

Vantage Report

User's Guide

Default Login Details

IP Address	http://{Vantage Report server's IP address}:8080/ vrpt
User Name	root
Password	root

Software Version 3.6
Edition 1, 5/2011

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Vantage Report using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Information

- Download software and documentation (User's Guide, Quick Start Guide, Datasheet, Support Notes) from one of the FTP sites:
Europe: ftp://ftp.zyxel.dk/Vantage_Report
Rest of World: ftp://ftp.zyxel.com/Vantage_Report
- Vantage Report Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

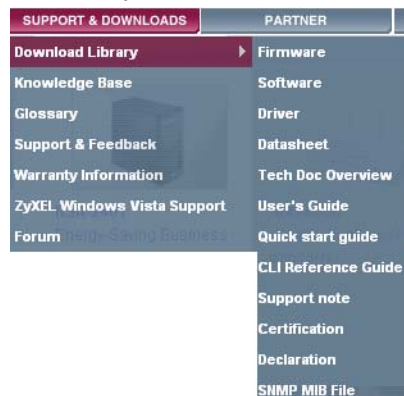
Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

Need More Help?

More help is available at www.zyxel.com.



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The version number on the title page is the version of Vantage Report that is documented in this User's Guide.
- Enter means for you to type one or more characters and press the carriage return. Select or Choose means for you to use one of the predefined choices.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a right angle bracket (>). For example, click **Report** > **Network Traffic** > **WEB** > **Top Hosts** means first click the **Report** main menu and then **Network Traffic**, **WEB** and finally click **Top Hosts**.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons.

Computer 	Server 	Prestige Device 
ZyWALL Device 	User 	Internet 
VPN Tunnel 		

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

Introduction 19

 Introducing Vantage Report 21

 The Vantage Report Server 23

 The Web Configurator 33

Monitors, Reports and Logs 63

 Monitor 65

 Network Traffic 95

 Secure Remote Access 183

 Network Security 269

 E-Mail Security 333

 Web Security 383

 Security Policy Enforcement 443

 Event 499

 Schedule Report 509

 Logs 527

System Setting, User Management and Troubleshooting 547

 System Setting 549

 User Management 577

 Troubleshooting 583

Appendices and Index 587

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Contents Overview	7
Table of Contents.....	9
 Part I: Introduction.....	 19
 Chapter 1	
Introducing Vantage Report.....	21
1.1 Introduction	21
1.2 License Versions	22
1.3 Hardware Requirements	22
 Chapter 2	
The Vantage Report Server	23
2.1 Starting and Stopping the Vantage Report Server	23
2.2 E-Mail in the Vantage Report Server	24
2.3 Time in the Vantage Report Server	25
2.4 Common Terms	25
2.5 Common Icons	27
2.6 ZyXEL Device Configuration and Source Data	27
 Chapter 3	
The Web Configurator	33
3.1 Web Configurator Requirements	33
3.2 Web Configurator Access	33
3.3 Main Menu Bar	37
3.3.1 The About Screen	37
3.4 Device Window	37
3.5 Menu Panel	41
3.6 Report and Setting Window	52
3.6.1 Device Information Screen	53
3.6.2 Monitors and Statistical Reports	54
3.6.3 View Logs	59
3.7 System Dashboard	59

Part II: Monitors, Reports and Logs 63**Chapter 4****Monitor 65**

4.1 Monitor (Folder)	65
4.1.1 Customize the Column Fields	66
4.2 Dashboard	67
4.3 Dashboard	69
4.4 CPU Usage Monitor	71
4.5 Memory Usage Monitor	72
4.6 Session Usage Monitor	73
4.7 Port Usage Monitor	74
4.8 Interface Usage Monitor	75
4.9 Web Monitor	77
4.10 FTP Monitor	78
4.11 E-Mail Monitor	79
4.12 Site to Site (IPSec) VPN Monitor	80
4.13 Client to Site (IPSec) VPN Monitor	81
4.14 Client to Site (SSL) VPN Monitor	82
4.15 Firewall Access Control Monitor	83
4.16 Attack Monitor	84
4.17 Intrusion Hits	85
4.18 Anti-Virus Monitor	86
4.19 E-Mail Virus Found Monitor	87
4.20 Spam Monitor	88
4.21 E-Mail Intrusion Hits Monitor	89
4.22 Web Security - Security Threat Monitor	90
4.23 Web Security Virus Found Monitor	91
4.24 Web Security Intrusion Hits Monitor	92
4.25 Content Filter Monitor	93
4.26 Application Patrol Monitor	94

Chapter 5**Network Traffic 95**

5.1 Bandwidth	95
5.1.1 Bandwidth Summary	95
5.1.2 Bandwidth Summary Drill-Down	99
5.1.3 Bandwidth Top Protocols	100
5.1.4 Bandwidth Top Protocols Drill-Down	104
5.1.5 Top Bandwidth Hosts	106
5.1.6 Top Bandwidth Hosts Drill-Down	110
5.1.7 Top Bandwidth Users	112
5.1.8 Top Bandwidth Users Drill-Down	115

