
<tr>
<td>Zone name</td>
<td>Activates zone protection based on the zone name. This is the default activation method.</td>
</tr>
<tr>
<td>By packet</td>
<td>Activates zone protection when it receives traffic that is destined to the zone. The Guard scans the zone database and activates the zone that has an address range that includes the received packet IP address. If you have configured several zones with an address range that includes the received packet IP address, the Guard activates the zone with the longest prefix match (the zone that has the most specific address range that includes the received packet IP address). The received IP address or subnet must be completely included in the zone IP address range.</td>
</tr>
</tbody>
</table>

**Note** When you configure a zone with a protection activation method of packet, the Guard changes the way that it handles traffic that is not destined to an active zone. If you have configured injection for that traffic, the Guard forwards the traffic instead of dropping it. |

To configure the activation method to by packet, check the **By packet** check box.
**Table 4-2 Zone Configuration Form Fields (continued)**

| Activation interface (continued) | • By IP address—Activates zone protection when it receives a command from an external device, such as a Detector, that consists of an IP address or subnet that is part of the zone. The Guard scans the zone database and activates the zone that has an address range that includes the received IP address or subnet. If you have configured several zones with an address range that includes the received IP address, the Guard activates the zone with the longest prefix match (the zone that has the most specific address range that includes the received IP address). The received IP address or subnet must be completely included in the zone IP address range.

To configure the activation method to by packet, check the **By IP address** check box.

• By IP Address or By Packet—Activates zone protection when it receives traffic (a packet) that is destined to the zone or when it receives a command from an external device, such as the Detector, that consists of an IP address or subnet that is part of the zone address range. See the By IP address and By packet bullets in this section for more information.

To configure the activation method to By IP Address or By Packet, check both the **By IP address** check box and the **By packet** check box.

---

**Note** You must manually divert traffic to the Guard when the zone is attacked if you configure the protection activation to By Packet or By IP Address or By Packet. For more information about the Activation interface options, see the “Understanding the Protection Activation Methods” section.

| Activation extent | Defines whether the Guard activates zone protection for the entire zone or for a part of the zone when the Guard receives an external indication to activate zone protection. The activation extent can be one of the following:

• IP address only—Activates protection only for the specified IP address or subnet within the zone. This is the default activation extent setting.

• Entire zone—Activates protection for the entire zone.

For more information about the Activation extent options, see the “Understanding the Extent of Zone Protection” section.

| Packet Dump parameters | Auto Packet Dump: Check the check box next to one of the following options:

• On—Enables auto packet dump

• Off—Disables auto packet dump (default setting)

| Max. disk space | Enter the maximum amount of disk space in megabytes to use for auto packet dumps. This field applies to the Cisco Guard (appliance) only and does not affect the Cisco Traffic Anomaly Detector Module.

---

**Step 6** Click **OK** to save the new zone.
Creating a Zone from an Existing Zone

To create a new zone using an exiting zone as a template, perform the following steps:

**Step 1** From the navigation pane, choose a zone to be used as a zone template. The zone main menu appears.

**Step 2** From the zone main menu, choose **Main > Save as**. The Zone Save as screen appears.

**Step 3** Define the new zone name. In the Name text field, enter the zone name as an alphanumeric string of 1 to 63 characters. The string must start with a letter, can contain underscores, but cannot contain spaces.

**Step 4** Click **OK** to save the new zone. The zone general view screen appears.

Configuring the Zone IP Address Range

You must configure at least one IP address that is not excluded before you can activate zone anomaly detection, but you can add or delete IP addresses from the zone IP address range at any time.

This section contains the following topics:

- Adding an IP Address to the Zone IP Address Range
- Deleting an IP Address from the Zone IP Address Range
- Updating the Zone Policies

Adding an IP Address to the Zone IP Address Range

You can configure a large subnet and then exclude specific IP addresses from that subnet so that they are not part of the zone IP address range.

To add an IP address to the zone configuration, perform the following steps:

**Step 1** From the navigation pane, select a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose **Configuration > General**. The zone general view screen appears.

**Step 3** Click **Add** (located below the second table). The Add Zone IP screen appears.

**Step 4** Enter the following IP address information:

- **IP Address**—Zone IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.100.32).
- **IP Mask**—Zone IP address mask. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.224). The default subnet mask is 255.255.255.255.

**Step 5** (Optional) Check the **Exclude** check box to exclude the IP address from the zone IP address range.

**Step 6** Click **OK** to save the zone configuration. The zone general view screen appears.

**Step 7** Update the zone policies. See the “Updating the Zone Policies” section for more information.
Deleting an IP Address from the Zone IP Address Range

To delete an IP address from the zone IP address range, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the navigation pane, select a zone. The zone main menu appears.</td>
</tr>
<tr>
<td>2</td>
<td>From the zone main menu, choose <strong>Configuration &gt; General</strong>. The zone general view screen appears.</td>
</tr>
<tr>
<td>3</td>
<td>Check the check box next to each IP address that you want to delete and then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Update the zone policies. See the “Updating the Zone Policies” section for more information.</td>
</tr>
</tbody>
</table>

Updating the Zone Policies

If you modify the zone IP address or subnet, perform one of the following tasks:

- If the new IP address or subnet consists of a new service that was not previously defined in the zone network, allow the Detector module to perform the policy construction phase before you activate zone protection or add the service manually. See the following sections for more information:
  - “Starting the Policy Construction Phase” section on page 7-4
  - “Adding a Service” section on page 8-10
- If zone protection and the learning process are enabled, mark the zone policies as untuned. Do not change the status of the zone policies to untuned if there is attack on the zone because that prevents the Detector module from detecting the attack and causes the Detector module to learn thresholds of malicious traffic. See the “Marking the Zone Policies as Tuned or Untuned” section for more information.
- If you did not enable zone anomaly detection and the learning process by selecting **Detect and Learn** and you do not plan to activate the two processes, activate the threshold tuning phase before activating zone protection. See the “Starting the Threshold Tuning Phase” section for more information.

Viewing and Modifying a Zone Configuration

You can view the parameter settings of a zone configuration at any time to verify the current configuration settings and to modify the configuration of needed.

To view the current parameter settings of a zone configuration, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the navigation pane, choose a zone. The zone main menu appears.</td>
</tr>
<tr>
<td>2</td>
<td>From the zone main menu, choose <strong>Configuration &gt; General</strong>. The General Configuration view screen appears, displaying the parameter settings of the zone configuration.</td>
</tr>
</tbody>
</table>
Table 4-3 describes the information that displays in the General Configuration area.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Zone Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name that you assign to the zone.</td>
</tr>
<tr>
<td>Description</td>
<td>Description to help identify the zone.</td>
</tr>
<tr>
<td>Operation mode</td>
<td>Mode the zone is configured to operate in (automatic or interactive).</td>
</tr>
<tr>
<td>Zone template</td>
<td>Template used to create the zone.</td>
</tr>
<tr>
<td>Rate (GUARD_templates only)</td>
<td>(GUARD_templates only) Amount of traffic that the Guard is allowed to inject back into the network.</td>
</tr>
<tr>
<td>Burst (GUARD_templates only)</td>
<td>(GUARD_templates only) Highest traffic peak that the Guard is allowed to pass to the zone.</td>
</tr>
<tr>
<td><strong>Attack Detection/Termination Parameters</strong></td>
<td>(GUARD_templates only)</td>
</tr>
<tr>
<td>Protection-end timer</td>
<td>Inactivity timeout that the Guard uses to terminate zone protection when there is no attack on the zone.</td>
</tr>
<tr>
<td>Malicious-rate detection threshold</td>
<td>Minimum rate of zone packets that are dropped.</td>
</tr>
<tr>
<td>Filter-rate termination threshold</td>
<td>Threshold value defined in packets per second, that together with the malicious-rate termination threshold, specifies when the Guard can deactivate dynamic filters created by policies that measure traffic rate in packets per second.</td>
</tr>
<tr>
<td>Filter-rate-pph termination threshold</td>
<td>Threshold value defined in packets per hour, that together with the filter-rate termination threshold, specifies when the Guard can deactivate dynamic filters created by policies that measure traffic rate in packets per hour.</td>
</tr>
<tr>
<td>Malicious-rate termination threshold</td>
<td>Threshold value, that together with the filter-rate termination threshold, specifies when the Guard can deactivate dynamic filters.</td>
</tr>
<tr>
<td><strong>Activation Parameters</strong> (GUARD_templates only)</td>
<td></td>
</tr>
<tr>
<td>Activation interface</td>
<td>Protection activation method that defines how the Guard identifies the zone for which it activates zone protection when it receives an external indication.</td>
</tr>
<tr>
<td>Activation extent</td>
<td>Scope of protection that the Guard activates to protect a zone (entire zone or a part of the zone) when the Guard receives an external indication to activate zone protection.</td>
</tr>
<tr>
<td><strong>Packet Dump Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Auto Packet Dump</td>
<td>State of the auto packet-dump capture function (on or off).</td>
</tr>
<tr>
<td>Max. disk space</td>
<td>Maximum amount of disk space (in megabytes) to use for auto packet dumps.</td>
</tr>
</tbody>
</table>
Table 4-4 describes the information that displays in the IP address table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Zone IP address.</td>
</tr>
<tr>
<td>Mask</td>
<td>Zone IP address mask.</td>
</tr>
<tr>
<td>Type</td>
<td>IP address to include or exclude from the zone IP address range (regular or excluded).</td>
</tr>
</tbody>
</table>

To modify the zone configuration, select one of the following function buttons:

- **Config**—Modify the general configuration parameters. The Zone Configuration Form appears. For information on each of the editable zone configuration fields, see Table 4-2 in the “Creating a Zone from a Zone Template” section.

- **Add**—Add an IP address to the zone configuration. The Zone IP Form appears. For information about each of the editable IP address fields, see the “Adding an IP Address to the Zone IP Address Range” section.

- **Delete**—Delete an IP address to the zone configuration. For information on deleting an IP address from the zone configuration, see the “Deleting an IP Address from the Zone IP Address Range” section.

## Deleting a Zone

To delete one or more zones, perform the following steps:

**Step 1** Click **Detector Summary** from the navigation pane. The Detector Summary menu appears.

**Step 2** Choose **Zones > Zone list** from the Detector module main menu. The Zone list screen appears.

**Step 3** Check the check box next to each zone that you want to delete, and then click **Delete**. To delete all the zones listed, check the check box in the header (next to Zone), and then click **Delete**. The Validation form appears.

**Step 4** Click **OK** to delete the zone.
Configuring Zone Filters

This chapter describes how to configure the zone filters that process the zone traffic on the Cisco Traffic Anomaly Detector Module (Detector module).

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding Zone Filters
- Managing Bypass Filters
- Managing Flex-Content Filters
- Managing User Filters for GUARD Zones

Understanding Zone Filters

The Detector module uses zone filters to manage traffic flow when protecting the zone or learning the zone traffic characteristics. Zone filters enable the Detector module to perform the following functions:

- Analyze zone traffic for anomalies
- Bypass the Detector module anomaly detection features

You can configure a set of zone filters that provide the Detector module with zone-specific rules for traffic management and Distributed Denial of Service (DDoS) attack anomaly detection. When you modify the configuration of a zone filter, the change is saved to the zone configuration and takes effect immediately.

The Detector module uses the following types of filters:

- Bypass filters—Prevent the Detector module from handling specific traffic flows. You can prevent the Detector module from analyzing trusted traffic by directing the traffic away from the Detector module anomaly detection features.
- Flex-content filters—Count a specific traffic flow that can filter according to fields in the IP and TCP headers, the payload content, and complex Boolean expressions.
Managing Bypass Filters

The bypass filter prevents the Detector module from analyzing specific traffic flows. You can configure a bypass filter to direct trusted traffic away from the Detector module anomaly detection features.

When you display the list of bypass filters in the following procedures, the Count column indicates the current bypass filter traffic rate, which is measured in packets per second (pps).

This section contains the following topics:
- Adding a Bypass Filter
- Deleting a Bypass Filter

Adding a Bypass Filter

To add a bypass filter, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the navigation pane, select a zone. The zone main menu appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the zone main menu, choose Configuration &gt; Filters &gt; Bypass filters. The Bypass Filters screen appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add. The Add Bypass Filters screen appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure the parameters of the new bypass filter. Table 5-1 describes the filter parameters listed in the Bypass Filter form.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5-1 Bypass Filter Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Source IP</td>
</tr>
<tr>
<td>Source subnet</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>
Managing Bypass Filters

Step 5
Choose one of the following options:

- **OK**—Saves the new bypass filter configuration. The Bypass Filters screen appears. If the zone was created using a Guard zone template, the bypass filter is added to both the Guard and the Detector module portion of the configuration files.

- **Cancel**—Exits the Bypass Filters form without saving any information. The Bypass filters screen appears.

### Deleting a Bypass Filter

To delete a bypass filter, perform the following steps:

**Step 1**
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**
From the zone main menu, choose **Configuration > Filters > Bypass filters**. The Bypass Filters screen appears.

**Step 3**
Check the check box next to each bypass filter that you want to delete and then click **Delete**. The bypass filter is deleted from the list of filters. To delete all the bypass filters listed, check the check box next to **Src IP** and then click **Delete**.

If you created the zone using a Guard zone template, the bypass filter is deleted from both the Guard and the Detector module portion of the configuration files.

### Table 5-1 Bypass Filter Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dst Port</td>
<td>Zone destination port of the traffic that you want to bypass the Detector module anomaly detection features. Enter the destination port number. To specify any source destination port, leave this field blank or enter an asterisk (*) .</td>
</tr>
</tbody>
</table>
| Fragments | Traffic type to be handled by the filter. From the Fragments drop-down list, choose one of the following options:  
  - without—Bypass filter processes nonfragmented traffic.  
  - with—Bypass filter processes fragmented traffic.  
  - *—Bypass filter processes both fragmented and nonfragmented traffic. |
Managing Flex-Content Filters

Flex-content filters filter zone traffic based on fields in the packet header or patterns in the packet payload. You can identify attacks that are based on patterns that appear in the incoming traffic. These patterns can identify known worms or flood attacks that have a constant pattern.

Note
A flex-content filter consumes a lot of CPU resources. We recommend that you limit the use of flex-content filters because they might affect the performance of the Detector module. If you are using a flex-content filter to monitor a specific attack that can be identified by a dynamic filter, such as TCP traffic to a specified port, we recommend that you filter the traffic using a dynamic filter.

The flex-content filter is a combination of a Berkley Packet Filter and a pattern filter with very selective filtering capabilities. Use the flex-content filters to count a desired packet flow and to identify a specific malicious source of traffic.

The flex-content filter applies the filtering criteria in the following order:
1. Filters packets based on the protocol and the port parameter values.
2. Filters packets based on the expression value.
3. Performs pattern matching with the pattern value on the remaining packets.

This section contains the following topics:
- Understanding the Flex-Content Expression Syntax
- Understanding the Flex-Content Filter Pattern Syntax
- Adding a Flex-Content Filter
- Deleting a Flex-Content Filter

Understanding the Flex-Content Expression Syntax

The tcpdump-expression is in the Berkley Packet Filter format and specifies the expression to be matched with the packet.

Note
You can use the tcpdump-expression to filter traffic based on the destination port and protocol. However, for network performance considerations, we recommend that you filter traffic based on these criteria using the flex-content filter protocol and port arguments.

The expression contains one or more elements. Elements usually consist of an ID (name or number) preceded by one or more qualifiers.

There are three types of qualifiers:
- Type qualifiers—Define the ID (name or number). Possible types are host, net, and port. The host type qualifier is the default.
- Direction qualifiers—Define the transfer direction. Possible directions are src, dst, src or dst, and src and dst. The direction qualifier src or dst is the default.
- Protocol qualifiers—Restrict the match to a particular protocol. Possible protocols are ether, ip, arp, rarp, tcp, and udp. If you do not specify a protocol qualifier, all protocols that apply to the type are matched. For example, port 53 means TCP or UDP port 53.
Table 5-2 describes the flex-content filter expression elements.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst host host_ip_address</td>
<td>Traffic to a destination host IP address.</td>
</tr>
<tr>
<td>src host host_ip_address</td>
<td>Traffic from a source host IP address.</td>
</tr>
<tr>
<td>host host_ip_address</td>
<td>Traffic to and from both source and destination host IP addresses.</td>
</tr>
<tr>
<td>net net mask mask</td>
<td>Traffic to a specific network.</td>
</tr>
<tr>
<td>net net/len</td>
<td>Traffic to a specific subnet.</td>
</tr>
<tr>
<td>dst port destination_port_number</td>
<td>TCP or UDP traffic to a destination port number.</td>
</tr>
<tr>
<td>src port source_port_number</td>
<td>TCP or UDP traffic from a source port number.</td>
</tr>
<tr>
<td>port port_number</td>
<td>TCP or UDP traffic to and from both source and destination port numbers.</td>
</tr>
<tr>
<td>less packet_length</td>
<td>Packets with a length equal to or less than the specific length in bytes.</td>
</tr>
<tr>
<td>greater packet_length</td>
<td>Packets with a length equal to or greater than the specific length in bytes.</td>
</tr>
<tr>
<td>ip proto protocol</td>
<td>Packets with a protocol number of the following protocols: ICMP, UDP, and TCP.</td>
</tr>
<tr>
<td>ip broadcast</td>
<td>Broadcast IP packets.</td>
</tr>
<tr>
<td>ip multicast</td>
<td>Multicast packets.</td>
</tr>
<tr>
<td>ether proto protocol</td>
<td>Ether protocol packets of a specific protocol number or name such as IP, Address Resolution Protocol (ARP), or Reverse Address Resolution Protocol (RARP). The protocol names are also keywords. If you enter the protocol name, you must use a backslash () as an escape character before the name.</td>
</tr>
<tr>
<td>expr relop expr</td>
<td>Traffic that complies with the specific expression. Table 5-3 describes the tcpdump-expression rules.</td>
</tr>
</tbody>
</table>

Table 5-3 describes the tcpdump-expression rules.
You can combine primitives using the following methods:

- A parenthesized group of primitives and operators (parentheses are special to the Shell and must be escaped)
- Negation—Use ! or not
- Concatenation—Use && or and
- Alternation—Use || or or

Negation has the highest precedence. Alternation and concatenation have equal precedence and are associated left to right. Explicit and tokens, not juxtaposition, are required for concatenation. If you specify an identifier without a keyword, the most recent keyword is used.

For a detailed explanation on the Berkley Packet filter configuration options, go to this website: http://www.freesoft.org/CIE/Topics/56.htm

The following example shows how to count only the unfragmented datagram and fragment zero of fragmented datagrams. This filter is implicitly applied to the TCP and UDP index operations. For instance, tcp[0] always indicates the first byte of the TCP header and never indicates the first byte of an intervening fragment:

ip[6:2]&0x1fff=0

The following example shows how to drop all TCP RST packets:

tcp[13]&4=0

The following example shows how to count all ICMP packets that are not echo requests/echo reply (ping):

"icmp [0]!=8 and icmp[0] != 0"

The following example shows how to count all TCP packets destined to port 80 that did not originate from port 1000:

"tcp and dst port 80 and not src port 1000"
Understanding the Flex-Content Filter Pattern Syntax

The pattern syntax is a regular expression that describes a string of characters. The pattern describes a set of strings without actually listing its elements. This expression is made up of normal characters and special characters. Normal characters include all printable ASCII characters that are not considered as special characters. Special characters are characters that have a special meaning and specify the type of matching that the Detector module performs on the pattern expression. The flex-content filter matches the pattern expression with the content of the packet (the packet payload). For example, the three strings `version 3.1`, `version 4.0`, and `version 5.2` are described by the following pattern: `version .*`.

Table 5-4 describes the special characters that you can use.

<table>
<thead>
<tr>
<th>Special character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.*</td>
<td>Matches a string that may be present and can contain zero or more characters. For example, the pattern <code>goo.*</code> matches <code>goos</code>, <code>goods</code>, <code>good for ddos</code>, and so on.</td>
</tr>
<tr>
<td>\</td>
<td>Removes the special meaning of a special character. To use the special characters in this list as single-character patterns, remove the special meaning by preceding each character with a backslash (<code>\</code>). For example, two backslashes (<code>\\</code>) match one backslash (<code>\</code>), and one backslash and a period (<code>\.</code>) match one period (<code>.</code>). You must also precede an asterisk (<code>*</code>) with a backslash.</td>
</tr>
<tr>
<td>\xHH</td>
<td>Matches a hexadecimal value where H is a hexadecimal digit and is not case sensitive. Hexadecimal values must be exactly two digits. For example, the pattern <code>\x41</code> matches the hexadecimal value A.</td>
</tr>
</tbody>
</table>

The following example shows how to drop packets with a specific pattern in the packet payload. The pattern in the example was extracted from the Slammer worm. The protocol, port, and tcpdump-expression are nonspecific.

`\x89\xE5Qh\.dllhel32hkernQhounthickChGetTf\xB9l1Qh32\.dhws2_f\xB9etQhsckf\xB9toQhsend\xB9\x18\x10\xAEB`

Adding a Flex-Content Filter

To add a flex-content filter, perform the following steps:

**Step 1**  From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  From the zone main menu, choose Configuration > Filters > Flex-Content filters. The Flex-Content Filters screen appears and displays the list of existing flex-content filters.

**Step 3**  Click Add. The Add Filter Step 2 screen appears.

**Step 4**  Configure the flex-content filter parameters.
Table 5-5 describes the filter parameters listed in the Flex-Content Filter form.

### Table 5-5  Flex-Content Filter Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Provides a description for the flex-content filter.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Processes traffic using a specific protocol. Enter a protocol number from 0 to 255. To specify any protocol type, enter an asterisk (*). Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid protocol numbers: <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a></td>
</tr>
<tr>
<td>Dst Port</td>
<td>Processes traffic that flows to a specific destination port. Enter a destination port number from 0 to 65535. To specify any destination port, enter an asterisk (*). Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid port numbers: <a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></td>
</tr>
<tr>
<td>Expression</td>
<td>Filters traffic based on the specified expression (see the “Understanding the Flex-Content Expression Syntax” section). Enter a string with up to 180 space-separated tokens.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Specifies the regular expression data pattern that is to be matched with the packet content (see the “Understanding the Flex-Content Filter Pattern Syntax” section). Enter the data pattern to use.</td>
</tr>
<tr>
<td>Match Case</td>
<td>Specifies whether or not the data pattern expression is case sensitive. Check the check box to define the data pattern expression as case sensitive.</td>
</tr>
<tr>
<td>Start Offset</td>
<td>Specifies the offset (in bytes) from the beginning of the packet content where the pattern matching begins. The default is 0, which is the start of the payload. The start offset applies to the pattern field. Enter an integer from 0 to 2047.</td>
</tr>
<tr>
<td>End Offset</td>
<td>Specifies the offset (in bytes) from the beginning of the packet content where the pattern matching ends. The default is the packet length, which is the end of the payload. The end offset applies to the pattern field. Enter an integer from 0 to 2047.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the action that the Detector module performs when the traffic matches the filter. The Detector module supports the count action only, which enables it to count the traffic flow packets that match the filter.</td>
</tr>
</tbody>
</table>
| Guard Action | Specifies the action that the Guard performs when the traffic matches the filter. The Guard Action field is applicable only if you created the zone using a GUARD zone template. Choose one of the following actions from the Guard Action drop-down list:  
  - count—Counts the traffic flow packets that match the filter  
  - drop—Drops the traffic flow packets that match the filter |
| State | Specifies the operating state of the flex-content filter. Choose one of the following operating states from the State drop-down list:  
  - enable—The Detector module applies the filter to the traffic flow and executes the configured action on the flow that matches the filter.  
  - disable—The Detector module does not apply the filter to the traffic flow. |
**Chapter 5: Configuring Zone Filters**

Managing User Filters for GUARD Zones

You can only configure user filters for zones that you create using a GUARD zone template because user filters are used by the Guard only. When you create a zone using a GUARD zone template, you can configure the user filters on the Detector module and then copy the zone configuration to a Guard.

The Guard activates user filters in the order in which they appear in the user filter list. User filters are activated in an ascending row-number order. When you add a new user filter, it is important that you place it in the desired location in the list.

To verify that a zone was created from a GUARD zone template, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Configuration > General. Verify that the name of the zone template begins with GUARD.

This section contains the following topics:

- Adding a User Filter
- Deleting a User Filter

---

### Deleting a Flex-Content Filter

To delete a flex-content filter, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Configuration > Filters > Flex-Content filters. The Flex-Content Filters screen appears and displays the list of existing flex-content filters.

**Step 3** Check the check box next to each flex-content filter that you want to delete and then click **Delete**. The flex-content filter is deleted. To delete all the flex-content filters listed, click the check box next to Source IP, and then click **Delete**.

If the zone was created using a Guard zone template, the flex-content filter is deleted from both the Guard and the Detector module portion of the configuration files.

