



Cisco Guard Web-Based Management (WMB) User Guide

Software Release 3.08
June 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-6112-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

Cisco Guard Web-Based Management (WMB) User Guide

Copyright © 2004 Cisco Systems, Inc. All rights reserved.



Preface	xiii
Audience	xiii
Organization	xiv
Conventions	xv
Obtaining Documentation	xvi
Cisco.com	xvi
Ordering Documentation	xvi
Documentation Feedback	xvii
Obtaining Technical Assistance	xvii
Cisco Technical Support Website	xvii
Submitting a Service Request	xviii
Definitions of Service Request Severity	xviii
Obtaining Additional Publications and Information	xix

CHAPTER 1

Introduction	1-1
System Requirements	1-1
Overview	1-2
What is DDos	1-2
The Cisco Guard	1-2
Areas of the User Interface	1-3
User Interface Conventions	1-5
Navigation	1-5
Configuration	1-7
WBM Screen Hierarchy	1-8

CHAPTER 2

WBM Basic Procedures 2-1

- Setting Up the WBM 2-1
 - Enabling WBM on the Guard 2-1
 - Enable the WBM Service 2-2
 - Granting Access Permission to the WBM Service 2-2
 - Connecting From the Remote Manager's Station 2-3

CHAPTER 3

Cisco Guard Operation and Diagnostics 3-1

- Guard Summary (Home) Screen 3-2
- Guard Diagnostics 3-4
 - Counters 3-4
 - Event Log 3-6
- User Management 3-8
 - Assigning Privilege Level Procedure 3-9
 - Creating Users 3-9
 - Users List 3-10
 - Changing a Password 3-11
 - Changing the Privilege Level 3-11

CHAPTER 4

Zone Creation and Configuration 4-1

- Overview 4-1
 - What is a Zone? 4-1
- The Zone "Home Page" 4-3
 - Zone Status Bar 4-4
 - Zone Traffic Summary 4-5
 - Zone Status Summary 4-6
 - Zone Recent Events 4-6

Zone Management	4-7
Creating Zones and Basic Zone Configuration	4-7
Reconfiguring a Zone	4-12
Deleting a Zone	4-12
Zone Status Icons	4-13

CHAPTER 5

Advanced Zone Procedures	5-1
Overview	5-1
Filters	5-1
Policy Templates and Policies	5-2
Zone Filter Configuration	5-3
User Filter Configuration	5-3
Bypass Filter Configuration	5-7
Flex Filter Configuration	5-8
Policy Templates	5-9
Configuring the Policy Template Operational Parameters	5-12

CHAPTER 6

Zone Traffic Learning and Policy Construction	6-1
Overview	6-1
Zone Traffic Learning	6-2
Constructing Policies	6-3
Terminating the Policy Construction Phase	6-4
Tuning Thresholds	6-5
Terminating the Threshold Tuning Phase	6-5
Zone Policies	6-6
Overview	6-6
Policy Configuration	6-11
Adding a Service	6-11
Removing a Service	6-12

- Configuring the Operational Parameters 6-13
- Specific IP Threshold Configuration 6-18
- Snapshot 6-19
- Compare Policies 6-20
- Accepting Policy Parameters Selectively 6-22

CHAPTER 7

Protecting Zones 7-1

- Overview 7-1
- Protecting the Zone 7-3
 - Activating Protection 7-3
 - Deactivating Protection 7-3
 - Zone Protection Verification 7-4
- Dynamic Filters 7-4
 - Dynamic Filter Termination 7-7
 - Dynamic Filter Details 7-7
 - Dynamic Filter Configuration 7-9
 - Deleting a Dynamic Filter 7-9
 - Adding a Dynamic Filter 7-10
- Interactive Recommendations Mode 7-12
 - Activating the Interactive Recommendations Mode 7-13
 - Viewing New Recommendations 7-14
 - Deciding on the Guard's Recommendations 7-16
 - Pending Dynamic Filters 7-17
 - Pending Dynamic Filter Details 7-20

CHAPTER 8

Zone Statistics and Diagnostics 8-1

- Zone Counters 8-1
 - Traffic Analysis 8-4
 - Problem Analysis 8-5

Zone Protection Summary Report	8-6
Protection Graph	8-7
Total Attack Statistics	8-8
Per Attack Summary	8-9
Zone Attack Reports	8-11
General Details	8-12
Attack Statistics	8-12
Dropped/Bounced Packets	8-14
Detected Anomalies	8-15
Detected Anomalies Details	8-19
Mitigated Attacks	8-21
Mitigated Attack Details	8-23
HTTP Detected Zombies	8-25
HTTP Zombies	8-25
Zone Event Log	8-26

GLOSSARY

INDEX



<i>Figure 1-1</i>	WBM User Interface	1-4
<i>Figure 1-2</i>	Zone List	1-6
<i>Figure 1-3</i>	Tree List View	1-6
<i>Figure 1-4</i>	List View	1-7
<i>Figure 3-1</i>	Guard Summary (Home) Page	3-2
<i>Figure 3-2</i>	Guard Global Counters/Rates	3-5
<i>Figure 3-3</i>	Event Log	3-7
<i>Figure 4-1</i>	Zone "home page"	4-4
<i>Figure 4-2</i>	Zones Sub-menu	4-7
<i>Figure 5-1</i>	User Filters	5-3
<i>Figure 5-2</i>	Adding a User Filter – Step 1	5-4
<i>Figure 5-3</i>	Policy Templates	5-12
<i>Figure 6-1</i>	Zone Learning Menu	6-3
<i>Figure 6-2</i>	Policy Table	6-6
<i>Figure 6-3</i>	Policy Table Section	6-16
<i>Figure 6-4</i>	Policy Details Tables	6-17
<i>Figure 6-5</i>	Policy Comparison	6-21
<i>Figure 7-1</i>	Protection Menu	7-3
<i>Figure 7-2</i>	Dynamic Filters Table	7-5
<i>Figure 7-3</i>	Dynamic Filter Details	7-8
<i>Figure 7-4</i>	Recommendations	7-14
<i>Figure 7-5</i>	Pending Dynamic Filters	7-18
<i>Figure 7-6</i>	Pending Dynamic Filter Details	7-20

<i>Figure 8-1</i>	Zone Counters	8-3
<i>Figure 8-2</i>	Problem analysis: Rcv \neq 0, Legitimate = 0	8-5
<i>Figure 8-3</i>	Zone Protection Summary Report – Protection Graph	8-7
<i>Figure 8-4</i>	Zone Protection Summary Report—Total Attack Statistics	8-8
<i>Figure 8-5</i>	Zone Protection Summary Report—Per Attack Summary	8-9
<i>Figure 8-6</i>	Attack Report—General Details	8-12
<i>Figure 8-7</i>	Attack Report—Attack Statistics	8-13
<i>Figure 8-8</i>	Attack Report—Dropped/Bounced Packets	8-14
<i>Figure 8-9</i>	Attack Report—Detected Anomalies	8-16
<i>Figure 8-10</i>	Attack Report—Mitigated Attacks	8-21
<i>Figure 8-11</i>	HTTP detected zombies	8-25
<i>Figure 8-12</i>	HTTP Zombies list	8-26
<i>Figure 8-13</i>	Zone Event Log	8-27



<i>Table 1-1</i>	Areas of the User Interface	1-4
<i>Table 3-1</i>	User Privilege Levels	3-8



Preface

The *Cisco Guard Web-Based Management (WBM) User Guide* describes the web-based Management, a graphical user interface (GUI) for remotely operating the Guard and monitoring the Guard's activity, condition and statistics. The WBM communicates with the Guard by translating its HTML pages into Guard commands. These are the same commands that you can enter with the command-line interface (CLI). This guide describes the Cisco Guard Web-Based Management (WBM) workflow, installation, and operation.

This user guide provides the general WBM operations needed for the Guard operation and explains how to use the WBM. It contains background information and instructions for using the WBM and the Guard.

Some of the Guard's configuration, relating to the Guard as a whole, can only be configured using the CLI and cannot be performed using the WBM. Refer to the *Cisco Guard User Guide* for further details.

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

Audience

The *Cisco Guard Web-Based Management (WBM) User Guide* is intended primarily for network operators who will be operating the Cisco Guard but who are not necessarily familiar with the tasks involved and the relationship between them, or the operations necessary to perform particular tasks.

Organization

This manual is divided into the following chapters:

Chapter	Title	Description
1	Introduction	Provides information on system requirements and an overview of the Cisco Guard Web Based Management (WBM).
2	WBM Basic Procedures	Provides an overview of the WBM basic procedures. It provides an explanation on how to enable the WBM in the Guard and how to connect to the Guard with the WBM.
3	Cisco Guard Operation and Diagnostics	Describes how to perform common monitoring and operational tasks on the Cisco Guard using the WBM.
4	Zone Creation and Configuration	Describes how to create and manage zones.
5	Advanced Zone Procedures	Describes how to perform advanced configuration tasks for zones on the Cisco Guard using the WBM: Zone Filter configuration and Policy Template configuration.
6	Zone Traffic Learning and Policy Construction	Describes how to create traffic-tailored policies for zones on the Cisco Guard using the WBM.
7	Protecting Zones	Describes how to perform tasks for protecting zones on the Cisco Guard using the WBM.
8	Zone Statistics and Diagnostics	Describes how to perform tasks used for monitoring zones and displaying various zone statistics and diagnostics on the Cisco Guard using the WBM.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>Italic font</i>	Indicates names in configuration samples and refers the reader to places in the document for further details.
Screen font	Information to be displayed or typed on the screen.
boldface screen font	Information you must enter is in boldface screen font .
Angle brackets (< >)	Indicates a command's parameter to be typed in.
Curly brackets ({ })	Indicates command parameters from which you must choose one.
Square brackets ([])	Indicates an optional command parameter.
	Separates two mutually exclusive choices in a syntax line. Type one of these choices, not the symbol.
admin@GUARD#	Indicates the default CLI prompt.

Notes use the following conventions:



Note

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

Cautions use the following conventions:



Caution

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Introduction

This chapter provides an overview of the Cisco Guard Web Based Management (WBM) interface. This chapter includes the following sections:

- [System Requirements](#)
- [Overview](#)
 - [What is DDos](#)
 - [The Cisco Guard](#)
- [Areas of the User Interface](#) (Describes the WBM main areas)
- [User Interface Conventions](#)
- [WBM Screen Hierarchy](#)

System Requirements

The Cisco Guard Web Based Management (WBM) interface supports an Internet Browser, Microsoft Internet Explorer 5 or higher, that supports HTML, Tables, Cookies, JavaScript and Frames.

We recommend that you use a screen resolution of minimum of 1024 by 768 pixels.

No software installation is required.

Overview

What is DDoS

The Distributed Denial of Service (DDoS) attacks are attacks in which malicious individuals cause thousands of compromised computers (“zombies”) to run automated scripts that cripple a protected server’s (the Zone) network resources with spurious requests for service. The attacks can be, for example, a flood of bogus home page requests to a web server that shuts out legitimate consumers, or efforts that compromise the availability and accuracy of Domain Name System (DNS) servers. Although often launched by an individual, the zombies actually executing the attacking code may number in the hundreds of thousands, and are distributed over multiple autonomous systems, administered by multiple organizations.

DDoS attacks continuously evolve as sophisticated hackers create damaging new exploits. In addition, their attack scripts are made widely available on the Internet and are routinely executed by individuals with minimal technical knowledge of networking. Thus, DDoS defense technology must be flexible and adaptive.

It must be capable of detecting an upcoming DDoS attack, differentiate between malicious and legitimate traffic, and perform those tasks without hindering the traffic flow of the attacked network element

The Cisco Guard

The Cisco Guard is a high performance network device deployed in a distributed upstream configuration, at the ISP/MSP/backbone level, protecting the entire network. When an attack is detected, the system diverts only the attacked zone’s traffic to the Guard. The data flow is analyzed; all DDoS components obstructed and clean traffic is allowed to continue flowing to the intended zone. The Guard is a system that allows a transparent zone traffic flow, constantly filters the traffic, and closely remains tuned to zone traffic characteristics to be on the alert for evolving attack patterns.

To accomplish the above-mentioned tasks the Cisco Guard employs the following components:

- Traffic diversion mechanisms that redirect (divert) the zone's traffic to the Guard Learning and Protection systems and then return (inject) the legitimate traffic flow back to the zone. This is performed while preventing the obstruction of network traffic.
- An algorithm-based learning system that learns the zone traffic, adopts itself to its particular characteristics, and supports the Protection system with references and protection instructions in the form of Thresholds and Policies. In addition, the Guard has 'On-Demand' protection to answer a situation in which the zone is under attack while the Guard hasn't completed its Learning and tuning to the zone traffic.
- A protection system that distinguishes between the legitimate and the suspicious traffic and filters the malicious traffic. Only the legitimate traffic is then let to pass on to the zone.

Integrating these components enables the Guard to assume its protective role upon attack, while remaining in the background for the rest of the time.

Areas of the User Interface

The WBM provides access to various Guard configuration and management screens, allowing you to view statistics, and permitting you to graphically monitor system status..

The WBM allows configuring and monitoring the Guard's various protection mechanisms. It provides a subset of the CLI functionality and mostly deals with protected zone configuration, status, and reports. Configuration parameters, relating to procedures such as initial Guard setup procedure and network-level setup of the Guard are only accessible through the CLI. See the *Cisco Guard User Guide* for further details.

Figure 1-1 displays the WBM user interface. The user interface is divided into three distinct areas as described in Table 1-1.

Figure 1-1 WBM User Interface

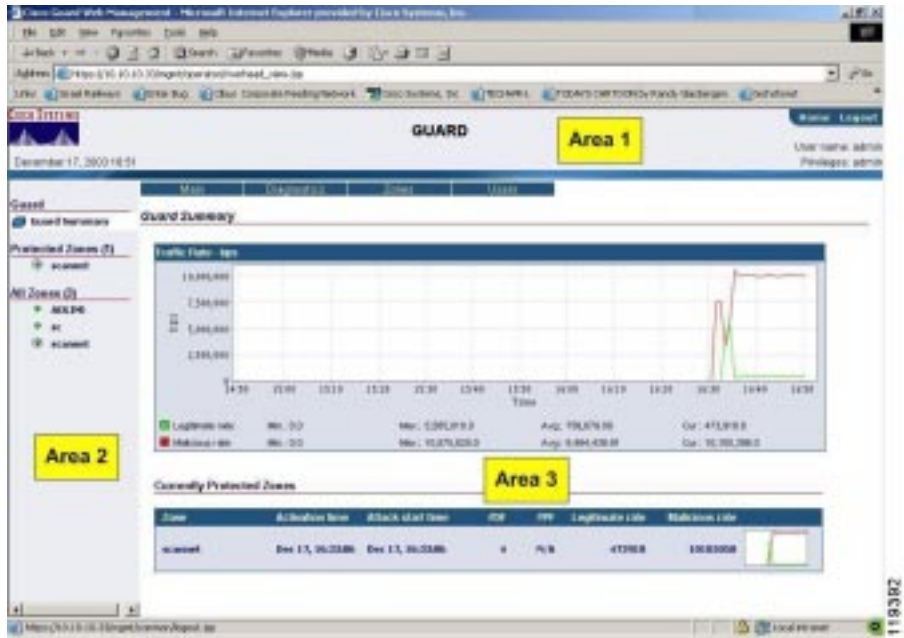


Table 1-1 Areas of the User Interface

Area	Function
1	The header area provides information on the logged in user, the Guard's date and time and a simple navigation bar that enables to log out or return to the Guard's main screen.

Table 1-1 *Areas of the User Interface*

Area	Function
2	<p>The navigation pane displays a list of links, divided by state. Each item provides a link to the “home page” of a zone or the Guard. The associated link will be displayed in the main area. (area 3). The selected item is marked by a white frame.</p> <p>The navigation pane is resizable.</p>
3	<p>The main area holds the user-selected views. It includes:</p> <ul style="list-style-type: none"> • The name of the view and the state (for example, Zone scannet (interactive)—Protected). • The location view, indicating the type of view (for example, Home>Zone>General>Config). • A menu bar—There are two fixed menu bars, for Guard or zone, which provide the main navigation mechanism. When selecting Guard Summary in the navigation pane, the menu bar displays the Guard’s main menu. When selecting one of the zones in the navigation pane, the menu bar displays the zone’s main menu. • Information area—Displays the required information, that is, tables and forms. <p>The main area is resizable.</p>

User Interface Conventions

Navigation

Navigation in the screen hierarchy can be performed either using the menus or by using the location view in the main area (area 3, as shown in the previous section).

When navigating using the location view, the black colored section indicates the current location.

The color of a selectable item turns grey when moving the mouse cursor over it.

Click on the grey item to display its page.

To navigate to one of the higher sections of the hierarchy, select the desired location and click the mouse.

For example, the location view: Home > Zone > Policies > Service indicates that the displayed location is Policy service configuration.

To navigate to the Policy menu list, select **Policies**.

To Navigate to the “home page” of the Guard or one of the zones, select a zone in the navigation pane (see [Figure 1-2](#)).

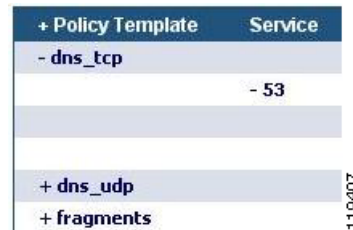
The item that is currently displayed in the main area is marked by a white frame.

Figure 1-2 Zone List



Tree Lists are displayed as shown in [Figure 1-3](#). Click + on the left side of the item to navigate in the tree hierarchy. Once the lower level hierarchy is displayed, click - on the higher level to close the view of the lower levels. Click the item in the tree hierarchy to open its configuration window. For example, in [Figure 1-3](#), click **53** to open the service configuration window for the dns_tcp template.

Figure 1-3 Tree List View



The **i** indicates that additional information is available. Click to display the additional information.

Configuration

Selection items in menus have a drop-down list. Selection items that are not available in the current view are grayed-out.

Configurable parameters appear in Forms. Parameters are configured in one of the following ways:

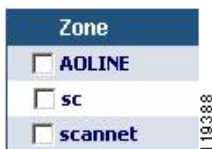
- A drop-down list—Allows only one item from a list to be selected.
- Text boxes—Allow entering an integer or expression as specified for each parameter.
- Radio button—Enable to choose between one of the shown items.
- Check boxes—Enable to choose several items.

Be sure to click **OK** or **Add** to confirm the new settings once a configuration change has been made.

Lists are displayed as shown in [Figure 1-4](#). To add an item to the list, click **Add** at the bottom of the screen.

To delete an item from the list, select the check box next to the desired item and click **Delete**.

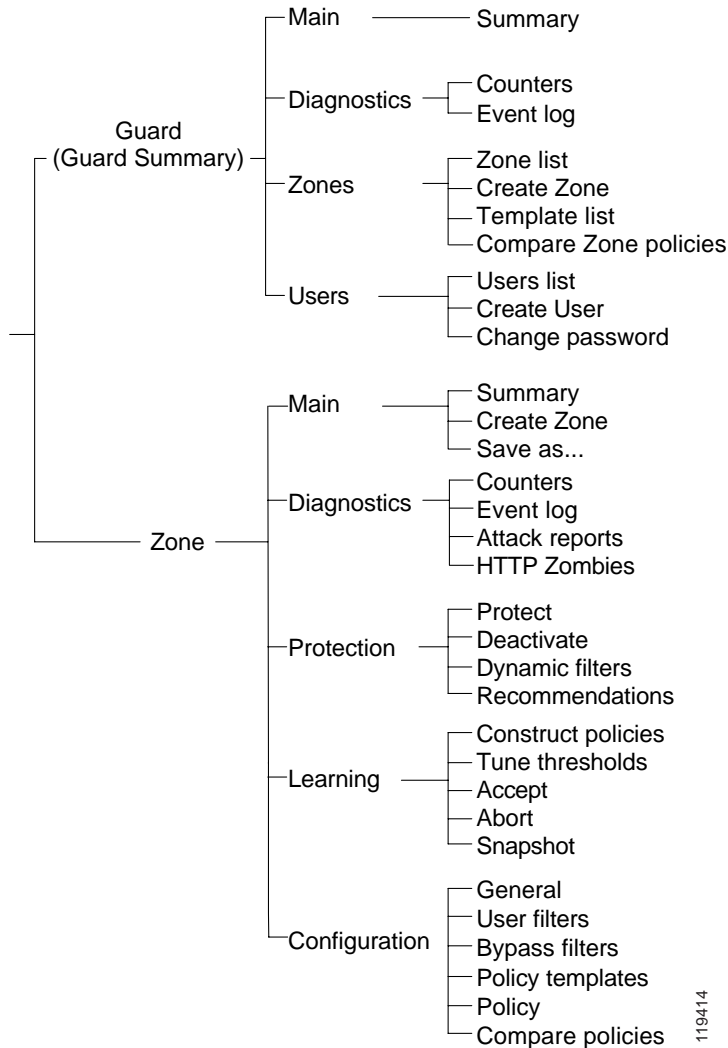
Figure 1-4 List View



You may choose which items are to be displayed in system defined lists, such as the counters list. However, items cannot be added to or deleted from these lists.