5.1.9 Top Bandwidth Destinations	117
5.1.10 Top Bandwidth Destinations Drill-Down	121
5.2 Web Traffic	123
5.2.1 Top Web Sites	123
5.2.2 Top Web Sites Drill-Down	126
5.2.3 Top Web Hosts	128
5.2.4 Top Web Hosts Drill-Down	131
5.2.5 Top Web Users	133
5.2.6 Top Web Users Drill-Down	136
5.3 FTP Traffic	138
5.3.1 Top FTP Sites	138
5.3.2 Top FTP Sites Drill-Down	141
5.3.3 Top FTP Hosts	143
5.3.4 Top FTP Hosts Drill-Down	146
5.3.5 Top FTP Users	148
5.3.6 Top FTP Users Drill-Down	151
5.4 Mail Traffic	153
5.4.1 Top Mail Sites	153
5.4.2 Top Mail Sites Drill-Down	156
5.4.3 Top Mail Hosts	158
5.4.4 Top Mail Hosts Drill-Down	161
5.4.5 Top Mail Users	163
5.4.6 Top Mail Users Drill-Down	166
5.5 Other Traffic	168
5.5.1 Platform Selection	169
5.5.2 Service Settings	169
5.5.3 Top Destinations of Other Traffic	170
5.5.4 Top Destinations of Other Traffic Drill-Down	173
5.5.5 Top Sources of Other Traffic	174
5.5.6 Top Sources of Other Traffic Drill-Down	177
5.5.7 Top Other Traffic Users	178
5.5.8 Top Users of Other Traffic Drill-Down	181
Chapter 6	
Secure Remote Access	183
6.1 Secure Remote Access - Site-to-Site (IPSec)	183
6.1.1 Secure Remote Access Link Status	183
6.1.2 Secure Remote Access Traffic Monitor	185
6.1.3 Top VPN Peer Gateways	186
6.1.4 Top VPN Peer Gateways Drill-Down	189
6.1.5 Top Secure Remote Access Sites	191
6.1.6 Top Secure Remote Access Sites Drill-Down	194
6.1.7 Top Secure Remote Access Tunnels	196

6.1.8 Top Secure Remote Access Tunnels Drill-Down	199
6.1.9 Top Secure Remote Access Protocols	201
6.1.10 Top Secure Remote Access Protocols Drill-Down	204
6.1.11 Top Secure Remote Access Hosts	206
6.1.12 Top Secure Remote Access Hosts Drill-Down	210
6.1.13 Top Secure Remote Access Users	212
6.1.14 Top Secure Remote Access Users Drill-Down	215
6.1.15 Top Secure Remote Access Destinations	217
6.1.16 Top Secure Remote Access Destinations Drill-Down	220
6.2 Secure Remote Access - Client-to-Site (IPSec)	222
6.2.1 Secure Remote Access User Status	223
6.2.2 Secure Remote Access User Status Drill-Down	225
6.2.3 Top Secure Remote Access Protocols	227
6.2.4 Top Secure Remote Access Protocols Drill-Down	230
6.2.5 Top Secure Remote Access Destinations	232
6.2.6 Top Secure Remote Access Destinations Drill-Down	235
6.2.7 Secure Remote Access Top Users	237
6.2.8 Secure Remote Access Top Users Drill-Down	240
6.3 Secure Remote Access - Client-to-Site (SSL)	242
6.3.1 Secure Remote Access User Status	243
6.3.2 Secure Remote Access User Status Drill-Down	245
6.3.3 Top Secure Remote Access Protocols	246
6.3.4 Top Secure Remote Access Protocols Drill-Down	249
6.3.5 Top Secure Remote Access Destinations	251
6.3.6 Top Secure Remote Access Destinations Drill-Down	254
6.3.7 Top Secure Remote Access Applications	256
6.3.8 Top Secure Remote Access Applications Drill-Down	259
6.3.9 Secure Remote Access Top Users	261
6.3.10 Secure Remote Access Top Users Drill-Down	263
6.4 Xauth	265
6.4.1 Secure Remote Access Successful Login	265
6.4.2 Secure Remote Access Failed Login	267
Chapter 7	
Network Security.....	269
7.1 Firewall Access Control	269
7.1.1 Top Users Blocked	269
7.1.2 Top Packets Blocked	272
7.2 Attack	275
7.2.1 Attack Summary	275
7.2.2 Attack Summary Drill-Down	278
7.2.3 Top Attacks	279
7.2.4 Top Attacks Drill-Down	282

7.2.5 Top Attack Sources	283
7.2.6 Top Attack Sources Drill-Down	286
7.2.7 Attack Types	288
7.2.8 Attack Types Drill-Down	290
7.3 Intrusion Hits	291
7.3.1 Intrusion Hits Summary	291
7.3.2 Intrusion Hits Summary Drill-Down	294
7.3.3 Top Intrusion Hits Signatures	296
7.3.4 Top Intrusion Hits Signatures Drill-Down	299
7.3.5 Top Intrusion Hits Sources	301
7.3.6 Top Intrusion Hits Sources Drill-Down	304
7.3.7 Top Intrusion Hits Destinations	306
7.3.8 Top Intrusion Hits Destinations Drill-Down	309
7.3.9 Intrusion Hits Severities	311
7.3.10 Intrusion Hits Severities Drill-Down	314
7.4 Antivirus	315
7.4.1 Antivirus Summary	315
7.4.2 Virus Summary Drill-Down	318
7.4.3 Top Viruses	319
7.4.4 Top Viruses Drill-Down	322
7.4.5 Top Virus Sources	323
7.4.6 Top Virus Sources Drill-Down	326
7.4.7 Top Virus Destinations	328
7.4.8 Top Virus Destinations Drill-Down	330
Chapter 8	
E-Mail Security	333
8.1 Virus Found	333
8.1.1 Virus Found Summary	333
8.1.2 Virus Found Summary Drill-Down	336
8.1.3 Top Viruses	337
8.1.4 Top Viruses Drill-Down	340
8.1.5 Top Virus Sources	341
8.1.6 Top Virus Sources Drill-Down	344
8.1.7 Top Virus Destinations	346
8.1.8 Top Virus Destinations Drill-Down	348
8.2 Spam	349
8.2.1 Spam Summary	349
8.2.2 Spam Summary Drill-Down	352
8.2.3 Top Spam Senders	353
8.2.4 Top Spam Sources	356
8.2.5 Spam Scores	359
8.3 Intrusion Hits	361