---

**Step 5** Choose one of the following options:

- **OK**—Saves the new flex-content filter. The Flex-Content Filters screen appears. If the zone was created using a Guard zone template, the flex-content filter is added to both the Guard and the Detector module portion of the configuration files.
- **Clear**—Reverts the form information back to the default values and clears any information that you added.
- **Cancel**—Exits the Flex-Content Filters screen without saving any information. The Flex-Content Filters screen appears.
Adding a User Filter

To add a new user filter, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the navigation pane, choose a zone that you created using a GUARD zone template. The zone main menu appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the zone main menu, choose Configuration &gt; Filter &gt; User filters. The list of user filters appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add. The Add Filter Step 1 screen appears with the list of user filters.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Insert column, click the row below where you want to add the user filter. The Insert Here text appears, indicating that the new user filter will be inserted above the row that you selected.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Next. The Add Filter Step 2 screen appears with the User Filter form.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure the parameters of the new user filter. Table 5-6 describes the filter parameters listed in the User Filter form.</td>
</tr>
</tbody>
</table>

Table 5-6   User Filter Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Directs traffic from a specific IP address to the user filter. Enter the source IP address. To specify any source IP address, leave this field blank or enter an asterisk (*).</td>
</tr>
<tr>
<td>Source subnet</td>
<td>Directs traffic from a specific subnet to the user filter. Choose the subnet from the Source subnet drop-down list.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Directs traffic from a specific protocol to the user filter. Enter the protocol number. To specify any protocol, leave this field blank or enter an asterisk (*).</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Directs traffic destined to a specific port to the user filter. Enter the destination port number. To specify any destination port, leave this field blank or enter an asterisk (*).</td>
</tr>
</tbody>
</table>
| Fragments  | Specifies the traffic type to be processed by the user filter. From the Fragments drop-down list, choose one of the following:  
  - without—User filter processes nonfragmented traffic.  
  - with—User filter processes fragmented traffic.  
  - *—User filter processes fragmented and nonfragmented traffic. |
| Rate       | Specifies the rate limitation. The user filter limits the traffic to the rate specified. Enter the rate limit value in the Rate field, and then choose the unit of measurement to use from the Rate drop-down list. Choose unlimit for the unit of measurement if you do not want the user filter to limit the traffic rate. |
| Burst      | Specifies the traffic burst limit. The user filter uses the same unit of measurement for the burst that you chose for rate (see the Rate entry in this table). |
Table 5-6  User Filter Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Action    | Specifies the action that the Guard executes when the traffic matches the filter. Choose one of the following actions from the Action drop-down list:  
  - permit—Prevents statistical analysis of the flow and anti-spoofing or anti-zombie protection functions from handling this flow. We recommend that you set a rate and burst limit to a filter with an action of permit because the traffic that the filter processes is not handled by other protection functions.  
  - basic/redirect—Authenticates applications over HTTP.  
  - basic/reset—Authenticates applications over TCP. We recommend that you use an action of basic/redirect for HTTP traffic flows.  
  - basic/safe-reset—Authenticates TCP application traffic flows that are not tolerant of a TCP connection reset. We recommend that you use an action of basic/redirect for HTTP traffic flows.  
  - basic/default—Authenticates non-TCP traffic flows.  
  - basic/dns-proxy—Authenticates TCP DNS traffic flows.  
  - basic/sip—Authenticates Voice-over IP (VoIP) protocols using Session Initiation Protocol (SIP) over UDP to establish the VoIP sessions and the Real-Time Transport Protocol/Real-Time Control Protocol (RTP/RTCP) to transmit voice data between the SIP endpoints after sessions are established.  
  - strong—Provides strong authentication for a traffic flow or you can use this action when the previous filters do not seem suitable for the application. Authentication is performed for every connection.  
  
  For TCP incoming connections, the Guard serves as a proxy. We recommend that you do not use this action for connections if you use access control lists, access policies, or load-balancing policies that are based on the incoming IP address in the network.  
  - drop—Drops traffic flows. |

Step 7  Choose one of the following options:  
  - OK—Saves the new user filter configuration. The User Filters screen appears.  
  - Cancel—Exits the User Filters form without saving any information. The User filters screen appears.
Deleting a User Filter

Caution
If you delete all user filters when the policy action is set to to-user-filter and then copy the zone configuration to a Guard, the Guard may pass unprotected traffic to the zone.

To delete a user filter, perform the following steps:

Step 1 From the navigation pane, choose a zone that you created using a GUARD zone template. The zone main menu appears.

Step 2 From the zone main menu, choose Configuration > Filters > User filters. The list of zone user filters appears.

Step 3 Check the check box next to the user filter to delete.

Step 4 Click Delete. The user filter is removed from the list of user filters.
Configuring Policy Templates

This chapter describes how to configure the zone policy templates that the Cisco Traffic Anomaly Detector Module (Detector module) uses to create zone policies.

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding Policy Templates
- Modifying the Configuration of a Policy Template

Understanding Policy Templates

A policy template is a collection of policy construction rules that the Detector module uses to create the zone policies during the policy construction phase of the learning process. When you create a new zone, the Detector module includes a set of policy templates in the zone configuration. Based on the characteristics of the zone traffic, each policy template enables the Detector module to produce a group of policies during the policy construction phase. The Detector module uses the policies to monitor the zone traffic for anomalies that indicate an attack on the zone. The zone policies are configured to take action against a particular traffic flow if the flow exceeds the policy thresholds.

Changes that you make to a zone policy template configuration affect the policy construction phase. Using the WBM, you can enable, disable, or modify the zone policy templates to control the policies that the Detector module creates during the policy construction phase.

To match the services of a traffic flow, the Detector module uses several types of policy templates during the policy construction phase. The name of the policy template is derived from the characteristics that are common to all the policies that it creates and can be a protocol such as Domain Name System (DNS), an application such as HTTP, or an objective such as ip_scan. For example, the policy template tcp_connections produces policies that relate to a connection, such as the number of concurrent connections.
Table 6-1 describes the Detector module policy template types.

Table 6-1  Policy Templates

<table>
<thead>
<tr>
<th>Policy template</th>
<th>Produces a set of policies relating to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns_tcp</td>
<td>DNS-TCP protocol traffic.</td>
</tr>
<tr>
<td>dns_udp</td>
<td>DNS-UDP protocol traffic.</td>
</tr>
<tr>
<td>fragments</td>
<td>Fragmented traffic.</td>
</tr>
<tr>
<td>http</td>
<td>HTTP traffic that flows, by default, through port 80 (or other user-configured ports).</td>
</tr>
<tr>
<td>ip_scan</td>
<td>IP scanning. A situation in which a client from a specific source IP address tries to access many destination IP addresses in the zone. This policy template is designed primarily for zones in which the IP address definition is a subnet. By default, this policy template is disabled. The default action for this policy template is notify. <strong>Note</strong> The policies that are produced from this policy template are resource consuming and can affect your network’s performance.</td>
</tr>
<tr>
<td>other_protocols</td>
<td>Non-TCP and non-UDP protocols.</td>
</tr>
<tr>
<td>port_scan</td>
<td>Port scanning. A situation in which a client from a specific source IP address tries to access many ports in the zone. By default, this policy template is disabled. The default action for this policy template is notify. <strong>Note</strong> The policies that are produced from this policy template are resource consuming and can affect your network’s performance.</td>
</tr>
<tr>
<td>tcp_connections</td>
<td>TCP connection characteristics.</td>
</tr>
<tr>
<td>tcp_not_auth</td>
<td>TCP connections that the Detector module anti-spoofing feature have not authenticated.</td>
</tr>
<tr>
<td>tcp_outgoing</td>
<td>TCP connections initiated by the zone.</td>
</tr>
<tr>
<td>tcp_ratio</td>
<td>Ratios between different types of TCP packets, such as SYN packets versus FIN/RST packets.</td>
</tr>
<tr>
<td>tcp_services</td>
<td>TCP services on ports other than HTTP-related ports, such as ports 80 and 8080.</td>
</tr>
<tr>
<td>udp_services</td>
<td>UDP services.</td>
</tr>
</tbody>
</table>
The Detector module includes additional policy templates for zones that were created from specific zone templates as described in Table 6-2.

### Table 6-2 Specific Policy Templates

<table>
<thead>
<tr>
<th>Zone Template</th>
<th>Policy Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>DETECTOR_WORM</td>
<td>worm_tcp—Constructs a group of policies relating to TCP worms. Worm TCP policies manage worm attacks, in which one or more source IP addresses create many nonestablished connections on the same port to many destination IP addresses. This policy template is designed primarily for zones in which the IP address definition is a subnet. The Detector module adds services to policies that are created from this policy template during the threshold tuning phase of the learning process instead of during the policy construction phase. The policy template parameters, max_services and min_threshold, do not apply to this policy template.</td>
</tr>
</tbody>
</table>

If you create a zone from a GUARD_ zone template, you can configure the parameters of additional policy templates that can be synchronized to a Guard. The Guard supports the following additional policy templates:

- **tcp_services_ns**—TCP services. By default, the policies created by the tcp_services_ns template relate to IRC ports (666X), Secure Shell (SSH), and Telnet. This policy template does not create policies with actions that apply the Strong protection level to the traffic flow.

- **tcp_connections_ns**, **tcp_outgoing_ns**, and **http_ns**—The Guard includes additional policy templates that can protect zones for which you do not want to use the TCP proxy anti-spoofing functions. You can use these policy templates if the zone is controlled based on the IP addresses, such as an Internet Relay Chat (IRC) server-type zone, or if you do not know the type of services that are running on the zone.

- If you define a zone with the GUARD_TCP_NO_PROXY zone template, the Guard replaces the policy templates http, tcp_connections, and tcp_outgoing with the policy templates http_ns, tcp_connections_ns, and tcp_outgoing_ns policies. The http_ns, tcp_connections_ns, and tcp_outgoing_ns policy templates do not create policies with actions that require the Guard to use the Strong protection level.
Modifying the Configuration of a Policy Template

During the learning process, the Detector module analyzes a copy of the zone traffic. Each active policy template produces a group of policies based on the policy definitions and the zone traffic characteristics. The Detector module ranks the services (protocol and port numbers) that the policy template monitors by the traffic volume level. The Detector module then selects the services that have the highest traffic volume and that have exceeded the defined minimum threshold, and it creates a policy for each service. Some of the policy templates create an additional policy to handle all traffic flows for which a specific policy was not added with a service of any.

You can modify policy template parameters as follows to manage the policy construction phase:

- Enable or disable the policy template. Only enabled policy templates can produce policies during the policy construction phase.
- Control when the policy template creates policies during the learning process based on the volume of traffic for a service.
- Define the maximum number of policies that the Detector module can produce using the policy template during the policy construction phase.

To modify the configuration of a policy template, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Configuration > Policy templates > View. The Policy Templates screen appears.

**Step 3** Choose a policy template. The Config Policy Template screen appears.

**Step 4** Modify the desired parameters of the policy template. Table 6-3 describes the policy template parameters that are listed in the Policy Template form. Depending on the type of policy template selected, some or all of the parameters listed in the table display for editing.

<table>
<thead>
<tr>
<th>Table 6-3 Policy Template Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Caution** Disabling a policy template may seriously compromise the ability of the Detector module to detect zone traffic anomalies. When you disable a policy template, the Detector module does not produce policies to manage the type of malicious traffic that the policy template is designed to manage.
Step 5 Choose one of the following options:

- **OK**—Saves the new policy template configuration. The Policy Template screen appears.
- **Clear**—Reverts the form information back to the default values and clears any information that you added.
- **Cancel**—Exits the Config policy template screen without saving any information. The Policy Template screen appears.
To add or remove services from all policies that were created from a specific policy template, see the “Adding a Service” or the “Deleting a Service” sections in Chapter 8, “Managing Zone Policies.”
Learning Zone Traffic

This chapter describes how to use the Cisco Traffic Anomaly Detector Module (Detector module) learning process to analyze zone traffic characteristics to create and tune the policies that the Detector module uses for zone anomaly detection.

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding the Learning Process
- Performing the Learning Process
- Performing the Learning Process Using Detect and Learn
- Marking the Zone Policies as Tuned or Untuned
- Managing Learning Process Snapshots
- Comparing Policy Configurations of Two Zones or Snapshots
Understanding the Learning Process

The learning process creates a baseline of normal zone traffic patterns. The baseline reference points are the zone policies, which enable the Detector module to determine when an anomaly exists in the zone traffic.

Use the learning process to optimize zone anomaly detection as follows:

- Create policies based on the services of the zone traffic.
- Tune the policy thresholds of a new zone that is configured with the default policies and policy thresholds of the zone template.
- Update an existing zone configuration when the zone traffic patterns change.

You activate the learning process during peak traffic times and when you are certain that there is no attack on the zone. During the learning process, the Detector module constructs the zone policies based on the traffic services and tunes the policy thresholds based on the traffic rates. While the Detector module learns the zone traffic, you can monitor the learning process and decide whether to accept or reject the current results of the learning process.

This section contains the following topics:

- Understanding the Phases of the Learning Process
- Understanding the Detect and Learn Feature
- Managing the Results of the Learning Process

Understanding the Phases of the Learning Process

The learning process consists of the following two phases:

- **Policy construction phase**—The Detector module analyzes the zone traffic to determine the services that the zone uses and then creates the zone policies using the policy templates for each service. The policy templates determine the default threshold value and policy action assigned to each new policy. The new policies override the existing ones.

  The policy templates define the types of zone policies that the Detector module creates. The policy templates also define the maximum number of services that the Detector module monitors closely and the minimum threshold that triggers the Detector module to create new policies. To change the rules for constructing zone policies, you must modify the policy template parameters before you initiate the policy construction phase. For information about modifying a policy template, see Chapter 6, “Configuring Policy Templates.”

  **Note**
  You cannot perform the policy construction phase on zones you create with a Guard_Link and the Detector_Link zone template.

- **Threshold tuning phase**—The Detector module tunes the traffic rate thresholds of the zone policies to values that allow normal traffic to be analyzed by the Detector module without activating a policy action. When looking for anomalies in the zone traffic, the Detector module applies the zone policies to the traffic flow and if the traffic exceeds a policy threshold, the Detector module creates a dynamic filter with the policy action.
Note

If the zone configuration contains the worm_tcp policy template, the Detector module uses the threshold tuning phase for both policy construction and threshold tuning.

To allow the learning process to take place, you must configure the switch to capture the traffic that is sent to the zone and pass a copy of it to the Detector module.

Understanding the Detect and Learn Feature

After the Detector module performs the policy construction phase of the learning process, you can activate the Detect and Learn feature that allows the Detector module to look for traffic anomalies (Detect) while performing the threshold tuning phase (Learn) simultaneously. With Detect and Learn activated, the Detector module can constantly update the policy thresholds based on normal zone traffic characteristics. When the Detector module detects an attack on the zone, it stops the learning process to prevent it from learning malicious traffic thresholds.

Managing the Results of the Learning Process

You can accept or reject the results of a policy construction or a threshold tuning phase when you stop the learning phase. You can also accept the current results and continue the learning phase. During either phase of the learning process, the Detector module does not modify the policies of the zone configuration until after you accept the results of the learning phase, at which time the Detector module updates the zone configuration and begins operating with the new policies or policy thresholds.

You can also save the current results of either learning phase at any time of the learning process by using the snapshot feature. A snapshot of the learning process allows you to save and view the policy information that the Detector module has created up to the point of the snapshot without affecting the current zone configuration. You can take as many snapshots as you like and you can update the zone configuration with the policy information saved in a snapshot at any time. For more information about using snapshots, see the “Managing Learning Process Snapshots” section.

Performing the Learning Process

This section describes how to start and stop the two different phases of the learning process; policy construction and threshold tuning. To ensure that the results of the learning process are accurate and configured for normal zone traffic, activate the learning process when the following zone traffic conditions exist:

- Zone traffic is normal (not experiencing an attack)—Ensures that the Detector module does not construct and tune the zone policies based on the traffic characteristics of a Distributed Denial of Service (DDoS) attack. If you initiate the learning process when the zone is under attack, the Detector module learns the traffic patterns of the attack and saves the learning results as the baseline for future reference. In this situation, the Detector module may not be able to detect future attacks because it may view the attacks as normal traffic conditions.
- Zone traffic is at its peak volume—Allows the Detector module to configure the policy thresholds to values that are appropriate for normal peak traffic and ensures that the Detector module does not perceive normal peak traffic conditions as an attack.
Performing the Learning Process

This section contains the following topics:

- Starting the Policy Construction Phase
- Accepting the Current Results of the Policy Construction Phase
- Stopping the Policy Construction Phase
- Starting the Threshold Tuning Phase
- Accepting the Current Results of the Threshold Tuning Phase
- Stopping the Threshold Tuning Phase

Starting the Policy Construction Phase

You can activate the policy construction phase after creating a new zone or when the zone configuration needs updating with new service policies. To allow the Detector module enough time to receive and analyze an accurate representation of normal zone traffic, we recommend that you let the policy construction phase run for at least 2 hours before terminating this phase.

Note

You cannot perform the policy construction phase on a zone that you create with one of the Guard_Link or Detector_Link zone templates.

Note

If the zone configuration uses the worm_tcp policy template, the Detector module uses the threshold tuning phase to construct worm policies and tune the threshold of each policy that it creates (see the “Starting the Threshold Tuning Phase” section).

After performing the policy construction phase, activate the threshold tuning phase to tune each policy threshold.

To start the policy construction phase, perform the following steps:

Step 1

From the navigation pane, choose a zone. The zone main menu appears.

Step 2

From the zone main menu, choose Learning > Construct Policies.

The zone status icon changes to Learning.

The Detector module begins analyzing the copy of the zone traffic for the services in the traffic flow and creates policies for the services that it detects. The Detector module does not replace the current policies in the zone configuration with the new policies until you accept the results of the policy construction phase (see the “Accepting the Current Results of the Policy Construction Phase” section).

Step 3

(Optional) Choose Learning > Snapshot at any time during the phase to save and review the current results and policy suggestions of the policy construction phase. Saving a snapshot does not change the current zone configuration. For more information about using snapshots, see the “Managing Learning Process Snapshots” section.
Accepting the Current Results of the Policy Construction Phase

To accept the results of the learning process but allow the Detector module to continue learning the zone traffic characteristics, perform the following steps:

**Step 1**  From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  From the zone main menu, choose **Learning > Accept**.

The Detector module deletes all of the current policies of the zone configuration and replaces them with the suggested zone policies. The Detector module does not stop the policy construction phase and continues to learn the zone services.

Stopping the Policy Construction Phase

To stop the policy construction phase, perform the following steps:

**Step 1**  From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  From the zone main menu, choose **Learning > Stop Learning**. The Stop Learning window opens.

**Step 3**  Choose one of the following options:

- **Reject**—Rejects the suggested zone policies
- **Accept**—Accepts the suggested zone policies

**Step 4**  Choose one of the following options:

- **OK**—The results of this selection vary depending on your choice to reject or accept the results of the policy construction phase:
  - If you chose **Reject**, the Detector module deletes all of the suggested zone policies. No changes are made to the zone configuration.
  - If you chose **Accept**, the Detector module replaces the current policies in the zone configuration with the suggested zone policies and then terminates the policy construction phase.
- **Clear**—The Stop Learning window reverts to its default setting of Accept.
- **Cancel**—The Stop Learning window closes and the policy construction phase continues.

Activate the threshold tuning phase after you accept the results of the policy construction phase. The threshold tuning phase ensures that the threshold values of the accepted policies are configured specifically for the zone traffic rates. Until you run the threshold tuning phase, the policies are configured with factory-default threshold values. For more information, see the “Starting the Threshold Tuning Phase” section.

Starting the Threshold Tuning Phase

You can activate the threshold tuning phase after performing the policy construction phase or any time that the zone policy thresholds need updating.
Performing the Learning Process

To allow the Detector module enough time to receive and analyze an accurate representation of the normal zone traffic, we recommend that you allow the threshold tuning phase to run for at least 24 hours before terminating this phase.

To start the threshold tuning phase, perform the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu appears.
Step 2  From the zone main menu, choose Learning > Tune Threshold.

The zone status learning icon appears in the work area next to the zone name in the navigation panel.

The Detector module begins analyzing the zone traffic and adjusts the threshold values of the zone policies to the characteristics of the traffic flow. The Detector module does not save the changes to the zone configuration until you accept the results of the threshold tuning phase (see the “Accepting the Current Results of the Threshold Tuning Phase” section).

Step 3  (Optional) From the zone main menu, choose Learning > Snapshot at any time during the phase to save and review the current results and threshold suggestions of the threshold tuning phase. Saving a snapshot does not change the current zone configuration.

For details about using snapshots, see the “Managing Learning Process Snapshots” section.

Accepting the Current Results of the Threshold Tuning Phase

To accept the current results of the threshold tuning phase and allow the Detector module to continue the threshold tuning phase, perform the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu appears.
Step 2  From the zone main menu, choose Learning > Accept. The Accept Thresholds window opens.
Step 3  Define the threshold selection method to use. Table 7-1 describes the parameters listed in the Accept Thresholds window.
Performing the Learning Process

Step 4

Choose one of the following options:

- **OK** — The Detector module updates the policies of the zone configuration with the current results of the threshold tuning phase and the threshold tuning phase continues.
- **Clear** — The Accept Thresholds window reverts to its default settings.
- **Cancel** — The Accept Thresholds window closes and the policy construction phase continues.

### Stopping the Threshold Tuning Phase

To accept or reject the current results of the threshold tuning phase and stop the threshold tuning phase, perform the following steps:

**Step 1**

From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**

From the zone main menu, choose **Learning > Stop Learning**. The Stop Learning window opens.

**Step 3**

Choose one of the following options from the Stop Learning window:

- **Reject** — Ignores the current results of the threshold tuning phase.
- **Accept** — Uses the current results of the threshold tuning phase in the zone configuration. Define the threshold selection method to use.
Table 7-2 describes the threshold selection method parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold selection method</td>
<td>Method for selecting the thresholds to accept. Choose one of the following options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Accept new thresholds—Saves the results of the learning process to the zone configuration.</td>
</tr>
<tr>
<td></td>
<td>• Accept max. thresholds—Compares the current policy threshold to the learned threshold and saves the higher of the two to the zone configuration. This is the default method.</td>
</tr>
<tr>
<td></td>
<td>• Accept weighted thresholds—Calculates the policy thresholds to save based on the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
<tr>
<td></td>
<td>Enter the weight value in the Weight field.</td>
</tr>
<tr>
<td></td>
<td>• Keep current thresholds—Rejects all of the suggested threshold values of the learning process and the policies retain their current thresholds.</td>
</tr>
<tr>
<td>Weight</td>
<td>Defines the weight that the Detector module uses to calculate new thresholds. This option is active only when you choose the Accept weighted thresholds method. Enter a weight value for the Detector module to use in the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
</tbody>
</table>

Step 4 Choose one of the following options:

- **OK**—The Detector module updates the policies of the zone configuration with the current results of the threshold tuning phase and stops the threshold tuning phase.
- **Clear**—The Stop Learning window reverts to its default settings.
- **Cancel**—The Stop Learning window closes and the threshold phase continues.
Performing the Learning Process Using Detect and Learn

This section describes how to manage the Detect and Learn operation in which the Detector module looks for anomalies in the zone traffic while learning the zone traffic and making policy threshold adjustments. The Detector module stops the learning process when it detects an attack on the zone.

Before you activate Detect and Learn, you can configure when and how the Detector module accepts the results of the learning process.

This section contains the following topics:
- Configuring the Automatic Learning Parameters
- Activating Detect and Learn
- Deactivating Detect and Learn

Configuring the Automatic Learning Parameters

You can configure the automatic learning parameters to control when and how the Detector module automatically accepts the current results of the learning process (threshold tuning phase) when you activate Detect and Learn.