WBM Screen Hierarchy

This section summarizes the screen hierarchy in the WBM, to provide you with a quick guide to finding the screen you want.





WBM Basic Procedures

This chapter provides an overview of the Web-Based Management (WBM) basic procedures. It provides an explanation on how to set up the WBM in the Guard and how to connect to the Guard's WBM.

Setting Up the WBM

Before setting up the Web-Based Management (WBM), some basic configuration of the Guard needs to be performed. The following information, at a minimum, must be known for the Guard to be managed:

- The IP address of the Guard
- Admin or config privileged user-name and password



Note

Admin and config privileged users can configure WBM access for dynamic and show privilege users.

Enabling WBM on the Guard

For detailed information on the Guard's CLI, refer to the *Cisco Guard User Guide*.

Enable the WBM Service

To enable the Guard web based management service, perform the following from the Guard's command line interface:

1. From the Configuration command group level type the following:

```
service wbm
```

2. Press **ENTER**. The following screen appears:

```
admin@GUARD-conf> service wbm
admin@GUARD-conf>
```

To disable the WBM service:

From the Configuration command group level type the following:

```
no service wbm
```

Granting Access Permission to the WBM Service

To Grant permission for an IP address to access the Guard's WBM service perform the following:

1. From the Configuration command group level type the following:

```
permit wbm <ip-addr> [<ip-mask>]
```

Where:

- *<ip-addr>*—Indicates the IP address of the permitted user, that is, the IP address of the remote manager. Use * to indicate any IP address.
- [*<ip-mask>*]—(Optional) Indicates the IP mask of the permitted user.

2. Press **ENTER**. The following screen appears:

```
admin@GUARD-conf> permit wbm 10.0.0.192 255.255.255.240
admin@GUARD-conf>
```



Note

We do not recommend permitting WBM access from any IP address after initial configuration due to security considerations.

To deny WBM access from a remote manager:

From the Configuration command group level type the following:

```
no permit wbm <ip-addr> [<ip-mask>]
```

Connecting From the Remote Manager's Station

To connect to the Guard WBM perform the following:

1. In the remote station, open the browser window.
2. Enter the Guard's IP address in the browser's address bar. Connect using **https** as shown below:

```
https://<ip-address>
```



Note **https** and not http is used.

The following login screen appears:



3. Type your username and password.

4. Click **OK**.

An error message appears if the user name or password entered is incorrect.

After the user name and password are entered correctly, the Guards's main screen is displayed (see [Figure 1-1](#)).



Note

If TACACS+ authentication is configured, the TACACS+ user database is used for user authentication rather than the local database. Refer to the “TACACS+ and Local Authentication Methods” section in Chapter 2, “Initial Procedures,” in the *Cisco Guard User Guide*.



Tip

If you fail to connect to the Guard:

- Make sure the correct user name and password are entered.
 - Make sure the correct IP address is entered in the URL field of the browser and that you connected using https.
 - Check the network connections of both the manager's station and the Guard.
 - Try to connect to the Detector using ssh and see if it is indeed reachable.
 - Verify that the WBM service is enabled and that access from the remote manager's IP address is permitted.
-



Cisco Guard Operation and Diagnostics

This chapter describes how to perform common monitoring and operational tasks on the Cisco Guard using the Web-Based Management (WBM).

This chapter includes the following sections:

- [Guard Summary \(Home\) Screen](#)
- [Guard Diagnostics](#)
- [User Management](#)—Creating users and viewing users list

For information on zone management, creating zones and viewing zones' status, see, [Chapter 4, “Zone Creation and Configuration.”](#)



Note

Guard configuration and Networking and Diversion configuration can only be assumed using the CLI. Refer to the *Cisco Guard User Guide* for further details.

Guard Summary (Home) Screen

The Guard's Summary (Home) screen (Figure 3-1) provides a summary of the current Guard activity.

To navigate to the Guard's summary (home) screen:

- Select **Guard Summary** from the navigation pane.
- Select **Home** from the upper right side of the header area.
- Select **Home** from the location bar on the zone pages.

Figure 3-1 Guard Summary (Home) Page



The Guard Summary includes two sections.

- **Guard Summary**—Provides a summary of the traffic, displayed in bits per second (bps), handled by the Guard in the past two hours. Legitimate traffic passed by the Guard to the protected zones, is displayed in green. Malicious traffic handled by the Guard, is displayed in red.

Below the graph, the following information is displayed:

Parameter	Description
Min	Indicates the minimum traffic rate in bps measured in the past two hours
Max	Indicates the maximum traffic rate in bps measured in the past two hours
Avg	Indicates the average traffic rate in bps measured in the past two hours
Cur	Indicates the current traffic rate in bps

The information is displayed separately for legitimate traffic and for malicious traffic.

- **Zones Under Detection**—Provides a list of the currently protected zones and a short summary of the status of each one of them. The zones are displayed according to the attack order. The most recently attacked zone is displayed at the top of the list.

The following information is provided for each zone:

Parameter	Description
Zone	Indicates the zone name. The zone name also provides a link to the zone's "home page."
Activation Time	Indicates the date and time detection for the zone was initiated.
Attack Start Time	Indicates the date and time the most recent attack on the zone was detected.
Legitimate Rate	Indicates the current rate legitimate traffic passed by the Guard to the zone, measured in bits per second (bps).

Parameter	Description
Malicious Rate	Indicates the current rate of malicious traffic, destined to the zone, measured in bps.
Thumbnail of the Zone traffic summary	A graph displaying a summary of the traffic destined to the zone in the past half hour. The traffic rate is displayed in bps. Legitimate traffic rate is displayed in green. Malicious traffic rate is displayed in red.

Guard Diagnostics

You may obtain diagnostics information on the Guard for troubleshooting and monitoring purposes.

To view the Guard's diagnostics:

From the Guard's main menu, select **Diagnostics**.

The following diagnostics are available:

- Counters
- Event Log

Counters

The Guard global counters report (Figure 3-2) provides additional information to the Guard summary displayed in the Guard's "home page".

To display the Guard global counters:

From the Guard's main menu, select **Diagnostics > Counters**.

The following counters are displayed:

- **Legitimate**—Legitimate traffic forwarded by the Guard to the zones.
- **Malicious**—Malicious traffic, destined to the zone, handled by the Guard. Malicious traffic is the sum of Dropped packets and Spoofed packets (which also include the Zombie packets).

- **Received**—Packets received and handled by the Guard. Received packets are the sum of legitimate traffic and malicious traffic.
- **Dropped**—Packets that were identified by the Guard as part of an attack and therefore dropped.
- **Replied**—Replied—Packets, destined to the zone, to which replies were sent to the initiating client as part of the anti-spoofing or anti-zombie mechanisms in order to verify if they are part of authentic traffic or part of an attack.
- **Spoofed**—Packets, destined to the zone, that were identified by the Guard as Spoofed packets and therefore not forwarded to the zone. Spoofed packets are Replied (bounced) packets to which no replies were received. The Spoofed packets include zombie packets.

Figure 3-2 Guard Global Counters/Rates



For each of the counters, the following information is provided:

Parameter	Description
Shown in Graph	Specifies whether the counter will be shown in the graph below.
Packets	Indicates the total amount of packets since the Guard was reloaded.

Parameter	Description
Bits	Indicates the total amount of bits since the Guard was reloaded.
pps	Indicates the current traffic rate measured in packets per second.
bps	Indicates the current traffic rate measured in bits per second.

By default, Legitimate and Malicious traffic are displayed for a period of the past two hours, measured in bits per second (bps).

Choose the period of time to be displayed and the graph units.

To update the graph according to the settings chosen:

Click **Update Graph** (see [Figure 3-2](#)).

Below the graph is a legend that identifies the counters. For each counter in the graph the minimum, maximum and average rate are displayed for the period of time and rate units chosen.

For a detailed explanation on interpreting the counters' significance, refer to Chapter 6 "On-Demand Protection," in the *Cisco Guard User Guide*.

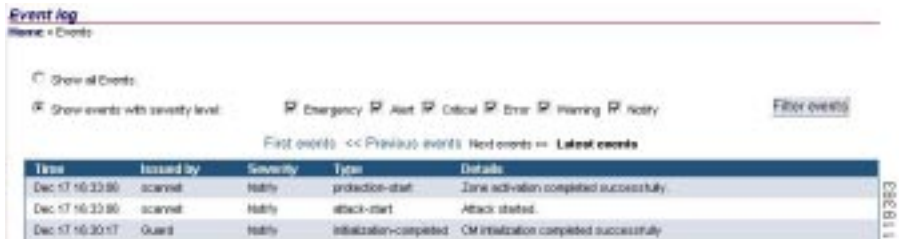
Event Log

The Event log ([Figure 3-3](#)) displays monitoring and troubleshooting information. Logs are displayed for events that relate to the protected zones and to the Guard operation.

To display the event log:

From the Guard's main menu, select **Diagnostics > Event log**.

Figure 3-3 Event Log



The event severity levels are:

Event Level	Description
Emergencies	System is unusable
Alerts	Immediate action required
Critical	Critical condition
Errors	Error condition
Warnings	Warning condition
Notifications	Normal but significant condition
Informational	Informational messages
Debugging	Debugging messages

You may choose to filter the events according to their severity level.

To filter events according to their severity level:

1. Select the check boxes next to the severity levels.
2. Click **Filter Events**.



Note

The event logs display zone related event logs only with a severity level of Emergency, Alert, Critical, Error, Warning and Notification. See [Chapter 8, “Zone Statistics and Diagnostics,”](#) for further details on zone event logs.

User Management

The access to the Guard is mapped according to user privilege levels. Each user privilege level is granted with a corresponding set of command group operations. [Table 3-1](#) displays the Guard user privilege levels and their corresponding command operation groups.

Table 3-1 User Privilege Levels

User Group	Command Group
Administrator (Admin)	Full access to all operations.
Configuration (Config.)	Full access to all operations except the operations relating to user definition, deletion, and modification.
Dynamic	The entire monitoring and diagnostics operations group, the detection, and the learning related operations. Dynamic privileged-users may also configure the Flex and Dynamic filters (see the note below).
Show	The entire monitoring and diagnostics operations group.



Note

We recommend that Administrator and Configuration privilege level users perform all filter configuration procedures. Lower privileged users can also perform dynamic filter addition and removal.

The Guard enables the Administrator to configure which authentication method the Guard utilizes when a user tries to log into the Guard. The Guard offers the following authentication options:

- Guard local authentication—Local authentication uses locally configured login passwords for authentication. This is the default authentication method.
- TACACS+ authentication—TACACS+ authentication authenticates users through a TACACS+ server or a list of TACACS+ servers.

**Note**

TACACS+ authentication can only be configured from the CLI. Refer to the “TACACS+ and Local Authentication Methods” section in Chapter 2, “Initial Procedures,” in the *Cisco Guard User Guide*.

Assigning Privilege Level Procedure

A preconfigured Administrator’s privilege level is provided, enabling you to define the Guard user types. Defining users enables you to divide the Guard user community into privilege levels.

**Note**

The admin user name grants Administrator's privilege level. The riverhead user name grants the Dynamic privilege level. The Detector uses this user name for remote activation of the Guard.

Creating Users

An administrator-privileged user may configure local users.

**Note**

If TACACS+ authentication is configured, the TACACS+ user database is used for user authentication rather than the local database. Refer to the “TACACS+ and Local Authentication Methods” section in Chapter 2, “Initial Procedures,” in the *Cisco Guard User Guide*.

To create a new user:

From the main menu, select **Users > Create user**.

For each user define the following:

Parameter	Description
User name	The User's user name.
Initial password	6-24 characters long excluding spaces.
Type	The user's privilege level. From the drop-down list choose: admin, config, dynamic or show, as defined above.

Alternatively, to create a new user:

On the Users list screen (see the [“Users List”](#) section), click **Add**.

Users List

You may view the list of users defined on the Guard.

To view the list of users defined on the Guard:

From the main menu, select **Users > Users list**.

The list of users is divided into two categories:

- System users—Users defined by the system. System users cannot be deleted. The system users are admin and riverhead.
- Users—Users defined by the operator.

To remove a user:

1. Select the check box next to the user name.
2. Click **Delete**.

To add a user:

Click **Add**.

The user's privilege level is displayed for each user (see [Table 3-1](#)).

To reconfigure a user:

Click on the user name.

Changing a Password

To change the password:

1. From the Guard's main menu select **Users > Change password**.
The Change Password window appears.
2. Enter the existing password in the **Old Password** box.
3. Enter a new password in the **New Password** box, and re-enter the new password to verify your choice.
4. Click **OK**.
5. If an invalid password is entered or the new password is not verified correctly, an error message is displayed. Click **Go Back** to try again.

Users that have an Administrator privilege level may configure and change the password of all users defined on the Guard.

To reconfigure or change the passwords of users, other than the current one:

1. From the main menu select **Users > Users list**.
2. Click on the required user name.
3. Click **Config**.
4. Enter the new password.
5. Click **OK**.

Changing the Privilege Level

To change the user privilege level:

- Delete the user (see the [“Users List”](#) section).
- Re-create the user (see the [“Creating Users”](#) section).



Zone Creation and Configuration

This chapter describes how to create and manage zones.

This chapter includes the following sections:

- [Overview](#) (What is a Zone)
- [The Zone “Home Page”](#)
- [Zone Management](#) (creating zones and basic zone configuration)
- [Zone Status Icons](#)

Overview

What is a Zone?

A zone is a network element protected by the Guard against DDoS attacks. A zone can be a network server, client or router; a network link or subnet or an entire network; an individual Internet user or a company doing business using the Internet; an Internet Service Provider (ISP), or any combination of or variant on these. The Guard can protect different zones simultaneously, as long as their network address ranges don't overlap.

A “Zone” on the guard is the definition of a zone element, configured so that the Guard can protect it from DDoS attacks. A zone on the Guard is assigned with a name, and referred to by the assigned name. A zone configuration on the Guard includes the following:

- **Zone basic configuration**—A zone’s basic configuration includes the zone’s name and description, the zone’s network address and operation definitions and basic networking characteristics such as the zone’s bandwidth. See the [“Zone Management”](#) section in this chapter for further details.
- **The Zone's Detection Policy**—The policies are the mechanisms that measure a particular traffic flow and take action against the flow as a result of threshold violation. The protection policies are constructed from policy templates, that provide the constructing guiding rules, in two learning phases (see [Chapter 7, “Protecting Zones,”](#) for further details). The action taken by the policies could range from merely notifying to directing the traffic to various Guard anti-spoofing or anti-zombie mechanisms and even dropping malicious traffic (see [Chapter 5, “Advanced Zone Procedures,”](#) for further details).
- **The Zone's filters**—The zone’s filters are the mechanism that directs the diverted traffic to the required protection modules. The Guard enables you to set its preferred filter configurations and thus design a variety of possibilities for customized traffic direction and anti-DDoS attack mechanisms. See [Chapter 5, “Advanced Zone Procedures,”](#) for further details.
- **Zone Diversion** - To protect the target host (zone) using the Cisco Guard, traffic destined to the host must be diverted to the Cisco Guard. This step includes traffic forwarding methods configuration per zone’s IP address. Zone diversion configuration is configured via the Guard routing configuration and is not part of the zone configuration file. For information about Zone Diversion configuration, refer to Appendix A, “Diversion Configuration,” in the *Cisco Guard User Guide*.

The Zone “Home Page”

The zone's “home page” (Figure 4-1) provides a summary of the zone's status.

To navigate to this screen perform one of the following:

- From the navigation pane under the **All Zones** list, click the zone's name.
- If the zone is currently in protect mode, from the navigation pane under the Protected Zones list, click the zone's name.
- On the zone pages, select **Zone** from the location view.
- From the zone list (**Guard Summary > Zones > Zone list**), click the zone name.

The zone “home page” is divided into four sections:

- Zone status bar
- Zone Traffic summary
- Zone status summary
- Zone recent events

In addition, the zone's home page has short cuts, displayed as buttons below the zone status bar.

- **Protect**—Switches the zone to protection mode. This is a shortcut to selecting **Protection > Protect** from the Zone's main menu. This button is present only if the zone is in stand by.
- **Deactivate**—Deactivates the zone's detection state. This is a shortcut to selecting **Protection > Deactivate** from the Zone's main menu.

This button is present only if the zone is in protection mode.

- **Report**—Provides a shortcut to the current attack report. This is a shortcut to selecting **Diagnostics > Attack** reports from the Zone's main menu and clicking on the current attack (the attack with an end time of “attack in progress”). This shortcut is available only if there is a current attack in progress. See [Chapter 8, “Zone Statistics and Diagnostics,”](#) for further details.

Figure 4-1 Zone “home page”



Zone Status Bar

The zone’s status bar provides a quick reference for the zone’s status. It provides details on the following:

- The zone’s name.
- The zone’s operation mode—The operation mode appears in brackets. It indicates whether the zone is in auto protection mode or in interactive protection mode. The operation mode is displayed only if the zone is active. See the [“Zone Management”](#) section in this chapter for further details.
- The Zone’s status—The zone’s status indicates the zone’s protection or learning mode. The zone’s status can be one of the following: protected, inactive, constructing policy and tuning thresholds. See the [“Zone Status Summary”](#) section in this chapter for further details.
- Indication on new recommendations—If the zone is in interactive mode, the zone’s status bar will include an indication on new recommendations. See the [“Interactive Recommendations Mode”](#) section in [Chapter 7, “Protecting Zones,”](#) for further details.

Zone Traffic Summary

The zone's traffic summary graph displays the zone related traffic rate, in bits per second (bps), in the past two hours. Legitimate traffic passed by the Guard to the zone, is displayed in green. Malicious traffic that was destined to the zone is displayed in red.

Below the graph, the following information is provided:

Parameter	Description
Min	Indicates the minimum traffic rate in bits per second (bps) measured in the past two hours
Max	Indicates the maximum traffic rate in bits per second (bps) measured in the past two hours
Avg	Indicates the average traffic rate in bits per second (bps) measured in the past two hours
Cur	Indicates the current traffic rate in bits per second (bps)

The information is displayed separately for legitimate traffic and malicious traffic.

Zone Status Summary

The zone’s status summary provides the following information:

- The number of active Dynamic filters.

Active dynamic filters provides a link to the Dynamic filters page. See the “[Dynamic Filters](#)” section in [Chapter 7, “Protecting Zones,”](#) for further details.

- The number of pending Dynamic filters.

The number of pending dynamic filters is greater than 1 when the zone is in interactive protection mode and there are new recommendations.

Pending dynamic filters provides a link to the recommendations page. See the “[Dynamic Filters](#)” section in [Chapter 7, “Protecting Zones,”](#) for further details on dynamic filters. See the “[Interactive Recommendations Mode](#)” in [Chapter 7, “Protecting Zones,”](#) for further details on recommendations.

- Last attack time—The date and time of the last attack on the zone.
- Activation time—The date and time that protection was activated.

Zone Recent Events

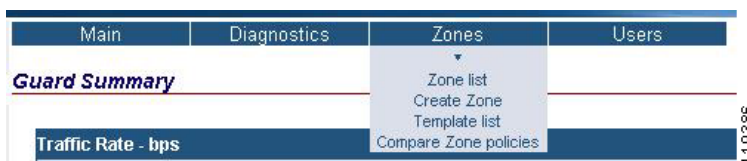
The recent events table displays the recent events issues by the zone. These events are also displayed in the zone event log and the Guard event log. The events displayed in this table have a minimum severity level of *notify*.

Zone Management

Creating Zones and Basic Zone Configuration

To protect a zone against DDoS attacks, the zone's network characteristics must be configured on the Guard.

Figure 4-2 Zones Sub-menu



To create a new zone, perform one of the following:

- From the Guard's main menu select **Zones > Create Zone**.
- From the Guard's main menu select **Zones > Zone list** and click **Add**.
- From the Zone's main menu select **Main > Create Zone**.
- From the Zone's main menu select **Main > Save as**.

This action copies the current zone basic configuration to a new zone. It is equivalent to the CLI command zone with the option copy-from-this. Refer to Chapter 4, "Zone Configuration," in the *Cisco Guard User Guide* for further details.

The Zone Form appears.

The zone's basic configuration includes the following:

Parameter	Description
Name	The zone name.
Description	A description of the zone.