8.3.1 Intrusion Hits Summary	361
8.3.2 Intrusion Hits Summary Drill-Down	363
8.3.3 Top Intrusion Hits Signatures	365
8.3.4 Top Intrusion Hits Signatures Drill-Down	367
8.3.5 Top Intrusion Hits Sources	368
8.3.6 Top Intrusion Hits Sources Drill-Down	371
8.3.7 Top Intrusion Hits Destinations	373
8.3.8 Top Intrusion Hits Destinations Drill-Down	376
8.3.9 Intrusion Hits Severities	378
8.3.10 Intrusion Hits Severities Drill-Down	380
 Chapter 9	
Web Security	383
9.1 Security Threat	383
9.1.1 Security Threat Summary	383
9.1.2 Security Threat Summary Drill-Down	385
9.1.3 Security Threat Top Web Sites	387
9.1.4 Security Threat Top Sites Drill-Down	390
9.1.5 Security Threat Top Users	391
9.1.6 Security Threat Top Users Drill-Down	394
9.1.7 Security Threat Top Hosts	395
9.1.8 Security Threat Top Hosts Drill-Down	398
9.1.9 Security Threat Categories	399
9.1.10 Security Threat Categories Drill-Down	401
9.2 Virus Found	403
9.2.1 Virus Found Summary	403
9.2.2 Virus Found Summary Drill-Down	406
9.2.3 Top Viruses	407
9.2.4 Top Viruses Drill-Down	409
9.2.5 Top Virus Sources	410
9.2.6 Top Virus Sources Drill-Down	413
9.2.7 Top Virus Destinations	414
9.2.8 Top Virus Destinations Drill-Down	417
9.3 Intrusion Hits	418
9.3.1 Intrusion Hits Summary	418
9.3.2 Intrusion Hits Summary Drill-Down	421
9.3.3 Top Intrusion Hits Signatures	423
9.3.4 Top Intrusion Hits Signatures Drill-Down	426
9.3.5 Top Intrusion Hits Sources	428
9.3.6 Top Intrusion Hits Sources Drill-Down	431
9.3.7 Top Intrusion Hits Destinations	433
9.3.8 Top Intrusion Hits Destinations Drill-Down	436
9.3.9 Intrusion Hits Severities	438

9.3.10 Intrusion Hits Severities Drill-Down	440
Chapter 10	
Security Policy Enforcement	443
10.1 EPS	443
10.1.1 What Endpoint Security Can Check	443
10.1.2 EPS Summary	444
10.1.3 View Logs	445
10.2 Content Filter (All)	446
10.2.1 Summary	446
10.2.2 Summary Drill-Down	448
10.2.3 Top Sites	450
10.2.4 Top Sites Drill-Down	453
10.2.5 Top Users	455
10.2.6 Top Users Drill-Down	458
10.2.7 Top Hosts	459
10.2.8 Top Hosts Drill-Down	462
10.2.9 By Category	463
10.2.10 By Category Drill-Down	466
10.3 Content Filter (Blocked)	467
10.3.1 Summary	467
10.3.2 Summary Drill-Down	469
10.3.3 Top Blocked Sites	471
10.3.4 Top Blocked Sites Drill-Down	474
10.3.5 Top Blocked Users	476
10.3.6 Top Blocked Users Drill-Down	479
10.3.7 Top Blocked Hosts	480
10.3.8 Top Blocked Hosts Drill-Down	483
10.3.9 Blocked Web Categories	484
10.3.10 Blocked Web Categories Drill-Down	487
10.4 Application Access Control	488
10.4.1 Top Applications Blocked	488
10.4.2 Top Users Blocked	491
10.4.3 Top Applications Allowed	494
Chapter 11	
Event	499
11.1 Successful Logins	499
11.2 Failed Logins	501
11.3 Top Sessions Per Host	502
11.4 Top Sessions Per User	505
Chapter 12	
Schedule Report	509

12.1 Scheduled Report Summary Screen	509
12.2 Customize Daily Report Screen	510
12.3 Customize Weekly Report Screen	518
12.4 Customize Overtime Report Screen	520
12.5 Configure Template List	522
12.6 Template Add/Edit	523
12.7 Logo Template	523
12.8 Logo Template Add/Edit	524
Chapter 13	
Logs	527
13.1 Log Viewer	527
13.2 Log Receiver	531
13.2.1 By Day (Summary)	531
13.3 By Device	533
13.3.1 Log Receiver > By Device > By Category Screen	535
13.4 VRPT System Logs	536
13.5 Log Archiving	538
13.5.1 File Archiving Settings	538
13.5.2 View Archived Files	541
13.5.3 Log Transfer	543
13.6 Log Remove	544
 Part III: System Setting, User Management and Troubleshooting ..	547
 Chapter 14	
System Setting	549
14.1 General Configuration Screen	549
14.1.1 Configuring for Hostname Reverse	551
14.2 Server Configuration Screen	554
14.3 Data Maintenance Screens	555
14.3.1 Data Backup and Data Restore Screen	555
14.3.2 Device List Screen	556
14.4 Upgrade Screen	557
14.5 Registration Screens	558
14.5.1 Registration Summary Screen	559
14.5.2 Registration > Upgrade Screen	560
14.6 Notification	561
14.6.1 Add/Edit a Notification	563
14.7 Rule-Based Alert	565
14.7.1 Add/Edit a Rule-based Alert	566