To configure the automatic learning parameters, perform the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu appears.
Step 2  From the zone main menu, choose Configuration > Policies > Learning Parameters. The Learning Parameters screen appears.
Step 3  Click Config. The Config Learning Parameters screen appears.
Step 4  Define the automatic learning parameters.
Table 7-3 describes the learning parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone is tuned</td>
<td>Marks the zone policies as follows:</td>
</tr>
<tr>
<td></td>
<td>• Tuned—Choose this option to mark the policies tuned, allowing the Detector module to immediately use the policies to detect anomalies in the zone traffic.</td>
</tr>
<tr>
<td></td>
<td>• Untuned—Deselect this option to mark the policies untuned, requiring you to accept the results of the threshold tuning phase before the Detector module can detect anomalies in the zone traffic. See the “Marking the Zone Policies as Tuned or Untuned” section for more information.</td>
</tr>
<tr>
<td>Set periodic learning</td>
<td>Enables the automatic learning process. Configure the following learning parameters when you choose this option:</td>
</tr>
<tr>
<td></td>
<td>• Learning cycle—Defines how often the Detector module saves the results of the learning process. Define the time period between saves in terms of weeks, days, hours, and minutes. Enter an integer from 0 to 1000 for each of the time fields.</td>
</tr>
<tr>
<td></td>
<td>• Learning results—Defines how the Detector module saves the results of the learning process. Choose one of the following methods:</td>
</tr>
<tr>
<td></td>
<td>‒ Automatic accept—Accepts the results of the learning process (policy thresholds) that the Detector module suggests at the specified interval. The Detector module saves a snapshot of the zone policies after accepting the newly suggested ones.</td>
</tr>
<tr>
<td></td>
<td>‒ Snapshot only—Saves a snapshot of the learning process (policy thresholds) at the specified interval. The Detector module does not accept the new policies and does not modify the policy thresholds in the zone configuration.</td>
</tr>
</tbody>
</table>
Performing the Learning Process Using Detect and Learn

Step 5

Choose one of the following options:

- **OK**—The Detector module saves the automatic learning parameters to the zone configuration.
- **Clear**—The Learning Parameters form reverts to its default settings.
- **Cancel**—The Config learning parameters screen closes.

### Activating Detect and Learn

Before activating Detect and Learn, you should verify whether the zone policies are marked as tuned or untuned because the Detector module functions differently depending on the tuned state of the zone policies. If the policies are marked as tuned when you activate Detect and Learn, the Detector module detects attacks and learns the zone traffic. If you activate Detect and Learn and the zone policies are marked as untuned, the Detector module functions in the following ways until the first time that the zone policy thresholds are accepted:

- The Detector module does not detect attacks in zone traffic.
- The Detector module activates a threshold selection method of Accept new thresholds (see the “Configuring the Automatic Learning Parameters” section).

After the first time that the zone policy thresholds are accepted, the Detector module marks the policies as tuned, which enables it to detect attacks while learning the zone traffic.

For more information about marking policies as tuned or untuned, see the “Marking the Zone Policies as Tuned or Untuned” section.

### Table 7-3 Learning Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold selection method</td>
<td>Defines the method that the Detector module uses to select the thresholds to accept. Choose one of the following options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Accept new thresholds—Saves the results of the learning process to the zone configuration.</td>
</tr>
<tr>
<td></td>
<td>• Accept max. thresholds—Compares the current policy threshold to the learned threshold and saves the higher of the two to the zone configuration. This is the default method.</td>
</tr>
<tr>
<td></td>
<td>• Accept weighted thresholds—Calculates the policy thresholds to save based on the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
<tr>
<td></td>
<td>Enter the weight value in the Weight field.</td>
</tr>
<tr>
<td>Weight</td>
<td>Defines the weight that the Detector module uses to calculate new thresholds. This option is active only when you select the Accept weighted thresholds method. Enter a weight value for the Detector module to use in the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
</tbody>
</table>
To activate Detect and Learn, perform the following steps:

**Step 1**  
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  
Click **Detect and Learn**.

You can also activate the threshold tuning phase of the learning process (from the zone main menu, choose **Learning > Tune Thresholds**) and zone anomaly detection (click **Detect**) separately. The order in which you activate the two operations does not matter.

The following actions occur:

- The Detector module begins analyzing the traffic flow for traffic anomalies.
- The Detector module begins the threshold tuning phase of the learning process.
- The zone name is added to the Under Detection list in the navigation pane and the Recent Events table lists an event type of *detection-start* with a detail listing of *Zone is under detection*.

**Deactivating Detect and Learn**

When you deactivate Detect and Learn, the Detector module allows you to deactivate one or both of the operations.

To deactivate Detect and Learn, perform the following steps:

**Step 1**  
From the navigation pane, choose a zone under detection. The zone main menu and the zone status screen appear.

**Step 2**  
Deactivate Detect and Learn using one of the following methods:

- From the zone status screen, click **Deactivate**.
- From the zone main menu, choose **Detection > Deactivate**.

The Deactivate window opens.

**Step 3**  
Check the check box next to the requested action. Choose one or both of the following actions:

- **Stop Detection**—Stops zone anomaly detection.
- **Stop Learning**—Stops the threshold tuning phase of the learning process. Choose one of the following options:
  - **Reject**—Ignores the current results of the threshold tuning phase.
  - **Accept**—Saves the current results of the threshold tuning phase to the zone configuration. Define the threshold selection method to use.
Table 7-4 describes the threshold selection method parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold selection method</td>
<td>Defines the method that the Detector module uses to select the thresholds to accept. Choose one of the following options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Accept new thresholds—Saves the results of the learning process to the zone configuration.</td>
</tr>
<tr>
<td></td>
<td>• Accept max. thresholds—Compares the current policy threshold to the learned threshold and saves the higher of the two to the zone configuration. This is the default method.</td>
</tr>
<tr>
<td></td>
<td>• Accept weighted thresholds—Calculates the policy thresholds to save based on the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
<tr>
<td></td>
<td>Enter the weight value in the Weight field.</td>
</tr>
<tr>
<td></td>
<td>• Accept current—Rejects the suggested threshold values of the learning process. The policies retain their prethreshold tuning phase values.</td>
</tr>
<tr>
<td>Weight</td>
<td>Defines the weight that the Detector module uses to calculate new thresholds. This option is active only when you choose the Accept weighted thresholds method. Enter a weight value for the Detector module to use in the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
</tbody>
</table>

The zone name is removed from the Protected Zones listing in the navigation pane and the Recent Events table lists an event type of detection-stop with a detail listing of Zone is not under detection. The zone status icon changes to Standby 🔄.
Marking the Zone Policies as Tuned or Untuned

The tuned state of the zone policies relates to the threshold values of the policies. The Detector module considers zone policies to be either tuned or untuned depending on the following conditions:

- **Untuned**—The zone policy thresholds may not be set to values that are appropriate for the zone traffic. The Detector module marks the zone policies untuned when you perform one of the following actions:
  - Create a new zone
  - Accept the policy construction phase results for a zone
  - Add a service to the zone policies or remove a service from the zone policies

- **Tuned**—The zone policy thresholds are set to values that are appropriate for the zone traffic. The Detector module marks the zone tuned after accepting the results of the threshold tuning phase, at which point the threshold values are tuned specifically to the zone traffic characteristics.

Knowing the tuned state of the zone is important when you activate Detect and Learn for the zone. If the tuned state of the zone is untuned when you activate Detect and Learn, the Detector module is unable to detect attacks on the zone until after the first time that it accepts the results of the threshold tuning phase. The Detector module can accept the results of the threshold tuning phase based on the automatic learning parameters (see the “Configuring the Automatic Learning Parameters” section) or you can manually accept the results. The Detector module uses the Accept new thresholds setting to accept the first results of the threshold tuning phase regardless of the configuration of the threshold selection method. From that point on, the Detector module uses the threshold selection method that you selected.

You can manually change the tuned state of a zone and may consider changing the state to tuned when one of the following conditions applies:

- You created the zone by copying an existing zone configuration with similar traffic characteristics.
- You have manually configured all of the policy thresholds.

You may consider changing the tuned state of the zone to untuned when one of the following conditions applies:

- A major change was made to the zone network.
- The zone IP address or subnet was modified.
- You have not initiated the Detect and Learn function during peak traffic time and want to prevent the Detector module from considering the traffic during peak time as an attack on the zone.

When you mark the zone untuned, the Detector module does not monitor the traffic for policy threshold violations and therefore, does not detect attacks on the zone.

To mark the zone as tuned or untuned, perform the following steps:

**Step 1**
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**
From the zone main menu, choose **Configuration > Policies > Learning Parameters**. The Learning parameters screen appears.

**Step 3**
Click **Config**. The Config learning parameters screen appears.

**Step 4**
From the Learning Parameters form, choose one of the following options:

- Check the **Zone is tuned** check box to mark the zone policies as tuned. The Detector module marks the policies as tuned and can immediately use the policies to detect anomalies in the zone traffic.
Panel the Zone is tuned check box to mark the zone policies as untuned. The Detector module marks the policies as untuned, requiring that you accept the results of the threshold tuning phase before the Detector module can use the policies to detect anomalies in the zone traffic.

**Step 5**

Choose one of the following options:

- **OK**—The Detector module saves the tuned setting to the zone configuration.
- **Clear**—The Detector module discards your changes and the form displays the current configuration.
- **Cancel**—The Config learning parameters screen closes.

For more information about the Learning Parameter form options, see the “Configuring the Automatic Learning Parameters” section.

### Managing Learning Process Snapshots

The Detector module snapshot feature allows you to save zone policy information so that you can view and compare policies. Using the snapshot feature, you can perform the following tasks:

- View the current results of the learning process.
- Save the snapshot policy information to the zone configuration.
- Compare the policy results of the snapshot with another snapshot or zone configuration (see the “Comparing Policy Configurations of Two Zones or Snapshots” section).
- Back up the current zone policies contained in the zone configuration.

At any stage of the learning process, you can save a snapshot of the current learning parameters (services, thresholds, and other policy-related data). The Detector module continues the learning phase while it records the snapshot information. You can also save a snapshot when the Detector module is not performing the learning process to create a copy of the current zone policies.

This section contains the following topics:

- Taking a Snapshot of the Learning Process Results
- Taking a Snapshot of the Current Zone Policies
- Displaying Snapshots
- Modifying the Configuration of Snapshot Policies
- Deleting Snapshots

### Taking a Snapshot of the Learning Process Results

To take a snapshot of the current learning process results (policy construction or threshold tuning) perform the following steps:

**Step 1**

From the navigation pane, choose a zone currently in a learning phase. The zone main menu appears.

**Step 2**

From the zone main menu, choose Learning > Snapshot. The Create Snapshot screen appears.

**Step 3**

Enter a name for the snapshot in the Snapshot name field.
Managing Learning Process Snapshots

Chapter 7  Learning Zone Traffic

Step 4  From the Threshold Selection Method drop-down list, choose the threshold selection method that the Detector module uses to accept the policy thresholds:

- Accept new thresholds—Saves the results of the learning process to the zone configuration.
- Accept max. thresholds—Compares the current policy threshold to the learned threshold and saves the higher of the two to the zone configuration. This is the default method.
- Accept weighted thresholds—Calculates the policy thresholds to save based on the following formula:
  \[
  \text{new-threshold} = \left(\frac{\text{learned-threshold} \times \text{Weight} + \text{current-threshold} \times (100 - \text{Weight})}{100}\right)
  \]
  Enter the weight value in the Weight field.
- Accept current—Rejects the suggested threshold values of the learning process. The policies retain their prethreshold tuning phase values.

Step 5  If you chose the Accept weighted thresholds method, enter the weight value that the Detector module uses to calculate the thresholds in the Weight field.

Step 6  Click OK to save the snapshot. The Detector module saves the zone policies and assigns a consecutive ID number to the snapshot.

Taking a Snapshot of the Current Zone Policies

When you take a snapshot of a zone that is not learning zone traffic (the zone is either in standby or zone anomaly detection is enabled), the Detector module creates a snapshot that contains the current policy information of the zone configuration. You can use this type of snapshot to create a backup of the zone policies or for comparison purposes.

To create a snapshot of the zone configuration policies, perform the following steps:

Step 1  From the navigation pane, choose a zone that is not currently in a learning phase. The zone main menu appears.

Step 2  From the zone main menu, choose Learning > Snapshot. The Create Snapshot screen appears.

Step 3  Enter a name for the snapshot in the Snapshot name field and then click OK. The Detector module saves the zone policies and assigns a consecutive ID number to the snapshot.

Displaying Snapshots

Display snapshots to get a comprehensive view of the zone learning results.

To display the snapshot results, perform the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu appears.

Step 2  From the zone main menu, choose Learning > Snapshot List. The Snapshot List table appears.

Table 7-5 describes the fields in the Snapshot List table.
Step 3 Click on any one of the snapshot fields in the table to display a snapshot. The Policies screen appears, displaying the policies that the Detector module recorded at the time of the snapshot.

Table 7-5 Field Descriptions for the Snapshot List Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Snapshot identification number.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the snapshot. The Detector module displays (automatic) for snapshots</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Date and time that the snapshot was taken.</td>
</tr>
<tr>
<td>Snapshot Type</td>
<td>Method that was used to take the snapshot. The snapshot types are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Manual—Taken by you.</td>
</tr>
<tr>
<td></td>
<td>• Periodic—Taken by the Detector module automatically based on how you</td>
</tr>
<tr>
<td></td>
<td>have the automatic learning parameters configured (see the “Configuring</td>
</tr>
<tr>
<td></td>
<td>the Automatic Learning Parameters” section).</td>
</tr>
<tr>
<td></td>
<td>• Automatic—Taken by the Detector module automatically when the learning</td>
</tr>
<tr>
<td></td>
<td>process was activated. You can use this snapshot as a backup when the zone</td>
</tr>
<tr>
<td></td>
<td>is under attack.</td>
</tr>
<tr>
<td>Operation</td>
<td>Operation mode of the zone when the snapshot was taken. The operation mode</td>
</tr>
<tr>
<td></td>
<td>can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Threshold Tuning—Threshold tuning phase of the learning process.</td>
</tr>
<tr>
<td></td>
<td>• Policy Construction—Policy construction phase of the learning process.</td>
</tr>
<tr>
<td></td>
<td>• N/A—Neither phase of the learning process.</td>
</tr>
<tr>
<td>Accept Method</td>
<td>Method that was used to accept the thresholds. The method can be one of the</td>
</tr>
<tr>
<td></td>
<td>following:</td>
</tr>
<tr>
<td></td>
<td>• Accept new thresholds—Accepts the new thresholds.</td>
</tr>
<tr>
<td></td>
<td>• Accept max. thresholds—Compares the current policy threshold to the</td>
</tr>
<tr>
<td></td>
<td>learned threshold and saves the higher of the two to the zone configuration.</td>
</tr>
<tr>
<td></td>
<td>• Accept weighted thresholds—Calculates the policy thresholds to save based</td>
</tr>
<tr>
<td></td>
<td>on the new threshold, the current threshold, and the weight that you</td>
</tr>
<tr>
<td></td>
<td>defined.</td>
</tr>
<tr>
<td></td>
<td>• Accept current—Saves the current thresholds without modifying them.</td>
</tr>
</tbody>
</table>

Modifying the Configuration of Snapshot Policies

You can use snapshots to perform the following tasks:

• Modify the policies in a snapshot.
• Copy zone policies from the snapshot to the zone configuration.
• Compare the learning parameters of two zone snapshots to verify the outcome of the learning process and trace the differences in policies, services, and thresholds (see the “Comparing Policy Configurations of Two Zones or Snapshots” section).
To configure the snapshot policies, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose **Learning > Snapshot List**. The Snapshot List table appears.

**Step 3** Click on any one of the snapshot fields in the table to display the snapshot that you want to configure. The Policies screen appears, displaying the policies that the Detector module recorded at the time of the snapshot.

**Step 4** (Optional) Click **Configure Selection** to reconfigure the parameters of one or more of the policies. See the “Modifying Policy Parameters” section in Chapter 8, “Managing Zone Policies” for more information.

**Step 5** (Optional) Click **Add service** to add a service to the policies. See the “Adding a Service” section in Chapter 8, “Managing Zone Policies” for more information.

**Step 6** (Optional) Click **Remove service** to remove a service from the policies. See the “Deleting a Service” section in Chapter 8, “Managing Zone Policies” for more information.

**Step 7** Click **Accept Thresholds** to save the policies of the snapshot to the zone configuration.

---

### Deleting Snapshots

You can delete old snapshots to free disk space.

To delete a snapshot, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose **Learning > Snapshot List**. The list of snapshots appears and displays the ID number and name of each snapshot with the date and time that the snapshot was taken.

**Step 3** Check the check box next to the ID number of the snapshot that you want to delete or check the check box in the header row to select all the snapshots, and then click **Delete**.

The Detector module deletes the selected snapshots from the Snapshot list.
Comparing Policy Configurations of Two Zones or Snapshots

You can compare the policy configurations of two zones, two snapshots, or a zone and snapshot. The Detector module traces differences in policy configuration services, policies, and policy thresholds. When comparing the policy configurations, you select one zone or snapshot to be the base zone and the other zone or snapshot to be the compared zone. You can delete or add policy configuration attributes to the base zone. Modifying the configuration of the base zone enables you to selectively accept the learned policy attributes.

This section contains the following topics:

- Viewing Policy Configuration Differences
- Deleting Services from the Base Zone
- Adding Services to the Base Zone
- Copying Policy Parameters to the Base Zone

Viewing Policy Configuration Differences

To compare and display the policy differences of two zones or snapshots, perform the following steps:

**Step 1**  
Use one of the following methods to begin the policy comparison process:

- From the Detector module summary main menu, choose **Zones > Compare Zone policies**.
- From the zone main menu, choose **Configuration > Policies > Compare Policies**.

The Policies Comparison Query screen appears.

**Step 2**  
Define the base and compared zones.

Table 7-6 describes the Policies Comparison Query parameters.

<table>
<thead>
<tr>
<th>Parameter 1</th>
<th>Parameter 2</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Zone</td>
<td>Zone</td>
<td>Name of the zone or snapshot. To change the configuration of a zone, choose the zone as a base zone. Choose the base zone from the drop-down list.</td>
</tr>
<tr>
<td>Policy Configuration</td>
<td>Policy Configuration</td>
<td>Policy configuration of the selected base zone. The default value is the current policy configuration of the zone. You can choose snapshots of the zone policies from the drop-down list.</td>
</tr>
</tbody>
</table>
Comparing Policy Configurations of Two Zones or Snapshots

Step 3

Choose one of the following options:

- **OK**—Compares the policy configurations of the two zones. The Policy Comparison screen appears and displays the differences in services and policy parameters (see Figure 7-1).

- **Cancel**—Exits the Policies Comparison query without comparing any zone policies.

Figure 7-1 shows an example of the policy comparison tables. The policy configuration attributes that are specific to the base zone display in black and the attributes that are specific to the compared zone display in red.

### Table 7-6 Policies Comparison Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter 1</th>
<th>Parameter 2</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compared Zone</td>
<td>Zone</td>
<td>Name of the zone or snapshot being compared to the base zone. You cannot modify the configuration of the compared zone. Choose the compared zone from the drop-down list.</td>
</tr>
<tr>
<td>Policy Configuration</td>
<td>Compared Zone</td>
<td>Policy configuration of the selected compared zone. The default value is the current policy configuration of the zone. You can choose snapshots of the zone policies from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimal difference Percentage of differences between the policy configuration of the base zone and the compared zone. The Detector module compares the two zones and displays only differences in policy thresholds that are higher than the specified value. The default percentage is 100%, where the Detector module displays only policies in which one of the thresholds is at least two times greater than the other threshold.</td>
</tr>
</tbody>
</table>
The Policy Comparison screen is divided into two sections:

- **Difference in services**—The two tables in this section display the following information:
  - Services present only in the base zone policies.
  - Services missing from the base zone. The services in this list are defined only in the compared zone.

**Note** The Detector module displays a check box only next to the services that you can add to or delete from the base zone. Some services cannot be added or deleted because they are not specific services, such as those of the type `any`.

- **Difference in policy parameters**—Displays differences in the operational parameters of the policies (state, action, threshold, and proxy-threshold). Each section in the table displays the differences found in a single policy. The first row in each section displays the base zone parameters. The second row of each section displays the compared zone parameters.

### Deleting Services from the Base Zone

To delete services from the base zone configuration, perform the following steps:

- **Step 1** From the Services Only In `zonename` table, check the check boxes next to the services that you want to delete from the base zone configuration. To choose all of the table entries, check the check box in the table header.

- **Step 2** Click **Delete**. The Detector module deletes the services from the base zone configuration.

### Adding Services to the Base Zone

To add services to the base zone configuration, perform the following steps:

- **Step 1** From the Services Missing From `zonename` table, check the check boxes next to the services that you want to add to the base zone configuration. To choose all of the table entries, click the check box in the table header.

- **Step 2** Click **Add**. The Detector module adds the selected services to the base zone policy configuration.

### Copying Policy Parameters to the Base Zone

To copy the policy parameters from the compared zone to the base zone, perform the following steps:

- **Step 1** From the Difference In Policy Parameters table, check the check boxes next to the policies that you want to copy to the base zone.

The policies of the base zone display in black and the policies of the compared zone display in red. To select all of the table entries, check the check box in the table header.
Step 2  Click Copy Parameters.

The Detector module copies the selected policies from the compared zone to the base zone policy configuration. The selected policies are removed from the table.
Managing Zone Policies

This chapter describes how to modify the policies and manually tune the protection capabilities of the zone configuration on the Cisco Traffic Anomaly Detector Module (Detector module).

This chapter refers to the Cisco Guard (Guard), the companion product of the Detector module. The Guard is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding Zone Policies
- Viewing Zone Policies
- Modifying Policy Parameters
- Configuring IP Addresses and Thresholds
- Adding or Deleting a Service
- Backing Up the Zone Policies
Understanding Zone Policies

The zone policies enable the Detector module to perform a statistical analysis of the zone traffic flow. Depending on the type of policy, a policy monitors traffic for one of the following traffic characteristics:

- **Traffic rate**—Rate of traffic measured in packets per second or packets per hour. Policies that monitor traffic in packets per hour, or PPH policies, are used to monitor zone traffic for low rate zombie attacks that can last for hours or days. For more information on PPH policies, see the “Modifying Policy Parameters” section.

| Note | Only zone configurations that you create using the 6.1 or 6.1-XG software release will contain PPH policies. Zones that you created using a previous software version will not contain PPH policies. |

- **Connections**—Number of concurrent connections.
- **Packet ratio**—Ratio of one packet type to another.

A zone policy identifies a traffic flow as malicious or abnormal when the flow exceeds the policy threshold, at which time the policy creates filters dynamically (dynamic filters) to protect the traffic flow according to the severity of the attack. You can configure the policy threshold and the action that the policy takes when it detects an anomaly.

Viewing Zone Policies

To view the policies of a zone configuration, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose **Configuration > Policies > View**. The Policies screen appears.

**Step 3** (Optional) Set a screen filter to display only the policies that you want to view or configure as follows:

- a. Click **Set screen filter**. The Policy Filter window opens.
- b. Configure the screen filters to use, and then click **OK**. **Table 8-1** describes the screen filter parameters listed in the Policy Filter window. Choose the desired display parameters from the corresponding drop-down lists.

To change multiple filter parameters, begin from the top and work your way down the parameters of the Policy Filter window. You must start from the top because when you change one of the filtering parameters, all the parameters listed below it are automatically reset to their default setting.

**Table 8-1  Policy Filter Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Restricts the display to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy template</td>
<td>Policies that were created from the selected policy template.</td>
</tr>
<tr>
<td>Service</td>
<td>Policies that were created for the selected service.</td>
</tr>
<tr>
<td>Protection level</td>
<td>Policies of the selected protection level.</td>
</tr>
<tr>
<td>Type</td>
<td>Policies of the selected packet type.</td>
</tr>
<tr>
<td>Policy</td>
<td>Policies of the selected key.</td>
</tr>
</tbody>
</table>
Chapter 8   Managing Zone Policies

Viewing Zone Policies

Table 8-1   Policy Filter Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Restricts the display to . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Policies of the selected operating state.</td>
</tr>
<tr>
<td>Action</td>
<td>Policies configured with the selected action.</td>
</tr>
<tr>
<td>Policies</td>
<td>Policies of the current configuration or of a snapshot (if available).</td>
</tr>
</tbody>
</table>

A partial list of the policies, meeting the criteria that you specified, is displayed. Details of the selected path, state, and action are displayed in the Screen Filter frame.

(Optional) To view the details of single policy only or to modify a policy configuration, click the Key type of the desired policy. The Policy Details screen appears. See the “Modifying Policy Parameters” section for information about modifying a policy configuration.

Table 8-2 describes the fields in the Policy Table.