Parameter	Description
From Template	<p data-bbox="532 237 1244 297">A template that defines the zone configuration. The Template could be one of the following:</p> <ul data-bbox="545 318 1231 846" style="list-style-type: none"> <li data-bbox="545 318 1110 345">• DEFAULT—The Guard default zone template. <li data-bbox="545 362 1231 545">• TCP_NO_PROXY—A template designed for a zone for which no TCP proxy is to be used. This template may be used if the zone is moderated according to IP addresses such as an Internet Relay Chat (IRC) server-type zone. Refer to Chapter 9, “Advanced Policy Procedures,” in the <i>Cisco Guard User Guide</i> for further details. <li data-bbox="545 561 1231 846">• Bandwidth Limited Link Templates—Templates designed and specifically tailored for On-Demand protection of large subnets segmented according to zones with known bandwidth. Protection for the zone should be assumed for the attacked subnet or range. It is recommended to define such a zone on the Detector with protect-ip-state of only-dest-ip (See Protect-IP state in the <i>Cisco Traffic Anomaly Detector Web-Based Management (WBM) User Guide</i> for further details). <p data-bbox="579 862 1231 922">The following Bandwidth Limited Link templates are available for 128K, 1M, 4M, and 512K links respectively:</p> <ul data-bbox="592 938 774 1101" style="list-style-type: none"> <li data-bbox="592 938 774 966">– LINK_128K <li data-bbox="592 982 753 1010">– LINK_1M <li data-bbox="592 1026 753 1053">– LINK_4M <li data-bbox="592 1070 774 1097">– LINK_512K <p data-bbox="532 1117 1163 1177">Note Learning Phase 1, policy construction, cannot be performed for these templates.</p>

Parameter	Description
Operation mode	<p>Indicates the mode used for zone Dynamic filters activation. The mode can be one of the following:</p> <ul style="list-style-type: none"> • Automatic—The dynamic filters will be activated automatically. • Interactive—The interactive mode enables you to define the action taken for each Dynamic filter. The Dynamic filters the policies recommend will appear as recommendations. You will specify whether to accept or reject each Dynamic filter. <p>See the “Interactive Recommendations Mode” section in Chapter 7, “Protecting Zones,” for further details.</p>
Max. Rate	<p>The amount of traffic (in the units specified from the drop-down list) allowed to pass to the zone. The amount is specified by an integer. The value should be configured according to the traffic volume the zone can handle.</p>
Burst	<p>The highest traffic peak allowed to pass to the zone. The peak is specified by an integer. The units are bits, kilo-bits, kilo-packets, mega-bits, and packets in correspondence to the rate units specified from the drop-down list.</p> <p>Note The drop-down list defines the units for both the Max. rate and the burst.</p>
Flex filter	<p>(Optional) Configure the flex filter. See the “Flex Filter Configuration” section in Chapter 5, “Advanced Zone Procedures,” for further details.</p>
Filter Action	<p>(Optional) Configure the Flex filter action. The following options are available:</p> <ul style="list-style-type: none"> • disable—The Flex filter is disabled. • count—The Flex filter is used to count the specified flow. • drop—The Flex filter is used to drop the specified flow. <p>Choose the action from the drop-down list.</p>

Parameter	Description
Protection-end Timer	<p>The timeout that specifies when protection may be terminated by the Guard.</p> <p>The Guard verifies whether an attack has ended by checking on added Dynamic filters. If, for a predefined span of time, there are no Dynamic filters in use and no new Dynamic filter is added, the Guard terminates the protection.</p> <p>Define this timeout from seconds to infinite.</p>
Filter-rate termination threshold	<p>The threshold that specifies, along with the Malicious-rate termination threshold, when Dynamic filters may be inactivated by the Guard.</p> <p>Define this threshold in packets per second (pps).</p> <p>See note below for further details.</p>
Malicious-rate termination threshold	<p>The threshold that specifies, along with the Filter-rate termination threshold, when Dynamic filters may be inactivated by the Guard.</p> <p>Define this threshold in packets per second (pps).</p> <p>See note below for further details.</p>
IP address	The zone's IP address.
Mask	The zone's address mask. Choose the address mask from the drop-down list.

**Note**

Dynamic filter termination

Once the Dynamic filter timeout expires, the Guard determines whether the Dynamic filter is to be inactivated when one of the following applies:

- The total Zone Malicious traffic rate (equaling the sum of the spoofed and dropped traffic) is less than or equal to the Malicious-rate termination threshold.
- The Filter-rate termination threshold is equal to or greater than both the following:
 - The Dynamic filter’s current traffic rate
 - The Dynamic filter’s average traffic rate during a user-configured time span (defined by the policy’s Timeout parameter)

See sections “[Configuring the Policy Operational Parameters](#)” in [Chapter 6](#), “[Zone Traffic Learning and Policy Construction](#),” and “[Dynamic Filter Termination](#)” in [Chapter 7](#), “[Protecting Zones](#),” for further details on the Dynamic filter timeout.

**Note**

It is recommended to set the bandwidth value to the highest bandwidth measured entering the zone. If unknown, leave the default burst and Max. rate blank and choose the units from the drop-down list to be unlimited.

**Note**

After creating a zone, the zone’s configuration is displayed in two tables. Additional IP addresses and subnets may be entered by clicking the **Add** button at the bottom of the IP table. This procedure should repeat per each zone IP address or subnet mask.

Additional IP addresses and subnets may be entered or deleted while the zone is active.

Reconfiguring a Zone

To reconfigure an existing zone:

1. From the Zone's menu select **Configuration > General**.
2. Click **Config**.

Deleting a Zone





To delete a zone:

1. From the Guard's main menu select **Zones > Zone list**.
2. Select the appropriate zone check box.
3. Click **Delete**.

Zone Status Icons

For illustration purposes, the zone's status is displayed by different icons. Each status is displayed by a different icon. These icons are used in the navigation pane and in the zone's status bar.

Table 4-1 *Zone status icons*

	Standby zone.
	Zone in one of the learning phases.
	Zone in protect mode.
	Indicates that new recommendations are available for the zone. This icon is displayed in addition to the zone icon.



Advanced Zone Procedures

This chapter describes how to perform advanced configuration tasks for zones on the Cisco Guard using the Web-Based Management (WBM).

This chapter includes the following sections:

- [Overview](#) (What are Policy templates, Policies and Filters)
- [Zone Filter Configuration](#) (configuring the Flex and Bypass filters)
- [Policy Templates](#) (configuring policy template parameters)

Overview

Filters

The zone's filters are the mechanism that directs the diverted traffic to the required protection modules. The Guard enables to set its preferred filter configurations and thus design a variety of possibilities for customized traffic direction and anti-DDoS attack mechanisms. There are four filter types used by the Cisco Guard:

- **User Filter**—The User filters are used to direct specified traffic flow to the desired Guard protection modules.
- **Bypass filter**—Bypass filters are used to prevent specific traffic flows from being handled by the Guard protection mechanisms.

- Flex filter—The Flex filter is used to count or drop a specified packet flow. It is a Berkley Packet filter that provides extremely flexible filtering capabilities such as filtering according to fields in the IP and TCP headers and filtering according to content bytes. The flex filter enables to use complex Boolean expressions. Only a single flex filter can be configured per zone.
- Dynamic filter—Dynamic filters are created by the Guard as the result of the analysis of traffic flow. This set of filters is continuously adapted to the zone traffic and the type of the DDoS attack. Dynamic filters have a limited life span and are erased after the attack has terminated. See the “[Dynamic Filters](#)” section in [Chapter 7, “Protecting Zones,”](#) for further details.

**Note**

Changes in the zone's filter configuration take effect immediately.

For detailed information on the Guard's filters, refer to Chapter 8, “Advanced Filter Procedures,” in the *Cisco Guard User Guide*.

Policy Templates and Policies

The policies are the mechanisms that measure a particular traffic flow and take action against the flow as a result of threshold violation. The protection policies are constructed from policy templates.

A Policy Template is a collection of policy constructing guiding rules that will be used during the learning phases to construct the zone's policies (see [Chapter 6, “Zone Traffic Learning and Policy Construction,”](#) for further details).

Zone Filter Configuration

User Filter Configuration

The User filters constitute the zone configuration and define how to handle traffic flows suspected as DDoS attacks. The User filters offer the ability to customize the Guard protection. They enable to set guiding rules to handle desired traffic flows when an attack is suspected and to direct a specified traffic flow to the desired protection module, to a Guard anti-spoofing or anti-zombie mechanism or even to be dropped.

Zone configuration includes a default set of User filters. The Guard continuously analyses traffic destined to the protected zone. It initializes its protection cycle once suspected traffic is identified, and uses that default set of User filters to filter the suspected traffic.

The User filters are activated according to their order. Therefore, it is important, when adding a new User filter, to place it in the desired location in the list.

Figure 5-1 User Filters

	Src IP	Protocol	Dest Port	Fragments	Rate	Burst	Action	Rate (pps)
<input type="checkbox"/>	*	6	80	without			blockdetect	0.00
<input type="checkbox"/>	*	6	8080	without			blockdetect	0.00
<input type="checkbox"/>	*	6	8080	without			blockdetect	0.00

To configure the User filters:

From the Zone main menu, select **Configuration > User filters**.

To delete existing User filters:

1. Select the check box next to the User filter's description.
2. Click **Delete**.

Adding a new User filter involves a two-step process.

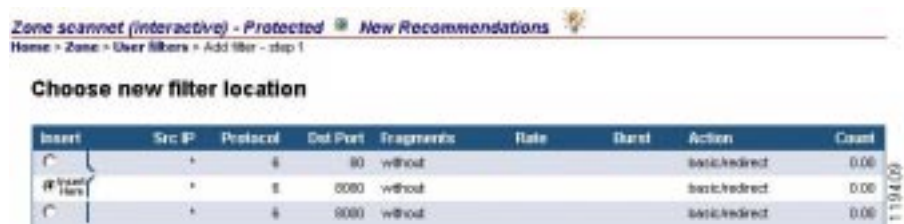
To add a new User filter:

- Click **Add**.

Step 1 screen, Choose the new filter location (Figure 5-2), appears:

- Choose the location of the new user filter. Click the button in the Insert column. The new user filter is added above the selected row.

Figure 5-2 Adding a User Filter – Step 1



- Click **Next**.

Step 2, User filter form, appears:

- Enter the User filter configuration.

Enter the following information to configure the User filter:

Parameter	Description
Source IP	Directs traffic coming from a specified IP address to the User filter. Leave blank or enter * for 'any'.
Source subnet	Directs traffic coming from a specified subnet to the User filter. Choose the subnet from the drop-down list.
Protocol	Directs traffic from a specified protocol to the User filter. The protocol is denoted by the its well known number. Leave blank or enter * for 'any'.
Dst Port	Directs traffic destined to a specified port to the User filter. Leave blank or enter * for 'any'.

Parameter	Description
Fragments	<p>Denotes specified traffic type to be handled by the filter. Choose from the drop-down list one of the following:</p> <ul style="list-style-type: none">• without—The User filter acts on non-fragmented traffic.• with—The User filter acts on fragmented traffic.• *—The User filter acts on fragmented and non-fragmented traffic.
Rate	<p>Denotes the rate limitation. The User filter limits the traffic to a specified rate. Choose the rate units from the drop-down list.</p>
Burst	<p>Denotes the traffic burst limit. The units are bits, kilo-bits, kilo-packets, mega-bits, and packets in correspondence to the rate units specified from the drop-down list.</p> <p>Note The drop-down list defines the units for both the rate and the burst.</p>

Parameter	Description
Action	<p data-bbox="581 237 1186 297">Denotes the action the filter performs on the specified traffic type. This could be either of the following:</p> <ul data-bbox="592 315 1231 1196" style="list-style-type: none"> <li data-bbox="592 315 1231 435">• permit—Used to direct traffic to avoid the Guard anti-spoofing or anti-zombie protection mechanisms. It is advisable to set a rate and burst limit for the permit User filter. <li data-bbox="592 456 1112 516">• basic/redirect—Used for authentication of applications over http. <li data-bbox="592 532 1217 592">• basic/reset—Used for authentication of applications over TCP, excluding http. <li data-bbox="592 609 1217 701">• basic/safe-reset—Used for authentication of applications, that are not tolerant of TCP connection reset, over TCP, excluding http. <li data-bbox="592 717 1231 837">• basic/default—Used for UDP traffic or when you are not sure which action is to be chosen. The basic/default filter examines the flow and determines which action is to be taken. <li data-bbox="592 854 1197 914">• basic/dns-proxy—Used for authentication of TCP DNS applications. <li data-bbox="592 930 1231 1151">• strong—Used when strong authentication for a traffic flow is required or when the previous filters do not seem suitable for the application. Authentication is performed for every connection. The Guard serves as a proxy therefore this filter is not to be used if the network is moderated according to IP addresses (such as using ACL - access control lists). <li data-bbox="592 1167 1009 1196">• drop—Used to drop traffic flows.

In the User filter table, the rate denotes the current traffic rate measured for the User filter in packets per second (pps).

For a comprehensive explanation on the User filter parameters, and examples, refer to Chapter 8, “Advanced Filter Procedures,” in the *Cisco Guard User Guide*.

Bypass Filter Configuration

The Bypass filter is a filter designed to support protection policy decisions that the user thinks should not involve the Guard's protection mechanisms. It is used to prevent specific traffic flows from being handled by the Guard's Dynamic filters, protection modules, and the Rate-limiter. Decisions of such a kind may, for example, be letting a trusted traffic flow bypass the Guard's protection modules including the anti-spoofing and anti-zombie mechanisms. Using the Bypass filter you can direct trusted traffic away from the Guard's protection mechanisms and forward it directly to the zone.

**Note**

Note that traffic handled by the Bypass filter does not go through the rate-limiter module. It is therefore additional to the bandwidth configured for the client.

To create a Bypass filter:

1. From the Zone's main menu select **Configuration > Bypass filters**.
2. Click **Add**.

There are no default Bypass filters defined.

Enter the following information to configure the Bypass filter:

Parameter	Description
Source IP	Directs traffic coming from a specified IP address to bypass the Guard filter system. Leave blank or enter * for 'any'.
Source subnet	Directs traffic coming from a specified subnet to bypass the Guard filter system. Choose the subnet from the drop-down list.
Protocol	Directs traffic from a specified protocol to bypass the Guard filter system. The protocol is denoted by the its well known number. Leave blank or enter * for 'any'.

Parameter	Description
Dst Port	Directs traffic destined to a specified destination port to bypass the Guard filter system. Leave blank or enter * for 'any'.
Fragments	Denotes specified traffic type to be handled by the filter. Choose from the drop-down list one of the following: <ul style="list-style-type: none"> • without—The Bypass filter acts on non-fragmented traffic. • with—The Bypass filter acts on fragmented traffic. • *—The Bypass filter acts on fragmented and non-fragmented traffic.

In the Bypass filter table, the counter denotes the current Bypass filter traffic rate measured in packets per second (pps) that was filtered by the Bypass filter.

To delete a Bypass filter:

1. Select the check box next to the Bypass filter's description.
2. Click **Delete**.

For a comprehensive explanation on the Bypass filter parameters, and examples, refer to Chapter 8, "Advanced Filter Procedures," in the *Cisco Guard User Guide*.

Flex Filter Configuration

The Flex filter is a Berkley Packet filter which facilitates you with extremely flexible filtering capabilities. It is used to drop, or count a desired packet flow. The Flex filter is useful in upfront blocking a minutely defined malicious source of traffic. This filter is very flexible and easily tailored to a specific traffic flow due to its parameter variety. However, only a single flex filter can be configured and it is resource consuming. We recommend to use the Flex filter attentively due to its potential performance penalty.

To configure the Flex filter:

1. If the zone is already defined, from the Zone's menu select **Configuration > General**.
2. Click **Config**.

Alternatively, the Flex filter may be configured while creating a new zone (see the “[Creating Zones and Basic Zone Configuration](#)” section in [Chapter 4](#), “[Zone Creation and Configuration](#),” for further details).

For a detailed explanation on the Berkley Packet filter configuration options see: <http://www.freesoft.org/CIE/Topics/56.htm>.

For a comprehensive explanation on the Flex filter parameters, and examples, refer to Chapter 8, “Advanced Filter Procedures,” in the *Cisco Guard User Guide*.

Policy Templates

A Policy Template is a collection of policy constructing guiding rules and the output of each template is a group of policies. The Guard policy templates consist of the following:

Policy Template	Brief Description
<code>dns_tcp</code>	This policy template produces a group of policies related to DNS-TCP protocol traffic.
<code>dns_udp</code>	This policy template produces a group of policies related to DNS-UDP protocol traffic.
<code>fragments</code>	This policy template produces a group of policies related to fragmented traffic.
<code>http</code>	This policy template produces a group of policies related to HTTP traffic flowing (by default) through port 80 (or other user-configured ports).

Policy Template	Brief Description
ip_scan	<p>This policy template produces a group of policies relating to IP scanning (A situation in which a Source IP tries to access many Destination IPs on the zone). This policy template is relevant when the zone is defined as a subnet.</p> <p>By default, this policy template is disabled. The default action for this policy template is “notify”.</p> <p>Note The policies created by the ip_scan policy template are resource consuming. Therefore, we recommend to use it attentively due to its potential performance penalty.</p>
other_protocols	<p>This policy template produces a group of policies relating to non TCP or UDP protocols.</p>
port_scan	<p>This policy template produces a group of policies relating to port scanning (A situation in which a Source IP tries to access many ports on the zone).</p> <p>By default, this policy template is disabled. The default action for this policy template is “notify”.</p> <p>Note The policies created by the port_scan policy template are resource consuming. Therefore, we recommend to use it attentively due to its potential performance penalty.</p>
tcp_connections	<p>This policy template produces a group of policies related to TCP connection characteristics.</p>
tcp_not_auth	<p>This policy template produces a group of policies related to TCP connections that haven’t been authenticated by the Guard’s anti-spoofing mechanisms.</p>
tcp_outgoing	<p>This policy template produces sets of policies related to TCP connections initiated by the zone.</p>
tcp_ratio	<p>This policy template produces sets of policies related to ratios between different types of TCP packets. For example, SYN packets versus FIN/RST packets.</p>
tcp_services	<p>This policy template produces a group of policies related to TCP services on ports other than HTTP-related (such as ports 80, 8080, etc.).</p>

Policy Template	Brief Description
tcp_services_ns	This template produces a group of policies related to TCP services. By default the policy relates to IRC ports (666X), ssh and telnet. This policy template does not create policies with actions that direct traffic flows to the Strong protection module.
udp_services	This template produces a group of policies related to UDP services.

**Note**

The Guard first relates to indicators of TCP traffic on especially dedicated ports 6660 to 6670 and ports 21 to 23. Then:

- If traffic is traced on those ports then the tcp_services_ns policy template produces its group of policies and the tcp_services policy template would relate to TCP services on other ports.
- If no traffic is traced on the above-mentioned ports, then the tcp_services policy template assumes its ordinary function. The tcp_services_ns policy template will not be operated.
- You can add services to this policy as to any other.

The Guard supplies additional policy templates designed to tailor the Guard protection to Zones for which no proxy is to be used. These templates may be used if the zone is moderated according to IP addresses such as an Internet Relay Chat (IRC) server-type zone.

Policy Template	Brief Description
tcp_connections_ns	This policy template produces a group of policies related to TCP connection characteristics. However, this policy template does not create policies with actions that direct traffic flows to the Strong protection module.
tcp_outgoing_ns	This policy template produces a group of policies related to TCP connections initiated by the zone. However, this policy template does not create policies with actions that direct traffic flows to the Strong protection module.

To configure policy templates:

1. From the Zone's main menu, select **Configuration > Policy templates**.
2. Click on the required policy template name.

Figure 5-3 Policy Templates

The screenshot shows the configuration page for a policy template. The page title is "Zone scanner (Interactive) - Protected" with a "New Recommendations" button. The breadcrumb is "Home > Zone > Policies > Policy details". There are links for "View Dynamic Filters (0)", "Remove Dynamic Filters (0)", "Activate Policy", and "Deactivate Policy".

Policy Template	Service	Level	Type	Key
dms_jsp	53	analysis	pta	dst_ip

State	Operation mode	Action	Threshold	Timeout
active	interactive	to-user-Mem	2000	800

A "Config" button is located at the bottom right of the table.

Configuring the Policy Template Operational Parameters

During the Learning phases, the zone's traffic flows transparently through the Guard. Each active policy template produces a group of specified policies, according to the Zone's traffic characteristics. The Guard enables the user to define the maximum number of policies the Guard will produce from a specified policy template. This is configured according to the parameter: Max Services. The Guard ranks the services the policy template relates to by their level of traffic volume. The Guard will then pick up the services that have exceeded the defined minimum threshold (as defined by the parameter Min Threshold) with the highest traffic volume and create a policy for each one of them. Some of the policy templates will create an additional policy to handle all traffic flows for which a specific policy was not added. These policies will be added with a service of 'any'.

For each of the Policy Templates, the following operational parameters may be configured:

Parameter	Description
State	Specifies the policy template state. The policy template can be enabled or disabled. Disabling a policy template prevents it from producing policies once the Guard undergoes the Policy Construction phase.
Min Threshold	<p>Specifies the minimum traffic volume threshold for a service. Once the threshold is exceeded, the Guard produces policies that relate to the services' traffic according to the particular traffic flow that violated the threshold.</p> <p>This parameter cannot be configured for policy templates that are essential for proper zone protection and therefore always produce a policy, such as fragments.</p> <p>Setting the threshold enables the user to better adopt the Guard protection to the traffic volume of the user's zone services.</p>
Max Services	<p>Specifies the maximum number of policies (each relating to a service) that will be produced from the specified policy template. The Guard ranks the services the policy template relates to by their level of traffic volume. The Guard will then pick up the services that have exceeded the defined minimum threshold (as defined by the parameter Min Threshold) with the highest traffic volume and create a policy for each one of them. An additional policy to handle all other traffic flows service (such as dns_tcp that relates to service 53), or for policy templates that relate to a specified traffic characteristic (such as fragments).</p> <p>Limiting the service number allows the user to better tailor the Guard protection policies to its preferred traffic flow requirements.ith the characteristics of the policy template may be added with a service of 'any'.</p> <p>This parameter may be defined only for policy templates that detect services, such as tcp_services. It cannot be configured for policy templates that relate to a specified</p>

**Caution**

Disabling a policy template results in the Guard's inability to protect the zone from traffic of the kind the policy template relates to. This may seriously compromise the Guard's protection.