Chapter 15	
User Management	577
15.1 Group Screen	577
15.1.1 Group > Add/Edit Group Screen	578
15.2 Account Screen	579
15.2.1 Account > Add/Edit User Account Screen	580
Chapter 16	
Troubleshooting	583
Part IV: Appendices and Index	587
Appendix A Product Specifications	589
Appendix B ZyWALL USG Series and ZyWALL 1050 Log Descriptions	599
Appendix C ZyNOS Log Descriptions	645
Appendix D Open Software Announcements	671
Appendix E Legal Information	709
Index	711

PART I

Introduction

Introducing Vantage Report (21)

The Vantage Report Server (23)

The Web Configurator (33)

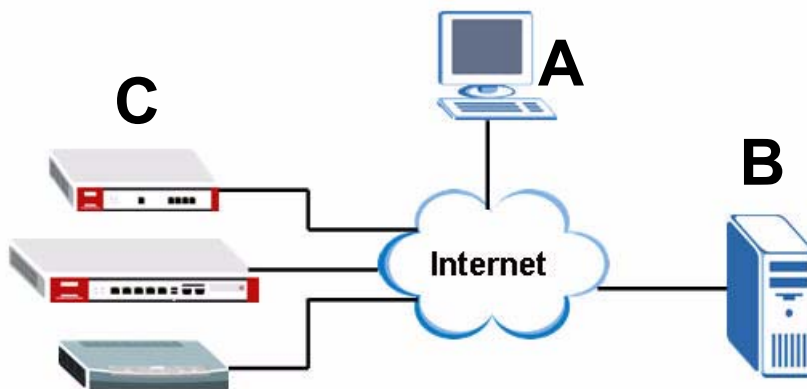
Introducing Vantage Report

Please see the Quick Start Guide for Vantage Report setup requirements, installation, and access. This chapter introduces Vantage Report. See [Appendix A on page 589](#) for a list of key features.

1.1 Introduction

Vantage Report is a cost-effective, browser-based global management solution that allows an administrator from any location to easily manage, monitor and gather statistics on ZyXEL devices located worldwide. With Vantage Report, you can monitor network access, enhance security, and anticipate future bandwidth needs. A typical application is illustrated in [Figure 1](#).

Figure 1 Typical Vantage Report Application



In this example, you use the **web configurator (A)** to set up the **Vantage Report server (B)**. You also configure the **ZyXEL devices (C)** to send their logs and traffic statistics to the Vantage Report Server. The Vantage Report server collects this information. Then, you can

- monitor the whole network
- look at historical reports about network performance and events
- examine device logs

The Vantage Report server can also send statistical reports to you by e-mail.

1.2 License Versions

This is independent from the version number, 3.6 for example. There are two versions of Vantage Report, the basic version and the full version. When you install Vantage Report, you get the basic version.

Note: This User's Guide discusses the features in the full version.

Register Vantage Report to use the full version to manage one device. Purchase E-Vantage Report license keys to add more devices. See [Section 14.5 on page 558](#) for more information.

1.3 Hardware Requirements

Minimum hardware requirements:

- Intel Pentium 4 processor 1 GHz
- 512 Mb RAM
- 8 GB free hard disk space

The following table shows the recommended hardware specifications. The more powerful your computer, the more devices you can manage.

Table 1 Hardware Specification Recommendations

NUMBER OF DEVICES	LOG HANDLING CAPABILITY (LOGS/ SEC)	CPU SPEC (GHZ)	MEMORY SPEC	LOG SPACE REQUIRED (GB/ DAY)
0 - 5	0 - 75	Intel P4 2.6 GHz	512 MB	0 - 1
5 - 50	75 - 750	Intel P4 2.6 GHz	1 GB	1 - 12
50 - 100	750 - 1500	Intel P4 3.2 GHz	1 GB	12 - 24

The Vantage Report Server

This chapter explains several characteristics of the Vantage Report server.

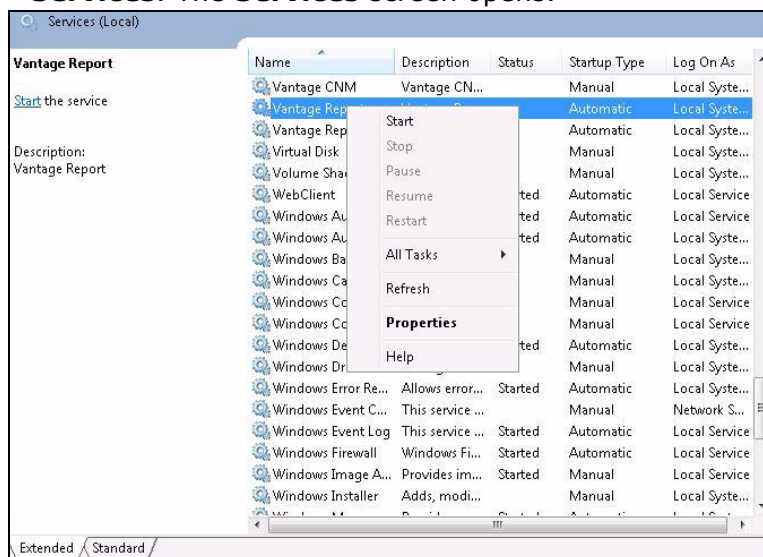
2.1 Starting and Stopping the Vantage Report Server

Note: Make sure the port Vantage Report uses for web services is not used by other applications, especially web servers.