Table 8-2   Field Descriptions for Policy Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Template</td>
<td>Policy template that the Detector module used to construct the policy. Each policy template relates to specific traffic characteristics that the Detector module requires to detect a specific DDoS threat.</td>
</tr>
<tr>
<td>Service</td>
<td>Service in the traffic flow that the policy monitors. A service is either a port number or a protocol number. See the “Adding or Deleting a Service” section in Chapter 8, “Managing Zone Policies” for more information. The Detector module displays a service value of any for all traffic that does not specifically match other services created from the same policy template.</td>
</tr>
<tr>
<td>Level</td>
<td>Level of anomaly detection that the policy applies to the traffic flow, which for the Detector module is always Analysis.</td>
</tr>
</tbody>
</table>
Chapter 8  Managing Zone Policies

Viewing Zone Policies

Table 8-2  Field Descriptions for Policy Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Packet types that the Detector module monitors. Packet type values are as follows:</td>
</tr>
<tr>
<td></td>
<td>- auth_pkts—Packets for which either a TCP handshake or UDP authentication was performed.</td>
</tr>
<tr>
<td></td>
<td>- auth_tcp_pkts—Packets for which a TCP handshake was performed.</td>
</tr>
<tr>
<td></td>
<td>- auth_udp_pkts—Packets for which UDP authentication was performed.</td>
</tr>
<tr>
<td></td>
<td>- in_nodata_conns—Zone incoming connections that have no data transfer on the connection (packets without a data payload).</td>
</tr>
<tr>
<td></td>
<td>- in_conns—Zone incoming connections.</td>
</tr>
<tr>
<td></td>
<td>- in_pkts—Zone incoming DNS query packets.</td>
</tr>
<tr>
<td></td>
<td>- in_unauth_pkts—Zone incoming unauthenticated DNS queries.</td>
</tr>
<tr>
<td></td>
<td>- non_estb_conns—Nonestablished connections. Zone incoming failed connections. TCP connection requests (SYN packets) for which no reply was received.</td>
</tr>
<tr>
<td></td>
<td>- num_sources—Packets that have TCP source IP addresses that are destined to the zone and that have been authenticated by the Detector module anti-spoofing functions.</td>
</tr>
<tr>
<td></td>
<td>- out_pkts—Zone incoming DNS reply packets.</td>
</tr>
<tr>
<td></td>
<td>- reqs—Request packets with data payload (measured in packets per second).</td>
</tr>
<tr>
<td></td>
<td>- reqs_pph—Request packets with data payload (measured in packets per hour). A policy with this packet type is designed to monitor the zone traffic for low rate zombie attacks. PPH policies by default are set to the disabled state when you create a new zone because they may increase the amount of memory used by the zone and also affect Detector module performance. To enable the zone PPH polices, you must change the policy states to active (see the “Modifying Policy Parameters” section).</td>
</tr>
<tr>
<td></td>
<td>- syns—Synchronization packets (TCP SYN flagged packets that are measured in packets per second).</td>
</tr>
<tr>
<td></td>
<td>- syns_pph—Synchronization packets (TCP SYN flagged packets that are measured in packets per hour). A policy with this packet type is designed to monitor the zone traffic for low rate zombie attacks. PPH policies by default are set to the disabled state when you create a new zone because they may increase the amount of memory used by the zone and also affect Detector module performance. To enable the zone PPH polices, you must change the policy states to active (see the “Modifying Policy Parameters” section).</td>
</tr>
<tr>
<td></td>
<td>- syn_by_fin—SYN and FIN flagged packets. The Detector module verifies the ratio between the number of SYN flagged packets and the number of FIN flagged packets.</td>
</tr>
<tr>
<td></td>
<td>- unauth_pkts—Packets that did not undergo a TCP handshake.</td>
</tr>
<tr>
<td></td>
<td>- pkts—All packet types that do not fall under any other category in the same protection level.</td>
</tr>
</tbody>
</table>
### Table 8-2 Field Descriptions for Policy Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Traffic characteristic that was used to aggregate the policies. Click the key name to view the details. Key name values are as follows:</td>
</tr>
<tr>
<td></td>
<td>- dst_ip—Traffic destined to a zone IP address.</td>
</tr>
<tr>
<td></td>
<td>- dst_ip_ratio—Ratio of SYN and FIN flagged packets destined to a specific IP address.</td>
</tr>
<tr>
<td></td>
<td>- dst_port_ratio—Ratio of SYN and FIN flagged packets destined to a specific port.</td>
</tr>
<tr>
<td></td>
<td>- global—Summation of all traffic flow as defined by the other policy sections.</td>
</tr>
<tr>
<td></td>
<td>- src_ip—Traffic destined to the zone aggregated according to the source IP address.</td>
</tr>
<tr>
<td></td>
<td>- dst_port—Traffic destined to a specific zone port.</td>
</tr>
<tr>
<td></td>
<td>- protocol—Traffic destined to the zone aggregated based on the protocol.</td>
</tr>
<tr>
<td></td>
<td>- src_ip_many_dst_ips—Traffic from a single IP address that probes a large number of zone IP addresses on the same port. This key is used for IP scanning.</td>
</tr>
<tr>
<td></td>
<td>- src_ip_many_ports—Traffic from a single IP address that probes a large number of ports on a zone destination IP address. This key is used for port scanning.</td>
</tr>
<tr>
<td></td>
<td>- scanners—Histogram of the number of source IP addresses that scan zone destination IP addresses on a specific destination port.</td>
</tr>
<tr>
<td>State</td>
<td>Operating state of the policy. The policy operates in one of the following states:</td>
</tr>
<tr>
<td></td>
<td>- Active—The Detector module applies the policy to the traffic flow. The policy executes an action when the traffic flow exceeds the policy threshold.</td>
</tr>
<tr>
<td></td>
<td>- Inactive—The Detector module applies the policy to the traffic flow. The policy does not execute an action when the traffic flow exceeds the policy threshold.</td>
</tr>
<tr>
<td></td>
<td>- Disabled—The Detector module does not apply the policy to the traffic flow.</td>
</tr>
<tr>
<td>Action</td>
<td>Action assigned to the policy. The policy executes the action when the traffic flow exceeds the policy threshold. See the “Modifying Policy Parameters” section for more information.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Policy threshold traffic rate. When the traffic flow exceeds the policy threshold, the policy executes its assigned action. You can configure the policy threshold manually or allow the Detector module to configure it during the threshold tuning phase of the learning process. By default, the threshold is set to a value appropriate for on-demand protection.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Minimum amount of time that the policy applies its assigned action to the traffic flow.</td>
</tr>
</tbody>
</table>
Chapter 8      Managing Zone Policies

Modifying Policy Parameters

This section describes how to modify policy parameters. You can modify a zone policy only when the Detector module is not learning the zone traffic or detecting anomalies in the zone traffic. You can modify the parameters of a single policy or modify the parameters of several policies simultaneously.

Note
Changes that you make to a policy parameter may be lost if you perform the policy construction phase after changing the parameter because when you accept the results of the policy construction phase, the Detector module replaces the current zone policies with the new policies.

To modify the policy parameters, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu appears.

Step 2 From the zone main menu, choose Configuration > Policies > View. The Policies screen appears.

Step 3 Choose the policies to configure as follows:

- To configure a single policy, click the Key type of the policy that you want to configure (the Policy Details screen appears) and then click Config (which is located under the Learning Parameters table). The Zone Policy Form appears.
- To configure a group of policies, check the check box next to the policies that you want to reconfigure and then click Config Selection. The Zone Policy Parameter Form appears.

A value of Multiple for a policy section specifies that the policy section does not have the same value in all the policies that you selected.

Step 4 Reconfigure the policy parameters and then click OK.

If you leave the field of a policy parameter blank, the Detector module does not change the value of the parameter in the policies that you selected.

---

### Table 8-2  Field Descriptions for Policy Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>Policy threshold operating status. A check mark indicates the threshold is a fixed value that cannot be modified during the threshold tuning phase of the learning process. An x indicates that the threshold value is not fixed, which means that the Detector module can modify the policy threshold during the threshold tuning process.</td>
</tr>
<tr>
<td>Learning Multiplier</td>
<td>Factor by which the Detector module multiplies the threshold when it accepts the results of the threshold tuning phase.</td>
</tr>
<tr>
<td>Detection Time</td>
<td>Parameter that defines the time period over which a PPH policy calculates the average packet rate. PPH policies are policies that monitor zone traffic for low rate zombie attacks and measure traffic rate in packets per hour rather than packets per second (see the “Understanding Zone Policies” section).</td>
</tr>
</tbody>
</table>

---
Table 8-3 describes the policy parameters in the Zone Policy form and the Zone Policy Parameter form.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the policy. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• active—The Detector module applies the policy to the traffic and the policy executes its assigned action when the traffic exceeds the policy threshold.</td>
</tr>
<tr>
<td></td>
<td>• inactive—The Detector module applies the policy to the traffic, but the policy does not execute its assigned action when the traffic exceeds the policy threshold.</td>
</tr>
<tr>
<td></td>
<td>• disabled—The Detector module does not apply the policy to the traffic.</td>
</tr>
<tr>
<td></td>
<td>Caution: Setting the policy state to inactive or disabled may compromise the ability of the Detector module to detect anomalies in the zone traffic. When you set the policy state to disabled, the enabled zone policies assume responsibility for the traffic that was managed by the disabled policy. After you disable a policy and before the Detector module performs anomaly detection, you must perform the threshold tuning phase to update the thresholds of the enabled policies.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that the policy executes when the traffic exceeds the policy threshold. Choose a policy action from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• notify—Notifies you when the traffic exceeds the policy threshold.</td>
</tr>
<tr>
<td></td>
<td>• remote_activation—Activates a Guard, which diverts the zone traffic to itself and manages the zone protection process. You define the Guard that the Detector module activates by using the CLI to configure the remote Guard list.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Threshold traffic rate for the policy. When the traffic exceeds the threshold, the policy executes an action to protect the zone.</td>
</tr>
<tr>
<td></td>
<td>You can configure the threshold for a single policy only.</td>
</tr>
<tr>
<td></td>
<td>The threshold is measured in packets per second except for policies that are constructed from the following policy templates:</td>
</tr>
<tr>
<td></td>
<td>• num_sources—The threshold is measured in the number of IP addresses or ports.</td>
</tr>
<tr>
<td></td>
<td>• tcp_connections—The threshold is measured in the number of connections.</td>
</tr>
<tr>
<td></td>
<td>• tcp_ratio—The threshold is measured as the ratio number.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Factor by which the thresholds of the policies are increased or decreased.</td>
</tr>
<tr>
<td>multiplier</td>
<td>You can configure a threshold multiplier for a group of policies only.</td>
</tr>
<tr>
<td></td>
<td>Enter a factor to increase or decrease the thresholds of the policies when the thresholds are not appropriate for the zone traffic.</td>
</tr>
<tr>
<td></td>
<td>Note: The new value may change in subsequent threshold tuning phases if you do not set it as fixed.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Minimum time for dynamic filters that are produced by the policy to apply their action.</td>
</tr>
<tr>
<td></td>
<td>Enter the timeout value in seconds.</td>
</tr>
</tbody>
</table>
To avoid false attack detections by the Detector module when traffic increases on a known high traffic source or destination IP address, you can configure a policy with a threshold for traffic that is associated with that IP address. Add an IP address and threshold to a policy for the following network applications:

- **High volume source IP address**—When the zone normally receives a high volume of traffic from a specific source IP address, you can configure a policy with a threshold that the Detector module applies to traffic originating from the source IP address.

- **High volume destination IP address**—When you define a zone with two or more IP addresses and sections of the zone normally receive a high volume of traffic, you can configure a policy with a threshold that the Detector module applies to traffic targeting the destination IP address within the zone.

You can configure IP thresholds for the following policies only:

- Policies with traffic characteristic of destination IP address (dst_ip).

- Policies with traffic characteristics of source IP address (src_ip) where the default policy action is drop. The default policy action is the action that the Detector module applies to the policy when you create a new zone. You can configure the threshold list for such policies even if you change the policy action.
You can configure a maximum of 10 IP addresses and thresholds for each policy.

This sections contains the following topics:

- Adding an IP Address and Threshold
- Deleting an IP Address and Threshold

### Adding an IP Address and Threshold

To add an IP address and threshold to a policy, perform the following steps:

**Step 1**
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**
From the zone main menu, choose **Configuration > Policies > View**. The Policies screen appears.

**Step 3**
Click the Key type (located under the Key column) of the policy that you want to configure. The Policy Details screen appears.

**Step 4**
Click **Add** (located under the Threshold list table). The Add Threshold IP Entry screen appears.

**Step 5**
Define the source or destination IP address and the threshold value. *Table 8-4* describes the parameters in the Threshold IP Entry form.

**Table 8-4**  Threshold IP Entry Form

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP address. Enter the source or destination IP address.</td>
</tr>
</tbody>
</table>
| Threshold | IP address traffic threshold. When the traffic exceeds the threshold, the policy executes its configured action. Enter the threshold value in packets per second (pps) except for the following policy types:
  - tcp_connections—Unit of measurement that is the number of connections.
  - tcp_ratio—Unit of measurement that is the ratio number. |

**Step 6**
Choose one of the following options:

- **OK**—Saves the policy IP address information to the zone configuration. The Threshold IP Entry form closes and the Policy details screen appears, displaying any policy configuration changes.
- **Clear**—Clears any information that you added to the Threshold IP Entry form.
- **Cancel**—Exits the Threshold IP Entry form without making any changes to the policy configuration.

### Deleting an IP Address and Threshold

To delete a policy IP address and threshold, perform the following steps:

**Step 1**
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**
From the zone main menu, choose **Configuration > Policies > View**. The Policies screen appears.
Adding or Deleting a Service

You can manually add a service (application port or protocol) to the zone configuration that the Detector module did not discover during the policy construction phase. We recommend that you define specific policies for the zone main services to obtain the anomaly detection operation that is best suited for the zone.

Caution

Do not add the same service (port number) to more than one policy because it may decrease your network performance.

When you add or delete a service from the zone policies, the Detector module marks the zone policies as untuned. Because the zone is untuned, the Detector module cannot detect anomalies in the zone traffic when you activate Detect and Learn until you perform one of the following actions:

- Perform the threshold tuning phase of the learning process and accept the results (see the “Starting the Threshold Tuning Phase” section in Chapter 7, “Learning Zone Traffic”)
- Mark the zone policies tuned (see the “Marking the Zone Policies as Tuned or Untuned” section in Chapter 7, “Learning Zone Traffic”)

This section contains the following topics:

- Adding a Service
- Deleting a Service

Adding a Service

You can add services to all policies that were created from a specific policy template. The Detector module adds the new service to the services that it discovered during the policy construction phase and configures the new service with a default threshold value. You can define the threshold manually, but we recommend that you run the threshold tuning phase of the learning process to tune the policies to the zone traffic.

You can add a new service to policies that were created from the following policy templates:

- tcp_services, udp_services, tcp_services_ns, worm_tcp
  The service designates a port number.
- other_protocols
  The service designates a protocol number.

Note

If you activate the policy construction phase after adding a service, new services may override the service that you added manually.
You may need to manually add a service for the following reasons:

- A new application or service was added to the zone network, but you do not want to activate the policy construction phase to add the service to the zone configuration.
- You did not allow the policy construction phase to run long enough to detect all of the network services. For example, you may know of applications or services that are active only once a week or during the night when you do not have the policy construction phase activated.

To add a service to a policy type, perform the following steps:

**Step 1**  
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  
From the zone main menu, choose **Configuration > Policy Templates > Add Service**. The Add Service Step 1 screen appears.

You can also navigate to the Add Service Step 1 screen by performing one of the following actions:

- From the zone main menu, choose **Configuration > Policies > View**, and then click **Add service** in the Policies screen.
- From the zone main menu, choose **Configuration > Policy templates > View**, and then click **Add service** in the Policies Templates screen.

**Step 3**  
From the Policy Template list, choose a policy template and then click **Next**. The Add Service Step 2 screen appears.

See the “Understanding Policy Templates” section in Chapter 6, “Configuring Policy Templates” for information about policy template types.

**Step 4**  
Enter the new service in the **Add Service Form**.

**Step 5**  
Choose one of the following options:

- **OK**—Adds the new policies for the service to the zone configuration. The Detector module marks the zone policies as untuned. The policies of the new service are configured with default threshold values.
- **Clear**—Clears the **Add Service Form** information.
- **Cancel**—Exits the Add Service Form without adding any new service to the zone configuration.

**Step 6**  
(Optional) Define the thresholds of the new policies. You can define the threshold manually, but we recommend that you run the threshold tuning phase of the learning process to tune the policies to the zone traffic. See the “Starting the Threshold Tuning Phase” section in Chapter 7, “Learning Zone Traffic” for more information.

You can mark the zone policies as tuned even if you do not run the threshold tuning phase of the learning process. See the “Marking the Zone Policies as Tuned or Untuned” section in Chapter 7, “Learning Zone Traffic” for more information.

### Deleting a Service

You can delete a specific service for any policy template. The Detector module deletes the service from all policies that were created from the specific policy template.
If you delete a service, the zone policies cannot monitor the traffic of that service, which may compromise zone anomaly detection.

You can remove services from the following policy templates:
- tcp_services, udp_services, tcp_services_ns, worm_tcp
  The service designates a port number.
- other_protocols
  The service is a protocol number.

If you do not activate the policy construction phase of the learning process, you may need to manually remove a service for the following reasons:
- An application or service was removed from the network.
- An application or service was identified during the policy construction phase but you do not want to enable it because it is uncommon for the network environment.

Note: If you activate the policy construction phase after removing a service, the Detector module may add the same service back again.

To delete a service from a policy, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu appears.

Step 2 From the zone main menu, choose Configuration > Policy Templates > Remove service. The Remove Service screen appears.

You can also navigate to the Remove Service screen by performing one of the following actions:
- From the zone main menu, choose Configuration > Policies > View, and then click Remove service in the Policies screen.
- From the zone main menu, choose Configuration > Policy templates > View, and then click Remove service in the Policies Templates screen.

Step 3 Choose the service that you want to remove from the list, and then click Delete. The delete verification screen appears.

Step 4 Choose one of the following options:
- OK—Removes the selected service from the zone configuration. The Detector module marks the zone as untuned.
- Cancel—Exits the Remove Service form without removing any new service from the zone configuration.

Step 5 (Optional) Change the zone configuration from untuned to tuned after deleting a service by performing one of the following actions:
- Perform the threshold tuning phase of the learning process and accept the phase results (see the “Starting the Threshold Tuning Phase” section in Chapter 7, “Learning Zone Traffic”).
- Mark the zone as tuned (see the “Marking the Zone Policies as Tuned or Untuned” section in Chapter 7, “Learning Zone Traffic”).
Backing Up the Zone Policies

You can use the snapshot feature to create a backup of the current zone policies.

To back up the zone policies, perform the following steps:

**Step 1** From the navigation pane, choose a zone that is not currently in a learning phase. The zone main menu appears.

**Step 2** From the zone main menu, choose **Learning > Snapshot**. The Create Snapshot screen appears.

**Step 3** Enter a name for the snapshot in the Snapshot name filed, and then click **OK**. The Detector module saves the zone policies and assigns a consecutive ID number to the snapshot.
CHAPTER 9

Activating Anomaly Detection

This chapter describes how to activate anomaly detection using the WBM. When you activate anomaly detection for a zone, the Cisco Traffic Anomaly Detector Module (Detector module) applies the zone policies to the copy of the zone traffic that it receives. When a traffic anomaly triggers a policy action by exceeding the policy threshold (indicating an attack), the Detector module either sends you a notification or activates a Cisco Anomaly Guard (Guard).

The Guard, which is the companion product of the Detector module, is a Distributed Denial of Service (DDoS) attack detection and mitigation device that cleans the zone traffic as the traffic flows through it, dropping the attack traffic and injecting the legitimate traffic back into the network. When the Detector module determines that the zone is under attack, it can activate the Guard attack mitigation services. The Detector module can also synchronize zone configurations with the Guard. For more information about the Guard, see the Cisco Anomaly Guard Module Configuration Guide or the Cisco Guard Configuration Guide.

This chapter contains the following sections:

- Understanding the Anomaly Detection Activation Options
- Managing Anomaly Detection
- Managing Dynamic Filters
- Activating Automatic or Interactive Detect Mode
- Managing Detector Module Recommendations for Dynamic Filters
Understanding the Anomaly Detection Activation Options

The Detector module provides you with several options for performing anomaly detection. For example, you can allow the Detector module to manage all aspects of the anomaly detection operation or you can monitor and direct the Detector module during an attack.

This section contains the following topics:
- Detect, Detect and Learn
- Automatic and Interactive Operation Modes

Detect, Detect and Learn

When you activate zone anomaly detection, the Detector module provides you with the following options:

- Detect—Analyzes the zone traffic and begins producing dynamic filters when it detects a traffic anomaly.
- Detect and Learn—Analyzes zone traffic for traffic anomalies and at the same time begins the threshold tuning phase of the learning process. While analyzing the traffic for the threshold tuning phase, the Detector module can automatically adjust the policy thresholds of the zone configuration with new threshold information. If the Detector module detects an attack while analyzing the traffic, it stops the threshold tuning phase to prevent it from learning attack traffic threshold values.

Automatic and Interactive Operation Modes

You can configure the Detector module to detect traffic anomalies in a zone in either one of the following modes of operation:

- Automatic detect mode—Automatically activates the dynamic filters that it creates during an attack.
- Interactive detect mode—Creates dynamic filters during an attack but does not activate them. Instead, the Detector module groups the dynamic filters as recommendations, which you review and decide whether to accept, ignore, or direct the recommendations to automatic activation.
Managing Anomaly Detection

This section describes how to manually activate and deactivate zone traffic anomaly detection.

This section contains the following topics:

- Activating Anomaly Detection
- Verifying Traffic Anomaly Detection
- Deactivating Anomaly Detection

Activating Anomaly Detection

To activate zone anomaly detection, perform the following steps:

1. From the navigation pane, choose a zone. The zone main menu and zone status screen appear.
2. Use one of the following methods to activate anomaly detection:
   - To activate Detect only, click Detect or choose Detection > Detect from the zone main menu.
   - To activate Detect and Learn, click Detect & Learn.

The Detector module begins analyzing the traffic flow for traffic anomalies.

The zone name is added to the Under Detection zone listing in the navigation pane and the Recent Events table lists an event type of detection-start with a detail listing of Zone is under detection.

The zone status icon changes to Detection.

Verifying Traffic Anomaly Detection

From the zone status screen, you can view the traffic counter to verify that the anomaly detection process is functioning properly.

Click a zone under detection from the navigation pane to display the zone status screen. Anomaly detection is functioning if the following conditions exist:

- The Recent Events table lists an event type of detection-start with a detail listing of Zone is under detection.
- The Traffic Rate table shows the Received traffic rate is greater than zero.

Deactivating Anomaly Detection

To deactivate anomaly detection, perform the following steps:

1. From the navigation pane, click a zone under detection. The zone main menu and the zone status page appear.
Step 2  Use one of the following methods to deactivate anomaly detection:

- From the zone status screen, click Deactivate.
- From the zone main menu, choose Detection > Deactivate.

If the Detect function was enabled, the Detector module stops analyzing zone traffic and the zone status changes to Standby.

If the Detect and Learn function was enabled, the Deactivate window appears (continue to Step 3).

Step 3  Check the Stop Detection check box.

Step 4  (Optional) Check the Stop Learning check box to stop the threshold tuning phase of the learning process and define how the Detector module handles the new thresholds by choosing one of the following options from the Deactivate window:

- **Reject**—Ignores the current results of the threshold tuning phase.
- **Accept**—Uses the current results of the threshold tuning phase in the zone configuration. Define the threshold selection method to use.

Table 9-1 describes the threshold selection method parameters.

**Table 9-1  Threshold Terminating Method**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold selection method</td>
<td>Method for selecting the thresholds to accept. Choose one of the following options from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>- Accept new thresholds—Saves the results of the learning process to the zone configuration.</td>
</tr>
<tr>
<td></td>
<td>- Accept max. thresholds—Compares the current policy threshold to the learned threshold and saves the higher of the two to the zone configuration. This is the default method.</td>
</tr>
<tr>
<td></td>
<td>- Accept weighted thresholds—Calculates the policy thresholds to save based on the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
<tr>
<td></td>
<td>Enter the weight value in the Weight field.</td>
</tr>
<tr>
<td></td>
<td>- Keep current thresholds—Rejects all of the suggested threshold values of the learning process and the policies retain their current thresholds.</td>
</tr>
<tr>
<td>Weight</td>
<td>Defines the weight that the Detector module uses to calculate new thresholds. This option is active only when you choose the Accept weighted thresholds method. Enter a weight value for the Detector module to use in the following formula:</td>
</tr>
<tr>
<td></td>
<td>new-threshold = (learned-threshold * Weight + current-threshold * (100 – Weight)) / 100</td>
</tr>
</tbody>
</table>

Step 5  Click OK to confirm your selection.

The Detector module stops analyzing zone traffic, and the zone name is removed from the Under Detection list in the navigation pane.
Managing Dynamic Filters

Dynamic filters apply the required protection level to the traffic flow and define how to handle the attack. The Detector module creates dynamic filters when it identifies an anomaly in the zone traffic, which occurs when the flow exceeds the zone policy thresholds, and continuously adapts this set of filters to the zone traffic and the type of Distributed Denial of Service (DDoS) attack. You can view and manage dynamic filters only when the zone is under attack because the Detector module creates dynamic filters only when you have anomaly detection activated and the zone is under attack.

To manually control zone anomaly detection during an attack, you can add or delete a dynamic filter during an attack. The Detector module deletes all dynamic filters when the attack ends. The Detector module supports a maximum of 150,000 dynamic filters that are concurrently active in all zones.