Zone Traffic Learning and Policy Construction

This chapter describes how to create traffic-tailored policies for zones on the Cisco Guard using the Web-Based Management (WBM).

This chapter includes the following sections:

- [Overview](#)
- [Zone Traffic Learning](#) (constructing policies and tuning policy thresholds using the learning processes)
- [Zone Policies](#)
- [Snapshot](#) and [Compare Policies](#) (a mechanism used to verify the learning process outcome)

Overview

The policies are the mechanisms that measure a particular traffic flow and take action against the flow as a result of threshold violation. The protection policies are constructed from policy templates.

A Policy Template is a collection of policy constructing guiding rules that will be used during the learning phases to construct the zone's policies.

The learning process constitutes two phases, during which the Guard learns the zone's traffic and adopts itself to its particular characteristics:

1. **The Policy Construction Phase**—In this phase the zone policies are created using the Guard Policy Templates. This phase consists of traffic flowing transparently through the Guard, enabling it to discover the main services used by the zone.
2. **The Threshold Tuning Phase**—In this phase the policies are tuned to fit the zone services traffic rates. This phase consists of traffic flowing transparently through the Guard, enabling it to tune the thresholds for the services discovered in the policy construction phase.

During this process, the Guard learns the zone's traffic characteristics to acquire a basis to which to compare zone traffic and trace any anomalies that might, in turn, become malicious.

After the policies are created, you may add and delete policies or change policy parameters such as thresholds, services, timeouts and actions.

The action taken by the policies could range from merely notifying to directing the traffic to various Guard protection mechanisms or even dropping malicious traffic.

For a comprehensive review of the learning process, refer to Chapter 5, “Zone Configurations,” in the *Cisco Guard User Guide*.

For a comprehensive review of the policy procedures, refer to Chapter 9, “Advances Policy Procedures,” in the *Cisco Guard User Guide*.

Zone Traffic Learning

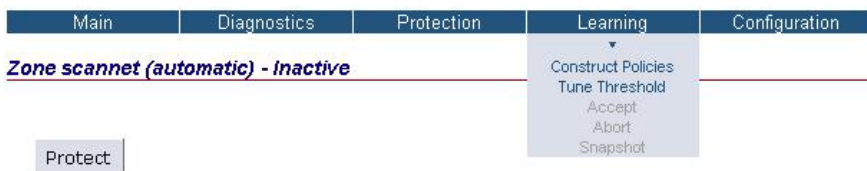
During the Learning phases, the Guard learns the zone's traffic characteristics. The results of this stage will be translated into protection policies. The Learning system constructs the Guard protection policies. These instruct the Guard Protection system how to regard the zone traffic flows. The Guard Learning phase begins with the Guard traffic diversion mechanisms that divert the zone routine traffic to the Guard.

**Note**

Diversion must be configured before the learning process is initiated. zone diversion configuration is configured via the Guard routing configuration. For information regarding zone Diversion configuration, refer to Appendix A, “Diversion Configuration,” in the *Cisco Guard User Guide*.

The Guard’s tools for constructing protection policies are the Policy Templates. These define the types of zone policies to be created according to traffic characteristics. The policy templates also define the Maximum Services and Minimum Threshold for each service policy in accordance to the guiding parameters provided (see [Chapter 5, “Advanced Zone Procedures,”](#) for further details).

Figure 6-1 Zone Learning Menu



119389

Constructing Policies

In this stage the zone policies are created. Zone traffic flows transparently through the Guard, enabling it to discover the main services used by the zone.

To initiate Learning Phase 1—Policy Construction:

From the Zone's main menu, select **Learning > Construct Policies**.

**Note**

We recommend letting the Learning Phase 1—Policy Construction continue for at least two hours prior to proceeding to the next phase.

After a sufficient period of time, end the Policy Construction phase.

Terminating the Policy Construction Phase

After a sufficient period of time (see not above), abort the learning process. You may decide how to handle the newly constructed policies.

To accept the Guard's suggested policies:

From the Zone's menu, select **Learning > Accept** (see [Figure 6-1](#)).

In this case, the Guard erases its previously learned policies and thresholds.



Note

After accepting the newly constructed policies, you may manually add or remove policies or change the policy parameters. See the [“Adding a Service”](#), [“Removing a Service”](#) and [“Configuring the Operational Parameters”](#) sections for further details.

To accept the Detector's suggested policies selectively, see the [“Accepting Policy Parameters Selectively”](#) section.

To reject the Guard's suggested policies:

From the Zone's menu, select **Learning > Abort** (see [Figure 6-1](#)).

In this case, the Guard stops the process and erases all its learned data. As a result, the Guard falls back into its default settings (in the case of a new zone) or to the zone traffic configurations it had prior to the learning abortion.

To view the learning process outcomes prior to making a decision:

Use the snapshot procedure (see the [“Snapshot”](#) section in this chapter for further details).

Tuning Thresholds

In this stage, the Guard further analyses the zone traffic and defines threshold for the policies constructed in the previous phase. The other policy operational parameters (the Timeout and Action) are configured by default. The Guard enables to configure its policy operational parameters.

To initiate Learning Phase 2—Threshold Tuning:

From the Zone's main menu, select **Learning > Tune Threshold**.

**Note**

It is recommended to run the threshold-tuning phase during traffic peak time (the busiest day) for a period of a minimum 24 hours.

Terminating the Threshold Tuning Phase

After a sufficient period of time (see not above), abort the learning process. You may decide how to handle the newly constructed policies.

To accept the Guard's suggested policies:

From the Zone's main menu, select **Learning > Accept** (see [Figure 6-1](#)).

In this case, the Guard erases its previously learned thresholds.

**Note**

After accepting the new thresholds, you may manually change the policy parameters. See the “[Configuring the Operational Parameters](#)” section for further details.

To accept the Detector's suggested policies selectively, see the “[Accepting Policy Parameters Selectively](#)” section.

To reject the Guard's suggested policies:

From the Zone's main menu, select **Learning > Abort** (see [Figure 6-1](#)).

In this case, The Guard stops the Threshold Tuning phase and adopts the Policy Construction Phase results and the former thresholds results the Guard has. This results in a situation in which newly constructed policies have thresholds that were obtained according to past traffic characteristics.

To view the learning process outcomes prior to making a decision:

Use the snapshot procedure (see the “[Snapshot](#)” section in this chapter for further details).

Zone Policies

Overview

The Guard policy structure consists of sections. Each policy section has different role in relating to different traffic protection aspects.

To view the zone policies:

From the Zone's main menu select **Configuration > Policy**.

Figure 6-2 Policy Table

Zone scanner (automatic) - Inactive
Home > Zone > Policies
View All (246) View Active (105) View Inactive (0) View Disabled (55)

+ Policy Template	Service	Level	Type	Key	Threshold	Action	Timeout
- dns_top	- 53						
		- analysis					
			- pkts				
				dst_ip	40.0	to-user-flags	600
				global	40.0	to-user-flags	600
				src_ip	10.0	to-user-flags	600
				src_port	150.0	to-user-flags	600
		+ sysa					
		+ basic					
+ dns_top							
+ fragments							

119360

To navigate in the tree hierarchy, click the plus icon (+) or the minus icon (-) next to the tree or branch that you want to expand or collapse. Click the plus icon (+) in the tables header to expand all policy levels.

To open the configuration window, click an item in the tree hierarchy. For example, in [Figure 6-2](#), click **53** to open the service configuration window for the `dns_tcp` policy template.

The term Policy refers to a complete policy path:

`<policy-template-name><Service><Level><Type><Key>`. For example:
`dns_tcp/53/analysis/pkts/dst_ip`.

The term Policy section refers to a partial policy such as

`<policy-template-name><Service>` or

`<policy-template-name><Service><Level>`. For example, the policy section `http` or `dns_tcp/53`.

Tree items can have one of the following statuses:

- **Active**—marked in bold
- **Inactive**—marked as grayed out
- **Disabled**—marked as grayed out and crossed out

Below the zone location bar, a filter bar enables to selectively choose the policies to be displayed according to their state (Active/Inactive/Disabled/All).

The Policy Table parameters consist of the following:

Parameter	Description
Policy Template	Indicates the policy template that was used to construct this policy.
Service	<p>Indicates the services the policy relates to. The Guard enables to add a service to better tailor the produced policies to the zone specific services. After adding a new service, you may define the threshold manually, however, it is recommended to run the threshold tuning phase (see the “Tuning Thresholds” section in this chapter for further details) to attune the policies to the zone's traffic.</p> <p>The service ‘any’ relates to all traffic that does not specifically match other services created from the same policy template.</p> <p>Note A new service may be added to the following policy templates:</p> <ul style="list-style-type: none"> • tcp_services, udp_services, tcp_services_ns—The added service designates a port number. • other protocols—The added service designates a protocol number.
Level	Indicates the Protection module used to process the traffic flow (analysis, basic or strong).

Parameter	Description
Type	<p data-bbox="606 238 1184 266">Indicates the packet type. The packet types include:</p> <ul style="list-style-type: none"> <li data-bbox="606 285 1184 342">• auth_pkts—Packets that underwent either TCP handshake or UDP authentication. <li data-bbox="606 362 1184 418">• auth_tcp_pkts—Packets that underwent TCP handshake. <li data-bbox="606 438 1184 495">• auth_udp_pkts—Packets that underwent UDP authentication. <li data-bbox="606 514 1231 607">• in_nodata_conns—Zone incoming connections that have no data transfer on the connection (packets without a data payload). <li data-bbox="606 626 1099 654">• in_conns—Zone incoming connections. <li data-bbox="606 673 1166 701">• in_pkts—Zone incoming DNS query packets. <li data-bbox="606 721 1220 779">• in_unauth_pkts—Zone incoming unauthenticated DNS queries. <li data-bbox="606 799 1231 891">• num_sources—Number of TCP source IPs, destined to the zone, that have been authenticated by the Guard’s anti-spoofing mechanisms. <li data-bbox="606 911 1177 938">• out_pkts—Zone incoming DNS reply packets. <li data-bbox="606 958 1123 985">• reqs—Request packets with data payload. <li data-bbox="606 1005 1231 1063">• syms—Synchronization packets—TCP SYN flagged packets. <li data-bbox="606 1083 1184 1198">• 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. <li data-bbox="606 1218 1206 1276">• unauth_pkts—Packets that did not undergo TCP handshake. <li data-bbox="606 1295 1204 1354">• pkts—All packet types that do not fall under any other category in the same detection level.

Parameter	Description
Key	<p data-bbox="606 238 1231 297">Indicates the key (traffic characteristics) that was used to aggregate the policies.</p> <p data-bbox="606 315 1231 342">Open the Type branch to view the key. The keys include:</p> <ul data-bbox="606 360 1231 1112" style="list-style-type: none"> <li data-bbox="606 360 1166 388">• dst_ip—Traffic destined to a zone IP address. <li data-bbox="606 406 1210 464">• dst_ip_ratio—The ratio of SYN and FIN flagged packets destined to a specific IP address. <li data-bbox="606 482 1231 540">• dst_port_ratio—The ratio of SYN and FIN flagged packets destined to a specific port. <li data-bbox="606 558 1231 617">• global—A summation of all traffic flow as defined by the other policy sections. <li data-bbox="606 634 1190 693">• src_ip—Traffic destined to the zone aggregated according to source IP address. <li data-bbox="606 711 1204 769">• src_net—Traffic destined to the zone aggregated according to source subnet IP address. <li data-bbox="606 787 1217 815">• dst_port—Traffic destined to a specific zone port. <li data-bbox="606 833 1217 891">• protocol—Traffic destined to the zone aggregated according to protocol. <li data-bbox="606 909 1231 998">• src_ip_many_dst_ips—This is the key used for ip scanning. Traffic from a single IP destined to many zone IP addresses. <li data-bbox="606 1016 1231 1112">• src_ip_many_ports—This is the key used for port scanning. Traffic from one IP destined to many zone ports.
Threshold	<p data-bbox="606 1131 1231 1312">Indicates the threshold traffic rate for a specific policy. Once violated, the policy assumes an action to protect the zone. The threshold is set by default to a value appropriate for on-demand protection. It is adjusted by the threshold-tuning phase in the learning procedure, and can be manually configured.</p>

Parameter	Description
Action	Indicates the action a policy assumes as a result of a threshold violation. See the “ Configuring the Operational Parameters ” section below for further details.
Timeout	Indicates the minimum time span for the policy to apply its action. Once the timeout expires, the Guard runs a procedure in order to determine whether or not to deactivate a dynamic filter that was produced by the policy (see the “ Dynamic Filter Termination ” section in Chapter 7, “Protecting Zones,” for further details).

Policy Configuration

After completing the learning processes, you may wish to view specific policy operational parameters. Displaying these parameters may help you decide whether the policy operational parameters suit the zone’s traffic. You may, when required, configure the policy operational parameters to better tailor the policy to the zone’s traffic requirements.

To view the zone policies:

From the Zone's main menu, select **Configuration > Policy**.

To configure a policy or policy section:

Click the required policy in the policy tree.

Adding a Service

The new service is added to all policies that were created from the specified policy template.

To add a service to a policy:

1. Click the required policy in the Policy tree.
The Policy table is displayed.
2. Click **Add Service**.

The new service is defined with default values. You may define the threshold manually, however, it is recommended to run the threshold-tuning phase (see the “[Tuning Thresholds](#)” section in this chapter for further details) to attune the policies to the zone's traffic.

**Note**

A new service may be added to the following policy templates:

- **tcp_services, udp_services, tcp_services_ns**—The added service designates a port number.
 - **other_protocols, http**—The added service designates a protocol number.
-

Removing a Service

**Caution**

You may remove a specific service relating to a desired policy template.

Removing a service prevents the Guard policies from relating to the removed traffic service and may compromise the zone protection.

To remove a service from a policy:

1. Click the service number for the required policy in the Policy tree.
The Service table appears.
2. From the bar, click **Remove Service**.

Configuring the Operational Parameters

Operational Parameters Overview

Once the zone policies are constructed and the thresholds tuned, you may manually configure the policy operational parameters.

The following Operational parameters may be configured:

Parameter	Description
State	Indicates the state of the policy section. These can be: <ul style="list-style-type: none">• Active—The policy is active.• Inactive—The policy measures traffic flow but does not take action if the threshold is violated.• Disabled—The policy is disabled.
Operation mode	Indicates the interactive-status the pending Dynamic filters, created by the policy, assume. See the “Interactive Recommendations Mode” section in Chapter 7 , “Protecting Zones,” for further details. Note Interactive-Status can be viewed and configured only for protected zones in interactive mode.

Parameter	Description
Action	<p>Indicates the actions a policy assumes as a result of a threshold violation. These are:</p> <ul style="list-style-type: none"> • block-unauthenticated—The policy adds a filter that blocks traffic that was not authenticated by the anti-spoofing mechanism. • filter/strong—The policy adds a filter directing the traffic to the Strong protection module mechanisms. • to-user-filters—The policy adds a filter directing the traffic to the user filters. • filter/drop—The policy adds a filter directing the traffic to the Drop protection module to be dropped. • notify—The policy notifies the user of the threshold violation. • redirect/zombie—The policy adds a filter that enhances authentication for all User filters with an action of <i>redirect</i>.
Threshold	<p>Indicates the threshold traffic rate for a specific policy. Once violated, the policy assumes an action to protect the zone. The threshold is measured in packets per second (pps) apart for the following policies:</p> <ul style="list-style-type: none"> • tcp_connections—measured in number of connections • tcp_ratio—measured as the ratio number
Timeout	<p>Indicates the minimum time span for the policy to apply its action. Once the timeout expires, the Guard runs a procedure in order to determine whether or not to deactivate a dynamic filter that was produced by the policy (see the “Dynamic Filter Termination” section in Chapter 7, “Protecting Zones,” for further details).</p>

The policy state may be configured from all policy sections.

The operational parameters action, threshold and timeout can only be configured from the key level.

Configuring the Policy State

The Guard supports the following policy states:

- **Disable**—The policy does not relate to the traffic flow and so no threshold is obtained. As a result, the policies will have to undergo a new learning threshold-tuning phase to ensure correct thresholds are applied for the policies.



Note When a policy is disabled other policies regard its targeted traffic as theirs and so all policies would have to undergo a new learning threshold-tuning phase before the policies are applied in protect mode.

- **Inactivate**—The policy relates to the traffic and obtains the threshold but launches no action when a threshold is violated. This procedure frees you from the need to pass the policy through a new learning threshold-tuning phase. By default, all the Guard policies are activated.
- **Activate**—The policy relates to the traffic and issues an action once the thresholds is violated.



Caution Unnecessarily inactivation or disabling may prevent the Guard policies from assuming their protective role and may compromise the zone protection.



Note You may disable a desired policy section before or after any of the Learning Phases.

You may deactivate a desired policy section to prevent the policy from issuing actions regarded as unwanted.



Note Running the policy-construction phase after disabling a policy might result in the policy reconfiguration according to traffic flow. This could result in the policy re-activation.

The policy action, timeout and threshold may be changed at every section of the policy path. However, more policies are affected when these parameters are changed at the initial policy sections (such as Policy template or Port sections). Configuring these parameters at a high-level policy path hierarchy will change these parameters in all its sub-policy paths.

To change the policy state of a policy section:

1. Click on the desired policy section.
2. Click the required policy state from the policy state bar (see [Figure 6-3](#)).

Figure 6-3 Policy Table Section

Policy Template	Service	Level	Type	Active	Inactive	Disabled
dst_ip	53			12	0	4

The policy section table provides additional information on the state and number of policies that are constructed from the viewed policy section.

To configure the policy's state, open the policy details tables. See the [“Configuring the Operational Parameters”](#) section for further details.

Configuring the Policy Operational Parameters

Once the zone policies are constructed and the thresholds tuned, you may manually configure the policy operational parameters.

To configure the operational parameters:

1. Open the policy up to the key level.
2. Click on the key of the policy to configure (for example, in [Figure 6-2](#), click on **dst-ip**, **global**, **src_ip** or **src_net**).

The Policy details tables (Figure 6-4) are displayed.

The Policy details includes three tables:

- The policy's definition— Policy Template, service, level, type and key
- The policy's operational parameters—state, action, threshold and timeout
- Specific IP threshold—this table is available only for specified policies (see the “[Specific IP Threshold Configuration](#)” section for further details)

Figure 6-4 Policy Details Tables

Policy Template	Service	Level	Type	Key
dmz_jsp	SS	analyze	pts	dmz_jsp

State	Operation mode	Action	Threshold	Timeout
active	interactive	so-user-libs	200.0	800

Config

To configure the operational parameters:

Click **Config**.

The Zone Policy Form is displayed. See the “[Operational Parameters Overview](#)” section for further information on the operational parameters.

Specific IP Threshold Configuration

In case of known high-volume traffic IP source, you may configure a particular threshold to apply to that IP source address.

In case of a non-homogenous zone (that is, a zone that has more than a single IP defined) for which there is known high-volume traffic only to part of the zone, you may configure a particular threshold to apply to that IP destination address.

Specific IP threshold can be configured for policies with traffic characteristics of source IP and subnet with the action of drop and a policy with traffic characteristic of destination IP with the actions of to-user, strong, notify, and drop (that is, Policies with a key of `src_ip`, `dst_ip` and `src_net`).

For these policy keys, an additional policy details table is available.

To configure a specific IP threshold:

1. Click **Add**.
2. Enter the IP in the IP box and the threshold in the Threshold box.
3. Click **OK**.

To delete a specific IP threshold

1. Select the check box next to the specified IP address.
2. Click **Delete**.

Snapshot

The snapshot, along with the compare policies, is a mechanism used to verify the learning process outcome.

You may save a snapshot of the learning parameters (services, thresholds and other policy related data) at any time of the Learning phase, and later review it. The file containing the snapshot learning phase parameters, along with the zone configuration parameters, is saved under a user defined zone name. Thus, a new zone would be created bearing the configurations and policy parameters (number of services, thresholds, action, timeout, etc.) of the zone at snapshot time.

**Note**

The Guard continues its Learning phases as the snapshot is taken.

To create a snapshot of the zone's learning parameters:

1. From the Zone's main menu, select **Learning > Snapshot**.



Note The **snapshot** command is applicable while the zone is in Learning only.

2. Enter the Snapshot's name.

**Note**

The Snapshot creates a new zone. After verifying the snapshot parameters, or comparing two snapshots, you may choose to delete the snapshot. Alternatively, you may keep the snapshot and delete the originating zone.

See the [“Compare Policies”](#) section to compare the Policy parameters of two snapshots.