The Vantage Report server runs as a service on the Vantage Report server. By default, this service starts automatically when you log in to the Vantage Report server. You can use the services management screen to start, stop, or configure this service. To open this screen:

- 1 In Windows 2000, click **Start > Settings > Control Panel > Administrative Tools > Services**. The **Services** screen opens.
- 2 In Windows XP, click **Start > Control Panel > Performance and Maintenance > Administrative Tools > Services**. The **Services** screen opens.

- 3 In Windows Vista or Windows 7, click **Start > Control Panel > Administrative Tools > Services**. The **Services** screen opens.



- 4 Right-click on **Vantage Report**. A menu appears.
- 5 Select **Start** or **Stop** to start or stop the Vantage Report service. Select **Properties** to configure the service.

2.2 E-Mail in the Vantage Report Server

Note: Before the Vantage Report server can send e-mail to anyone, you have to configure the SMTP mail server. See [Section 14.2 on page 554](#) for more information.

The Vantage Report server can use e-mail to send information in several situations. In some situations, it sends e-mail to the e-mail address that is associated with a specific user (see [Section 14.3 on page 555](#)). In other situations, it sends e-mail to any valid e-mail address.

- **scheduled report** - The Vantage Report server can send one or more statistical reports regularly or one-time to any valid e-mail address. See [Chapter 12 on page 509](#) for more information.
- **system notifications** - When certain system parameters cross a threshold (minimum or maximum) value, the Vantage Report server sends e-mail to the Vantage Report administrator (the e-mail address associated with the `root` account). Some of these messages are warnings; in some situations, however, the Vantage Report server starts or stops receive logs. See [Appendix A on page 589](#) for a list of parameters and threshold values. One of the threshold values can be configured. See [Section 14.1 on page 549](#).

- **forgotten password** - A user clicks **Forget Password?** in the **Login** screen. In this case, the Vantage Report server sends the account information to the e-mail address associated with the specified user name. See [Section 3.2 on page 33](#) for an example of the **Login** screen.
- **test message** - The Vantage Report administrator tests the SMTP mail server settings. The Vantage Report server sends an e-mail message to the e-mail address associated with the `root` account. See [Section 14.2 on page 554](#) for more information.

2.3 Time in the Vantage Report Server

- In Vantage Report, clock time is the time the Vantage Report server receives information (log entries or traffic statistics) from the ZyXEL devices, not the time the device puts in the entry. As soon as the Vantage Report server receives information, it replaces device times with the current time in the Vantage Report server.
- The Vantage Report server processes log entries and traffic statistics before the information is available in any screen (including log viewers). For performance reasons, the Vantage Report server does not process this information right away. Instead, the processing time depends on the way the information is used in Vantage Report. See the following table for processing times for each menu item.

Table 2 Processing Times by Menu Item

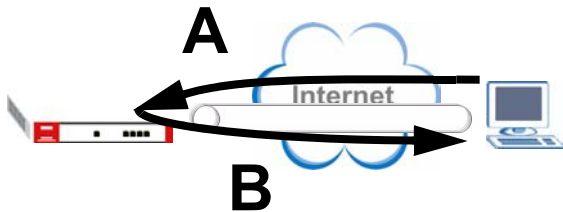
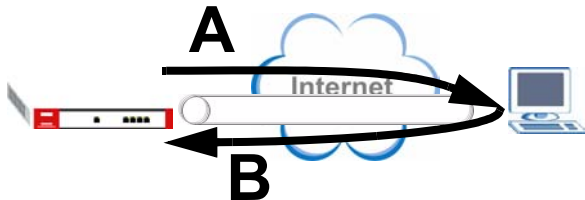
MENU ITEM	TIME (MIN)
Monitor	5
Report (Network Traffic, Secure Remote Access, Network Security, E-Mail Security, Web Security, Security Policy Enforcement, Authentication)	5
Logs (Log Viewer)	5

2.4 Common Terms

The following table describes the terms that appear frequently in this document.

Table 3 Common Terms

TERM	DESCRIPTION
ZLD-based ZyXEL Devices	ZLD (ZyXEL Linux Distribution) is ZyXEL's platform based on Linux. ZLD models include ZyWALL USG series and ZyWALL 1050.
ZyNOS-based ZyXEL Devices	ZyNOS is ZyXEL's Networking Operating System. ZyNOS models include ZyWALL 5, ZyWALL 35, and ZyWALL 70, etc.

TERM	DESCRIPTION
Drill-down Report	Click a link in a report to display details in another screen. For example, click Secure Remote Access > Client-to-Site (IPSec) > User Status , then click a user's link to display a report of the services for which the user sent the most traffic.
Host	A host represents a computer with an IP address.
Remote User	A user login the device with a legal user's account. Figure 2 Remote User 
Remote VPN User	A VPN user is a user who is allowed to send traffic through VPN tunnel. Figure 3 Remote VPN User 
Incoming VPN Traffic	A diagram is referred to in following figure. In this example, incoming VPN traffic is encrypted data that the ZyXEL Device receives from VPN tunnels (A) and the traffic sent back (B). Figure 4 Incoming VPN Traffic 
Outgoing VPN Traffic	A diagram is referred to in following figure. In this example, outgoing VPN traffic is encrypted data that the ZyXEL Device forwards through VPN tunnels (A) and the returned traffic (B). Figure 5 Outgoing VPN Traffic 

2.5 Common Icons

The following table describes common icons.