This section contains the following topics:

- Displaying the Dynamic Filters List
- Displaying Dynamic Filter Details
- Adding Dynamic Filters
- Deleting Dynamic Filters
- Preventing the Creation of Unwanted Dynamic Filters

Displaying the Dynamic Filters List

To display the list of dynamic filters, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the navigation pane, choose a zone under detection. The zone main menu and the zone status screen appear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Use one of the following methods to display the list of dynamic filters:</td>
</tr>
<tr>
<td></td>
<td>• From the zone main menu, choose Detection &gt; Dynamic filters.</td>
</tr>
<tr>
<td></td>
<td>• From the Zone Status table, click Active Dynamic filters.</td>
</tr>
</tbody>
</table>

The Dynamic Filters screen appears.

The Dynamic Filters table displays the dynamic filters filtered according to the policy that created them and provides information about the ongoing attack. Table 9-2 describes the information in the Dynamic Filters table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created by</td>
<td>Policy that created the dynamic filter. Click on the policy name to display the policy details.</td>
</tr>
<tr>
<td>Activation</td>
<td>Date and time that the dynamic filter was activated.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Time that the filter is due to expire. After this time, the dynamic filter is deleted.</td>
</tr>
<tr>
<td>Src IP</td>
<td>Source IP address of the traffic that the filter processes.</td>
</tr>
</tbody>
</table>
Managing Dynamic Filters

Chapter 9  Activating Anomaly Detection

Table 9-2  Field Descriptions for Dynamic Filters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dst IP</td>
<td>Destination IP address on which the dynamic filter is applied. The Detector module activates protection on the Guard based on the destination IP address and the value of the Protect-IP state that is configured for the zone.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol number of the traffic that the filter processes.</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Destination port of the traffic that the filter processes.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Fragmentation settings of the traffic flow, which specifies whether the attack stream contains fragmented packets.</td>
</tr>
<tr>
<td>Action</td>
<td>Action taken by the dynamic filter.</td>
</tr>
<tr>
<td>Rate (pps)</td>
<td>Current traffic rate in packets per second that is measured for this filter.</td>
</tr>
<tr>
<td>Details</td>
<td>Indication that additional information is available for this filter. Click i to view additional information.</td>
</tr>
</tbody>
</table>

The Src IP, Protocol, and Dst Port may be nonspecific. An asterisk (*) indicates that the filter acts on all field values or that more than one value was matched for the filter.

See the “Displaying Dynamic Filter Details” section for information about viewing the details of a specific dynamic filter.

Displaying Dynamic Filter Details

To display detailed information for a specific dynamic filter, perform the following steps:

Step 1  From the navigation pane, choose a zone under detection. The zone main menu and the zone status screen appear.

Step 2  Use one of the following methods to view the list of dynamic filters:
  - From the zone main menu, choose Detection > Dynamic filters.
  - From the Zone Status table, click Active Dynamic filters.

The Dynamic Filters screen appears.

Step 3  Click i in the Details column of the dynamic filter for which you want to display the details. The Dynamic Filter Details screen appears.

The Dynamic Filter Details screen contains three tables that describe the following information:
  - The policy that created the dynamic filter.
  - Information about the attack flow.
  - Information about the trigger that created the dynamic filter. Table 9-3 describes the trigger parameters.
Adding Dynamic Filters

During an attack on the zone, you can add a dynamic filter to manage zone anomaly detection. You can configure a dynamic filter to activate the Guards that are defined in the remote Guard lists to protect the zone. The destination IP address of the dynamic filter must match the Protect-IP state and the address range that is configured for the zone or the remote Guard activation fails. You can configure the dynamic filter to activate zone protection on the remote Guard in one of the following ways:

- **Activate zone protection on the remote Guard for the entire zone**—To activate zone protection for the entire zone, enter an asterisk (*) in the Destination IP field or leave the field blank. You must configure the Protect-IP state of the zone to Entire Zone or Policy type.

- **Activate zone protection on the remote Guard for a specific IP address within the zone IP address range only**—To activate zone protection for a specific IP address, enter the IP address in the Destination IP field. You must configure the Protect-IP state of the zone to Only Dst IP (only destination IP address).

You can configure remote Guard lists using the CLI only. See the Cisco Traffic Anomaly Detector Configuration Guide for information about using the CLI.

See the “Configuring Guard Zones” section in Chapter 4, “Creating and Configuring Zones” for more information about the zone Protect-IP state.

To add a dynamic filter, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose a zone under detection from the navigation pane. The zone main menu and the zone status screen appear.</td>
</tr>
<tr>
<td>2</td>
<td>Use one of the following methods to view the list of dynamic filters:</td>
</tr>
<tr>
<td></td>
<td>• From the zone main menu, choose <strong>Detection &gt; Dynamic filters</strong>.</td>
</tr>
<tr>
<td></td>
<td>• From the zone status table on the zone status page, click <strong>Active Dynamic filters</strong>.</td>
</tr>
<tr>
<td></td>
<td>The Dynamic filters screen appears.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Add</strong>. The Add Dynamic Filter screen appears.</td>
</tr>
<tr>
<td>4</td>
<td>Define the dynamic filter parameters as described in Table 9-4.</td>
</tr>
</tbody>
</table>

### Table 9-3 Field Descriptions for Triggers

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Threshold</td>
<td>Policy threshold that was exceeded by the attack flow.</td>
</tr>
<tr>
<td>Triggering rate</td>
<td>Approximate attack rate that triggered the creation of the dynamic filter.</td>
</tr>
</tbody>
</table>

### Adding Dynamic Filters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP</td>
<td>The Detector module activates protection on the remote Guard based on the destination IP address and the value of the Protect-IP state that is configured for the zone. Leave blank or enter an asterisk (*) for any IP address.</td>
</tr>
</tbody>
</table>
Managing Dynamic Filters

Step 5 Click OK to activate the dynamic filter.

Deleting Dynamic Filters

You can delete a dynamic filter, but deleting the filter is effective for a limited period of time only because the Detector module continues to configure new dynamic filters as changes to the attack traffic occur. To prevent the Detector module from producing unwanted dynamic filters, see the “Preventing the Creation of Unwanted Dynamic Filters” section.

To delete a dynamic filter, perform the following steps:

Step 1 From the navigation pane, choose a zone under detection. The zone main menu and the zone status screen appear.

Step 2 Use one of the following methods to view the list of dynamic filters:

- From the zone main menu, choose Detection > Dynamic filters.
- From the Zone Status table, click Active Dynamic filters.

The Dynamic filters screen appears.

Step 3 Check the check box next to the dynamic filter that you want to delete.

Step 4 Click Delete to delete the dynamic filter.

Preventing the Creation of Unwanted Dynamic Filters

You can prevent the Detector module from producing unwanted dynamic filters by performing one of the following actions:

- Deactivate the policy that produces the dynamic filters. See the “Modifying Policy Parameters” section in Chapter 8, “Managing Zone Policies” for information about changing the policy operating state. To view the list of dynamic filters and find out which policy produced the unwanted dynamic filters, see the “Displaying the Dynamic Filters List” section.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Action</th>
<th>Timeout (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Action that the Detector module performs when the traffic matches the filter. The Detector module supports the remote-activate action only, which enables it to activate the remote Guards that you have defined in the remote Guard lists to protect the zone. Use the CLI to configure the remote Guard lists. For more information about accessing and using the Detector module CLI, see the Cisco Traffic Anomaly Detector Module Configuration Guide.</td>
<td>Action that the Detector module performs when the traffic matches the filter. The Detector module supports the remote-activate action only, which enables it to activate the remote Guards that you have defined in the remote Guard lists to protect the zone. Use the CLI to configure the remote Guard lists. For more information about accessing and using the Detector module CLI, see the Cisco Traffic Anomaly Detector Module Configuration Guide.</td>
<td>Minimum time that the filter is active. Choose one of the following filter timeout options:</td>
</tr>
<tr>
<td>Time (Sec)</td>
<td>Minimum time that the filter is active. Choose one of the following filter timeout options:</td>
<td>Action that the Detector module performs when the traffic matches the filter. The Detector module supports the remote-activate action only, which enables it to activate the remote Guards that you have defined in the remote Guard lists to protect the zone. Use the CLI to configure the remote Guard lists. For more information about accessing and using the Detector module CLI, see the Cisco Traffic Anomaly Detector Module Configuration Guide.</td>
<td>Minimum time that the filter is active. Choose one of the following filter timeout options:</td>
</tr>
<tr>
<td></td>
<td>• Check the Forever check box for an infinite amount of time.</td>
<td>Action that the Detector module performs when the traffic matches the filter. The Detector module supports the remote-activate action only, which enables it to activate the remote Guards that you have defined in the remote Guard lists to protect the zone. Use the CLI to configure the remote Guard lists. For more information about accessing and using the Detector module CLI, see the Cisco Traffic Anomaly Detector Module Configuration Guide.</td>
<td>Minimum time that the filter is active. Choose one of the following filter timeout options:</td>
</tr>
<tr>
<td></td>
<td>• Check the seconds check box and enter the amount of time in seconds.</td>
<td>Action that the Detector module performs when the traffic matches the filter. The Detector module supports the remote-activate action only, which enables it to activate the remote Guards that you have defined in the remote Guard lists to protect the zone. Use the CLI to configure the remote Guard lists. For more information about accessing and using the Detector module CLI, see the Cisco Traffic Anomaly Detector Module Configuration Guide.</td>
<td>Minimum time that the filter is active. Choose one of the following filter timeout options:</td>
</tr>
</tbody>
</table>

Table 9-4 Field Descriptions for Dynamic Filters (continued)
• Configure a bypass filter for the desired traffic flow. For information about configuring a bypass filter, see the “Managing Bypass Filters” section in Chapter 5, “Configuring Zone Filters.”
• Increase the threshold of the policy that produced the undesired dynamic filter. For information about modifying the policy threshold, see the “Modifying Policy Parameters” section in Chapter 8, “Managing Zone Policies”.

Activating Automatic or Interactive Detect Mode

You can control activation of the zone dynamic filters by configuring the Detector module to operate in one of the following modes when detecting anomalies in the zone traffic:

• Automatic detect mode—The Detector module activates the dynamic filter as soon as it creates the filter for the zone. This operation mode is the default.
• Interactive detect mode—The Detector module does not automatically activate the dynamic that it creates for the zone. Instead, it saves the dynamic filters and groups them as recommendations. You review the list of recommendations and decide which recommendations to accept, ignore, or direct to automatic activation.

You configure the anomaly detection operating mode as part of the zone configuration and can change the operating mode setting at any time, including when the zone is under attack.

This section contains the following topics:
• Activating Automatic Detect Mode
• Activating Interactive Detect Mode
• Taking Action When the Number of Pending Dynamic Filters Exceeds 1000

Activating Automatic Detect Mode

To activate the zone in automatic detect mode, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
Step 2 Choose Configuration > General from the zone main menu. The General screen appears.
Step 3 Click Config. The Config screen displays.
Step 4 From the Operation Mode parameter drop-down list, choose automatic.
Step 5 Click OK. The Detector module updates the zone configuration with the new operation mode setting. If the zone operation is currently active, the Detector module automatically activates all pending and new dynamic filters.

Activating Interactive Detect Mode

To activate the zone in interactive detect mode, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.
Step 2 Choose Configuration > General from the zone main menu. The General screen appears.
Chapter 9  Activating Anomaly Detection

Activating Automatic or Interactive Detect Mode

Step 3  Click **Config**. The Config screen displays.

Step 4  From the Operation Mode parameter drop-down list, choose **interactive**.

Step 5  Click **OK**. The Detector module updates the zone configuration with the new operation mode setting. If anomaly detection is currently active, the Detector module produces recommendations when an attack is detected.

Taking Action When the Number of Pending Dynamic Filters Exceeds 1000

When the number of pending dynamic filters exceeds 1000, the Detector module performs the following actions:

- Displays an error message that instructs you to deactivate the zone and reactivate it in automatic detect mode.
- Records the recommendations in the zone log file and report and then discards them.

To detect anomalies in the zone traffic when the Detector module has more than 1000 pending dynamic filters you must configure the zone for automatic detect mode by performing the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

Step 2  Click **Deactivate**. The Detector module stops anomaly detection and deletes all pending dynamic filters.

Step 3  Choose **Configuration > General** from the zone main menu. The General screen appears.

Step 4  Click **Config**. The Config screen displays.

Step 5  From the Operation Mode drop-down list, choose **automatic** and then click **OK**. The zone configuration is updated with the new anomaly detection setting.

Step 6  Click **Protect**. The Detector module begins the automatic detect mode operation and activates all dynamic filters as it creates them.
Managing Detector Module Recommendations for Dynamic Filters

When the Detector module performs anomaly detection for the zone in interactive detect mode, it generates a list of the dynamic filters that it creates during an attack. The dynamic filters on the list are known as pending dynamic filters. The Detector module groups the pending dynamic filters according to the policies that produced them and presents them to you as Detector module recommendations.

The recommendations provide a summary of the pending filters and include information about the name of the policy that caused the creation of the pending dynamic filters, the data on the traffic anomaly that resulted in the policy activation, the number of pending dynamic filters, and the recommended action. You can choose to act on a Detector module recommendation (including all of the pending dynamic filters associated with it) or you can act on each pending dynamic filter separately.

This section contains the following topics:

- Viewing Recommendations
- Managing Recommendations
- Viewing the Pending Dynamic Filters of a Recommendation
- Viewing Pending Dynamic Filter Details
- Accepting a Pending Dynamic Filter

Viewing Recommendations

The Detector module displays the recommendations icon when new recommendations are available in the following locations:

- The navigation pane, next to the zone icon in the All Zones list
- The navigation pane, next to the zone icon in the Under Detection list
- The zone status page, in the zone status bar
- The Zone List table

When the Detector module has new recommendations, the number of pending dynamic filters is greater than zero. The Detector module displays the number of pending dynamic filters in the zone status screen in the Zone Status table.

To view the list of Detector module recommendations, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

**Step 2** Use one of the following methods to display the list of recommendations:

- From the zone main menu, choose Detection > Recommendations.
- From the zone status table on the zone status screen, click Pending Dynamic filters.

The Recommendations screen appears.
Table 9-5 describes the fields in the Recommendations table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identification number that the Detector module assigned to the recommendation.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Action that the Detector module recommends.</td>
</tr>
<tr>
<td>Created By</td>
<td>Policy that created the filter. Click on the policy name to view the policy details.</td>
</tr>
<tr>
<td># of PFs</td>
<td>Number of pending dynamic filters that are associated with the recommendation. Each pending filter was created as a result of traffic flow that exceeded the policy threshold. Click on the number to view the pending dynamic filters associated with the recommendation.</td>
</tr>
</tbody>
</table>
| Attack flow    | Attack flow information. The following attack flow details are provided:  
                  * Src IP—Source IP address  
                  * Protocol—Protocol number  
                  * Dst Port—Destination port  
                  * Dst IP—Destination IP address |
| Thr.           | Policy threshold that the attack flow exceeded.                                                                                                                                                              |
| Min.           | Minimum attack rate. The rate of the lowest pending dynamic filter is displayed for recommendations that include several pending filters.                                                               |
| Max.           | Maximum attack rate. The rate of the highest pending dynamic filter is displayed for recommendations that include several pending filters.                                                               |
| Creation       | Date and time that the recommendation was created.                                                                                                                                                           |

The Detector module uses an asterisk (*) as a wildcard for one of the parameters to indicate the following:
- The value is undetermined.
- More than one value was measured for the parameter. To display the different values, view the complete list of pending dynamic filters.

Managing Recommendations

You can decide whether or not to activate Detector module recommendations. You can apply your decision to all recommendations, a specific recommendation, or to a specific pending dynamic filter. Your decisions determine whether or not the pending dynamic filters in a policy become dynamic filters and for how long.

You can instruct the Detector module to automatically activate the pending dynamic filters of a specific policy. You can also instruct the Detector module to prevent policies from producing recommendations.

The Detector module policies continue to produce recommendations if the zone is in interactive protect mode and a DDoS attack is in progress. We recommend that you display the zone status when you manage recommendations in order to verify the zone status and determine if additional actions are required.
To manage recommendations, perform the following steps:

---

**Step 1**  From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

**Step 2**  Use one of the following methods to display the list of recommendations:
- From the zone main menu, choose Detection > Recommendations.
- From the zone status table on the zone status screen, click Pending Dynamic filters.

The Recommendations screen appears.

**Step 3**  In the Filters timeout box, enter the timeout value in seconds for the filter.

**Step 4**  Check the check box next to the recommendations that you want to accept.

**Step 5**  Choose one of the required actions:
- **accept**—Accepts the specific recommendation. The Detector module activates the pending dynamic filters associated with the recommendation.
- **always-accept**—Accepts the specific recommendation. The decision applies automatically whenever the recommendation policy produces new recommendations. Pending dynamic filters automatically become dynamic filters. If you take this action, the Detector module no longer displays such recommendations.
- **always-ignore**—Ignores the specific recommendation. No dynamic filter or pending dynamic filters are produced. The decision automatically applies to all future recommendations produced by the policy. If you decide to always ignore a recommendation, the Detector module no longer displays it. To prevent a policy from producing recommendations in future attacks, disable or deactivate the policy (see the “Modifying Policy Parameters” section in Chapter 8, “Managing Zone Policies”).

**Note**  You can change an always-ignore decision made on a specific recommendation by changing the interactive-status of the policy that created the pending dynamic filters of the recommendation.

---

You can selectively accept pending dynamic filters instead of accepting all the pending dynamic filters associated with a recommendation. See the “Accepting a Pending Dynamic Filter” section for more information.

---

**Viewing the Pending Dynamic Filters of a Recommendation**

To view the pending dynamic filters associated with a Detector module recommendation, perform the following steps:

---

**Step 1**  From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

**Step 2**  Use one of the following methods to display the list of recommendations:
- From the zone main menu, choose Detection > Recommendations.
- From the zone status table on the zone status screen, click Pending Dynamic filters.

The Recommendations screen appears.
Step 3 Click the numeric value that is listed in the # of PFs (Pending Filters) column of the recommendation. The Pending dynamic filters screen appears.

Table 9-6 describes the fields in the Pending Dynamic Filters table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created by</td>
<td>Policy that created the filter. Click on the policy name to display the policy details. See Chapter 8, “Managing Zone Policies” for more information.</td>
</tr>
<tr>
<td>Activation</td>
<td>Date and time that the filter was created.</td>
</tr>
<tr>
<td>Src IP</td>
<td>Source IP address of the attack stream.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol number of the attack stream.</td>
</tr>
<tr>
<td>Dst Port</td>
<td>Destination port of the attack stream.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Fragmentation setting of the filter, which indicates if the attack stream contains fragmented packets.</td>
</tr>
<tr>
<td>Action</td>
<td>Action taken by the filter.</td>
</tr>
<tr>
<td>Recent rate</td>
<td>Current attack rate measured by the filter.</td>
</tr>
<tr>
<td>Rate (pps)</td>
<td>Triggering rate. The approximate attack rate that triggered the production of the pending dynamic filter.</td>
</tr>
<tr>
<td>Details</td>
<td>Status of whether or not additional information is available for this filter. Click i for additional information.</td>
</tr>
</tbody>
</table>

The Detector module uses an asterisk (*) as a wildcard for one of the parameters to indicate:

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

The Detector module activates the pending dynamic filters that are produced by the policies for at least a user-defined time span (filter timeout).

**Viewing Pending Dynamic Filter Details**

To display the detailed information of a dynamic filter, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.

**Step 2** Use one of the following methods to display the list of recommendations:

- From the zone main menu, choose **Detection > Recommendations**.
- From the zone status table on the zone status screen, click **Pending Dynamic filters**.

The Recommendations screen appears.

**Step 3** Click the numeric value listed in the # of PFs (Pending Filters) column of the recommendation. The Pending Dynamic Filters screen appears.
Step 4  Click i in the details column of the desired pending dynamic filter. The Filter Details screen appears.

The Filter Details screen contains three tables that provide the following information:
- Policy that created the filter.
- Attack flow.
- Trigger for the filter creation (displays the policy threshold that the attack flow exceeded and the approximate attack rate that triggered the production of the filter).

### Accepting a Pending Dynamic Filter

To selectively accept a pending dynamic filter, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the navigation pane, choose a zone. The zone main menu and the zone status screen appear.</td>
</tr>
</tbody>
</table>
| Step 2 | Use one of the following methods to display the list of recommendations:  
  - From the zone main menu, choose Detection > Recommendations.  
  - From the Zone Status table on the zone status screen, click Pending Dynamic filters.  
  The Recommendations screen appears. |
| Step 3 | Click the numeric value that is listed in the # of PFs (Pending Filters) column of the recommendation. The Pending Dynamic Filters screen appears. |
| Step 4 | In the Filters timeout box, enter the timeout value in seconds for the dynamic filter. |
| Step 5 | Check the check box next to the pending dynamic filters that you want to activate. |
| Step 6 | Click Accept to activate the pending dynamic filters. |
Monitoring Detector Module and Zone Operations

This chapter describes how to monitor the status of the Cisco Traffic Anomaly Detector Module (Detector module) and its zones and diagnose the problems that are related to the zone traffic flow.

This chapter contains the following sections:

- Viewing the Detector Summary Screen
- Using the Detector Module Global Diagnostic Tools
- Viewing the Zone Status Screen
- Using the Zone Diagnostic Tools

Viewing the Detector Summary Screen

The Detector Summary screen (see Figure 10-1) provides a summary of the current Detector module activity and is the first screen to appear when you connect to the Detector module WBM. You can access this screen from the following locations within the interface:

- Click Detector Summary from the navigation pane.
- Click Home from the information area.
Viewing the Detector Summary Screen

Figure 10-1 Detector Module Summary Screen

The Detector Summary screen includes the following two areas:

- **Detector Summary**—Graphical summary of the received traffic rate that the Detector module handled over the last two hours in bits per second (bps).

  Table 10-1 describes the information that appears below the graph.

  **Table 10-1 Field Descriptions for Detector Summary Graph**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min.</td>
<td>Minimum traffic rate measured during the last 2 hours in bits per second.</td>
</tr>
<tr>
<td>Max.</td>
<td>Maximum traffic rate measured during the last 2 hours in bits per second.</td>
</tr>
<tr>
<td>Avg.</td>
<td>Average traffic rate measured during the last 2 hours in bits per second.</td>
</tr>
<tr>
<td>Cur.</td>
<td>Current traffic rate in bits per second.</td>
</tr>
</tbody>
</table>

- **Zones Under Detection**—Status information of the zones that the Detector module is currently monitoring for traffic anomalies. The zone information can vary depending on which of the following anomaly detection modes that you activate:

  - **Detect**—Displays the zone information when the zone is under attack and when normal traffic conditions exist.
  
  - **Detect and Learn**—Displays zone information only when the zone is under attack.

  The Detector module lists the zones in the order in which they encountered attacks with the most recently attacked zone appearing at the top of the list. Click on the information that the Detector module displays in each row to view the associated zone summary screen.

  Table 10-2 describes the fields for zones under detection.
Displaying the Global Counters

The Counters screen provides an in-depth analysis of the counter information that the Detector module displays in the Detector module Summary screen. From the Counters screen, you can filter the information that the Detector module displays in the traffic rates graph.

To display the Detector module counters, perform the following steps:

**Step 1** From the navigation pane, click **Detector Summary**. The Detector Summary menu appears.

**Step 2** From the Detector Summary menu, choose **Diagnostics > Counters > Device Counters**. The Counters screen appears.

By default, the traffic rate graph displays counter information recorded in the last 2 hours, measured in bits per second.

**Step 3** (Optional) Modify the unit of measurement that the Detector module uses in the traffic rate graph. Choose a unit of measurement from the Graph Type drop-down list:

- **pps**—Packets per second
- **bps**—Bits per second

---

**Table 10-2  Field Descriptions for Zones Under Anomaly Detection**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>Zone name. The zone name also provides a link to the status screen of the specific zone.</td>
</tr>
<tr>
<td>Activation Time</td>
<td>Date and time that zone protection was activated.</td>
</tr>
<tr>
<td>Attack Start Time</td>
<td>Date and time that the most recent attack on the zone was detected.</td>
</tr>
<tr>
<td>#DF</td>
<td>Number of dynamic filters. Because the Detector module creates a dynamic filter only when it detects an anomaly, a #DF value greater than zero indicates an attack on the zone.</td>
</tr>
<tr>
<td>#PF</td>
<td>Number of pending dynamic filters. The display is N/A if the zone is operating in automatic protect mode (not interactive protect mode).</td>
</tr>
<tr>
<td>Receive Rate</td>
<td>Current rate of traffic (in bits per second) destined to the zone.</td>
</tr>
<tr>
<td>Thumbnail of the zone traffic summary</td>
<td>Graph that displays a summary of the traffic (in bits per second) to the zone in the last 30 minutes.</td>
</tr>
</tbody>
</table>
Step 4  Click Update Graph. The Detector module updates the graph.