See the [“Accepting Policy Parameters Selectively”](#) section to selectively accept the snapshot parameters.

Compare Policies

You may compare between the snapshot Learning parameters and the zone Learning parameters. The comparison is held to trace differences in policies, services, and thresholds. You may define the comparator's differing sensitivity.

In case differences are observed, you may change the base zone's policy according to the compared zone policy parameters. This provides a powerful tool that enables you to accept learnt policy parameters selectively (see the [“Accepting Policy Parameters Selectively”](#) section for further details).

To compare between two learning parameter files:

1. Perform one of the following:
 - From the Zone's main menu, select **Configuration > Compare policies**.
 - From the Guard's main menu, select **Zones > Compare Zone policies**.

The policy comparison query window appears.

2. Enter the following parameters:

Parameter	Description
Base Zone	The name of the base zone whose learning parameters are compared. The base zone's policies may be changed according to the compared zone's policy parameters.
Compared Zone	The name of the zone or snapshot the learning parameters of the base zone are compared to.
Minimal difference	The traced differing percentage. The Detector will trace any parameters that differ above the defined percentage.

3. Click **OK**.

The policy comparison tables are displayed (see [Figure 6-5](#)).

Figure 6-5 Policy Comparison

The screenshot displays the 'Policy Comparison' window. At the top, it shows 'Base zone: scanet' and 'Compared zone: scanetSnapshot'. Below this, there are two sections:

Difference in services

- Services only in scanet:** A table with one row containing 'other_protocols?'. A 'Delete' button is located below this table.
- Services missing from scanet:** A table with one row containing 'other_protocols?'. An 'Add' button is located below this table.

Difference in policy parameters

Policy name	Threshold	Proxy Thresh.	Action	State
udp_services/any/basic/auth_plits/global	100.0	0.0	notify	active
tcp_services/any/string/req/dst_port	200000.0	0.0	notify	active
tcp_services/any/string/req/dst_port	30.0	0.0	notify	active
tcp_rate/any/string/syn_by_fin/dst_ip_ratio	484	0.0	notify	active
	10.0	0.0	notify	active

A 'Copy Parameters' button is located at the bottom left of the table. A vertical ID 't119356' is visible on the right side of the screenshot.

The policy comparison consists of tables grouped into two sections. These are:

- **Difference in services**—The services in this section are displayed in two tables:
 - Services present only in the base zone policies.
 - Services missing from the base zone. These services are defined only in the compared zone.
- **Difference in policy parameters**—Differences in the policy operational parameters (state, action, threshold, proxy-threshold) are displayed. Each section in the table presents the differences found in a single policy. The upper row presents the policy and the operational parameters of the base zone. The lower row presents the policy and the operational parameters of the compared zone.

Accepting Policy Parameters Selectively

In case differences are observed while comparing policies, you may change the base zone's policy according to the compared zone policy parameters. This provides a powerful tool that enables you to accept learnt policy parameters selectively.

Figure 6-5 displays the policy comparison tables (see the “Compare Policies” section for further details).

The policy comparison consists of tables grouped into two sections. These are:

- **Difference in services**—The services in this section are displayed in two tables:
 - Services present only in the base zone policies. You may choose to remove these services.
 - Services missing from the base zone. These services are defined only in the compared zone. You may choose to add these services to the base zone policies.

To remove services from the base zone policies:

1. Select the check box next to the required services under **Services only in** *<Zone-name>*.
2. Click **Delete**.

To add these services to the base zone policies:

1. Select the check box next to the required services under **Services missing from** *<Zone-name>*.
2. Click **Add**.

- **Difference in policy parameters**—Differences in the policy operational parameters (state, action, threshold, proxy-threshold) are displayed. Each section in the table presents the differences found in a single policy. The upper row presents the policy and the operational parameters of the base zone. The lower row presents the policy and the operational parameters of the compared zone.

To copy the policy operational parameters from the compared zone to the base zone (from the lower row to the upper row):

1. Select the check box next to the required policies.
2. Click **Copy Parameters**.



Note

Select the checkbox at the table header to select all table entries.



Note

The snapshot procedure creates a new zone. After comparing two zones (or snapshots) and modifying the base zone policies, you may choose to delete the compared zone.

■ Accepting Policy Parameters Selectively



Protecting Zones

This chapter describes how to perform tasks for protecting zones on the Cisco Guard using the Web-Based Management (WBM).

Processes described in this chapter must be performed after completing the Cisco Guard configuration and zone configuration described in the previous chapters of this guide.

This chapter includes the following sections:

- [Overview](#)
- [Protecting the Zone](#) (activate/deactivate protection)
- [Dynamic Filters](#) (View or add Dynamic filters during attack)
- [Interactive Recommendations Mode](#) (using the Guard's recommendations)

Overview

Before activating the Cisco Guard's protection for a zone, it is recommended to let the Guard study the zone's traffic patterns. The learning process allows the Cisco Guard to learn the traffic patterns of each zone and to create sets of recommended thresholds according to statistical analysis of the traffic.

In case of an attack on the zone prior to completion of the zone learning phases, when the Guard hasn't yet adopted its protection policy to suite the zone traffic, the Guard has its 'On-Demand' protection. In such a situation, the zone protection activates the Guard's anti-spoofing and anti-zombie mechanisms quickly. The

default thresholds configured for a new zone, enable effective ‘On-Demand’ protection. Refer to Chapter 6, “On-Demand Protection,” in the *Cisco Guard User Guide* for further details.

After learning the zone traffic characteristics, the Guard is ready to protect the zone. You may wish to wait for an external indication (from the Cisco Detector or any other means) of an attack before setting the Guard to protect the zone, or command the Guard to protect the zone right after completing the zone configuration. During the zone protection process, the Guard diverts the zone traffic and applies its protection policies.

When the Guard protection policies sense abnormal or malicious traffic (by means of threshold violation), they dynamically configure a set of filters (Dynamic Filters) to direct the traffic to the appropriate protection module according to the attack severity.

The Guard’s protection can be activated in two operation modes:

- Automatic protection mode—Activation of the dynamic filters is carried out without user intervention.
- Interactive protection mode—Dynamic filters are activated manually, in an interactive mode. The Dynamic filters are grouped as recommendations that await user decision. You may review these recommendations and manually decide which of them to accept, ignore, or direct to automatic activation.

The operation mode is configured for each zone separately. See the “[Creating Zones and Basic Zone Configuration](#)” section in [Chapter 4, “Zone Creation and Configuration,”](#) for further details.

The Cisco Guard system provides a series of tools for adjusting a zone’s protection mechanism while protection is active.

**Note**

Before activating the Cisco Guard’s protection, traffic diversion for the zone’s traffic must be configured. For further information on zone diversion configuration, refer to Appendix A, “Diversion Configuration,” in the *Cisco Guard User Guide*.

Protecting the Zone

After learning the zone traffic characteristics, the Guard is ready to protect the Zone. During the zone protection process, the Guard diverts the zone traffic and applies its protection policies.

Figure 7-1 Protection Menu



119404

Activating Protection

To activate zone protection, perform one of the following:

- On the Zone's "home page", click **Protect**.
- From the Zone's main menu, select **Protection > Protect**.



Note

The Guard has its 'On-Demand' protection to answer the situation in which the zone is under attack while the Guard hasn't completed its learning phase and so hasn't adopted its protection policy to suite the zone traffic.

Refer to Chapter 6, "On Demand Protection," in the *Cisco Guard User Guide* for further details.

Deactivating Protection

To deactivate the zone's protection, perform one of the following:

- On the Zone's "home page", click **Deactivate**.
- From the Zone's main menu, select **Protection > Deactivate**.

Zone Protection Verification

You may wish, now, to view the zone status and verify that the protection process is functioning properly. View the zone counters.

To view the zone counters:

From the Zone main menu, select **Diagnostics > Counters**.

To verify whether an attack is in progress, check the following:

Malicious traffic rate is greater than zero.

To verify the zone protection is functioning properly while an attack is in progress, check the following:

- The number of active Dynamic filters (as can be viewed from the Zone's "home page") is greater than zero.
- Legitimate traffic rate is greater than zero.

In case there is no attack on the zone and no indications of suspicious traffic, the Guard designates all diverted traffic as legitimate traffic and forwards it on to the zone. The Legitimate traffic counter would then equal that of the Received traffic counter.

See [Chapter 8, "Zone Statistics and Diagnostics,"](#) for further details.

Dynamic Filters

The Guard analyses the diverted zone traffic in search of policy threshold violation. Once a policy threshold violation is observed, the Guard analyses results into a set of filters that are continuously adapted to the zone traffic and type of DDoS attack. This filter set consists of the Dynamic filters. Once abnormal traffic is detected, the Dynamic filter, by default, refers the Guard to the User filters to compare between the User filters suggested action and the Guard suggested protection. You may access the dynamic filters and configure them to your needs.

For a comprehensive overview of Dynamic filters, refer to Chapter 8, "Advanced Filter Procedures," in the *Cisco Guard User Guide*.

To view the Dynamic filters, perform one of the following:

- From the Zone’s main menu, select **Protection > Dynamic filters**.
- On the Zone’s “home page”, click **Active dynamic filters** in the zone’s status summary table.

Figure 7-2 Dynamic Filters Table

ID	Created by	Activation	Expiration	Src IP	Protocol	Src Port	Fragments	Action	Rate type	Details
1	dsl_ip	Dec 10 11:35:41	11/18/41	*	*	*	with	SOA:00:00:00		
2	protocol	Dec 10 11:35:41	11/18/41	*	80	*	without	SOA:00:00:00		
3	protocol	Dec 10 11:35:41	11/18/41	*	12	*	without	SOA:00:00:00		

The Dynamic filters table (Figure 7-2) displays the dynamic filters filtered according to the policy that created them.

The information in the table is related to the ongoing attack. The table includes the following information:

Parameter	Description
Created by	Indicates the policy that created the filter. Clicking on the policy name will display the Policy details (see the “ Zone Policies ” section in Chapter 6 , “ Zone Traffic Learning and Policy Construction ,” for further details).
Activation	Indicates the date and time the filter was activated.
Expiration	Indicates the filter expiration time. Once the filter expires, the Guard decides whether or not to deactivate the Dynamic filter that was produced by the policy according to the Dynamic filter termination criteria (see the “ Dynamic Filter Termination ” section for further details).
Src IP	Indicates the source IP address the Dynamic filter is applied on.
Protocol	Indicates the protocol number the Dynamic filter is applied on.

Parameter	Description
Dst Port	Indicates the destination port the Dynamic filter is applied on.
Fragments	Indicates whether the attack stream contains fragmented packets.
Action	<p>Indicates the action taken by the filter. The following actions apply for the Dynamic filters:</p> <ul style="list-style-type: none"> • to-user-filters—Forwards the specified traffic to the user configured User filters. • filter/strong—Applies Strong protection anti-spoofing mechanisms to the specified traffic. • filter/drop—Drops the traffic. • block-unauthenticated-basic—Drops unauthenticated traffic flow that has not been authenticated by the Basic anti-spoofing mechanisms. • block-unauthenticated-strong—Drops unauthenticated traffic flow that has not been authenticated by the Strong anti-spoofing mechanisms. • block-unauthenticated-dns—Drops unauthenticated traffic flow, flowing to DNS servers, that has not been authenticated by the DNS anti-spoofing mechanisms. • redirect/zombie—The policy adds a filter that enhances authentication for all User filters with an action of <i>redirect</i>.
Rate (pps)	Indicates the approximate attack rate.
Details	Indicates whether additional information can be viewed for this filter. Click i for additional information.

A value of “*” for any of the parameters indicates one of the following:

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

To display detailed information on the filter:

Click **i** in the details column.

See the “[Dynamic Filter Details](#)” section for further details.

Dynamic Filter Termination

Once the Dynamic filter timeout expires, the Guard determines whether the Dynamic filter is to be inactivated. If the Guard decides not to deactivate the Dynamic filter, the filter’s activation timeout resumes for another time span. The dynamic filters will be inactivated when one of the following applies:

- The total zone Malicious traffic rate (equaling the sum of the spoofed and dropped traffic) is less than or equal to the Malicious-rate termination threshold.
- The Dynamic filter does not have an action of to-user-filter (the filter rate counter does not display N/A) and the Filter-rate termination threshold is equal to or greater than **both** the following:
 - The Dynamic filter’s current traffic rate
 - The Dynamic filter’s average traffic rate during a user-configured time span (defined by the policy’s Timeout parameter)

See the “[Creating Zones and Basic Zone Configuration](#)” section in [Chapter 4](#), “[Zone Creation and Configuration](#),” for further details on threshold configuration.

Dynamic Filter Details

The Dynamic Filter Details provides detailed information on the dynamic filters.

To display the detected anomalies details table:

From the details column in the Dynamic Filter table, click **i**.

The Dynamic filter details screen (Figure 7-3) includes three tables:

- Information on the policy that created the filter, as detailed above.
- Information on the attack flow—Information on the attack that was mitigated, as detailed above.



Note The flow mitigated could be of a wider range than the detected attack flow. For example, a non-spoofed attack on port 80 will block all TCP traffic from the originating source IP and not only port 80.

- Information on the filter creation trigger:

Parameter	Description
Policy Threshold	Indicates the threshold defined for the policy that was violated by the attack.
Triggering rate	Indicates the approximate attack rate that triggered the production of the dynamic filter.

Figure 7-3 Dynamic Filter Details

Zone scanner (automatic) - Protected

Home > Zone > Dynamic Filters > Filter details

Dynamic filter #1 - created by fragments/any/analysis/any/auth_globs/det_ip

Src IP	Protocol	Dst Port	Fragments	Action	Count
*	*	*	with	is-use-filter	

Attack Flow

Src IP	Src Port	Protocol	Dst IP	Dst Port	Fragments
*	*	*	192.168.100.34	*	with

Rates

Policy Threshold	Triggering Rate
100.00	7,271.01

T19381

Dynamic Filter Configuration

You may add or delete dynamic filters and configure them your needs.



Note

You may access the Guard's Dynamic filters and configure them to fit your protection policy. However, you should note that dynamic filters are designed to meet dynamically changing protection needs and so the Guard assigns them a limited lifespan (Timeout). The implication is that user-configured dynamic filters that do not out-weight the Guard's Recognition decision will not be implemented. The user-configured dynamic filters are removed once the protection ends.

Deleting a Dynamic Filter

You may wish to delete a Dynamic filter.

To delete a Dynamic filter:

1. Select the check box next to the filter in the Dynamic Filters Details Table (see [Figure 7-2](#)).
2. Click **Delete**.

You may remove all Dynamic filters. The action is effective for a limited period of time since the Guard, being in Protection operation mode, continues to configure new Dynamic filters to adopt its protection to the dynamically changing traffic state.

**Note**

To prevent undesired Dynamic filters from being reproduced, deactivate the policy that produces them (see the “[Policy Configuration](#)” section in [Chapter 6, “Zone Traffic Learning and Policy Construction,”](#) for further details). To find out which policy produced the undesired Dynamic filters see the sections about viewing Dynamic filters in this chapter. Alternatively, you may perform one of the following:

- Configure a Bypass filter for the desired traffic flow (see the “[Bypass Filter Configuration](#)” section in [Chapter 5, “Advanced Zone Procedures,”](#) for further details).
- Increase the Threshold of the policy that produced the undesired Dynamic filter (see the “[Configuring the Policy Operational Parameters](#)” section in [Chapter 6, “Zone Traffic Learning and Policy Construction,”](#) for further details).

Adding a Dynamic Filter

To add a Dynamic filter:

In the Dynamic Filters Details Table (see [Figure 7-2](#)), click **Add**.

The Dynamic Filter Form is displayed.

Enter the following information to configure the Dynamic filter:

Parameter	Description
Source IP	Directs traffic coming from a specified IP address to the Dynamic filter. Leave blank or enter * for ‘any’.
Source Subnet	Directs traffic coming from a specified subnet to the Dynamic filter. Choose the subnet from the drop-down list.
Protocol	Directs traffic from a specified protocol to the Dynamic filter. The protocol is denoted by the its well known number. Leave blank or enter * for ‘any’.
Dst Port	Directs traffic destined to a specified port to the Dynamic filter. Leave blank or enter * for ‘any’.

Parameter	Description
Fragments	<p>Denotes specified traffic type for the filter to operate on. Choose from the drop-down list one of the following:</p> <ul style="list-style-type: none"> • without—The Dynamic filter acts on non-fragmented traffic. • with—The Dynamic filter acts on fragmented traffic. • *—The Dynamic filter acts on fragmented and non-fragmented traffic.
Action	<p>Indicates the action the filter performs on the specified traffic type. Choose the action from the drop-down list:</p> <ul style="list-style-type: none"> • to-user-filters—Forwards the specified traffic to the user configured User filters • filter/strong—Applies Strong protection anti-spoofing mechanisms to the specified traffic. • filter/drop—Drops the traffic. • block-unauthenticated-basic—Drops unauthenticated traffic flow that has not been authenticated by the Basic anti-spoofing mechanisms. • block-unauthenticated-strong—Drops unauthenticated traffic flow that has not been authenticated by the Strong anti-spoofing mechanisms. • block-unauthenticated-dns—Drops unauthenticated traffic flow, flowing to DNS servers, that has not been authenticated by the DNS anti-spoofing mechanisms. • redirect/zombie—The policy adds a filter that enhances authentication for all User filters with an action of <i>redirect</i>.

Parameter	Description
Timeout (Sec)	<p>Indicates the minimal time for the filter to be active (see the “Dynamic Filter Termination” section for further details).</p> <p>Enter an integer to specify the desired time measured in seconds.</p> <p>Leave Blank for unlimited time.</p> <p>Note Unlimited time Dynamic filters are also deleted once protection is aborted.</p>

Interactive Recommendations Mode

In the Interactive Recommendation mode, the Guard enables you to decide on the activation of the filters the policies launch. The Guard functions in accordance with your decision to accept or ignore the filter’s activation. In this way, the Guard lets you decide on the production of its protection measures in real time. The Guard in an interactive mode enhances your control over the activation of the Guard’s protective measures as a DDoS attack progresses.

The recommendations are a summary of the pending dynamic filters aggregated according to the policies that produced them. The Guard recommendation data consists of the policy name that recommended it, data on the traffic anomaly that resulted in policy activation, the number of pending filters and the recommended action.

For a comprehensive overview of the Interactive recommendations mode, refer to Chapter 10, “Interactive Recommendations Mode,” in the *Cisco Guard User Guide*.

**Note**

Note that when the number of pending filters is higher than 1000, the newly added recommendations are recorded in Guard's log-file and then discarded. You are advised to perform the following:

1. Deactivate the zone (click **Deactivate** on the Zone's home page).
 2. Change the operation mode to automatic (see the “[Creating Zones and Basic Zone Configuration](#)” section in [Chapter 4, “Zone Creation and Configuration,”](#) for further details).
 3. Re-activate zone protection (click **Protect** on the Zone's home page).
-

Activating the Interactive Recommendations Mode

The operation mode is a characteristic of a zone.

To activate the interactive recommendations mode:

1. From the Zone's main menu select **Configuration > General**.
2. Click **Config**.
3. Set the operation mode to **interactive**.
4. Click **OK**.

See the “[Creating Zones and Basic Zone Configuration](#)” section in [Chapter 4, “Zone Creation and Configuration,”](#) for further details.

You may choose to end the interactive mode of operation at any time and thus return to the automatic operation mode. This results in the Guard disregarding the decisions made while in the interactive mode. The policies resume their role of automatically producing and activating their filters and automatically accept all pending Dynamic filters and recommendations.

Viewing New Recommendations

New recommendations are indicated by following icon.



The recommendations icon appears in the following locations:

- On the navigation pane, next to the zone's icon in the All Zones list
- On the navigation pane, next to the zone's icon in the Protected Zones list
- On the Zone's "home page", in the zone status bar
- In the Zone list table

When the Guard offers new recommendations, an additional indication is apparent in the form of a number of pending Dynamic filters that is greater than zero. This can be viewed in the Zone's status summary on the Zone's "home page" under **Pending Dynamic filters**.

To view new recommendations, perform one of the following:

- From the Zone's main menu select **Protection > Recommendations**.
- On the Zone's "home page", click **Pending Dynamic filters** in the zone's status summary.

Figure 7-4 Recommendations

Zone scanner (interactive) - Protected

Home - Zone - Recommendations

Snapshot Time: December 10 11:15:01

Filter limit: 1000 seconds

ID	Recommendation	Created By	Attack Flow				Accept Rate				Creation	
			# of PPs	Src IP	Protected	Dest Port	Dest IP	Th.	Mis.	Max.		
205	filesharing	http/80/ basic/pkts/sec_ip	10	*	0	*	*	84.40	197.27	437.47	Dec 10, 11:13:28	
130	videoconfer	tcp_connections/any/ basic/navi_source/global	3	*	0	*	*	192.168.108.34	80.8	112.0	112.0	Dec 10, 11:14:08

Accept Always accept Always ignore

The Recommendations table provides the following information:

Parameter	Description
ID	Indicates the protection recommendation ID number.
Recommendation	Indicates the recommended action.

