



CHAPTER 1

Product Overview

This chapter provides an overview of the Cisco Guard (Guard) Web-Based Manager (WBM) that you can use to remotely operate and monitor the Guard. The WBM is a graphical user interface that communicates with the Guard by translating its HTML pages into Guard commands.

This chapter contains the following sections:

- [User Interface Requirements](#)
- [Guard Requirements for WBM Operation](#)
- [Understanding the Cisco Guard](#)
- [Understanding DDoS](#)
- [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 Guard 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 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.
-

Guard Requirements for WBM Operation

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

- Configure the network interfaces—Configures the Guard network interfaces. You cannot connect to the Guard until you configure the Guard interfaces for operation in your networking environment.
- Configure traffic diversion—Configures traffic diversion so that the Guard can divert the zone traffic to itself and then inject the legitimate traffic back into the network when you activate zone protection.
- Enable the WBM service and permit access—Enables the WBM service on the Guard and permits access to the Guard 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 Cisco Guard

The Guard is a Distributed Denial of Service (DDoS) attack mitigation device that diverts suspect traffic from its normal network path to itself for cleaning. During the traffic cleaning process, the Guard identifies and drops the attack packets and forwards the legitimate packets to their targeted network destinations.

Typically, you deploy the Guard in a distributed upstream configuration at the backbone level.

You define the network elements, or *zones*, that the Guard protects against DDoS attacks. When a zone is under attack, the Guard diverts only the network traffic that is destined for the targeted zone, identifies and drops specific attack packets, and forwards legitimate traffic packets to the zone. The Guard constantly filters the zone traffic and modifies the attack mitigation process as the attack pattern

evolves. When the Guard determines that the attack on the zone has ended, it stops diverting the zone traffic to itself. By diverting network traffic only when needed, the Guard can assume its protective role when there is an attack but remain unobtrusively in the network background for the rest of the time.

The Guard 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 Guard 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 Guard uses to determine when the zone traffic is normal or abnormal (indicating an attack on the zone).
- **Traffic protection**—Distinguishes between legitimate and malicious traffic and filter the malicious traffic so that only the legitimate traffic is allowed to pass on to the zone.
- **Traffic diversion**—Diverts the zone traffic from its normal network path to the Guard learning and protection processes and then returns the legitimate zone traffic to the network.

Understanding DDoS

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 Guard protects 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 Guard configures the zone with a default set of policies and policy thresholds to detect anomalies in the zone traffic.

The Guard can protect 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 Guard 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 Guard and zone operations. Some features of the Guard, mostly related to the initial installation and configuration of the Guard, can only be configured using the CLI and cannot be configured using the WBM. See the *Guard 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 RHTwGuard web interface. At the top right, there are links for Home, Logout, and About, and the user information: User name: admin, Privileges: admin. Below this is a navigation bar with tabs: Main, Diagnostics, Protection, Learning, and Configuration. The main content area is titled 'Zone scannet (automatic) - inactive' and shows a table of attributes and values for this zone. On the left, there is a sidebar with 'Guard Summary' and 'Protected Zones (0)'. Below that, 'All Zones (3)' lists 'scannet', 'Scannet-MailServ', and 'Scannet-MailServ'. A table at the bottom shows IP addresses and masks for the zone.

Attribute	Value
Name	scannet
Description	
Operation mode	automatic
From Template	DEFAULT
Rate	unlimited
Burst	unlimited
Flexible Filter	
Flexible Filter Action	disable
Flexible Filter Drop Count	0 packets
Protection-end timer	Never
Filter-rate termination threshold	2.0 spps
Malicious-rate termination threshold	50.0 spps

ID	Mask
192.168.250.120	255.255.255.255

119661

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"> • Guard Summary menu—Provides access to the following Guard statistical and configuration options: <ul style="list-style-type: none"> – Guard status and diagnostic tools – List of defined zones – User profile manager <p>To view the Guard summary menu, click Guard 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 Guard 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 Guard 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 Guard on cisco.com.
5	<p>Work Area—Displays the information that you choose. 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 Guard is not learning zone traffic or monitoring zone traffic for anomalies.
	Zone is active and in a phase of the learning process. The Guard 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 Guard 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 Guard 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](#)). The selection items in the menus have a drop-down list. The 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:

- Guard Summary menu—Provides access to general Guard statistical and configuration tools. To view the Guard Summary menu, click **Guard Summary** in the navigation area or click **Home** in the Information area. [Table 1-2](#) provides a map of the Guard Summary menu levels.

Table 1-2 Guard Summary Menu

Level 1	Level 2	Level 3
Main	Summary	
	Protect IP	
Diagnostics	Counters	Guard counters
		Real-time counters
	Event log	

Table 1-2 *Guard 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
Protection	Protect	
	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