Step 5  (Optional) Click Clear Counters to clear the Detector module counters. The Detector module clears the current counters and the traffic rates. You can clear the Detector module counters if you are going to perform testing and want to be sure that the counters include information from the testing session only.

The Received packets counter provides information on the total number of packets that the Detector module received and analyzed.

Table 10-3 describes the fields for the Received packets counter.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>Total amount of packets since the Detector module was reloaded.</td>
</tr>
<tr>
<td>Bits</td>
<td>Total amount of bits since the Detector module was reloaded.</td>
</tr>
<tr>
<td>pps</td>
<td>Current traffic rate measured in packets per second.</td>
</tr>
<tr>
<td>bps</td>
<td>Current traffic rate measured in bits per second.</td>
</tr>
</tbody>
</table>

Clearing the Detector Module Counters

You can clear the Detector module counters if you are going to perform testing and want to be sure that the counters include information from the testing session only.

To clear the Detector module counters, perform the following steps:

Step 1  From the navigation pane, click Detector Summary. The Detector Summary menu appears.
Step 2  From the Detector Summary menu, choose Diagnostics > Counters > Device Counters. The Counters screen appears.
Step 3  Click Clear Counters. The Detector module clears the current counters and the traffic rates.

Viewing the Global Received Counter in Real Time

The Detector module allows you to view the Received packets counter information in real time. The Received packets counter provides information on the total number of packets that the Detector module received and analyzed.

You must have Java Runtime Environment (JRE) installed on the client to view the counter information in real time (see the “Installing Java 2 Runtime Environment” section in Chapter 1, “Product Overview”).

To view the counters in real time, perform the following steps:

Step 1  From the navigation pane, click Detector Summary. The Detector Summary menu appears.
Step 2  From the Detector Summary menu, choose Diagnostics > Counters > Real time counters. The Real Time Counters screen appears.

Step 3  (Optional) Change the unit of measurement that the Detector module uses in the traffic rate graph by choosing one of the following Graph Type options:

- **bps**—Bits per second
- **pps**—Packets per second

The Detector module updates the traffic rate graph.

---

**Viewing the Event Log**

The Detector module automatically logs system activity and events that relate to the zones under detection and to Detector module operation. You can display the Detector module logs to review and track the Detector module activity.

Table 10-4 describes the event severity levels.

<table>
<thead>
<tr>
<th>Event Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergencies</td>
<td>System is unusable</td>
</tr>
<tr>
<td>Alerts</td>
<td>Immediate action required</td>
</tr>
<tr>
<td>Critical</td>
<td>Critical condition</td>
</tr>
<tr>
<td>Errors</td>
<td>Error condition</td>
</tr>
<tr>
<td>Warnings</td>
<td>Warning condition</td>
</tr>
<tr>
<td>Notifications</td>
<td>Normal but significant condition</td>
</tr>
<tr>
<td>Informational</td>
<td>Informational messages</td>
</tr>
<tr>
<td>Debugging</td>
<td>Debugging messages</td>
</tr>
</tbody>
</table>

**Note**

The event logs only display zone-related events with a severity level of Emergency, Alert, Critical, Error, Warning, and Notification. See the “Viewing the Zone Event Log” section for more information about zone event logs.

To view the contents of the event log, perform the following steps:

**Step 1**  From the navigation pane, click Detector Summary. The Detector Summary menu appears.

**Step 2**  From the Detector Summary menu, choose Diagnostics > Event log. The Events screen appears. Use the navigation tool provided above the Events table to scroll through the events.

**Step 3**  (Optional) Control which events display in the Events table by choosing one of the following options:

- **Show all Events**—Displays the events of every severity level.
- **Show events with severity level**—Displays only the events of the severity levels that you select (see Table 10-4).
Step 4  Click Filter Events. The Detector module updates the Events table.

## Monitoring Device Resources

You can display an overview of the resources that the Detector module is using to help analyze and monitor the system status.

To view the list of Detector module resources, perform the following steps:

### Step 1
From the navigation pane, click Detector Summary. The Detector summary menu appears.

### Step 2
From the Detector summary menu, choose Diagnostics > Device Resources. The Detector module Device Resources screen appears.

Table 10-5 describes the fields of the Device Resources screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host CPU1</td>
<td>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.</td>
</tr>
<tr>
<td>Flash space usage</td>
<td>Percentage of the allocated flash space that the Detector module is using. When the flash space usage reaches approximately 75 percent of the disk maximum capacity, the Detector module displays a warning message in its syslog and sends a trap. When flash usage reaches 80 percent of the disk maximum capacity, the Detector module erases information to reduce used disk space to approximately 75 percent. We recommend that you periodically store the Detector module records on a network server and delete the old records. If the flash space usage reaches 80 percent, you can export the zone attack reports to a network server and then delete the old attack reports (see the “Exporting Attack Reports” and “Deleting Attack Reports” sections).</td>
</tr>
<tr>
<td>Accelerator card memory usage</td>
<td>Percentage of memory that the accelerator card is using. If the accelerator card memory usage is higher than 85 percent, the Detector module generates an SNMP trap. A high value may indicate that the Detector module is monitoring a high volume of traffic.</td>
</tr>
<tr>
<td>Accelerator card CPU utilization</td>
<td>Percentage of the accelerator card CPU that is being utilized. If the accelerator card CPU utilization is higher than 85 percent, the Detector module generates an SNMP trap. A high value may indicate that the Detector module is monitoring a high volume of traffic.</td>
</tr>
</tbody>
</table>
Table 10-5  Field Descriptions of Device Resources Screen (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly detection engine used memory</td>
<td>Specifies the percentage of memory that the Detector module 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 non-spoofed traffic that the Detector module is monitoring. If the anomaly detection engine memory usage is higher than 90 percent, we strongly recommend that you lower the number of active zones.</td>
</tr>
<tr>
<td>Dynamic filters used</td>
<td>Total number of dynamic filters that are active in all the zones. The Detector module 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 Detector module supports, which is 150,000. If the number of active dynamic filters reaches 150,000, the Detector module generates an SNMP trap with a severity level of EMERGENCY. If the number of active dynamic filters reaches 135,000, the Detector module generates an SNMP trap with a severity level of WARNING. A high value may indicate that the Detector module is monitoring a high traffic volume of a DDoS attack.</td>
</tr>
<tr>
<td>Number of zones</td>
<td>Total number of zones defined on the Detector module.</td>
</tr>
<tr>
<td>Number of attacked zones</td>
<td>Total number of zones with zone protection activated and under attack.</td>
</tr>
<tr>
<td>Number of active zones</td>
<td>Total number of zones with zone protection or zone learning activated.</td>
</tr>
</tbody>
</table>

Viewing the Zone Status Screen

The zone status screen (see Figure 10-2) provides a summary of the zone operating status. You can navigate to this screen as follows:

- From the All Zones list in the navigation pane, click the zone name.
- If zone anomaly detection is currently enabled, click the zone name from the Under Detection list in the navigation pane.
- From the navigation path of any zone-specific screen, click Zone.
- From the zone list (Detector Summary > Zones > Zone list), click the zone name.
Viewing the Zone Status Screen

Chapter 10  Monitoring Detector Module and Zone Operations

The zone status screen is divided into four areas (zone status bar, zone traffic rate graph, zone status table, and zone recent events table) and is described in the following topics:

- Understanding the Zone Status Bar
- Understanding the Zone Traffic Rate Graph
- Understanding the Zone Status Table
- Understanding the Zone Recent Events Table

The zone status screen contains function buttons. The WBM displays different function buttons depending on the current operating mode of the zone.

If the zone is in standby, the following function buttons appear:

- Detect & Learn—Activates the detect and learn function. The detect and learn function enables the Detector module to detect zone traffic anomalies while performing the threshold tuning phase of the learning process. Using this button is equivalent to choosing Detection > Detect and then Learning > Tune Thresholds (the order is not important) from the zone main menu.
- Detect—Activates zone anomaly detection. Using this button is equivalent to choosing Detection > Detect from the zone main menu.

If zone anomaly detection or the detect and learn function are currently enabled, the following function buttons appear:

- Deactivate—Deactivates zone protection. Using this button is equivalent to choosing Detection > Deactivate from the zone main menu.

If the protect and learn function is enabled and you click Deactivate, you have the option of deactivating zone anomaly detection, the learning process, or both operations.

- Report—Provides a link to the current attack report. Using this button is equivalent to choosing Diagnostics > Attack reports > Attack Summary from the zone main menu and clicking on the current attack (the attack with an identification number (#) of Curr. The Report button is available only if an attack is in progress. See the “Understanding Attack Report Details” section for more information.
Understanding the Zone Status Bar

The zone status bar runs across the top of the zone status screen and provides a quick reference to the current operating status of the zone. The zone status bar provides the following information:

- Name of the zone.
- Mode in which the Detector module performs zone anomaly detection—Indicates whether the Detector module operates in automatic or interactive detect mode for the zone. See the “Automatic and Interactive Operation Modes” and “Activating Automatic or Interactive Detect Mode” sections in Chapter 9, “Activating Anomaly Detection” for information about zone operation mode settings.
- Zone operating state—Indicates the current operating state of the zone. The operating state can be Under Detection, Under Detection/Tuning Thresholds, Inactive, Constructing Policy, or Tuning Thresholds.
- New recommendations—Indicates that new dynamic filter recommendations are available for you to review and decide whether to accept, ignore, or direct the recommendations to automatic activation. This indication is available only when you have the zone operation mode set to interactive.

Understanding the Zone Traffic Rate Graph

The zone traffic rate graph displays the received traffic rate over the last 2 hours measured in bits per second.

Table 10-6 describes the fields that appear below the zone traffic rate graph.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>Minimum traffic rate measured over the last 2 hours in bits per second.</td>
</tr>
<tr>
<td>Max</td>
<td>Maximum traffic rate measured over the last 2 hours in bits per second.</td>
</tr>
<tr>
<td>Avg</td>
<td>Average traffic rate measured over the last 2 hours in bits per second.</td>
</tr>
<tr>
<td>Cur</td>
<td>Current traffic rate in bits per second.</td>
</tr>
</tbody>
</table>

Understanding the Zone Status Table

The zone status table provides information on the current operation of the zone and contains the following information:

- Active Dynamic filters—Number of active dynamic filters. The number of active dynamic filters is greater than 1 when the Detector module identifies anomalies in the zone traffic.
  
  Click Active Dynamic filters to view the Dynamic Filters screen. See the “Managing Dynamic Filters” section in Chapter 9, “Activating Anomaly Detection” for information about dynamic filters.

- Pending dynamic filters—Number of pending dynamic filters. The number of pending dynamic filters is greater than 1 when the zone is in interactive detect mode and there are new recommendations.
Understanding the Zone Recent Events Table

The recent events table displays the reported zone events with a minimum severity level of notify. The Detector module also records the events in the zone event log and the Detector module event log.

Using the Zone Diagnostic Tools

The Detector module provides diagnostic information that allows you to monitor and troubleshoot zone events. This section contains the following topics:

- Viewing the Zone Counters
- Using Zone Counters to Analyze Traffic Flow
- Clearing the Zone Counters
- Viewing the Zone Counters in Real Time
- Viewing the Zone Event Log
- Viewing the Attacks Summary Report
- Viewing Details of an Attack Report
- Understanding Attack Report Details
- Exporting Attack Reports
- Deleting Attack Reports
- Viewing the Policy Statistics Table

Viewing the Zone Counters

You can use the zone counters to enable you to analyze zone-specific traffic information to verify the zone status and determine if zone anomaly detection is functioning properly. You can adjust the period of time that is displayed in the zone counters graph view to see how zone protection is evolving.

To view the zone counter information, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Counters > Zone Counters. The zone Counters screen appears.

**Step 3** (Optional) Modify the period of time that is displayed in the graph. Choose a period of time from the Graph Period drop-down list, and then click Update Graph. The Detector module updates the graph. By default, the traffic rate graph displays counter information recorded in the last 2 hours.
Step 4  (Optional) Change the unit of measurement that the Detector module uses in the traffic rate graph by choosing a unit of measurement from the Graph Type drop-down list:

- **pps**—Packets per second
- **bps**—Bits per second

Step 5  Click **Update Graph**. The Detector module updates the graph.

Step 6  (Optional) Click **Clear Counters** to clear the Detector module counters. The Detector module clears the current counters and the traffic rates. You can clear the 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 Zone Current Counters/Rates table displays the following information:

- **Packets**—Total number of packets destined to the zone since the Detector module was last reloaded.
- **Bits**—Total number of bits destined to the zone since the Detector module was last reloaded.
- **pps**—Current traffic rate destined to the zone, measured in packets per second.
- **bps**—Current traffic rate destined to the zone, measured in bits per second.

A legend that identifies the counters appears below the traffic rates graph. The minimum, maximum, and average rates for each counter display for the time period that you select.

### Using Zone Counters to Analyze Traffic Flow

It is important that you analyze the traffic flow in order to determine if traffic is flowing properly to an active zone. The following information describes how to analyze traffic flow, recognize possible problems, and provide solutions:

- A number of received packets that is greater than zero indicates proper traffic flow to the zone.
- A number of received packets that equals zero could indicate one of the following situations:
  - If the current rate (pps or bps) of received packets for the Detector module or for other zones is equal to zero, this could indicate a problem with either the traffic-capturing configuration or traffic destined to the zone or zones is blocked before it reaches the switch or router in which the Detector module is installed.
  - If the received packets current rate (pps or bps) of the Detector module or other zones is greater than zero, verify that a bypass filter is not defined for the zone.

### Clearing the Zone Counters

You can clear the zone counters if you are going to perform testing and want to be sure that the counters include information from the testing session only.

To clear the zone counters, perform the following steps:

**Step 1**  From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  From the zone main menu, choose **Diagnostics > Counters > Zone Counters**. The zone Counters screen appears.
**Viewing the Zone Counters in Real Time**

The Detector module allows you to view the zone counter information in real time.

---

**Note**

You must have JRE installed on the client to view the counter information in real time (see the “Installing Java 2 Runtime Environment” section in Chapter 1, “Product Overview”).

---

To view the zone counter information in real time, perform the following steps:

**Step 1**

From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**

From the zone main menu, choose **Diagnostics > Counters > Real Time Counters**. The zone Real Time Counters/Rates screen appears.

**Step 3**

(Optional) Change the unit of measurement that the Detector module uses in the traffic rate graph by choosing one of the following Graph Type options:

- **bps**—Bits per second
- **pps**—Packets per second

The Detector module updates the traffic rate graph.

---

For information about using the counter information to analyze zone traffic, see the “Using Zone Counters to Analyze Traffic Flow” section.

**Viewing the Zone Event Log**

The Detector module automatically logs system activity and events. You can display the Detector module logs to review and track the Detector module activity.

To view the contents of the zone event log, perform the following steps:

**Step 1**

From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**

From the zone main menu, choose **Diagnostics > Event log**. The zone Events screen appears.

**Step 3**

(Optional) Control which events display in the events table by choosing one of the following options:

- **Show all Events**—Displays the events of each severity level (see Table 10-4 for a list of possible event levels).
- **Show events with severity level**—Displays only the events of the severity levels that you select.

**Step 4**

Click **Filter Events**. The Detector module updates the events table.
Viewing the Attacks Summary Report

The Detector module provides a high level summary report for each zone to help you analyze the attacks on the zone that the Detector module detects. The report summarizes the DDoS attacks made on the zone during a user-defined period of time. The Detector module records information during an attack and organizes the data into different categories. The report provides details of the total number and intensity of the attacks with a short summary for each of the attacks. The Detector module also presents the attack data in a graph format.

To view the zone attacks summary report, perform the following steps:

**Step 1**
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**
From the zone main menu, choose **Diagnostics > Attack Reports > Attack Summary**. The Attacks Summary screen appears. By default, the report displays attack information for the last month.

**Step 3**
(Optional) Change the period of time of the attack report. Enter the period of time that you want to display in the **Period from** and to dates and then click **Get Reports**. You can enter the dates manually or click on the calendar icon at the right of each date field and then choose a date from the calendar popup window.

The Attack Summary Report screen consists of the following areas:
- Detection graph—Provides a graphical summary of the attacks during the period of time that you defined.
- Total Attack Statistics table—Provides information about the number of attacks on the zone and the aggregated attack details during the period of time that you defined.

**Figure 10-3**  
Zone Detection Summary Report—Detection Graph

![Detection graph](image)

The X-axis displays the time over which the attack occurred. The Y-axis displays the average attack rate in packets per second (pps). Each attack is represented by a bar. If you hold your mouse over any of the attack bars for a few seconds, the average attack rate displays.

To view attack details, click on the attack bar in the graph to open the attack report (see the “Viewing Details of an Attack Report” section).

- Total Attack Statistics table—Provides information about the number of attacks on the zone and the aggregated attack details during the period of time that you defined.

**Table 10-7**  
Field Descriptions for Total Attack Statistics Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks Detected</td>
<td>Number of attacks detected.</td>
</tr>
<tr>
<td>Attacks Duration</td>
<td>Aggregated duration of the detected attacks.</td>
</tr>
</tbody>
</table>
Using the Zone Diagnostic Tools

Chapter 10  Monitoring Detector Module and Zone Operations

Table 10-7  Field Descriptions for Total Attack Statistics Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Traffic Rate</td>
<td>Maximum rate of traffic destined to the zone.</td>
</tr>
<tr>
<td>Total Rx</td>
<td>Total amount of traffic destined to the zone.</td>
</tr>
</tbody>
</table>

- Per Attack Summary table—Provides a table with a list of the DDoS attacks on the zone during the period of time that you defined. You can delete the information currently displayed in the Per Attack Summary table (see the “Deleting Attack Reports” section) or export the contents of an attack report (see the “Exporting Attack Reports” section).

Table 10-8 describes the fields in the columns of the Per Attack Summary table.

Table 10-8  Field Descriptions for Summary Report

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Identification number (ID) of the detected attack. The Detector module displays a value of Curr for an ongoing attack.</td>
</tr>
<tr>
<td>Start time</td>
<td>Date and time of the detected attack.</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration of the detected attack in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of detected attack. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Tcp connections—Detected flow with an unusual number of concurrent TCP connections, with or without data.</td>
</tr>
<tr>
<td></td>
<td>• HTTP—Unusual HTTP traffic flow.</td>
</tr>
<tr>
<td></td>
<td>• Tcp incoming—Detected flow that attacks a TCP service when the zone is a server.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Unauthenticated tcp—Detected flow that the Detector anti-spoofing functions have not succeeded in authenticating. For example, ACK flood, FIN flood, or any other flood of unauthenticated packets.</td>
</tr>
<tr>
<td></td>
<td>• DNS (UDP)—Attacking DNS-UDP protocol flow.</td>
</tr>
<tr>
<td></td>
<td>• DNS (TCP)—Attacking DNS-TCP protocol flow.</td>
</tr>
<tr>
<td>Type (continued)</td>
<td>• UDP—Attacking UDP protocol flow.</td>
</tr>
<tr>
<td></td>
<td>• Non tcp/udp protocols—Non-TCP/UDP attacking protocol flow.</td>
</tr>
<tr>
<td></td>
<td>• Fragments—Detected flow with an unusual quantity of fragmented traffic.</td>
</tr>
<tr>
<td></td>
<td>• Hybrid—Attack composed of several attacks with different characteristics.</td>
</tr>
<tr>
<td></td>
<td>• IP scan—Detected flow initiated from a source IP address that tried to access many zone destination IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• port scan—Detected flow initiated from a source IP address that tried to access many zone ports.</td>
</tr>
<tr>
<td></td>
<td>• user detected—Anomaly flow detected by user definitions.</td>
</tr>
<tr>
<td></td>
<td>• worm_tcp—Worm attack over the TCP/IP protocol.</td>
</tr>
</tbody>
</table>
Chapter 10 Monitoring Detector Module and Zone Operations

Using the Zone Diagnostic Tools

### Chapter 10 Monitoring Detector Module and Zone Operations

#### Using the Zone Diagnostic Tools

**Note**

To view attack details, click in any of the rows of the Per Attack Summary table (see the “Viewing Details of an Attack Report” section).

### Viewing Details of an Attack Report

The Detector module allows you to display details of an attack report listed in the Attacks Summary screen. The attack report provides details of the attack, starting with the production of the first dynamic filter and ending either by a user decision or after a defined period of time that no new dynamic filters were added.

The Detector module records the information during an attack and organizes the data into categories. You can view the details of past and current attacks.

To view the details of an attack report, perform the following steps:

1. From the navigation pane, choose a zone. The zone main menu appears.
2. From the zone main menu, choose **Diagnostics > Attack Reports > Attack Summary**. The Attacks Summary screen appears.
3. (Optional) Change the period of time of the attack report, enter the period of time that you want to display in the **Period from** and **to** dates and then click **Get Reports**. You can enter the dates manually or click on the calendar icon at the right of each date field and then choose a date from the calendar popup window.

You can also click on any of the fields for the attack in the Per Attack Summary table.

The Detector module displays a value of *Curr* for the identification number (#) of an ongoing attack.

When an attack on a zone is in progress, the Detector module displays a Report button on the status screen of the zone under attack. Click **Report** to display the information that the Detector module is gathering on the current attack.

### Understanding Attack Report Details

The attack report contains data fields and tables that are grouped together in the following sections:

- **General Attack Information**
- **Attack Statistics**
- **Detected Anomalies**
General Attack Information

The first section of the attack report provides information about the timing of the attack, which includes when the attack started, when it ended, and how long it lasted.

To view additional report details, click i or click Show details for all events.

All counters are integers except for the rate. You can choose the statistics unit of measurement from the general attack information area of the screen.

To change the statistic unit of measurement, perform the following steps:

**Step 1** Choose the desired units to use from the Statistics units drop-down list.

**Step 2** Click Set units. The Detector module updates the display.

Attack Statistics

The attack statistics provides information on the received packets.

*Table 10-9* describes the information that is provided on the attack statistics.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Total number of packets in the category.</td>
</tr>
<tr>
<td>Max Rate</td>
<td>Maximum packet rate that was measured.</td>
</tr>
<tr>
<td>Average Rate</td>
<td>Average packet rate.</td>
</tr>
</tbody>
</table>

The traffic rate is displayed in the units that were selected from the drop-down list in the General Attack area (see the “General Attack Information” section).

Detected Anomalies

The Detected Anomalies table provides details about the anomalies that the Detector module detected in the zone traffic. The Detector module classifies the traffic as being an anomaly when it requires the production of a dynamic filter. Traffic anomalies can occur infrequently or can turn into systematic DDoS attacks. The Detector module clusters anomalies with the same type and flow parameters (such as source IP address or destination port) under one anomaly type.

*Table 10-10* describes the information that is provided for each anomaly.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Identification number (ID) of the detected anomaly.</td>
</tr>
<tr>
<td>Start time</td>
<td>Date and time that the anomaly was detected.</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration of the anomaly in hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>
### Table 10-10 Field Descriptions for Detected Anomalies (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Type**            | Type of the detected anomaly. 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 that attacks a TCP service when the zone is a server.  
|                     | - Tcp outgoing—Detected attack flow in which the client appears 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, ACK flood, 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.  
| **Type** (continued) | - Non tcp/udp protocols—Non-TCP/UDP attacking protocol flow.  
|                     | - Fragments—Detected flow with an unusual amount of fragmented traffic.  
|                     | - TCP ratio—Detected flow with an unusual ratio between different types of TCP packets (for example, SYN packets instead of FIN/RST packets).  
|                     | - 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.  
|                     | - user detected—Anomaly flow detected by user definitions.  
|                     | - Worm Tcp—Worm attack over the TCP/IP protocol.  |
| **Triggering rate** | Anomaly traffic rate that exceeded a policy threshold.  |
| **% Threshold**     | Percentage by which the triggering rate is above the policy threshold.  |
| **Anomaly Flow**    | Anomaly traffic flow. The parameters of the common flow characteristics are displayed. The information includes parameters such as the anomaly protocol number, the destination IP address of the traffic flow, and the flow packet type.  
|                     | If the anomaly flow is on a specific port, it is displayed as dst=ip address:port  |
| **Details**         | Indicates whether additional information can be viewed for this filter. Click i for additional information (see the “Viewing Details of Detected Anomalies” section).  |

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.
Viewing Details of Detected Anomalies

The Detected Anomalies Details table provides additional information about the dynamic filters that are related to the detected anomaly.

To display the Detected Anomalies Details table, click i in the details column for the filter in the Detected Anomalies table.