Parameter	Description
Created By	Indicates the policy that created the filter. Click on the policy name to display the Policy details (see the “Configuring the Policy Operational Parameters” section in Chapter 6, “Zone Traffic Learning and Policy Construction,” for further details).
# of PFs	Indicates the number of pending Dynamic filters that constitute the recommendation. Each pending filter was created as a result of traffic flow that violated the policy threshold. Click on the number to view the pending dynamic filters that constitute the recommendation.
Attack flow	Provides Information on the attack flow: <ul style="list-style-type: none"> • Src IP—The source IP address of the attack stream • Protocol—The protocol number of the attack stream • Dst Port—The destination port of the attack stream • Dst IP—The destination IP address of the attack stream
Thr.	Indicates the policy threshold, in pps, that was violated.
Min.	Recent Rate: Minimum attack rate measured in pps. Note The rate of the lowest pending filter is displayed for Recommendations that aggregate several pending filters.
Max.	Recent Rate: Maximum attack rate measured in pps. Note The rate of the highest pending filter is displayed for Recommendations that aggregate several pending filters.
Creation	The date and time the recommendation was created.

A value of “*” for any of the parameters indicates one of the following:

- The value is undetermined.
- More than one value was measured for the filter's parameter. To display the different values constituting '*', view the complete list of pending filters.

Deciding on the Guard's Recommendations

The Guard enables you to decide on its policy's recommendations. Your decisions determine whether a pending filter will be activated, and for how long, or deactivated. You may also instruct the Guard to automatically, always activate, a specific policy's pending filters. This results in the Guard no longer displaying that policy's filters for you to decide on.

You may, alternatively, decide to instruct the Guard to prevent a policy from producing recommendations (and their pending filters). To prevent a policy from producing recommendations, the policy should be disabled or inactivated. See the [“Configuring the Policy Operational Parameters”](#) section in [Chapter 6, “Zone Traffic Learning and Policy Construction,”](#) for further details.

As the DDoS attack continues and changes its characteristics, so the Guard's policies continue to produce recommendations that you will have to view and decide on. Alternatively, you may change the operation mode to automatic during the ongoing attack.

The Guard activates the Dynamic Filters (see the [“Dynamic Filters”](#) section in this chapter for further details) produced by the policies for at least a user-defined (**Filters timeout**) time span.



Note

Once the filter timeout expires, the Guard runs a checkout procedure in order to decide whether or not to deactivate the Dynamic filter that was produced by the policy (see the [“Dynamic Filter Termination”](#) section for further details).

To decide on the Guard's recommendations:

1. Enter the filter's timeout, in the **Filters timeout** box (the filter timeout is measured in seconds).
2. Select the checkbox next to the recommendation.
3. Click the required action (Accept, Always accept, Always ignore).

The available actions are:

Accept	Accept the specific recommendation. The recommendations pending filters are activated.
Always Accept	Accept the specific recommendation. The decision applies automatically whenever the recommendation policy produces new recommendations. Note The Guard doesn't display the 'always-accept' recommendations.
Always Ignore	Ignore the specific recommendation. No dynamic filter or filters will be produced by the recommendation. The decision automatically applies to all future recommendations produced by the recommendation's policy. Note The future Dynamic filters will only be ignored for the current protection. To prevent a policy from producing recommendations, the policy should be disabled or inactivated.

You may also decide to selectively accept Pending Dynamic filters as opposed to accepting the recommendation. See the [“Pending Dynamic Filters”](#) section in this chapter for further details.



Note

You may change an always-ignore decision made on a specific recommendation by changing the interactive-status of the policy that created the recommendation's pending filters.

Pending Dynamic Filters

The pending Dynamic filters measure each flow that violated a threshold. Pending Dynamic filters that were produced by the same policy are shown as a single recommendation.

To view the Pending Dynamic filters:

Click on the number of pending filters (“# of PFs” column) in the recommendations table (see [Figure 7-4](#)).

Figure 7-5 Pending Dynamic Filters



The Pending Dynamic filters table (Figure 7-5) provides the following information:

Parameter	Description
Created by	Indicates the policy that created the filter. Clicking on the policy name will display the Policy details (See the “ Zone Policies ” section in Chapter 6, “Zone Traffic Learning and Policy Construction,” for further details.).
Activation	Indicates the date and time the filter was created.
Src IP	Indicates the source IP address of the attack stream.
Protocol	Indicates the protocol number of the attack stream.
Dst Port	Indicates the destination port of the attack stream.
Fragments	Indicates whether the attack stream contains fragmented packets.
Action	Indicates the action taken by the filter.
Recent rate	Indicates the current attack rate measured by the filter in pps.
Rate (pps)	Indicates the triggering rate. The approximate attack rate that triggered the production of the dynamic filter.
Details	Indicates whether additional information is available for this filter. Click i for additional information.

A value of “*” for any of the parameters indicates one of the following:

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

Guard activates the Dynamic Filters (see the “[Dynamic Filters](#)” section in this chapter for further details) produced by the policies for at least a user-defined time span (filter timeout).

**Note**

Once the filter timeout expires, the Guard runs a checkout procedure in order to decide whether or not to deactivate the Dynamic filter that was produced by the policy (see the “[Dynamic Filter Termination](#)” section for further details).

To selectively accept a pending Dynamic filter:

1. Enter the timeout in the **Filters timeout** box (the filter timeout is measured in seconds).
2. Select the checkbox next to the required filter.
3. Click **Accept**.

To display detailed information for the filter:

Click **i** in the details column.

See the “[Pending Dynamic Filter Details](#)” section for further details.

Pending Dynamic Filter Details

The pending Dynamic filter details includes three tables:

- Information on the policy that created the filter—as detailed above.
- Information on the attack flow—as detailed above.
- Information the trigger for the filter creation:

Parameter	Description
Policy Threshold	Indicates the threshold defined for the policy that was violated by the attack.
Triggering rate	Indicates the approximate attack rate that triggered the production of the dynamic filter.
Recent Rate	Indicates the Current rate measured by the filter in pps.

Figure 7-6 Pending Dynamic Filter Details

Zone scanner (Interactive) - Protected 

Home - Zone - Dynamic filters - Filter details

Pending filter #37 - created by tcp_services/any/analysis/syns/dst_ip

Src IP	Protocol	Dst Port	Fragments	Action	Count
*	6	*	without	to-user-filter	

Attack Flow

Src IP	Src Port	Protocol	Dst IP	Dst Port	Fragments
*	*	6	192.168.100.34	*	without

Rates

Policy Threshold	Triggering Rate	Recent Rate
30.00	4,444.44	4,468.47

11/25/14



Zone Statistics and Diagnostics

This chapter describes how to perform tasks used for monitoring zones and displaying various zone statistics and diagnostics on the Cisco Guard using the Web-Based Management (WBM).

This chapter includes the following sections:

- [Zone Counters](#)
- [Zone Protection Summary Report](#)
- [Zone Attack Reports](#)
- [HTTP Zombies](#)
- [Zone Event Log](#)

Zone Counters

The zone counters ([Figure 8-1](#)) enable you to analyze the zone's traffic in order to verify the zone's status and to determine whether the zone protection is functioning properly. The zone counters are graphically displayed for a configurable period of time and enable you to view how the zone protection is evolving. The counter information relates to the current zone.

To view the zone counters:

From the Zone's main menu select **Diagnostics > Counters**.

The following Counters are displayed:

- **Legitimate**—Legitimate traffic forwarded by the Guard to the zone.
- **Malicious**—Malicious traffic, destined to the zone, handled by the Guard. Malicious traffic is the sum of dropped packets and spoofed packets (which also include the zombie packets).
- **Received**—Total packets received, destined to the zone, handled by the Guard. Received packets are the sum of legitimate traffic and malicious traffic.
- **Dropped**—Packets that were identified by the Guard as part of an attack, destined to the zone, and therefore dropped.
- **Replied**—Packets, destined to the zone, to which replies were sent to the initiating client as part of the anti-spoofing or anti-zombie mechanisms in order to verify if they are part of authentic traffic or part of an attack.
- **Spoofed**—Packets, destined to the zone, that were identified by the Guard as spoofed packets and therefore not forwarded to the zone. Spoofed packets are replied (bounced) packets (see Replied counter above for further details) for which no replies were received.

Zombie packets are also counted in the spoofed packets counter.

Figure 8-1 Zone Counters



For each of the counters, the following information is available:

- **Shown in Graph**—Specifies whether the counter will be shown in the graph below.
- **Packets**—Total amount of packets, destined to the zone, since last reload.
- **Bits**—Total amount of bits, destined to the zone, since last reload.
- **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.

By default, legitimate and malicious traffic counters are displayed for a period of the past two hours and are measured in bits per second (bps).

To update the graph:

1. Select the check boxes next to the counters to be displayed.
2. Choose the period of time.
3. Choose the traffic rate units.
4. Click **Update Graph**.

Below the graph is a legend that identifies the counters. For each counter in the graph, the minimum, maximum and average rate are displayed for the period of time and rate units chosen.

Traffic Analysis

It is important to analyze the traffic flow in order to determine whether traffic is flowing properly to the zone. The following section provides guiding details to help you analyze the traffic flow and provide an indication on possible problems and their solutions.

Having Received and Legitimate (forwarded to the zone) packets greater than zero indicates a proper functioning of the Guard diversion mechanism.

A received packets number greater than the legitimate, and a malicious packets number greater than zero indicate proper protection functioning. This isn't an absolute indicator for fully traffic-tailored functioning and you may also wish to view the Dynamic filters.

A Received packets number greater than the legitimate packets number, and dynamic filters produced, provide an indication that the Guard has identified an attack.

You should observe the following in light of both work experience and traffic knowledge:

- If there are dropped packets, you should verify whether a trusted IP source is blocked by a Dynamic filter. You may wish to have that source IP bypass the Guard filters (see the [“Bypass Filter Configuration”](#) section in [Chapter 5](#), [“Advanced Zone Procedures,”](#) for further details).
- If a policy has produced filters that drop too many IP flows, you should verify whether filters are blocking flows from source IP addresses that seem legitimate but are sending traffic in rates above the thresholds. In such a situation, you may wish to increase the policy's threshold or prevent its further production by deactivating it (see the [“Zone Policies”](#) section in [Chapter 6](#), [“Zone Traffic Learning and Policy Construction,”](#) for further details).
- In case the Received packets current rate (pps and bps) = 0, or the number of legitimate packets stays constant for a long period of time, refer to the [“Problem Analysis”](#) section in this chapter.

Note that the counters (Packets or Bits) would display a constant number as they are accumulated. The graph and the legitimate traffic current rate (pps and bps), displayed in the legend, would display legitimate packets = 0 as they display the current traffic rate.

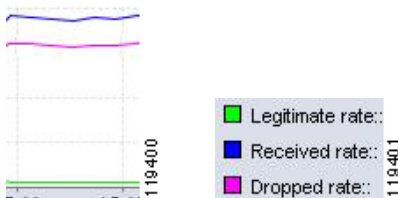
Problem Analysis

When the Received counters (Packets or Bits) or Legitimate counters (Packets or Bits) equals 0, this could indicate a problem. This problem could be either or both of the following:

- A case in which the Guard does not receive the packets destined to the zone (Received counters = 0)—This indicates a diversion problem or a network configuration problem. Refer to Appendix B, “Diversion Troubleshooting,” in the *Cisco Guard User Guide* for further details.
- A case in which the Guard receives the zone’s diverted traffic packets but blocks them from being forwarded to the zone (Received counters \neq 0 and Legitimate current rate (pps or bps) = 0 across a period of time)—This may indicate legitimate traffic was falsely identified as malicious traffic and is being dropped.

The example shown in [Figure 8-2](#) describes a situation in which almost all the traffic destined to the zone is dropped.

Figure 8-2 Problem analysis: Rcv \neq 0, Legitimate = 0



- Erase the drop-action Dynamic filter.
- Deactivate the protection policy that produced the drop-action Dynamic filter so that no policies of the kind that produced the drop-action Dynamic filter would be reproduced (avoiding taking this action would result in the drop-action filter re-appearing).

**Caution**

Deactivating the protection policy that produced the Dynamic filter compromises the zone protection.

The above-mentioned problem could occur in one of the following situations:

- The protected zone receives no traffic.
- All the traffic destined to the zone is identified by the Guard as malicious.

**Tip**

These situations are likely to occur in a lab setup and are less likely to occur in real-world networks.

Zone Protection Summary Report

The Guard provides a protection summary report for each zone to help in forming a clearer picture of the detected attacks on the zone. It provides a summary of the DDoS attacks on the zone during a user-defined period of time. The Guard records the relevant details during attacks and organizes the data under the report categories. The report details the total number and intensity of the attacks. In addition, the report provides a list of the attacks with a short summary. The reports are accompanied with a graphical presentation of the data.

To view the zone Detection Summary report:

From the Zone's main menu, select **Diagnostics > Attack Reports**.

The zone protection summary report consists of data fields and tables. These are grouped in three sections:

- [Protection Graph](#)
- [Total Attack Statistics](#)
- [Per Attack Summary](#)

By default, the report is displayed for a period of the past month.

To change the report tables display settings:

1. Enter the required period of time (enter the **Period from** and **to** dates):
 - a. Click on the calendar icon (on the right side of each field).

- b. Select a date.
2. Click **Get Reports**.

Protection Graph

The protection graph provides a graphical summary of the attacks during the user-defined period of time.

Figure 8-3 Zone Protection Summary Report – Protection Graph



The X-axis displays the time during 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 place your mouse cursor over any of the attack bars and hold it there for a few seconds, a small box (a ToolTip) appears displaying the average attack rate.

The bar also provides a link to the attack report.

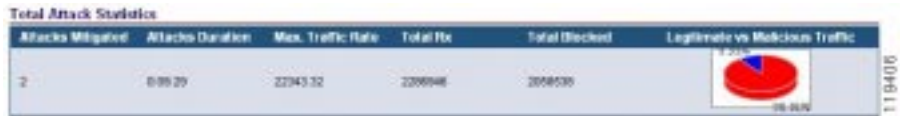
To display the attack report:

- Click on the attack bar.

Total Attack Statistics

The total attack statistics table (Figure 8-4) provides information on the number of attacks on the zone and the aggregated attack details during the user-defined period of time.

Figure 8-4 Zone Protection Summary Report—Total Attack Statistics



The following information is provided:

Parameter	Description
Attacks Mitigated	Indicates the number of attacks mitigated
Attacks Duration	Indicates the aggregated duration of the mitigated attacks
Max. Traffic Rate	Indicates the maximum amount of malicious traffic (measured in packets), destined to the zone, handled by the Guard
Total Rx	Indicates the total amount of traffic (measured in packets), destined to the zone, handled by the Guard
Total Blocked	Indicates the total amount of traffic (measured in packets), destined to the zone, that was dropped by the Guard
Legitimate vs. Malicious Traffic	A pie chart that displays the percentage of Malicious traffic (displayed in red), and Legitimate traffic (displayed in blue) within the total amount of zone traffic

Per Attack Summary

The Per Attack Summary provides a list of the DDoS attacks on the zone during the user-defined period of time.

Figure 8-5 Zone Protection Summary Report—Per Attack Summary

#	Start time	Duration	Type	Peak(pps)	Received Pkts	Legitimate vs. Malicious Traffic
3	Dec 06, 03 16:09:15	00:00:55	swoofed	31656.14	1,673,174.00	99.95%
2	Dec 06, 03 14:35:30	1:32:00	Hybrid	214.65	956,065.00	74.9%
1	Dec 06, 03 14:25:15	00:02:20	Hybrid	22343.32	2,206,947.00	98.91%

The table columns provide the following information on each attack:

Parameter	Description
#	Indicates the mitigated attack identification number (ID).
Start time	Indicates the mitigated attack date and time.
Duration	Indicates the mitigated attack duration in hours, minutes, and seconds.

Parameter	Description
Type	<p>Indicates the mitigated attack type:</p> <ul style="list-style-type: none"> • Client Attack—All non-spoofed traffic anomalies • Malformed Packets—All traffic anomalies identified as consisting of maliciously malformed packets • Spoofed—Traffic anomalies identified as a DDoS attack coming from a spoofed source • User Defined—All anomalies handled by the user filters. These could either function by default or be user configured • Zombie—Traffic anomalies identified as originated by zombies • Hybrid—An attack composed of several attacks with different characteristics • Traffic Anomaly—An anomaly that was detected for a short period of time and therefore did not require mitigation
Peak (pps)	Indicates the maximum attack rate measured in packets per second.
Received Pkts	Indicates the Total amount of packets, destined to the zone, that was handled by the Guard during the attack.
Legitimate vs. Malicious Traffic	A pie chart that displays the percentage of Malicious traffic (displayed in red), and Legitimate traffic (displayed in blue) within the total amount of traffic during the attack.

Each field in the table provides a link to the attack report.

Zone Attack Reports

The Guard provides an attack report for each zone to help in forming a clearer picture of an attacked zone. The attack report details an attack that begins at the production of the first dynamic filter and ends at protection termination (either by a user decision or by the action of the Protection-end Timeout parameter). The Guard records the relevant details during an attack and organizes the data under the report category columns. The produced report (or reports) is available for view. Attack reports are available not only on past attacks but also on the current attack (termed as “Attack in progress”).

To view the list of the zone attack reports:

From the Zone’s main menu, select **Diagnostics > Attack Reports**.

To view the attack details, perform one of the following:

- In the Protection Graph, click on the attack bar.
- In the Per Attack Summary table, click on one of the fields of the required attack.

A shortcut to the current attack (“Attack in progress”) details is also provided from the Zone’s “home page”.

To view the current attack details:

On the Zone's “home page”, click **Report**.

The attack report consists of data fields and tables. These are grouped in three sections:

- [General Details](#)
- [Attack Statistics](#)
- [Dropped/Bounced Packets](#)
- [Detected Anomalies](#)
- [Mitigated Attacks](#)
- [HTTP Detected Zombies](#)

General Details

The general details section (Figure 8-6) provides information related to attack timing. It consists of information on the attack start time, the attack end time and the attack duration.

Figure 8-6 Attack Report—General Details

Zone scannet (interactive) - Protected 

Home > Zone > Reports > Attack report

Attack Report #13

Attack start time:	Dec 18, 03 09:38:42
Attack end time:	Dec 18, 03 10:22:54
Attack duration:	0:44:12

Statistics units:

i Show details for all events 118375



Note

Counters that do not denote rate are specified by an integer. The units are bits, kilo-bits, kilo-packets, mega-bits, and packets in correspondence to the statistics units specified from the drop-down list.

To change the units by which the report is displayed:

1. Choose the units from the drop-down list.
2. Click **Set units**.

Attack Statistics

The attack statistics table (Figure 8-7) provides information on the following packet types:

- **Received**—Traffic, destined to the zone, received by the Guard.
- **Forwarded**—The clean and legitimate traffic forwarded to the zone.
- **Replied**—Traffic, sent to the client as part of the Guard's anti spoofing and anti-zombie mechanisms.

- **Dropped**—The total amount of packets, destined to the zone, dropped by the Guard.

Figure 8-7 Attack Report—Attack Statistics

	Total	Max. rate	Avg. rate	%
Received	6,529,540.00	6,123.64	5,903.74	
Forwarded	1,115,323.00	3,956.38	1,008.43	17.03%
Replied	4,335,480.00	4,045.24	3,919.96	71.96%
Dropped	1,078,736.00	1,060.64	975.35	11.02%

119379

The following information is provided on each packet type:

Parameter	Description
Total	Indicates the total amount of packets of the specified category
Max Rate	Indicates the maximum measured packet rate
Average Rate	Indicates the average packet rate
%	Indicates the percentage the packets make of the received packets

The traffic rate is displayed in the units selected from the drop-down list in the general details section.

Dropped/Bounced Packets

The Dropped/Bounced table (Figure 8-8) classifies packets that were identified as malicious traffic and therefore dropped or replied (bounced). The packets are categorized by the mechanism that identified them (the table rows). The table columns represent different quantification units.

Figure 8-8 Attack Report—Dropped/Bounced Packets

Dropped/Bounced packets				
	Total	Max. rate	Avg. rate	%
Rate limiter	1,327,646.00	1,305.37	1,200.40	13.28%
Flex filter	0.00	0.00	0.00	
User filter	0.00	0.00	0.00	
Dynamic filter	0.00	0.00	0.00	
Spoofed	8,670,960.00	8,090.47	7,839.93	86.72%
Malformed	0.00	0.00	0.00	

119377

The table rows represent the following filters:

- **Rate limiter**—Packets dropped by the rate limiter or by filters for which a rate limit was configured. The rate limiter limits the traffic rate to the zone (see the “Zone Management” section in Chapter 4, “Zone Creation and Configuration,” for further details).
- **Flex filter**—Packets dropped by the Flex filter. The Flex filter is used to count or drop a specified packet flow (see the “Flex Filter Configuration” section in Chapter 5, “Advanced Zone Procedures,” for further details).
- **User filter**—Packets dropped by the User filter. The User filter is used to direct a specified traffic flow to the desired Guard protection modules (see the “User Filter Configuration” section in Chapter 5, “Advanced Zone Procedures,” for further details).
- **Dynamic filter**—Packets dropped by the Dynamic filter. Dynamic filters are created by the Guard as the result of the analysis of traffic flow (see the “Dynamic Filters” section in Chapter 7, “Protecting Zones,” for further details).
- **Spoofed**—Packets that were identified by the Guard as Spoofed packets or packets originated by zombies and therefore not forwarded to the zone. Spoofed packets are Replied (bounced) packets to which no replies were received.

