



CHAPTER 1

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](#)

- [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 select **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).
- Configure remote Guard lists—Defines the remote Guards that the Detector module can activate when the Detector module detects anomalies in the zone traffic.
- Configure a communication channel between the Detector module and each Guard—Configures the Secure Sockets Layer (SSL) or Secure Shell (SSH) communication channel between the Detector module and the Guards on the remote Guard lists. The Detector module can use the communication channel to activate the Guard when the Detector module detects an anomaly in the zone traffic.
- Copy zone traffic—Configures the supervisor engine to pass a copy of the zone traffic to the Detector module for analysis.

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

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.

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 WBM 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

The screenshot shows the TWdetector web-based manager interface. The top navigation bar includes 'Home', 'Logout', and 'About' (callout 4). Below the navigation bar are tabs for 'Main', 'Diagnostics', 'Detection', 'Learning', and 'Configuration'. The left sidebar (callout 1) contains a tree view with 'Detector' (callout 2) expanded to show 'Zone scannet (automatic) - Inactive'. Under 'Zone scannet', there are sub-sections: 'Under detection (1)', 'All Zones (0)', 'MailServer', 'scannet', and 'tw' (callout 3). The main content area displays configuration details for the 'Zone scannet (automatic) - Inactive' zone, including a table of attributes and an IP/Mask table. The attribute table (callout 5) lists settings such as Name, Description, Operation mode, From Template, Protect-IP state, Flexible Filter, Flexible Filter Action, and Flexible Filter Drop Count. The IP/Mask table shows a single entry with IP '192.168.250.120' and Mask '255.255.255.255'. A 'Config' button is visible below the attribute table, and 'Add' and 'Delete' buttons are below the IP/Mask table. The page number '119672' is located at the bottom right.

Table 1-1 WBM Window Sections

Section	Function
1	<p>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:</p> <ul style="list-style-type: none"> • Detector Summary menu—Provides access to the following Detector module statistical and configuration options: <ul style="list-style-type: none"> – Detector module status and diagnostic tools – List of defined zones – User profile manager <p>To view the Detector module summary menu, click Detector Summary in the navigation pane (3).</p> • Zone main menu—Provides access to detailed zone information and configuration options. <p>To view the zone-specific menu, click on a zone that is listed in the navigation area (3).</p>
2	<p>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.</p>
3	<p>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.</p> <p>To resize the navigation area, drag the frame bar between the navigation and the display areas.</p>

Table 1-1 *WBM Window Sections (continued)*

Section	Function
4	<p>Information Area—Displays information on the username and privilege level of the current user and provides the following links:</p> <ul style="list-style-type: none"> • 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	<p>Work Area—Displays the information that you select. To resize the work area, drag the frame bar between the navigation and work areas.</p>

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*





Icon	Status
	Zone is inactive. The Detector module is not learning zone traffic or monitoring zone traffic for anomalies.
	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.

Table 1-2 Zone Status Icons (continued)

Icon	Status
	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.
	Zone is active. The Detector module is monitoring an attack on the zone and new zone protection recommendations are available that require your attention.

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 1-2 Detector Summary Menu

Level 1	Level 2	Level 3
Main	Summary	
Diagnostics	Counters	Detector counters
		Real-time counters
	Event log	

Table 1-2 *Detector Summary Menu (continued)*

Level 1	Level 2	Level 3
Zones	Zone list	
	Create zone	
	Template list	
	Compare zone policies	
Users	User list	
	Create user	
	Change password	

- 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 1-3](#) provides a map of the zone menu levels.

Table 1-3 *Zone Menu*

Level 1	Level 2	Level 3
Main	Summary	
	Create zone	
	Save as . . .	
Diagnostics	Counters	Zone Counters
		Real-time counters
	Event log	
	Attack reports	Attack Summary
		HTTP Zombies
	Statistics	Policy statistics
		Drop Statistics
	Packet-Dump	Start Packet-Dump
		Stop Packet-Dump
		Packet-Dump List

Table 1-3 Zone Menu (continued)

Level 1	Level 2	Level 3
Detection	Detect	
	Deactivate	
	Dynamic Filters	
	Recommendations	
Learning	Construct Policies	
	Tune Thresholds	
	Deactivate	
	Stop Learning	
	Accept	
	Snapshot	
	Snapshot List	
Configuration	General	
	Filters	User Filters
		Bypass Filters
		Flex-Content Filters
	Policy Templates	View
		Add Service
		Remove Service
	Policies	View
		Compare Policies
		Learning Parameters