Table 10-11 describes the detailed anomaly information that the Detector module provides.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>Date and time that the anomaly was detected.</td>
</tr>
<tr>
<td>End time</td>
<td>Expiration date and time of the dynamic filter.</td>
</tr>
<tr>
<td>Rate (pps)</td>
<td>Rate measured in packets per second:</td>
</tr>
<tr>
<td></td>
<td>• Thresh—Indicates the policy threshold that was violated by the detected anomaly.</td>
</tr>
<tr>
<td></td>
<td>• Triggered—Indicates the anomaly traffic rate that violated a policy threshold.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of packets that were handled by the dynamic filter.</td>
</tr>
<tr>
<td>Detected flow</td>
<td>Information about the detected attack flow that caused the production of the dynamic filter:</td>
</tr>
<tr>
<td></td>
<td>• Prot.—Protocol number.</td>
</tr>
<tr>
<td></td>
<td>• Src IP—Source IP address.</td>
</tr>
<tr>
<td></td>
<td>• Src Port—Source port number.</td>
</tr>
<tr>
<td></td>
<td>• Dst IP—Destination IP address.</td>
</tr>
<tr>
<td></td>
<td>• Dst Port—Destination port number.</td>
</tr>
<tr>
<td></td>
<td>• frag.—Fragmentation characteristics of the detected traffic flow.</td>
</tr>
<tr>
<td></td>
<td>• Type—Detected anomaly type.</td>
</tr>
<tr>
<td>Action flow</td>
<td>Information about the action flow that was addressed by the dynamic filter. The action flow can have a wider range than the detected flow. For example, the detected flow could indicate a specific source port for a specific source IP. The action flow could indicate all source ports for the specific source IP. The columns represent the dynamic filter traffic data:</td>
</tr>
<tr>
<td></td>
<td>• Prot.—Protocol number.</td>
</tr>
<tr>
<td></td>
<td>• Src IP—Source IP address.</td>
</tr>
<tr>
<td></td>
<td>• Src Port—Source port number.</td>
</tr>
<tr>
<td></td>
<td>• Dst IP—Destination IP address.</td>
</tr>
<tr>
<td></td>
<td>• Dst Port—Destination port number.</td>
</tr>
<tr>
<td></td>
<td>• frag.—Fragmentation characteristics of the action flow.</td>
</tr>
</tbody>
</table>
Exporting Attack Reports

To export attack reports to a network server, perform the following steps:

**Step 1** Choose a zone from the navigation pane. The zone main menu appears.

**Step 2** Choose Diagnostics > Attack Reports > Attack Summary from the zone main menu. The Attacks Summary screen appears.

**Step 3** (Optional) Change the time period of the attack report, enter the desired Period from and to dates, and then click Get Reports. You can enter the dates manually or click on the calendar icon located at the right of each field and select a date.

**Step 4** From the Per Attack Summary table, click the check box next to the attack report to export. To choose all of the reports listed in the table, click the check box in the table header next to the number symbol (#).

**Step 5** Click Export. The Export File Server Parameters window opens.

**Step 6** From the Select File Server Parameters form, choose and define the network server to use:

- **Use automatic export file server definitions**—Exports the attack reports to the network servers that you defined in the Detector module configuration by using the CLI export reports command.

- **Use the following server definition**—Exports the attack reports to the network server that you define. Enter the following network server information:
  - **Transfer method**—The Detector module supports the File Transfer Protocol (FTP) method only for exporting attack reports.
  - **Address**—IP address of the network server.
  - **Path**—Full pathname. If you do not specify a path, the server saves the file or files in your home directory.
  - **Username**—Network server login name. The server login name. The username argument is optional when you define an FTP server. When you do not insert a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
  - **Password**—(Optional) Password for the remote FTP server. If you enter a username but do not enter a password, the Detector module prompts you for the password.

**Step 7** Click OK to export the attack reports to the network server.

Deleting Attack Reports

To delete attack reports, perform the following steps:

**Step 1** Choose a zone from the navigation pane. The zone main menu appears.

**Step 2** Choose Diagnostics > Attack Reports > Attack Summary from the zone main menu. The Attacks Summary screen appears.

**Step 3** (Optional) Change the time period of the attack report, enter the desired Period from and to dates, and then click Get Reports. You can enter the dates manually or click on the calendar icon (at the right of each field) and choose a date.

**Step 4** From the Per Attack Summary table, click the check box next to the attack report to export. To select all of the reports listed in the table, click the check box in the table header next to the number symbol (#).
Viewing the Policy Statistics Table

The policy statistics table enables you to view the rate of the traffic that flows through each policy for a specific zone. You can use this table to determine whether only legitimate traffic is passed to the zone and to manually tune thresholds.

To view the policy statistics table, perform the following steps.

**Step 1** Choose a zone from the navigation pane. The zone main menu appears.

**Step 2** Choose Diagnostics > Statistics > Policy Statistics from the zone main menu. The Policies Statistics screen appears.

**Step 3** (Optional) Filter the information displayed as follows:
   a. Click Set Screen Filter. The Policy Filter window opens.
   b. Choose the values of the parameters from the drop-down lists in the Policy Filter window.
   c. Click OK. The Policy statistics screen is updated and displays only the selected parameters. Details of the selected path and the maximum keys per policy appear in the Screen Filter frame.

The policy statistics table displays the information in four sections. The information in each section is sorted by value with the highest values appearing at the top:

- **Rate**—Rate of traffic that flows through the policy.
- **Ratio**—Ratio between the number of SYN flagged packets and the number of FIN/RST flagged packets. This information is available only for syn_by_fin policies.
- **Connections**—Number of concurrent connections or source IP addresses. This information is available for tcp_connections policies and the in_nodata_conns.
- **Dst IPs**—Number of zone destination IP addresses that were scanned. This information is available for worm_tcp policies.

For easier management of the information displayed, you can set screen filters to display only a partial list of the statistics available.

When you change one of the display parameters, the Detector module automatically clears all the parameters listed below the one that you changed. You must enter new values for the cleared parameters.

Table 10-12 describes the policy statistics fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy template</td>
<td>Policy template that was used to construct the policy.</td>
</tr>
<tr>
<td>Service</td>
<td>Services to which the policy relates.</td>
</tr>
<tr>
<td>Level</td>
<td>Level used to process the traffic flow.</td>
</tr>
</tbody>
</table>
### Table 10-12  Policy Statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Packet type. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• auth_pkts—Packets that underwent either a TCP handshake or UDP authentication.</td>
</tr>
<tr>
<td></td>
<td>• in_nodata_conns—Zone incoming connections that have no data transfer on the connection (packets without a data payload).</td>
</tr>
<tr>
<td></td>
<td>• in_pkts—Zone incoming DNS query packets.</td>
</tr>
<tr>
<td></td>
<td>• in_unauth_pkts—Zone incoming unauthenticated DNS queries.</td>
</tr>
<tr>
<td></td>
<td>• non_estb_conns—Nonestablished connections. Zone incoming failed connections. TCP connection requests (SYN packets) for which no reply was received.</td>
</tr>
<tr>
<td></td>
<td>• out_pkts—Zone incoming DNS reply packets.</td>
</tr>
<tr>
<td></td>
<td>• reqs—Request packets with data payload.</td>
</tr>
<tr>
<td></td>
<td>• syns—Synchronization packets—TCP SYN flagged packets.</td>
</tr>
<tr>
<td></td>
<td>• syn_by_fin—SYN and FIN flagged packets. Verifies the ratio between the number of SYN flagged packets and the number of FIN flagged packets.</td>
</tr>
<tr>
<td></td>
<td>• unauth_pkts—Packets that did not undergo a TCP handshake.</td>
</tr>
<tr>
<td></td>
<td>• pkts—All packet types that do not fall under any other category in the same protection level.</td>
</tr>
<tr>
<td>Policy</td>
<td>Policy identifier.</td>
</tr>
</tbody>
</table>
### Table 10-12 Policy Statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
<td>Key (traffic characteristics) used to aggregate the policies.</td>
</tr>
<tr>
<td></td>
<td>In policies that relate to worms, the key is the source IP address that scans the zone network addresses, colon, and the destination port that is being scanned. For example, 192.128.100.3:70. Possible values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• dst_ip—Traffic destined to a zone IP address.</td>
</tr>
<tr>
<td></td>
<td>• dst_ip_ratio—Ratio of SYN and FIN flagged packets destined to a specific IP address.</td>
</tr>
<tr>
<td></td>
<td>• dst_port_ratio—Ratio of SYN and FIN flagged packets destined to a specific port.</td>
</tr>
<tr>
<td></td>
<td>• global—Summation of all traffic flow as defined by the other policy sections.</td>
</tr>
<tr>
<td></td>
<td>• src_ip—Traffic destined to the zone aggregated according to source IP address.</td>
</tr>
<tr>
<td></td>
<td>• dst_port—Traffic destined to a specific zone port.</td>
</tr>
<tr>
<td></td>
<td>• protocol—Traffic destined to the zone aggregated according to protocol.</td>
</tr>
<tr>
<td></td>
<td>• src_ip_many_dst_ips—Key used for IP scanning. Traffic from a single IP address destined to many zone IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• src_ip_many_port—Key used for port scanning. Traffic from one IP address destined to many zone ports.</td>
</tr>
<tr>
<td></td>
<td>• scanners—Histogram of the number of source IP addresses that scan zone destination IP addresses on a specific destination port.</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Rate, ratio, or number of connections depending on the section of the table. The information in each section is sorted by value with the highest value appearing first.</td>
</tr>
</tbody>
</table>
CHAPTER 11

Monitoring Network Traffic and Extracting Attack Signatures

This chapter describes how to record and observe zone traffic patterns by using the packet-dump capture function, which provides nonintrusive network taps.

This chapter contains the following sections:

- Understanding Packet-Dump Capture
- Enabling Automatic Packet-Dump Capture
- Disabling Automatic Packet-Dump Capture
- Activating Manual Packet-Dump Captures
- Viewing Packet-Dump Captures
- Managing Packet-Dump Capture Files
- Extracting and Using Signatures from Packet-Dump Captures

Understanding Packet-Dump Capture

You can configure the Cisco Traffic Anomaly Detector Module (Detector module) 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 Detector module recorded previously under normal traffic conditions.

You can configure filters so that the Detector module records only traffic that meets certain criteria or you can record all traffic data and filter the traffic information that the Detector module displays.

The Detector module saves the traffic in a PCAP format, which is compressed and encoded by the gzip (GNU zip) program with an accompanying file in an Extensible Markup Language (XML) format that describes the recorded data.

From the recorded traffic, you can determine if there are any common patterns or signatures that appear in the payload of the attack packets. The Detector module can analyze the recorded traffic and extract a signature, which you can use to configure a flex-content filter to block all traffic containing the packet payloads that match the signature.
The Detector module can record traffic as follows:

- **Automatically**—Continuously records traffic data in packet-dump capture files. New packet-dump capture files replace any previously recorded capture files. To save previously recorded packet-dump capture files, you must export them to a network server.

- **Manually**—Records traffic in packet-dump capture files when you activate a recording session. New packet-dump capture files replace previously recorded capture files. To save a previously recorded capture file, export the file to a network server before you activate a new recording session.

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 Detector module can perform manual recording sessions for up to four zones simultaneously.

The Detector module allocates, by default, 20-MB disk space for manual packet-dump capture files of all zones. It can save up to 80 MB of 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.

### Enabling Automatic Packet-Dump Capture

You can activate the Detector module to automatically record network traffic for troubleshooting network problems or analyzing attack traffic. By using packet-dump capture filters, you can configure the Detector module to record only the traffic that meets the criteria that you specify. You can also record all traffic and apply packet-dump capture filters to the recorded traffic when you view it.

The Detector module records traffic in a capture buffer. When the capture buffer size reaches 20 MB, or after 10 minutes have elapsed, the Detector module saves the buffered information to a local file in a compressed format, clears the buffer, and then continues recording traffic.

Within a packet-dump capture file, the Detector module provides an IP summarization, which is a summary of the most frequently detected source IP addresses (according to the volume of traffic).

The Detector module applies a naming convention to automatic packet-dump capture files that provides information about when the Detector module recorded the traffic and how it handled the traffic. Table 11-1 describes the sections of the automatic packet-dump capture filename.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function/Zone Name</td>
<td>Zone function that the Detector module was performing at the time of the packet-dump capture and the zone name. The zone functions are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>detect</strong>—The Detector module recorded the traffic during zone anomaly detection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>learn</strong>—The Detector module recorded the traffic during the zone learning process or the protect and learning process.</td>
</tr>
<tr>
<td>Capture start time</td>
<td>Time that the Detector module started recording the traffic.</td>
</tr>
<tr>
<td>Capture end time</td>
<td>(Optional) Time that the Detector module finished recording the traffic. If the Detector module is currently recording the traffic to the file, the end time is not displayed.</td>
</tr>
<tr>
<td>Dispatch</td>
<td>Method that the Detector module used to handle the traffic. The Detector module supports the <strong>dropped</strong> method only because it drops all traffic that it receives.</td>
</tr>
</tbody>
</table>
Disabling Automatic Packet-Dump Capture

The Detector module saves one packet-dump capture file from the learning process and the following two types of packet-dump capture files when zone protection is enabled:

- Traffic from the previous 10 minutes
- Current traffic

When you activate zone protection or activate the Detector module to automatically record network traffic, the Detector module erases all previous packet-dump capture files that it recorded during the protection process and creates new ones. To save previous packet-dump capture files, you must export them to a File Transfer Protocol (FTP) server (see the “Exporting Packet-Dump Capture Files” section).

To enable the automatic packet-dump feature, perform the following steps:

**Step 1**  
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  
From the zone main menu, choose **Configuration > General**. The General screen appears, displaying the current zone configuration.

**Step 3**  
Click **Config**. The Config screen appears.

**Step 4**  
From the Packet-Dump Parameters area of the Zone form, click **On**.

**Step 5**  
Click **OK** to save the auto packet-dump setting. The Detector module begins recording all the zone traffic.

Disabling Automatic Packet-Dump Capture

You can disable the automatic packet-dump feature to stop the Detector module from recording the zone traffic.

To disable the automatic packet-dump feature, perform the following steps:

**Step 1**  
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  
From the zone main menu, choose **Configuration > General**. The General screen appears, displaying the current zone configuration.

**Step 3**  
Click **Config**. The Config screen appears.

**Step 4**  
From the Packet-Dump Parameters area of the Zone form, click **Off**.

**Step 5**  
Click **OK** to disable the auto packet-dump. The Detector module stops recording the zone traffic.
Activating Manual Packet-Dump Captures

You can activate the Detector module to start recording traffic so that you can record traffic during a specific period or change the criteria that the Detector module uses to record the traffic.

The Detector module 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.

Within a packet-dump capture file, the Detector module provides an IP summarization, which is a summary of the most frequently detected source IP addresses (according to the volume of traffic).

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 Detector module can record manual packet-dump captures for up to 10 zones simultaneously.

The Detector module allocates by default, 20 MB of disk space for manual packet-dump capture files of all zones. It can save up to 80 MB of manual and automatic packet-dump capture files of all zones. To free disk space for additional packet-dump capture files, delete any packet-dump capture files that you no longer need (see the “Deleting Packet-Dump Capture Files” section).

This section contains the following topics:
- Starting a Manual Packet-Dump Capture
- Stopping a Manual Packet-Dump Capture

Starting a Manual Packet-Dump Capture

The zone must be active (learning zone traffic or detecting anomalies in the zone traffic) before you can start a manual packet-dump capture.

To start a manual packet-dump capture, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Packet-Dump > Start Packet-Dump. The Start Packet-Dump screen appears.

**Step 3** Configure the parameters of the packet-dump capture.

Table 11-2 describes the parameters listed in the Start Packet-Dump form.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture name</td>
<td>Name for the packet-dump capture file. Enter an alphanumeric string from 1 to 63 characters. The string can contain underscores but cannot contain spaces.</td>
</tr>
<tr>
<td>Packet-Dump filter</td>
<td>(Optional) Filter that you apply to specify the traffic to record. The Detector module captures only traffic that complies with the filter expression. The expression syntax is identical to the syntax of the Flex-content filter Expression (see the “Understanding the Flex-Content Expression Syntax” section in Chapter 5, “Configuring Zone Filters”).</td>
</tr>
<tr>
<td>Dispatch value</td>
<td>Zone traffic that the Detector module captures. The Dispatch value for the Detector module is Dropped.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring Network Traffic and Extracting Attack Signatures

Viewing Packet-Dump Captures

Table 11-2  Start Packet-Dump Form Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample rate</td>
<td>Sample rate in packets per second. Enter a value from 1 to 10000. The Detector module supports a maximum accumulated packet-dump capture rate of 10000 packets per second for all concurrent manual captures.</td>
</tr>
<tr>
<td></td>
<td>A packet-dump capture configured with a high Sample Rate value consumes Detector module resources. We recommend that you use high-rate values cautiously.</td>
</tr>
<tr>
<td>Number of packets</td>
<td>Number of packets to record. When the Detector module records the number or packets that you specify, it stops the manual packet-dump capture and saves the information in the capture buffer to a file. Enter an integer from 1 to 5000.</td>
</tr>
</tbody>
</table>

Step 4  Click OK to start the manual packet-dump capture.

Stopping a Manual Packet-Dump Capture

The Detector module 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 Detector module records the specified number of packets.

To stop a manual packet-dump capture, perform the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu appears.

Step 2  From the zone main menu, choose Diagnostics > Packet-Dump > Stop Packet-Dump. The Detector module stops the manual packet-dump capture.

Viewing Packet-Dump Captures

This section describes how to view a list of packet-dump capture files, view the content of a single packet-dump capture file, and how to compare the results of two packet-dump captures.

This section contains the following topics:

- Viewing the Packet-Dump Capture List
- Viewing the Packet-Dump Capture Details
- Changing the Packet-Dump Capture Details Screen View
- Comparing Two Packet-Dump Captures
Viewing the Packet-Dump Capture List

To view the list of packet-dump capture files, perform the following steps:

**Step 1**  
From the navigation pane, choose a zone. The zone main menu appears.

**Step 2**  
From the zone main menu, choose **Diagnostics > Packet-Dump > Packet-Dump List**. The Packet-Dump List screen appears.

Table 11-3 describes the fields of the packet-dump list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the packet-dump capture file.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Date and time that the packet-dump capture began.</td>
</tr>
<tr>
<td>Stop Time</td>
<td>Date and time that the packet-dump capture ended.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the packet-dump capture, which can be automatic or manual.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the file generated by the packet-dump capture.</td>
</tr>
<tr>
<td>Packet Dump Filter</td>
<td>User-defined filter that the Detector module used when recording traffic. The filter is in TCPDump format. The expression syntax is identical to the syntax of the flex-content filter expression (see the “Understanding the Flex-Content Expression Syntax” section in Chapter 5, “Configuring Zone Filters”).</td>
</tr>
<tr>
<td>Dispatch</td>
<td>Traffic type that the Detector module recorded. The dispatch value can be Dropped or All. Both values indicate that the Detector module recorded all the traffic.</td>
</tr>
</tbody>
</table>

Table 11-4 describes the function buttons of the Packet-Dump List screen.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Stop/Start | Controls the manual packet-dump operation. This button toggles between Stop and Start depending on the current operating status of the manual packet-dump feature:  
  - **Start**—Begins a manual packet-dump capture. This button displays only when no manual packet-dump capture is currently running.  
  - **Stop**—Ends the current manual packet-dump capture. This button displays only when a manual packet-dump capture is currently running. |
| View    | Displays detailed information of one or two packet-dump capture files (see the “Viewing the Packet-Dump Capture Details” and “Comparing Two Packet-Dump Captures” sections). |
| Rename  | Changes the name of a packet-dump capture file (see the “Renaming a Manual Packet-Dump Capture File” section). |
Viewing Packet-Dump Captures

To view the details of a packet-dump capture, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-Dump List screen appears.

**Step 3** Check the check box next to the packet-dump capture that you want to view and then click **View**.

The Packet-Dump capture analysis screen appears. For information about applying a screen filter to the information displayed, see the “Changing the Packet-Dump Capture Details Screen View” section.

**Table 11-5** describes the information that the Detector module displays in the Capture and View parameter areas of the Packet-Dump Capture Analysis screen.

### Table 11-5  Packet-Dump Capture and View Parameters

<table>
<thead>
<tr>
<th>Screen Area</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture parameters</td>
<td>Name</td>
<td>Name of the capture file.</td>
</tr>
<tr>
<td></td>
<td>Start time</td>
<td>Time that the capture started.</td>
</tr>
<tr>
<td></td>
<td>End time</td>
<td>Time that the capture ended.</td>
</tr>
<tr>
<td></td>
<td>Packets</td>
<td>Number of packets that the capture file contains.</td>
</tr>
<tr>
<td></td>
<td>Packet Dump filter</td>
<td>User-defined filter that the Detector module used when recording traffic. The filter is in TCPDump format. The expression rules are identical to the Flex-content filter expression rules.</td>
</tr>
<tr>
<td></td>
<td>Dispatch</td>
<td>Traffic type that the Detector module recorded. The dispatch value can be Dropped or All. Both values indicate that the Detector module recorded all the traffic.</td>
</tr>
</tbody>
</table>

**Table 11-4  Packet-Dump List Function Buttons (continued)**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Copies a packet-dump capture file (see the “Copying a Packet-Dump Capture File” section).</td>
</tr>
<tr>
<td>Export/Import</td>
<td>Exports or imports a packet-dump capture file (see the “Exporting Packet-Dump Capture Files” and “Importing Packet-Dump Capture Files” sections).</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a packet-dump capture file (see the “Deleting Packet-Dump Capture Files” section).</td>
</tr>
</tbody>
</table>
Table 11-5  Packet-Dump Capture and View Parameters (continued)

<table>
<thead>
<tr>
<th>Screen Area</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Parameters</td>
<td>Query</td>
<td>Data profile that the Detector module uses to display the capture information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distribution: SrcIP / DstIP / SrcPort / DstPort / SrcReservedPorts /</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DstReservedPorts / Protocol / TTL / Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Table 11-6 for details on the information that the Detector module</td>
</tr>
<tr>
<td></td>
<td></td>
<td>displays for each of the query types.</td>
</tr>
<tr>
<td></td>
<td>Display filter</td>
<td>Filter that the Detector module uses when displaying the packet-dump</td>
</tr>
<tr>
<td></td>
<td></td>
<td>capture file. The Detector module displays only the portion of the packet-dump</td>
</tr>
<tr>
<td></td>
<td></td>
<td>capture file that matches the filter criteria. The expression rules are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>identical to the flex-content filter expression rules.</td>
</tr>
</tbody>
</table>

The Packet-Dump capture analysis screen contains the following buttons:

- Change View—Changes the view parameters (see the “Changing the Packet-Dump Capture Details Screen View” section).
- Save—Saves a copy of the packet-dump capture to a different filename (see the “Copying a Packet-Dump Capture File” section).
- Extract Signatures—Extracts the traffic signature from the packet-dump capture (see the “Extracting an Attack Signature from a Packet-Dump Capture” section).

Table 11-6 describes the capture information that the Detector module displays, which varies based on the type of query that you chose (see the “Changing the Packet-Dump Capture Details Screen View” section).

Table 11-6  Capture Parameters Table and Graph Details

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 20/Criteria</td>
<td>#</td>
<td>Sequential number that the Detector module assigned to each incident that it</td>
</tr>
<tr>
<td>The Criteria can be one of the following:</td>
<td></td>
<td>records during the packet-dump capture.</td>
</tr>
<tr>
<td>SrcIP</td>
<td>Key</td>
<td>IP address, port number, or protocol number, which varies based on the</td>
</tr>
<tr>
<td>DstIP</td>
<td></td>
<td>query type that you select.</td>
</tr>
<tr>
<td>SrcPort</td>
<td>Packets</td>
<td>Number of packets in the packet-dump capture.</td>
</tr>
<tr>
<td>DstPort</td>
<td>%</td>
<td>Percentage of packets in the packet-dump capture that fit the criteria.</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Changing the Packet-Dump Capture Details Screen View

To change the view of the Packet-Dump Capture details screen, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-Dump List screen appears.

**Step 3** Click Change View. The Change Packet-Dump View Parameters window opens.

**Step 4** Configure the viewing parameters of the packet-dump capture. Table 11-7 describes the parameters of the Change Packet-Dump View Parameters form.