- **Malformed**—Packets, destined to the zone, dropped because they were analyzed as malformed.

The following information is available on each packet quantification:

Parameter	Description
Total	Indicates the total amount of dropped/bounced packets
Max Rate	Indicates the maximum measured packet rate
Average Rate	Indicates the average packet rate
%	Indicates the percentage the packets make of the total dropped/bounced packets

The traffic is measured in the units selected by the drop-down list in the general details section.

Detected Anomalies

The Detected Anomalies table (Figure 8-9) details the traffic anomalies the Guard detected in the zone's traffic. The Guard classifies a flow as an anomaly when it requires the production of a Dynamic filter. These anomalies may be occasional or of the kind that turns into systematic DDoS attacks. The Guard clusters anomalies with identical type and flow parameters (such as source IP address, destination port) under one anomaly type.

Figure 8-9 Attack Report—Detected Anomalies

Detected Anomalies							
#	Start time	Duration	Type	Triggering rate rate	% Breach	Anomaly Flow	Details
1	Nov 19 11:33	1:13:45	Non tcp/udp protocols	12,230.77	122,207.70%	dst=192.168.100.34 protocol=1 type=pkts	
2	Nov 19 11:33	1:13:45	Tcp incoming	30.00	2.93%	dst=192.168.100.34 protocol=6 type=syns	
3	Nov 19 11:34	1:13:25	tcp_connections	17,901.00	15,909.82%	dst=192.168.100.34 protocol=6 type=in_noWds_conns	
4	Nov 19 11:34	1:12:43	Tcp ratio	2,749.50	107,302.34%	dst=192.168.100.34 protocol=6 type=syn_by_fin	
5	Nov 19 11:35	1:12:26	Udp	3,896.00	3,596.00%	dst=192.168.100.34 protocol=17 type=pkts	
6	Nov 19 12:02	0:45:14	Tcp outgoing	46,153.85	153,746.17%	dst=192.168.100.34:80 protocol=6 type=syns	

The following information is provided for each anomaly:

Field Name	Description
#	Indicates the detected anomaly identification number (ID).
Start time	Indicates the anomaly detection date and time.
Duration	Indicates the anomaly duration in hours, minutes, and seconds.

Field Name	Description
Type	<p data-bbox="579 240 989 267">Indicates the detected anomaly type:</p> <ul style="list-style-type: none"> <li data-bbox="592 285 1184 375">• Tcp_connections—A detected flow with unusual number of TCP concurrent connections with or without data. <li data-bbox="592 393 1072 420">• HTTP—An unusual HTTP traffic flow. <li data-bbox="592 438 1184 496">• Tcp incoming—A detected flow attacking a TCP service when the zone is a server. <li data-bbox="592 514 1231 638">• Tcp outgoing—A 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. <li data-bbox="592 656 1231 779">• Unauthenticated tcp—A detected flow that the Guard anti-spoofing mechanisms haven't succeeded in authenticating. For example, ACK flood, FIN flood or any other flood of unauthenticated packets. <li data-bbox="592 797 1220 824">• DNS (Udp)—An attacking DNS-UDP protocol flow. <li data-bbox="592 842 1210 870">• DNS (Tcp)—An attacking DNS-TCP protocol flow. <li data-bbox="592 888 1072 915">• Udp—An attacking UDP protocol flow. <li data-bbox="592 933 1220 992">• Non tcp/udp protocols—A non TCP/UDP attacking protocol flow. <li data-bbox="592 1010 1231 1068">• Fragments—A detected flow with an unusual quantity of fragmented traffic. <li data-bbox="592 1086 1197 1175">• TCP ratio—A detected flow with an unusual ratio between different types of TCP packets (e.g. SYN packets versus FIN/RST packets). <li data-bbox="592 1193 1220 1282">• IP scan—A detected flow initiated from source IP address that tried to access many zone destination IP addresses. <li data-bbox="592 1300 1220 1359">• port scan—A detected flow initiated from source IP address that tried to access many zone ports. <li data-bbox="592 1377 1231 1404">• user detected—An anomaly flow detected by the user.

Field Name	Description
Triggering rate	Indicates the anomaly traffic rate that violated a policy threshold.
% Threshold	Indicates the percentage by which the triggering rate is above the policy threshold.
Anomaly Flow	Indicates the 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 types. If the anomaly flow is on a specified 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.

A value of “*” for any of the parameters indicates one of the following:

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

A value of “#” for any of the parameters indicates the number of values measured for that anomaly's parameter.

Detected Anomalies Details

The detected anomalies details table provides information on the dynamic filters, clustered according to the producing policy, that constitute the detected anomaly.

To display the detected anomalies details table:

From the details column in the detected anomalies table, click **i**.

The following information is provided:

Parameter	Description
Start time	Indicates the date and time the anomaly was detected.
End time	Indicates the expiration date and time of the Dynamic filter that was activated.
Rate (pps)	Indicates the rate measured in packets per second. <ul style="list-style-type: none"> • Thresh—Indicates the policy threshold that was violated by the detected anomaly. • Triggered—Indicates the anomaly traffic rate that violated a policy threshold.
Count	Indicates the number of packets that were handled by the Dynamic filter.
Detected flow	Provides information on the detected attack flow—the flow that caused the production of the Dynamic filter. <ul style="list-style-type: none"> • Prot.—Indicates the detected flow protocol number. • Src IP—Indicates the detected flow source IP. • Src Port—Indicates the detected flow source port. • Dst IP—Indicates the detected flow destination IP. • Dst Port—Indicates the detected flow destination port. • frag.—Indicates the fragmentation characteristics of the detected traffic flow. • Type—Indicates the detected anomaly type. Refer to the “Detected Anomalies” section in Chapter 11, “Attack Reports,” in the <i>Cisco Guard User Guide</i> for further details.

Parameter	Description
Action flow	<p data-bbox="579 240 1231 456">Provides information on the action flow - the flow that was addressed by the Dynamic filter. The action flow could be of a wider range than the detected flow. For example, the detected flow could indicate a specific source port for a specific source IP whereas the action flow will indicate all source ports for the specified source IP. The columns represent the dynamic filter traffic data.</p> <ul data-bbox="592 477 1231 756" style="list-style-type: none"><li data-bbox="592 477 1214 505">• Prot.—Indicates the detected flow protocol number.<li data-bbox="592 521 1147 548">• Src IP—Indicates the detected flow source IP.<li data-bbox="592 565 1197 592">• Src Port—Indicates the detected flow source port.<li data-bbox="592 609 1201 636">• Dst IP—Indicates the detected flow destination IP.<li data-bbox="592 652 1231 680">• Dst Port—Indicates the detected flow destination port.<li data-bbox="592 696 1221 756">• frag.—Indicates the fragmentation characteristics of the action flow.

Mitigated Attacks

The Mitigated Attacks table (Figure 8-10) details the actions the Guard took against the traffic anomalies (described in the Detected Anomalies table) that proved to be a hazard for the zone. These actions could take the form of anti-spoofing or anti-zombie mechanisms, user filters with a drop action, rate limit, etc. The Guard clusters mitigation actions with identical types and flow parameters and displays them under the same mitigation action.

Figure 8-10 Attack Report—Mitigated Attacks

Mitigated Attacks									
#	Start time	Duration	Attack type	Triggering rate rate	% Events	Anomaly Flow	Action flow	Dropped	Details
1	Dec 09 09:53	1:19:00	spoofedMac (src)	7,506.40		N/A, protocol=6	protocol=6	26,815,730.00	
2	Dec 09 09:53	1:19:00	spoofedMac (src)	7,506.25		N/A, protocol=17 type=unauth	protocol=17 type=unauth	26,498,571.00	
3	Dec 09 09:53	1:19:00	user definedRate limit	7,506.40		N/A, protocol=1		25,079,389.00	
4	Dec 09 11:12	0:00:00	zombieHTTP	40.83		N/A, protocol=6	protocol=6	2,493.00	
5	Dec 09 11:12	0:00:04	client attacktop_connections	11.80	10.00%	src=192.168.1.0/24 protocol=6 type=br_colina	src=192.168.1.0/24 protocol=6	N/A	

The following information is provided on each mitigated attack:

Field Name	Description
#	Indicates the mitigated attack identification number (ID).
Start time	Indicates the mitigated attack date and time.
Duration	Indicates the mitigated attack duration in hours, minutes, and seconds.

Field Name	Description
Attack Type	<p>Indicates the mitigated attack type:</p> <ul style="list-style-type: none"> • Spoofed—This type includes all traffic anomalies identified as a DDoS attack from a spoofed IP source. • Client Attack—This type includes all traffic anomalies determined as a DDoS attack from an unauthenticated IP source. • User Defined—This type includes DDoS attacks identified due to user filter definition. This includes all packets dropped due to user definitions such as anomalies handled by the user filters (see the “Zone Filter Configuration” section in Chapter 5, “Advanced Zone Procedures,” for further details). • Zombie—This type includes all traffic anomalies identified as a DDoS attack originated by zombies • Malformed Packets—This type includes all traffic anomalies determined as a DDoS attack consisting of maliciously malformed packets. <p>The protection modules basic or strong, are indicated in brackets.</p> <p>For a comprehensive overview of the sub-types of each attack type, refer to Chapter 11, “Attack Reports,” in the <i>Cisco Guard User Guide</i>.</p>
Triggering rate	Indicates the mitigated attack traffic rate. The triggering rate is applicable only for client attacks or user defined attacks. It is not applicable for spoofed or malformed attacks.
% Threshold	Indicates the mitigated attack rate percentage of the policy threshold.
Anomaly Flow	Indicates the traffic flow of the anomaly that was mitigated. 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 types.

Field Name	Description
Action flow	Indicates the traffic characteristics of the flow after the attack mitigation. The parameters of the common flow characteristics are displayed.
Dropped	Indicates the counter for traffic that was dropped during the attack mitigation.
Details	Indicates whether additional information can be viewed for this filter. Click i for additional information.

A value of “*” for any of the action flow or anomaly flow parameters indicates one of the following:

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

A value of “#” for any of the action flow or anomaly flow parameters indicates the number of values measured for that mitigated attack’s parameter.

Mitigated Attack Details

The mitigated attack details table provides information on the mechanisms that were used to mitigate the attack.

To display the mitigated attack details table:

From the details column in the mitigated attack table, click

The following information is provided:

Parameter	Description
Start time	Indicates the date and time the anomaly was detected.
End time	Indicates the expiration date and time of the Dynamic filter that was activated.
Rate (pps)	Indicates the rate measured in packets per second. <ul style="list-style-type: none"> • Thresh—Indicates the policy threshold that was violated by the detected anomaly. • Triggered—Indicates the anomaly traffic rate that violated a policy threshold.

Parameter	Description
Count	Indicates the number of packets that were handled by the Dynamic filter.
Detected flow	<p>Provides information on the detected attack flow - the detected flow that was mitigated.</p> <ul style="list-style-type: none"> • Prot.—Indicates the detected flow protocol number. • Src IP—Indicates the detected flow source IP. • Src Port—Indicates the detected flow source port. • Dst IP—Indicates the detected flow destination IP. • Dst Port—Indicates the detected flow destination port. • frag.—Indicates the fragmentation characteristics of the detected traffic flow. • Type—Indicates the detected anomaly type. Refer to the Detected Anomalies section in Chapter 11, “Attack Reports,” in the <i>Cisco Guard User Guide</i> for further details.
Action flow	<p>Provides information on the action flow - the flow that was addressed by the mitigation mechanism. The action flow could be of a wider range than the detected flow. For example, the detected flow could indicate a specific destination port for a specific destination IP whereas the action flow will indicate all destination ports for the specified destination IP. The columns represent the dynamic filter traffic data.</p> <ul style="list-style-type: none"> • Prot.—Indicates the detected flow protocol number. • Src IP—Indicates the detected flow source IP. • Src Port—Indicates the detected flow source port. • Dst IP—Indicates the detected flow destination IP. • Dst Port—Indicates the detected flow destination port. • frag.—Indicates the fragmentation characteristics of the action flow.

HTTP Detected Zombies

An indication of a detected HTTP zombie attack will appear in the General Details section (see [Figure 8-11](#)).

Figure 8-11 HTTP detected zombies

Attack Report - current attack

Attack start time: Jan 07, 04 14:37:01
 Attack end time: Attack in progress.
 Attack duration: Attack in progress

Statistics units:

i [Show HTTP detected zombies](#)
i [Show details for all events](#)

119387

To view the list of detected HTTP zombies:

Click **i**, or click **Show HTTP detected zombies**.

The http zombie list is displayed.

See the “[HTTP Zombies](#)” section in this chapter for further details.

HTTP Zombies

The HTTP Zombies list ([Figure 8-12](#)) enables you to analyze the zone’s traffic and view the list of zombies that initiated the attack. This provides the capability to take action against the zombies.

To view the list of HTTP Zombies:

From the Zone's main menu, select **Diagnostics > HTTP Zombies**.

Figure 8-12 HTTP Zombies list

IP	Start Time	Duration	"get" Requests
192.168.100.100	Dec 09, 2003 16:17:12	0:00:29	1
192.168.100.101	Dec 09, 2003 16:17:12	0:00:34	1
192.168.100.106	Dec 09, 2003 16:17:12	0:00:30	1
192.168.100.108	Dec 09, 2003 16:17:12	0:00:34	2

118413

The following information is provided on each Zombie:

Parameter	Description
IP	Indicates the zombie IP address
Start Time	Indicates the date and time the zombie connection was initially identified
Duration	Indicates the duration of the zombie attack
"get" Requests	Indicates the number of HTTP get requests sent by the zombie

Zone Event Log

The zone event log ([Figure 8-13](#)) displays monitoring and troubleshooting information that relate to the zone.

To view the zone event log:

From the Zone's main menu select **Diagnostics > Event log**.

Figure 8-13 Zone Event Log

The screenshot shows the 'Event Log' interface. At the top, there are checkboxes for 'Show all Events' and 'Show events with severity level'. Below these are radio buttons for severity levels: Emergency, Alert, Critical, Error, Warning, Notify, Info, and Debug. A 'Filter events' button is on the right. Below the filters, there are navigation arrows: 'First events', '<< Previous events', 'Next events >>', and 'Latest events'. The main table has the following data:

Time	Severity	Type	Details
Dec 31 17:18:16	Notify	protection-start	Zone activation completed successfully.
Dec 31 17:18:14	Notify	threshold-tuning-accept	Zone deactivation completed.
Dec 31 17:18:13	Info	information	Zone was active 5 minutes 57 seconds.
Dec 31 17:18:13	Info	information	Zone count before deactivation: received 46554 packets, forwarded 23277 packets, replied 0 packets, dropped 23277 packets.
Dec 31 17:18:16	Notify	threshold-tuning-start	Zone activation completed successfully.
Dec 31 17:18:08	Notify	policy-configuration-accept	Zone deactivation completed.

The event severity levels are:

Event Level	Description
Emergencies	System is unusable
Alerts	Immediate action required
Critical	Critical condition
Errors	Error condition
Warnings	Warning condition
Notifications	Normal but significant condition
Informational	Informational messages
Debugging	Debugging messages

To filter the events according to their severity level:

1. Select the check boxes next to the requested severity levels.
2. Click **Filter Events**.



A

- Access Control List (ACL)** ACL's act as a basic method of limiting access to the network. They constitute sequential lists of permit and deny conditions. The lists define the connections permitted to pass through a device, usually a router.
- Analysis Module** This module is active during the Guard Protection mode of operation. When no DDoS attack signs are indicated the Guard directs the diverted Zone traffic to flow through this module. The analysis module lets the Zone traffic flow unobstructed. The module analyzes the flows, allowing the recognition module to sample them.
- Anti-Spoofing** A security feature designed to prevent unauthorized access to a network through the technique known as IP spoofing. See *IP spoofing*.
- ARP Redirect Attack** An attack on a local subnet using the ARP protocol.

B

- Bandwidth Saturation Flood** A flood of simple HTTP requests for static content targeted towards Web servers; stresses routers, firewalls, IDS, and load balancers. A failure in any of these nodes constitutes network's susceptibility.
- basic/default** A User filter used when the user is not sure which action is to be chosen. The basic/default examines the flow and determines which action is to be taken. This User filter is used for UDP traffic.
- basic/dns-proxy** A User filter used for authentication of TCP DNS applications.
- basic/redirect** A User filter used for authentication of applications over http.

basic/reset	A User filter used for authentication of application over TCP, excluding http.
Basic Module	This module is active during the Guard Protection mode of operation. This module utilizes the Guard initial Challenge-and-Response based anti-spoofing mechanisms. The Guard directs the traffic to the Strong protection module either in the case of an escalation or in certain cases which require the Strong anti-spoofing mechanisms to handle the suspected traffic flows.
block-unauthenticated	A policy action that directs traffic to an anti-spoofing mechanism that deals with unauthenticated traffic.
block-unauthenticated-basic	A Dynamic filter action that drops unauthenticated traffic flow that has not been authenticated by the Basic anti-spoofing mechanisms.
block-unauthenticated-strong	A Dynamic filter action that drops unauthenticated traffic flow that has not been authenticated by the Strong anti-spoofing mechanisms.
block-unauthenticated-dns	A Dynamic filter action that drops unauthenticated traffic flows, flowing to DNS servers, that have not been authenticated by the DNS anti-spoofing mechanisms.
Burst/Burst-Size	The highest traffic peak (burst size rate) allowed to pass to the Zone. The burst-size units are: Kpps—Kilo packets per second; pps—Packets per second; Kbps—Kilo bits per second; Mbps—Mega Bits per second, and bps—Bits per second.
Bypass filter	A filter designed to enable the user to direct desired traffic flows to bypass the Guard protection mechanisms. Thus, the user can better adopt the Guard to its protection policy.

C

Client attack	Attacks from legitimate sources, which open half connections causing a server to exhaust.
Combination attack	Multi-platform DoS attack, which integrates BONK, JOLT, LAND, Nestea, Netear, SynDrop, and Winnuke—all into one attack. It is targeted at any/all network nodes (such as routers, firewalls, web servers, IDS systems).

Command Line Interface (CLI)	A prompt line interface from which the user performs its operations.
Comparator	A Guard module that compares between the input from the Guard Dynamic filters and the input from the Guard User filters. The Comparator then picks and executes the more severe protection means.
<hr/>	
D	
DDoS	See Distributed Denial of Service.
Denial of Service Attack (DoS)	Forms of computer network communication sabotage via exploitation of computer communication protocols. The purpose of the attack is overwhelming the target with spurious data in order to prevent legitimate connection attempts from succeeding. DoS attacks do not reveal sensitive data to the attacker in contrast to attacks whose purpose is to penetrate the target system. In these kinds of attacks, the skillful attacker tries to choke down networks and servers in vital network junctions. A successful attack may cause considerable revenue and resources loss. Examples of DoS attacks are SYN Flood, Tribal Flood Network (TFN), and ping of death.
Distributed Denial of Service (DDoS) Attack	A Denial of Service attack against a site or server launched from multiple sources. This is sometimes carried out by concealed exploiting servers to function as agents for transmitting the attacks. In many cases, the attacker will place client software on a number of unsuspecting remote computers and then use these computers to launch the attack. A Distributed Denial of Service attack is more effective than a simple Denial of Service attack, as the volume of traffic is considerably higher, and is more difficult to prevent. Examples of DDoS attacks are Syn flood, Smurf attack and Targa attack.
Divert-from Router	A router from which the Guard diverts the traffic destined to a Zone.
Diversion	To protect the target host (Zone) using the Cisco Guard, traffic destined to the host must be diverted to the Cisco Guard. This step includes traffic forwarding methods configuration per Zone's IP address. Zone diversion configuration is configured by the Guard routing configuration.

dns_tcp	A policy template that produces a group of policies related to DNS-TCP protocol traffic.
dns_udp	A policy template that produces a group of policies related to DNS-UDP protocol traffic.
DNS Attack	Flood of DNS requests causing a DNS server to saturate.
Drop Module	This module is active during the Guard Protection mode of operation. When all other protection mechanisms are insufficient or when user-configured filters direct the diverted Zone traffic to the Drop protection module. This module drops the malicious Zone traffic directed by the Flex, User, and Dynamic filters.
Dynamic filter	Dynamic filters are created by the Guard as the result of analysis of traffic flow. They are used to filter out DDoS attacks. This set of filters is continuously adapted to the Zone traffic and the type of the DDoS attack.