Table 4 Common Icons

ICON	DESCRIPTION
	The View Detail icon (in the Dashboard) lets you focus on an individual monitor report.
 	The Settings icons open a screen where you can modify the report display settings.
	The Print icon opens a screen for printing the screen.
	The Pie View icon displays the statistical report in a pie chart.
	The Bar View icon displays the statistical report in a bar chart.
	The Refresh icon updates the information in the screen.

2.6 ZyXEL Device Configuration and Source Data

The following table identifies the configuration required in ZyXEL devices for each screen in Vantage Report.

Table 5 ZLD-based (USG Series and ZyWALL 1050) Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	USG SERIES AND ZYWALL 1050		
	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Monitor > Hardware Status > CPU Usage	log entries	System Monitoring	--
Monitor > Hardware Status > Memory Usage	log entries	System Monitoring	--
Monitor > Network Traffic > Session Usage	log entries	System Monitoring	--
Monitor > Network Traffic > Bandwidth > Port Usage	log entries	INTERFACE STATISTICS	--
Monitor > Network Traffic > Bandwidth > Interface Usage	log entries	INTERFACE STATISTICS	--
Monitor > Network Traffic > Web	log entries	Traffic Log	--
Monitor > Network Traffic > FTP	log entries	Traffic Log	--
Monitor > Network Traffic > Mail	log entries	Traffic Log	--
Monitor > Secure Remote Access > Site-to-Site (IPSec)	log entries	Traffic Log	--

Table 5 ZLD-based (USG Series and ZyWALL 1050) Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	USG SERIES AND ZYWALL 1050		
	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Monitor > Secure Remote Access > Client-to-Site (SSL)	log entries	Traffic Log	--
Monitor > Network Security > Firewall Access Control	log entries	Firewall	--
Monitor > Network Security > Attack	log entries	Attack (ADP)	--
Monitor > Network Security > Intrusion Hits	log entries	IDP	--
Monitor > Network Security > AntiVirus	log entries	Anti-Virus	--
Monitor > E-mail Security > Virus Found	log entries	Anti-Virus	--
Monitor > E-mail Security > Spam	log entries	Anti-Spam	--
Monitor > E-mail Security > Intrusion Hits	log entries	IDP	--
Monitor > Web Security > Security Threat	log entries	Blocked web sites	--
Monitor > Web Security > Virus Found	log entries	Anti-Virus	--
Monitor > Web Security > Intrusion Hits	log entries	IDP	--
Monitor > Security Policy Enforcement > Content Filter		Blocked web sites, Forward web sites, Warning web sites	--
Monitor > Security Policy Enforcement > App Patrol		Application Patrol	--
Report > Network Traffic > Bandwidth	log entries	Traffic Log	--
Report > Network Traffic > FTP	log entries	Traffic Log	--
Report > Network Traffic > Mail	log entries	Traffic Log	--
Report > Network Traffic > Customization	log entries	Traffic Log	--
Report > Secure Remote Access > Site-to-Site(IPSec)	log entries	IPSec, User	--
Report > Secure Remote Access > Client-to-Site(IPSec)	log entries	IPSec, User	--
Report > Secure Remote Access > Client-to-Site(SSL)	log entries	SSL VPN, User	--
Report > Secure Remote Access > Xauth	log entries	IPSec, User	--
Report > Network Security > Firewall Access Control	log entries	Firewall	--
Report > Network Security > Attack	log entries	Attack (ADP)	--

Table 5 ZLD-based (USG Series and ZyWALL 1050) Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	USG SERIES AND ZYWALL 1050		
	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Report > Network Security > Intrusion Hits	log entries	IDP	--
Report > Network Security > AntiVirus	log entries	Anti-Virus	--
Report > E-mail Security > Virus Found	log entries	Anti-Virus	--
Report > E-mail Security > Spam	log entries	Anti-Spam	--
Report > E-mail Security > Intrusion Hits	log entries	IDP	--
Report > Web Security > Security Threat	log entries	Blocked web sites	--
Report > Web Security > Virus Found	log entries	Anti-Virus	--
Report > Web Security > Intrusion Hits	log entries	IDP	--
Report > Security Policy Enforcement > EPS	log entries	EPS	--
Report > Security Policy Enforcement > Content Filter(All)	log entries	Blocked web sites, Forward web sites, Warning web sites	--
Report > Security Policy Enforcement > Content Filter(Block)	log entries	Blocked web sites	--
Report > Security Policy Enforcement > Application Access Control	log entries	Application Patrol	--
Logs > Log Viewer	log entries	**	**

* - The names of categories may be different for different devices. Use the category that is appropriate for each device.

** - The log viewers display whatever log entries the ZyXEL devices record, including log entries that may not be used in other reports.