---

Table 11-6  Capture Parameters Table and Graph Details (continued)

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution/Criteria</td>
<td>x-axis</td>
<td>Units of the distribution attribute that you select, such as the IP address, the port number, or the protocol number.</td>
</tr>
<tr>
<td>The Criteria can be one of the following:</td>
<td>y-axis</td>
<td>Number of packets.</td>
</tr>
<tr>
<td>• SrcIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DstIP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SrcPort</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DstPort</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SrcReservedPorts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DstReservedPorts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• TTL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets List</td>
<td>#</td>
<td>Sequential number that the Detector module assigned to each incident it recorded during the packet-dump capture.</td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td>Time that the packet-dump was captured.</td>
</tr>
<tr>
<td>ScrIp</td>
<td></td>
<td>Source IP address of the packets.</td>
</tr>
<tr>
<td>ScrPort</td>
<td></td>
<td>Source port of the packets.</td>
</tr>
<tr>
<td>DstIp</td>
<td></td>
<td>Destination IP address of the packets.</td>
</tr>
<tr>
<td>DstPort</td>
<td></td>
<td>Destination port of the packets.</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
<td>Protocol number of the packets.</td>
</tr>
<tr>
<td>Info</td>
<td></td>
<td>Additional information on the packets.</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring Network Traffic and Extracting Attack Signatures

Comparing Two Packet-Dump Captures

To compare the details of two packet-dump captures, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.
Step 2  From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-Dump List screen appears.

Step 3  Check the check box next to the packet-dump capture that you want to view as the base capture.

Step 4  Check the check box next to the packet-dump capture that you want to view as the reference capture.

Step 5  Click View. The Packet-Dump capture analysis screen appears, displaying the details of the base and reference packet-dump captures.

Step 6  (Optional) Click Swap Base and Reference to switch the two packet captures, making the base capture the reference capture and the reference capture the base capture. Use this function when extracting a signature (the Detector module extracts the signature from the base capture). For information about extracting a signature, see the “Extracting and Using Signatures from Packet-Dump Captures” section.

For a description of the information that the Detector module displays in the Packet-Dump capture analysis screen, see the “Viewing the Packet-Dump Capture Details” section.

Managing Packet-Dump Capture Files

This section contains the following topics:

- Renaming a Manual Packet-Dump Capture File
- Copying a Packet-Dump Capture File
- Exporting Packet-Dump Capture Files
- Importing Packet-Dump Capture Files
- Deleting Packet-Dump Capture Files

Renaming a Manual Packet-Dump Capture File

You can rename a manual packet-dump capture file, but you cannot rename an automatic packet-dump capture file. To change the name of an automatic packet-dump capture file, you must copy the file (see the “Copying a Packet-Dump Capture File” section).

To rename a manual packet-dump capture, perform the following steps:

Step 1  From the navigation pane, choose a zone. The zone main menu appears.

Step 2  From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-Dump List screen appears.

Step 3  Check the check box next to the packet-dump capture that you want to rename, and then click Rename. The Rename window opens.

Step 4  In the New name field, enter a new name for the packet-dump capture file. The name is an alphanumeric string from 1 to 63 characters and can contain underscores and dashes but cannot contain spaces.

Step 5  Click OK to save the packet-dump capture using the new name.
Copying a Packet-Dump Capture File

You can copy a packet-dump capture file (or a portion of a file) under a new name. Because the Detector module overwrites existing automatic packet-dump capture files with new ones, the copy option enables you to save an automatic packet-dump capture file for use at a later time. When you copy an automatic packet-dump capture file or a manual packet-dump capture file, the Detector module saves them as manual files and does not delete the original packet-dump capture file. You must manually delete them if you need to free disk space (see the “Deleting Packet-Dump Capture Files” section).

To copy a packet-dump capture file, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-dump List screen appears.

**Step 3** Check the check box next to the packet-dump capture that you want to copy, and then click Copy. The Packet-Dump capture analysis screen appears.

**Step 4** In the New name field, enter a new name for the packet-dump capture file. The name is an alphanumeric string from 1 to 63 characters and can contain underscores and dashes but cannot contain spaces.

**Step 5** (Optional) Define the filter that the Detector module uses to copy the packet-dump capture file. The Detector module 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 expression rules (see the “Understanding the Flex-Content Expression Syntax” section in Chapter 5, “Configuring Zone Filters”).

**Step 6** Click OK to save the packet-dump capture using the new name.

You can also copy a file by displaying the packet-dump capture details (see the “Viewing the Packet-Dump Capture Details” section) and then click Save. The Detector module saves the portion of the files that is displayed. If you configure a filter that the Detector module uses to display the packet-dump capture file, the Detector module uses the same filter to save the portion of the packet-dump capture file that matches the filter criteria.

Exporting Packet-Dump Capture Files

You can manually export packet-dump capture files to a network server that uses File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), or Secure Copy Protocol (SCP) to transfer files. You can export a single packet-dump capture file or all packet-dump capture files of a specific zone. The Detector module exports the packet-dump capture files in a PCAP format, which is compressed and encoded by the gzip (GNU zip) program with an accompanying file in an 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 the Software Center at http://www.cisco.com/public/sw-center/.

To export a packet-dump capture, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-dump List screen appears.
Step 3 Check the check box next to the packet-dump capture files that you want to export, and then click Export. The Export File Server Parameters window opens.

To choose all of the packet-dump captures, check the check box in the table header.

Step 4 From the Select File Server Parameters form, choose the network server to use:

- **Use automatic export file server definitions**—Exports the packet-dump capture files to the network servers that you defined in the Detector module configuration by using the CLI `export packet-dump` command.

- **Use the following server definition**—Exports the packet-dump capture files to the network server that you define. Enter the following network server information:
  - **Transfer method**—Transfer protocol to use. The transfer method can be one of the following:
    - FTP—Specifies FTP.
    - SFTP—Specifies SFTP.
    - SCP—Specifies SCP.
    
    Because SFTP and SCP rely on Secure Shell (SSH) for their secure transport, if you do not configure the key that the Detector module uses for the secure communication before you export attack reports to an SFTP or SCP server, the Detector module prompts you for the password. You must use the Detector module CLI to configure the key for SFTP and SCP.
  
  - **Address**—IP address of the network server.
  
  - **Path**—Complete pathname where the Detector module saves the packet-dump capture files. If you do not specify a path, the network server saves the packet-dump capture files in your home directory.
  
  - **Username**—Network server login name. The username argument is optional when you define an FTP server. When you do not insert a login name, the FTP server assumes an anonymous login and does not prompt you for a password.
  
  - **Password**—(Optional) Password for the remote FTP server. If you enter a user name but do not enter a password, the Detector module prompts you for the password.

Step 5 Click OK to export the packet-dump capture files to the network server.

---

**Importing Packet-Dump Capture Files**

You can import packet-dump capture files from a network server to the Detector module to analyze past events or to compare current network traffic patterns with traffic patterns that the Detector module recorded previously under normal traffic conditions. The Detector module imports the packet-dump capture files in both XML and PCAP formats.

To import a packet-dump capture, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu appears.

Step 2 From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-dump List screen appears.

Step 3 Click Import. The Import FTP Server Parameters window opens.

Step 4 In the File Name field, enter the 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.
Managing Packet-Dump Capture Files

Note

Do not specify the file extension because it will cause the import process to fail.

Step 5 From the Select File Server Parameters form, choose the network server to use:

- **Use automatic export file server definitions**—Imports the packet-dump capture files from the
network servers that you defined in the Detector module configuration by using the CLI export
packet-dump command.

- **Use the following server definition**—Imports the packet-dump capture files from the network
server that you define. Enter the following network server information:

  - **Transfer method**—Transfer protocol to use. The transfer method can be one of the following:
    
    FTP—Specifies FTP.
    
    SFTP—Specifies SFTP.
    
    SCP—Specifies SCP.
    
    Because SFTP and SCP rely on SSH for their secure transport, if you do not configure the key
that the Detector module uses for the secure communication before you export attack reports to
an SFTP or SCP server, the Detector module prompts you for the password. You must use the
Detector module CLI to configure the key for SFTP and SCP.

  - **Address**—IP address of the network server.

  - **Path**—Complete pathname from where the Detector module imports the packet-dump capture
files. If you do not specify a path, the network server copies the packet-dump capture file from
your home directory.

  - **Username**—Network server login name. The username argument is optional when you define
an FTP server. When you do not insert a login name, the FTP server assumes an anonymous
login and does not prompt you for a password.

  - **Password**—(Optional) Password for the remote FTP server. If you enter a username but do not
enter a password, the Detector module prompts you for the password.

Step 6 Click **OK** to import the packet-dump capture file from the network server.

Deleting Packet-Dump Capture Files

The Detector module allocates by default, 20 MB of disk space for manual packet-dump capture files of
all zones. It can save up to 80 MB 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 a maximum of 10 packet-dump capture files on the Detector module. You must delete old
manual packet-dump capture files to allow space for new files.

To delete a packet-dump capture, perform the following steps:

Step 1 From the navigation pane, choose a zone. The zone main menu appears.

Step 2 From the zone main menu, choose **Diagnostics > Packet-Dump > Packet-Dump List**. The
Packet-dump List screen appears.
Chapter 11: Monitoring Network Traffic and Extracting Attack Signatures

Extracting and Using Signatures from Packet-Dump Captures

An attack signature describes the common pattern that appears in the payload of attack packets. You can activate the Detector module to generate the signature of anomalous traffic and then use this information to quickly identify future attacks of the same type. This feature allows you to detect new Distributed Denial of Service (DDoS) attacks and Internet worms even before the attack signatures are published (for example, from antivirus software companies or mailing lists).

The Detector module generates the attack signature using the flex-content filter pattern expression syntax. You can use this signature in the flex-content filter pattern to filter out anomalous traffic. See the “Understanding the Flex-Content Filter Pattern Syntax” section in Chapter 5, “Configuring Zone Filters” for more information.

You can specify an additional packet-dump capture file that the Detector module recorded during normal traffic conditions as a reference. If you specify a reference packet-dump capture file, the Detector module generates the signature from the anomalous traffic and specifies the percentage of time that the signature is present in traffic that was recorded during normal traffic conditions. If the attack signature appears in a high percentage of the normal traffic recording, the signature may not be an accurate representation of the attack pattern.

This section contains the following topics:

- Extracting an Attack Signature from a Packet-Dump Capture
- Adding an Attack Signature to a Flex-Content Filter
- Using an Attack Signature as a Display Pattern for Displaying Packet-Dump Captures

Extracting an Attack Signature from a Packet-Dump Capture

To extract an attack signature from a packet-dump capture file, perform the following steps:

**Step 1** From the navigation pane, choose a zone. The zone main menu appears.

**Step 2** From the zone main menu, choose Diagnostics > Packet-Dump > Packet-Dump List. The Packet-dump List screen appears.

**Step 3** Check the check box next to the packet-dump capture from which to extract the signature.

**Step 4** (Optional) Check the check box next to the packet-dump capture that you want to use as a reference. The reference should be a capture file of traffic that was recorded during normal traffic conditions.

**Step 5** Click View. The Packet-Dump Capture Analysis screen appears.

**Step 6** (Optional) Click Swap Base and Reference to switch the two packet captures, making the base capture the reference capture, and the reference capture the base capture. The Detector module extracts the signature from the base capture.
Step 7 Click Extract Signatures. The Detector module extracts the signatures from the base packet-dump capture and opens the Packet-Dump Signature Extraction window.

Table 11-8 describes the signature information that the Detector module displays in the Packet-Dump Signature Extraction window.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture name</td>
<td>Name of packet-dump capture from which the Detector module extracted the signature.</td>
</tr>
<tr>
<td>Pattern</td>
<td>List of the patterns (in an abbreviated format) that the Detector module extracted from the packet-dump capture. Move the mouse over the pattern to display the complete pattern.</td>
</tr>
<tr>
<td>Start offset</td>
<td>Offset, in bytes, from the beginning of the packet payload, where the pattern-matching begins. The default is 0, which is the start of the payload.</td>
</tr>
<tr>
<td>End offset</td>
<td>Offset, in bytes, from the beginning of the packet payload, where the pattern-matching ends. The default is the packet length, which is the end of the payload.</td>
</tr>
<tr>
<td>% Reference</td>
<td>Percentage of time that the signature is present in the reference capture file.</td>
</tr>
</tbody>
</table>

To add one of the signatures that the Detector module displays to a flex-content filter, see the “Adding an Attack Signature to a Flex-Content Filter” section.

Adding an Attack Signature to a Flex-Content Filter

The Detector module allows you to create a flex-content filter using a signature that it extracts from the packet-dump capture. You can then use the flex-content filter to block zone traffic that matches the attack signature.

To add an attack signature to a flex-content filter, perform the following steps:

Step 1 Extract the signatures from a packet-dump capture. See the “Extracting an Attack Signature from a Packet-Dump Capture” section for more information.

Step 2 From the Packet-Dump Signature Extraction window, choose the signature that you want to use in the flex-content filter, and then click Insert Content Filter. The Flex-Content Filters > Add Filter - Step 2 screen appears.

Step 3 Configure the Flex-Content filter parameters.

Table 11-9 describes the filter parameters listed in the Flex-Content Filter form.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Text that describes the flex-content filter.</td>
</tr>
</tbody>
</table>
### Table 11-9 Flex-Content Filter Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Processes traffic using a specific protocol. Enter a protocol number from 0 to 255. To specify any protocol type, enter an asterisk (*). Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid protocol numbers: <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a></td>
</tr>
<tr>
<td>Dst Port</td>
<td>Processes traffic flowing to a specific destination port. Enter a destination port number from 0 to 65535. To specify any destination port, enter an asterisk (*). Refer to the Internet Assigned Numbers Authority (IANA) website for a list of valid port numbers: <a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></td>
</tr>
<tr>
<td>Expression</td>
<td>Filters traffic based on the specified expression (see the “Understanding the Flex-Content Expression Syntax” section in Chapter 5, “Configuring Zone Filters”). Enter the expression to use.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Specifies the regular expression data pattern that is to be matched with the packet content (see the “Understanding the Flex-Content Filter Pattern Syntax” section in Chapter 5, “Configuring Zone Filters”). Enter the data pattern to use.</td>
</tr>
<tr>
<td>Match Case</td>
<td>Specifies whether the pattern expression that the filter matches is case sensitive or not case sensitive. Check the check box to define the data pattern expression as case sensitive.</td>
</tr>
<tr>
<td>Start Offset</td>
<td>Specifies the offset (in bytes) from the beginning of the packet content where the pattern matching begins. The default is 0, which is the start of the payload. The start offset applies to the pattern field. Enter an integer from 0 to 2047.</td>
</tr>
<tr>
<td>End Offset</td>
<td>Specifies the offset (in bytes) from the beginning of the packet content where the pattern matching ends. The default is the packet length, which is the end of the payload. The end offset applies to the pattern field. Enter an integer from 0 to 2047.</td>
</tr>
</tbody>
</table>
| Action      | Specifies the action that the flex-content filter performs on the traffic. Choose one of the following actions from the Action drop-down list:  
  - count—Counts the traffic flow packets that match the filter  
  - drop—Drops the traffic flow packets that match the filter |
| State       | Specifies the operating state of the flex-content filter. Choose one of the following operating states from the State drop-down list:  
  - enable—The Detector module applies the filter to the traffic flow and executes the configured action on the flow that matches the filter.  
  - disable—The Detector module does not apply the filter to the traffic flow. |

**Step 4** Click **OK** to save the new Flex-Content filter.
Using an Attack Signature as a Display Pattern for Displaying Packet-Dump Captures

The Detector module allows you to filter the packet-dump capture display using a signature that it extracts from the packet-dump capture.

To use an attack signature as a display pattern for displaying packet-dump captures, perform the following steps:

**Step 1** Extract the signatures from a packet-dump capture. See the “Extracting an Attack Signature from a Packet-Dump Capture” for more information.

**Step 2** From the Packet-Dump Signature Extraction window, choose the signature that you want to use as the display pattern, and then click Use as View Filter. The Packet-Dump capture analysis screen appears.

Table 11-10 describes the information that the Detector module displays in the Capture and View parameter areas of the Packet-Dump Capture analysis screen.

<table>
<thead>
<tr>
<th>Screen Area</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture parameters</td>
<td>Name</td>
<td>Name of the capture file.</td>
</tr>
<tr>
<td></td>
<td>Start time</td>
<td>Time that the capture started.</td>
</tr>
<tr>
<td></td>
<td>End time</td>
<td>Time that the capture ended.</td>
</tr>
<tr>
<td></td>
<td>Packets</td>
<td>Number of packets that the capture file contains.</td>
</tr>
<tr>
<td></td>
<td>PacketDump filter</td>
<td>User-defined filter that the Detector module used when recording traffic. The filter is in TCPDump format. The expression rules are identical to the Flex-content filter expression rules.</td>
</tr>
<tr>
<td></td>
<td>Dispatch</td>
<td>Traffic type that the Detector module recorded. The dispatch value can be DROPPED or ALL. Both values indicate that the Detector module recorded all the traffic.</td>
</tr>
<tr>
<td>View Parameters</td>
<td>Query</td>
<td>Data profile that the Detector module uses to display the capture information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Top 20: SrcIP / DstIP / SrcPort / DstPort / Protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Table 11-6 for details on the information that the Detector module displays for each of the query types.</td>
</tr>
<tr>
<td></td>
<td>Display filter</td>
<td>Filter that the Detector module uses when displaying the packet-dump capture file. The Detector module 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 expression rules.</td>
</tr>
</tbody>
</table>
Symbols

# (number sign) 10-17

A

AAA services 3-2
activation extent
   entire zone 4-10
   IP address only 4-10
activation interface
   by IP address 4-10
   by packet 4-9
active dynamic filters 10-9
analyzing traffic flow 10-11
anomaly detection
   activating 9-3
   verifying 9-3
anomaly detection engine memory usage 10-7
anomaly flow, common characteristics 10-17
attack report
   deleting 10-19
   exporting 10-19
   statistics 10-16
   understanding report details 10-15
attacks summary report 10-13
attack summary 10-14
attack type 10-14
auth packet types 8-4, 10-21
automatic detect mode 9-2
automatic learning, configuring 7-9
automatic operation mode 9-2
automatic protect operation mode 4-6, 4-7

B

banner, configuring login 2-3
base zone 7-19
base zone services
   adding 7-21
   copying policy parameters to the base zone 7-21
   deleting 7-21
basic filter actions 5-11
Berkley Packet filter 5-6
burst 4-8
bypass filter
   adding 5-2
   configuring 5-2
   deleting 5-3

C

changing password 3-5
compared zone 7-19
connections, concurrent or source IP addresses 10-20
constructing policies 7-2
copy wbm-logo command 2-3
counters
   clearing Detector 10-4
   clearing zone 10-11
   received packets 10-4
   viewing 10-3
   zone 10-10

D

DDoS
Index

nonspoofed attacks 1-4
overview 1-3
spoofed attacks 1-4
zombies 1-4
Detect and Learn feature
activating 7-11
deactivating 7-12
detected anomalies
types 10-17
viewing 10-16
viewing details 10-18
detected attack types 10-14
Detect feature
activating 9-3
deactivating 9-3
detect mode
activating 9-3
automatic 9-2
deactivating 9-3
interactive 9-2
Detector
counters, clearing 10-4
overview 1-3
recommendations, acting on 9-12
zone templates 4-5
device resources, monitoring 10-6
diagnostics, viewing 10-3
DNS
policy templates 6-2
tcp protocol flow 10-14
drop filter action 5-11
dst traffic characteristics 8-5
dynamic filter
actions 9-8
active 10-9
adding 9-7
deleting 9-8
fields 9-7
overview 9-5
pending 9-11, 10-9
preventing production of recommendations 9-8
viewing 9-5

E
event log
global 10-5
zone 10-12
exporting an attack report 10-19
extent of zone protection 4-4

F
filter
dynamic 9-5
flex-content 5-4
user 5-2
zone filter overview 5-1
filter-rate termination threshold 4-9
flex-content filter
adding 5-7
configuring 5-4
deleting 5-9
expression 5-4
pattern 5-7
fragments 10-14, 10-17

G
general attack information 10-16
global counters, viewing in real time 10-4
GUARD_VOIP zone template 4-6
Guard zones 4-2
Guard zone templates 4-6
H

http 10-17
HTTP policy template 6-2
hybrid 10-14

I

icons 1-7
information area 1-6
in packet types 10-21
interactive detect mode 9-2
interactive operation mode 9-2
interactive protect operation mode 4-6, 4-7
IP scan 6-2, 10-14, 10-17
IP summarization 11-2, 11-4
IP threshold configuration 8-8

J

Java 2 Runtime Environment (JRE), installing 1-2

L

learning process
  overview 7-2
  performing 7-3
  phases 7-2
policy construction phase
  accepting results 7-5
  starting 7-4
  stopping 7-5
threshold tuning phase 7-2
  accepting results 7-6
  starting 7-5
  stopping 7-7
login banner, configuring 2-3
logo, adding WBM 2-3

M

main menu bar 1-6
malicious-rate
detection threshold 4-9
termination threshold 4-9
marking zone policies tuned or untuned 7-14
memory usage, anomaly detection engine 10-7

N

navigation area 1-6
nonspoofed attacks 1-4

O

operation modes
  automatic protect 4-6, 4-7
  interactive protect 4-6, 4-7
other protocols, policy template 6-2
out_pkts packet types 10-21

P

packet-dump
  automatic
    activating 11-2
packet-dump capture
  automatic capture
    disabling 11-3
    enabling 11-2
  file
    deleting 11-14
    exporting 11-12
    importing 11-13
    renaming 11-11
    manual capture
      starting 11-4
stopping 11-5
overview 11-1
packet type
  auth 8-4
  out_pkts 10-21
  pkts 8-4, 10-21
  reqs 8-4
  syns 8-4
  unauth_pkts 8-4, 10-21
password, changing 3-5
pending dynamic filters
  accepting 9-15
  exceeding 1000 9-10
  fields 9-14
  overview 9-11
  viewing 9-13
  viewing number of 10-9
permit filter action 5-11
pkts packet type 8-4, 10-21
policy
  adding services 8-10
  constructing 7-2
  deleting services 8-11
  key 8-5
  service 8-3
  statistics 10-20
policy construction phase
  starting 7-4
  stopping 7-5
policy statistics table, viewing 10-20
policy template
  Guard policy templates for synchronization 6-3
  other_protocols 6-2
  overview 6-1
  template types 6-1
port scan 6-2, 10-14, 10-17
privilege levels, moving between 3-6
protection activation methods 4-3
protection-end time 4-9
protect-IP state
  entire zone 4-7
  only dst IP 4-7
  only dstIP by address 4-8
  policy type 4-8
R
  rate 4-8
  ratio, SYN to FIN/RST packets 10-20
recommendations
  activating 9-12
  fields 9-12
  viewing new 9-11
remote Guard, activating 9-7
replied IP summarization 11-2, 11-4
reqs packet type 8-4, 10-21
RTP/RTCP 4-6
S
  scanners traffic characteristics 8-5
  service
    adding 8-10
    deleting 8-11
SIP
  zone template 4-6
  SIP, user filter action 5-11
snapshot
  backing up zone policies 7-16
  comparing two snapshots 7-19
  taking a snapshot 7-15
spoofed attacks 1-4
src traffic characteristics 8-5, 10-22
status icons 1-7
status summary, zone 10-9
strong filter action 5-11
subzone 4-4
syn_by_fin packet type 10-21
sys packet types 8-4, 10-21
system requirements 1-2

T
TACACS+
AAA services 3-2
TCP
detected anomalies 10-14, 10-17
policy templates 6-2
template, zone 4-5
threshold
configuring IP threshold 8-8
filter-rate termination 4-9
malicious-rate termination 4-9
tuning 7-2
threshold tuning phase
overview 7-2
starting 7-5
stopping 7-7
troubleshooting WBM connection 2-2
tuning thresholds 7-2, 7-6

U
UDP policy template 6-2
unauth_pcks packet type 8-4, 10-21
user filter 5-2
action 5-11
adding 5-10
configuring 5-9
deleting 5-12
user privilege level, moving between 3-6
user profile
changing another user password 3-5
changing your password 3-5

W
WBM
enabling service 2-1
launching 2-2
navigation maps 1-7
overview 1-5
requirements
client 1-2
Detector 1-2
setting up 2-1
troubleshooting connection 2-2
WBM logo, adding 2-3
worm
  policy 8-5
  policy templates 6-3

z
zombies 1-4
zone
  counters
    clearing 10-11
    viewing 10-10
    viewing in real time 10-12
create
  methods 4-2
  using another zone 4-11
  using a zone template 4-4
delete 4-14
diagnostic tools 10-10
event log 10-12
extent of protection 4-4
Guard zone 4-2
IP address
  add 4-11
  delete 4-12
learning 7-2
overview 4-1
policies
  adding an IP address and threshold 8-9
  service, adding 8-10
  service, deleting 8-11
  tuned 7-14
  untuned 7-14
  viewing 8-2
protection activation methods 4-3
protection characteristics 4-3
recent events table 10-10
status 10-7
  status bar 10-9
  status icons 1-7
status table 10-9
summary 10-9
templates 4-5
traffic rate graph 10-9
zone templates
  Detector 4-5
  Guard 4-6