F

404 File Not Found Flood	Flood of valid HTTP requests for invalid content or files targeted directly at Web servers; used to validate both security policy and quantify effect on an end user.
filter/drop	An action (configured for a policy or a dynamic filter) that directs traffic to the Drop protection module to be dropped.
filter/strong	An action (configured for a policy or a dynamic filter) that directs traffic to the Strong protection module mechanisms.
Filters	The filters are the mechanism that directs the diverted traffic to the required protection modules. The Guard enables the user to set its preferred filter configurations and thus design a variety of possibilities for customized traffic direction and anti-DDoS attack mechanisms.
FIN Flood	Flood of connection resets from an invalid source to a targeted node; consumes network resources of an intended target. A FIN flood is also used to validate correct firewall/router policies.

Flex filter	The Flex filter is a Berkley Packet filter that facilitates the user with extremely flexible filtering capabilities such as filtering according to fields in the IP and TCP headers and filtering according to content bytes. It enables to use complex Boolean expressions. The Flex filter is used to count a specified packet flow.
Fraggle Attack	Sends UDP requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast request respond to the request and flood the target's network. It is similar to the Smurf attack, but rather than ICMP uses UDP to broadcast address for amplification.
fragments	A policy template that produces a group of policies related to fragmented traffic.
Fragmentation Attack	See IP Fragmentation Attack.

G

Guard	A system designed to protect network elements against DDoS attacks.
Guard event log	A log file containing the Guard activities, current events, performed actions and the protective measures it undertook.
Guard User community (privilege domain)	The Guard enables access domains to several groups of users (Show, Dynamic, Configuration, and Administrator). These are classified by their authority and hence their ability to perform a scope of operations. The highest and utmost privileged is the Administrator and the least privileged is the Show user level.
GUI	Graphical user interface.

H	
http	A policy template that produces a group of policies related to HTTP traffic flowing (by default) through port 80 (or other user-configured ports).
HTTP Connection Flood	Flood of HTTP half-requests targeted at the Web server connection resources. Also used to validate correct firewall policies (that is, limit connections per source). A Web server or OS network-level failure, also seen as connection failures on a client-side, constitutes network's susceptibility.
https	(Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol, developed by Netscape, built into browsers, that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is the use of Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.)
<hr/>	
ICMP Redirect Attack	ICMP redirects can cause data overload to the system being targeted.
ICMP Unreachable Attack	The attacker sends ICMP unreachable packets from a spoofed address to a host. This causes all legitimate TCP connections on the host to the spoofed address to be torn down. This causes the TCP session to retry and as more ICMP unreachables are sent, a DoS condition occurs.
Inject-to router	A router to which the Guard forwards the clean traffic destined to a Zone.
Interactive	A Zone detection mode in which the user will activate the dynamic filters in an interactive manner. The Dynamic filters that the policies recommend will appear as recommendations, and the user will specify the action to be taken for each filter.
ip_scan	A policy template that produces a group of policies relating to IP scanning (A situation in which a source IP tries to access many destination IPs on the Zone). See IP scanning.

IP Fragmentation Attack	Flood of valid but heavily fragmented HTTP requests targeted at a Web server; stresses IDS. Used to quantify resilience and scalability of IDS systems.
IP Scanning	The act of sending systematic queries to hosts in a network in attempt to find hosts (IP addresses) through which an attacker can pass traffic. IP scanning is often used to find vulnerable targets for attack on the Internet.
IP Traffic Diversion	A process consisting of transparently diverting the traffic of one or more Zones to the Guard, and returning the legitimate, cleaned traffic from the Guard to the original data path and on to the Zone. Traffic diversion is also performed for learning purposes.
IRDP Attack	ICMP Router Discovery Protocol can be spoofed and cause fake routing entries to be entered into a Windows machine. IRDP has no authentication. Upon startup, a system running MS Windows95/98 will always send 3 ICMP Router Solicitation packets to the 224.0.0.2 multicast address. If the machine is NOT configured as a DHCP client, it ignores any Router Advertisements sent back to the host. However, if the Windows machine is configured as a DHCP client, any Router Advertisements sent to the machine will be accepted and processed.

L

Land Attack	The sent packets have the same Source and destination IP addresses causing a response to loop.
Looping UDP Ports Attack	The attack uses two UDP services. Chargen (port 19) and echo (port 7), that can be spoofed into sending data to each other.

M

Maximum Transfer Unit (MTU) The largest frame size that can be transmitted over the network. Messages longer than the MTU must be divided into smaller frames.

N

Network Time Protocol (NTP) A protocol for synchronizing the Guard with a Time Synchronization Server.

notify A policy action that notifies the user of a policy threshold violation.

O

On-Demand Protection This protection is activated in a situation when the Zone is attacked while the Guard hasn't completed its Learning phases. As a result, the Guard hasn't adopted its protection policies to the Zone traffic requirements.

Open/close Attack The open/close attack opens and closes connections at a high rate to any port serviced by an external service through inetd. The number of connections allowed is hard-coded inside inetd.

other_protocols A policy template that produces a group of policies relating to non TCP or UDP protocols.

P	
Pending Dynamic filters	The pending dynamic are dynamic filters the user has not yet defined the action for (accept or ignore). Pending Dynamic filters are created only if the Zone is in interactive detection mode. A group of pending Dynamic filters constitute a recommendation. See Recommendations.
Ping Flood	Flood of ICMP echo requests; stresses routers, firewalls, load balancers, and Web servers. Poor end-user response time or failure to connect constitutes susceptibility.
Ping of death	ICMP packets greater than 65536. A ping of death attack can bring down a system.
Policy Construction Phase	In this phase the Guard, based on the Zone traffic characteristics, produces the protection policies with the aid of the Policy Templates. This phase consists of traffic flowing transparently through the Guard, enabling it to discover which services are used by the Zone.
Policy Operational Parameters	This is a set of parameters that relate to the policy operations. This set consists of the following: Threshold, Proxy-threshold, Timeout, and Action.
Policy Templates	The policy templates are a collection of policy constructing guiding rules and the output of each template after concluding the Policy Construction phase is a group of policies. The Policy Templates user-configured parameters are the Minimum Threshold and Maximum Services.
port_scan	A policy template that produces a group of policies relating to port scanning (A situation in which a source IP tries to access many ports on the Zone). See Port scanning.
Port Scanning	The act of sending systematic queries to hosts in an attempt to find open ports through which an attacker can pass traffic. Port scanning is often used to find vulnerable targets for attack on the Internet.

Protection Policy The Guard policies are the mechanisms that measure a particular traffic flow and take an action against the flow as a result of a threshold violation. A policy may, for example, direct the guard to produce a Dynamic filter that would direct a specific traffic to the Strong anti-spoofing mechanisms upon violating a certain threshold.

Protection-end Timer This parameter determines the timeout period after which if there are no filters in use and no new filter is added, the Guard will terminate the protection.

R

Rate-Limiter A Guard module that rate-limits Zone traffic. The Guard Rate-limiter does not consider the bypassed traffic bandwidth.

Recognition Module The Guard's module that receives input from a sampling unit and analyses the Zone traffic. Based on its recommendations, the Guard constructs its protection measures.

Recommendations Recommendations are a mechanism that enables the user to decide on the activation of the filters the policies launch. They are created when a Zone is configured in interactive mode. The recommendations are a summary of the pending dynamic filters aggregated according to the policies that produced them.

S

Sampler A Guard module that samples all traffic for the Guard Recognition module to configure protection measures.

Secured Shell (SSH) Management The user may access the Guard via Secured Shell (SSH) to enable controlling the Guard from any network.

Smurf Flood ICMP (Internet Control Message Protocol) ping requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast ping request respond to the request and flood the target's network.

Snapshots	A Guard mechanism used to verify the learning process outcome.
Spoofed attack	A DDoS attack technique that inserts a false sender IP address into an Internet transmission in order to gain unauthorized access to a computer system. To the computer system the request will seem as though it came from a trusted source, although the packet cannot be routed back to the initial source. IP spoofing presents potential for unnecessary network congestion and possible denial of service.
Strong Module	This module is active during the Guard Protection mode of operation. When a DDoS attack strengthens and the Guard analyses the current anti-spoofing mechanisms to be insufficient, it directs the diverted Zone traffic to the Strong protection module. This module has more severe anti-spoofing mechanisms. In case of further escalation, the Guard operates the Drop protection module.
strong	A User filter used when strong authentication for a traffic flow is required. Authentication is performed for every connection. The Guard serves as a proxy, therefore, this filter is not to be used if the network is moderated according to IP addresses (such as using access lists).
SYN Flood	Flood of connection requests from an invalid source to a targeted node; consumes network resources of an intended target. Used also to validate correct firewall/router policies.

T

Targa Attack	Floods of invalid ICMP-, UDP- and TCP- packets.
tcp_connections	A policy template that produces a group of policies related to TCP connection characteristics.
TCP_NO_PROXY policy templates	A template designed for a Zone for which no TCP proxy is to be used. This template may be used if the Zone is moderated according to IP addresses such as an Internet Relay Chat (IRC) server-type Zone.
tcp_not_auth	A policy template that produces a group of policies related to TCP connections that haven't been authenticated by the Guard's anti-spoofing mechanisms.

tcp_outgoing	This policy template produces sets of policies related to TCP connections initiated by the Zone.
tcp_ratio	This policy template produces sets of policies related to ratios between different types of TCP packets (e.g. SYN packets versus FIN/RST packets).
tcp_services	A policy template that produces a group of policies related to TCP services on ports other than HTTP-related (such as ports 80, 8080, etc.).
tcp_services_ns	A policy template that produces a group of policies related to TCP services. By default the policy relates to IRC ports (666X), ssh and telnet. When the threshold is violated, the traffic is blocked.
TCP flood	When TCP communicates, each TCP allocates some resources to each connection. By repeatedly establishing a TCP connection and then abandoning it, a malicious host can tie up significant resources on a server.
TCP Segmentation	Flood of heavily segmented TCP packets targeted at a Web server or application server. This attack stresses both IDS and the target machine's TCP stack.
Teardrop Attack	Sends overlapping IP fragments.
Threshold Tuning Phase	This is the stage in which the Guard further analyses the Zone traffic and defines threshold for the policies constructed in the Policy Construction phase. In this phase, the policies are tuned to fit the Zone services traffic rates.
to-user-filters	An action (configured for a policy or a dynamic filter) that directs traffic to the user filters.
Traffic Diversion	The Guard operates diversion techniques to direct the Zone traffic to pass through its protection mechanisms for traffic learning and malicious traffic filtering. The traffic would then be injected back to continue its path to the Zone.

U

- UDP Flood Attack** Flood of large numbers of raw UDP (User Datagram Protocol) packets targeted at routers, firewalls, load balancers, and IDS systems. The attack ties up network resources.
- udp_services** A template that produces a group of policies related to UDP services.
- UDP Reflectors Attack** All Web servers, DNS servers, and routers are reflectors, since they will return SYN acks or RSTs in response to SYN or other TCP packets; query replies in response to query requests; or ICMP Time Exceeded or Host Unreachable in response to particular IP packets. By spoofing IP addresses from slaves—a massive DDoS attack can be carried out.
- URL attacks** URL attacks attempt to overload an http server via various methods: http bombing; continuous requests for the same homepage or large web page; requesting the page with REFRESH so as to bypass any proxy server. Many of these attacks are not zombie attacks but rather human executed, by hundreds simultaneously.
- User filter** A user-customized filter that enables the user to set guiding rules to handle desired traffic flows when an attack is suspected. The user can configure its preferred anti-spoofing mechanisms or decide to drop a specified traffic flow.

V

- VPN attacks** Using specially crafted GRE or IPsec packets to attack the destination address of a VPN.

W

- WBM** See Web Based Management.
- Web Based Management** A GUI over HTTP Guard interface that enables the user to manage the Guard protection and Zones (excluding Guard configuration procedures) via the web using a browser.

Z

Zombie	A device that acts as an unaware participant in a distributed Denial of Service (DDoS) attack.
Zombie attack	A zombie attack is a type of attack that uses unaware participant machines to launch a DDoS attack. The attacker first spreads a Trojan to unsuspecting users, that are not the final target, and may later instruct this Trojan to perform “legitimate” connections to the Zone.
Zone	The Guard-protected network element. Also, a Guard file with all data relating to the protected Zone (configurations, policies, filters, etc).
Zone Bandwidth	The amount of traffic bandwidth the Guard allows to pass to the Zone. The Zone bandwidth is configured from the Burst size and Rate-limit.



A

active Dynamic filters [4-6](#)
Admin user privilege [3-8](#)
anomaly flow [8-18](#)
attack report [8-11](#)
 dropped/bounced packets [8-14](#)
attack statistics [8-12](#)
auth_pkts [6-9](#)
auth_tcp_pkts [6-9](#)
auth_udp_pkts [6-9](#)
authentication methods [3-9](#)
automatic [4-9](#)
automatic protection mode [7-2](#)

B

bandwidth limited link templates [4-8](#)
basic/default [5-6](#)
basic/dns-proxy [5-6](#)
basic/redirect [5-6](#)
basic/reset [5-6](#)
basic/safe-reset [5-6](#)
Berkley Packet filter [5-9](#)
block-unauthenticated [6-14](#)

block-unauthenticated-basic [7-6, 7-11](#)
block-unauthenticated-dns [7-6, 7-11](#)
block-unauthenticated-strong [7-6, 7-11](#)
Bypass filter [5-1](#)
 configuration [5-7](#)

C

change password [3-11](#)
CLI command
 permit wbm [2-2](#)
 service wbm [2-2](#)
client attack [8-10, 8-22](#)
compare policies [6-20](#)
Config user privilege [3-8](#)
counters
 dropped [3-5, 8-2, 8-13](#)
 forwarded [8-12](#)
 Guard [3-4](#)
 legitimate [3-4, 8-2](#)
 malicious [3-4, 8-2](#)
 received [3-5, 8-2, 8-12](#)
 replied [3-5, 8-12](#)
 spoofed [3-5, 8-2](#)
 Zone [8-1](#)

D

DDoS. See distributed denial of service

deactivate [4-3](#)

detected anomaly [8-15](#)

 details [8-19](#)

 type [8-10, 8-17](#)

diagnostics [3-4](#)

distributed denial of service [1-2](#)

DNS (tcp) [8-17](#)

DNS (udp) [8-17](#)

dns_tcp [5-9](#)

dns_udp [5-9](#)

documentation

 set [xvi](#)

 symbols and conventions [xvi](#)

drop [5-6, 6-18](#)

dropped/bounced packets [8-14](#)

dst_ip [6-10, 6-18](#)

dst_ip_ratio [6-10](#)

dst_port [6-10](#)

dst_port_ratio [6-10](#)

Dynamic filter [5-2, 7-4, 8-14](#)

 active [4-6](#)

 add [7-10](#)

 delete [7-9](#)

 details [7-7](#)

 pending [4-6, 7-17](#)

 prevent production of [7-10](#)

 termination [4-11](#)

Dynamic user privilege [3-8](#)

E

event log [3-6, 8-26](#)

 Guard [3-6](#)

F

filter/drop [6-14, 7-6, 7-11](#)

filter/strong [6-14, 7-6, 7-11](#)

filter-rate termination threshold [4-10, 4-11, 7-7](#)

Flex filter [4-9, 5-2, 8-14](#)

 configuration [5-8](#)

fragments [5-9, 8-17](#)

G

global [6-10](#)

Guard

 "home page" [3-2](#)

 counters [3-4](#)

 diagnostics [3-4](#)

 summary [3-2](#)

H

header area 1-4

http 5-9, 8-17

HTTP Zombies 8-25

hybrid 8-10

I

icons 4-13

in_conns 6-9

in_nodata_conns 6-9

in_pkts 6-9

in_unauth_pkts 6-9

interactive 4-9

interactive protection mode 7-2

interactive recommendations mode 7-12

 activate 7-13

ip_scan 5-10

IP scan 8-17

L

learning 6-2

 accept selectively 6-22

 phase 1 6-3

 phase 2 6-5

 policy construction 6-3

 terminating 6-4, 6-5

 threshold tuning 6-5

LINK_128K 4-8

LINK_1M 4-8

LINK_4M 4-8

LINK_512K 4-8

local authentication methods 3-9

M

main area 1-5

malformed 8-15

malformed packets 8-10, 8-22

malicious-rate termination threshold 4-10, 4-11,
7-7

mitigated attack 8-21

 action flow 8-23

 anomaly flow 8-22

 details 8-23

 type 8-22

N

navigation pane 1-5

new recommendations 7-14

notify 6-14, 6-18

O

On-Demand protection [7-3](#)
other_protocols [5-10, 6-12](#)
out_pkts [6-9](#)

P

pending Dynamic filters [4-6, 7-17](#)
 details [7-20](#)
 filters timeout [7-19](#)
per attack summary [8-9](#)
permit [5-6](#)
pkts [6-9](#)
policy [5-2, 6-6](#)
 action [6-14](#)
 activate [6-15](#)
 add service [6-11](#)
 compare [6-20](#)
 configuration [6-11](#)
 configure operational parameters [6-16](#)
 configure state [6-15](#)
 disable [6-15](#)
 inactivate [6-15](#)
 key [6-10](#)
 operational parameters [4-11, 6-13](#)
 operation mode [6-13](#)
 remove service [6-12](#)

 service [6-8](#)
 state [6-13](#)
 type [6-9](#)
policy construction [6-2, 6-3](#)
 terminating [6-4](#)
policy section [6-7](#)
policy template [5-2, 5-9](#)
 operational parameters [5-12](#)
 state [5-13](#)
port_scan [5-10](#)
port scan [8-17](#)
protect [4-3, 7-1](#)
 activate [7-3](#)
 deactivate [7-3](#)
Protection-end timer [4-10, 8-11](#)
protection graph [8-7](#)
protection mode
 automatic [7-2](#)
 interactive [7-2](#)
protection summary report [8-6](#)
protocol [6-10](#)

R

rate-limiter [5-7, 8-14](#)
recommendations
 accept [7-17](#)
 always accept [7-17](#)
 always ignore [7-17](#)

filters timeout [7-16, 7-19](#)
 view new [7-14](#)
 redirect/zombie [6-14, 7-6, 7-11](#)
 report [4-3](#)
 Zone protection summary report [8-6](#)
 reqs [6-9](#)

S

Show user privilege [3-8](#)
 snapshot [6-19](#)
 specific IP threshold configuration [6-18](#)
 spoofed [8-10, 8-14, 8-22](#)
 src_ip [6-10, 6-18](#)
 src_ip_many_dst_ips [6-10](#)
 src_ip_many_ports [6-10](#)
 src_net [6-10, 6-18](#)
 status icons [4-13](#)
 strong [5-6, 6-18](#)
 syn_by_fin [6-9](#)
 syns [6-9](#)
 System Requirements [1-1](#)

T

TACACS+ [3-9](#)
 tcp_connections [5-10, 8-17](#)
 tcp_connections_ns [5-11](#)
 TCP_NO_PROXY [4-8, GL-11](#)

tcp_not_auth [5-10](#)
 tcp_outgoing [5-10](#)
 tcp_outgoing_ns [5-11](#)
 tcp_ratio [5-10](#)
 tcp_services [5-10, 6-12](#)
 tcp_services_ns [5-11, 6-12](#)
 tcp incoming [8-17](#)
 tcp outgoing [8-17](#)
 TCP ratio [8-17](#)
 threshold
 filter rate termination [7-7](#)
 filter-rate termination [4-10, 4-11](#)
 malicious rate termination [4-11, 7-7](#)
 malicious-rate termination [4-10](#)
 specific IP threshold configuration [6-18](#)
 threshold tuning [6-2, 6-5](#)
 terminating [6-5](#)
 thumbnail [3-4](#)
 Total Attack Statistics [8-8](#)
 to-user [6-18](#)
 to-user-filters [6-14, 7-6, 7-11](#)
 traffic learning [6-2](#)
 troubleshooting WBM connection [2-4](#)
 Tune Threshold [6-5](#)

U

udp [8-17](#)
 udp_services [5-11, 6-12](#)

unauth_pkts [6-9](#)
unauthenticated tcp [8-17](#)
user defined [8-10, 8-22](#)
user detected [8-17](#)
User filter [5-1, 8-14](#)
 action [5-6](#)
 configuration [5-3](#)
users
 add [3-10](#)
 change password [3-11](#)
 creating [3-10](#)
 list [3-10](#)
 privilege level [3-8, 3-11](#)
 remove [3-10](#)

W

WBM

enable service [2-1](#)
login [2-3](#)
permit access [2-2](#)
setting up [2-1](#)
troubleshooting connection [2-4](#)

Z

zombie [8-10, 8-22](#)
 detected [8-25](#)
 list [8-25](#)
 packet counter [8-2](#)

Zone

"home page" [4-3](#)
attack reports [8-11](#)
configuration [4-7](#)
counters [8-1](#)
create new [4-7](#)
definition [4-1](#)
delete [4-12](#)
event log [8-26](#)
icons [4-13](#)
operation mode [4-9](#)
policies [6-6](#)
protection [7-1](#)
reconfigure [4-12](#)
templates [4-8](#)

Zone templates

bandwidth limited link templates [4-8](#)
DEFAULT [4-8](#)
LINK_128K [4-8](#)
LINK_1M [4-8](#)
LINK_4M [4-8](#)
LINK_512K [4-8](#)
TCP_NO_PROXY [4-8, GL-11](#)