Table 6 ZyNOS-based ZyWALL Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	ZYNOS-BASED ZYWALL		
	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Monitor > Bandwidth	traffic statistics	--	--
Monitor > Service	traffic statistics	--	--
Monitor > Attack	log entries	Attack	--
Monitor > Intrusion	log entries	IDP	IDP > Signature
Monitor > AntiVirus	log entries	Anti-Virus	Anti-Virus > General
Monitor > AntiSpam	log entries	Anti-Spam	--

Table 6 ZyNOS-based ZyWALL Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	ZYNOS-BASED ZYWALL		
	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Report > Traffic	traffic statistics	--	--
Report > VPN	log entries	IPSec	--
Report > Network Attack > Attack	log entries	Attack	--
Report > Network Attack > Intrusion	log entries	IDP	IDP > Signature
Report > Network Attack > AntiVirus	log entries	Anti-Virus	Anti-Virus > General
Report > Network Attack > AntiSpam	log entries	Anti-Spam	--
Report > Security Policy > Firewall Access Control	log entries	Access Control	--
Report > Security Policy > Application Access Control	N/A	N/A	N/A
Report > Security Policy > WEB Blocked	log entries	Blocked Web Sites	--
Report > Security Policy > WEB Allowed	log entries	Forward Web Sites	--
Report > Event > Login	log entries	System Maintenance	--
Report > Event > Session Per Host	log entries	Access Control	--
Report > EPS	N/A	N/A	N/A
Logs > Log Viewer	log entries	**	**

* - The names of categories may be different for different devices. Use the category that is appropriate for each device.

** - The log viewers display whatever log entries the ZyXEL devices record, including log entries that may not be used in other reports.

- **Source Data** - Some screens use log entries; some screens use traffic statistics. Some ZyXEL devices do not track traffic statistics. If Vantage Report does not get one of these, the screens are empty. See the Quick Start Guide for detailed instructions.
- **Log Settings** - If ZyXEL devices do not record some categories of log entries, Vantage Report does not have any information to display either. For example, if you want to look at VPN traffic for a particular device, the device has to record log entries for **IPSec**.

For most devices, go to the **Logs > Log Settings** screen, and select the appropriate categories. You may also use the command-line interface.

- **Additional** - In some cases, it is possible to control what log entries are recorded in even more detail. For example, in some ZyXEL devices, it is possible to control what attack types are logged.

For most devices, go to the screen indicated to select the appropriate log entries. You may also use the command-line interface.

The Web Configurator

This chapter provides the minimum requirements to use the web configurator, describes how to access the web configurator, and explains each part of the main screen in the web configurator.

3.1 Web Configurator Requirements

The web configurator is a browser-based interface that you can use to set up, manage, and use Vantage Report. You can run it on the Vantage Report server or on a different computer. Your web browser should meet the following requirements:

- Internet Explorer 6.0 or later, Firefox 1.07 or later (local or remote)
- JavaScript enabled
- Macromedia Flash Player 9 or later
- Recommended screen resolution: 1024 x 768 pixels

3.2 Web Configurator Access

To access the web configurator, follow these steps:

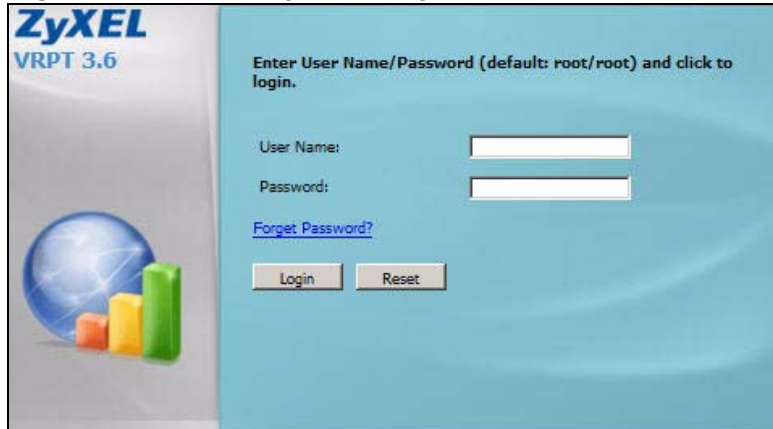
- 1 Make sure Vantage Report is installed and running properly. (See the Quick Start Guide.)
- 2 Open a browser window, and go to <http://a.b.c.d:xxxxx/vrpt>, where
 - [a.b.c.d](#) is the IP address of the Vantage Report server. If you open the web configurator on the same computer on which you installed Vantage Report, enter `localhost`.

- [xxxxxx](#) is the port number you entered during installation (default is 8080).

For example, you might enter <http://localhost:8080/vrpt> or <http://212.100.9.161:9090/vrpt>.

In either case, the web configurator **Login** screen displays.

Figure 6 Web Configurator Login Screen

The image shows the login screen for the ZyXEL VRPT 3.6 web configurator. On the left side, there is a logo for ZyXEL VRPT 3.6 and a graphic of a blue globe with three colored bars (orange, yellow, green) in front of it. The main area of the screen is light blue and contains the following text: "Enter User Name/Password (default: root/root) and click to login." Below this text are two input fields: "User Name:" and "Password:". Below the password field is a link that says "Forgot Password?". At the bottom of the form are two buttons: "Login" and "Reset".

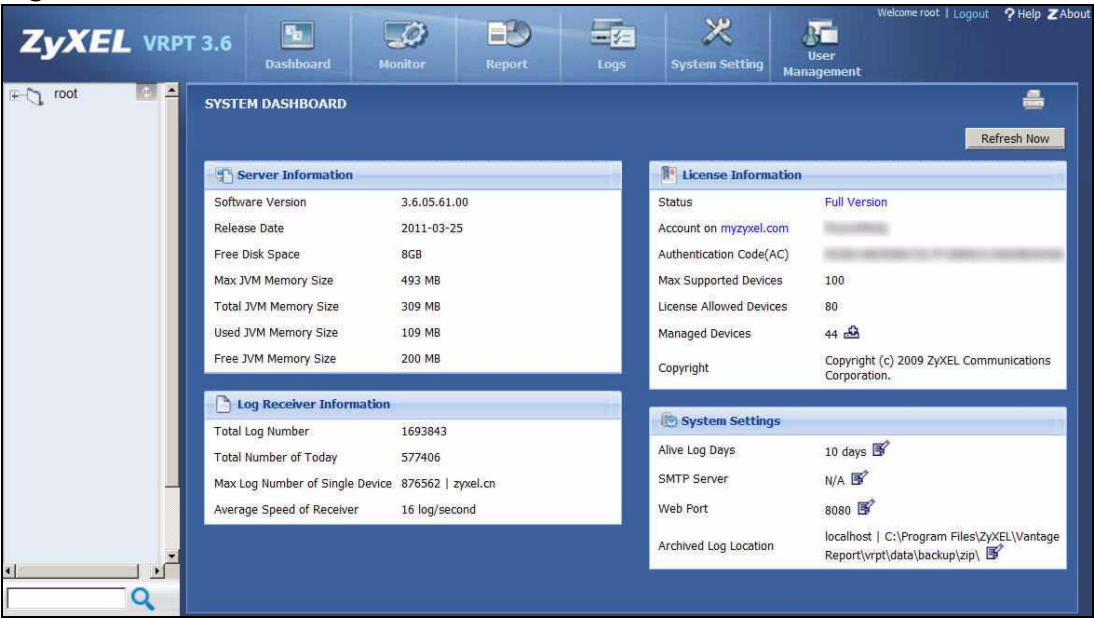
Note: If you forget your password, enter your user name, and click **Forget Password?**. Vantage Report sends your password to the e-mail address (if any) for your **User Name**. See [Section 2.2 on page 24](#) for more information about e-mail in Vantage Report and [Section 14.3 on page 555](#) for more information about SMTP configuration.

- 3 Enter the **User Name** (default: root) and **Password** (default: root).

Note: See [Section 14.3 on page 555](#) to change the password.

- 4 Click the **Login** button. The **System Dashboard** screen appears. See [Section 3.6.1 on page 53](#) for the field descriptions in this screen.

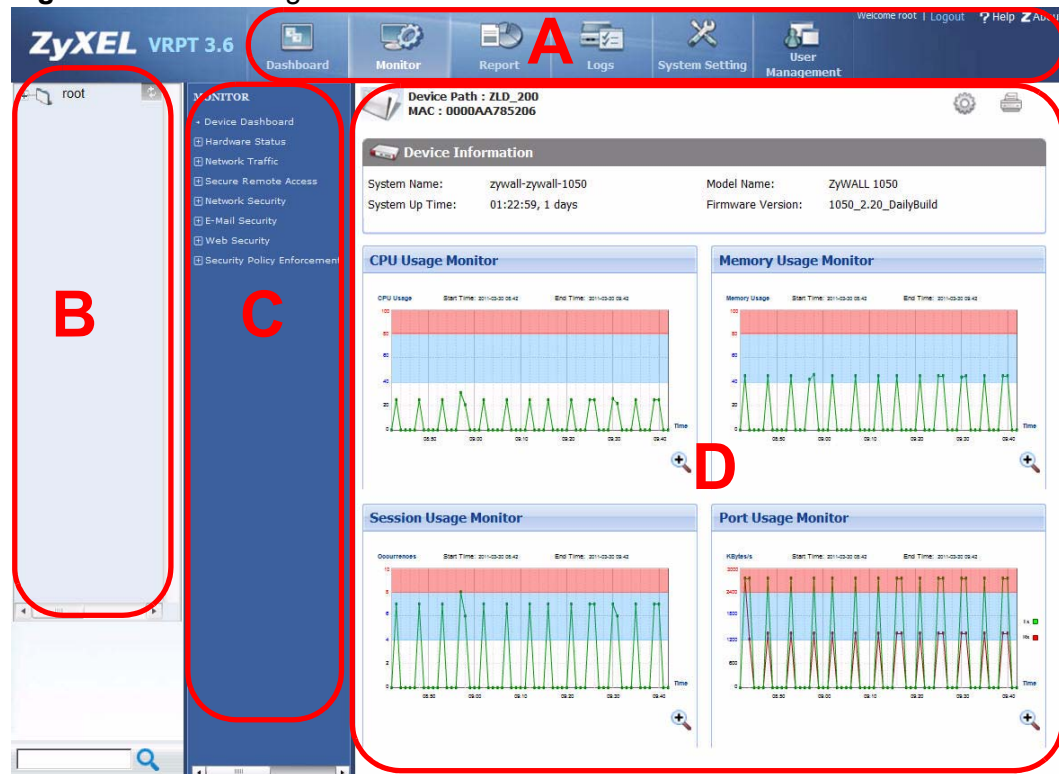
Figure 7 Dashboard



- 5 Manually add a device to Vantage Report. See [Table 8 on page 38](#) for how to add a device.

- 6 Select the device from the device list on the left of the screen and click a menu (for example, **Monitor**) on the top of the screen. The main screen in Vantage Report appears.

Figure 8 Web Configurator Main Screen



The main screen is divided into four parts:

- The **main menu bar (A)** - contains main menus and some icons that are useful anytime.
- The **device window (B)** - displays and organizes the ZyXEL devices that can provide information to Vantage Report.
- The **submenu window (C)** - lists the reports you can generate and organizes these reports into categories. It also lists the configuration menus used to manage and maintain the Vantage Report.
- The **report and setting window (D)** - shows the selected report for the selected device(s) or the related setting screens.

Note: For security reasons, Vantage Report automatically times out after fifteen minutes of inactivity. Log in again if this happens.

The rest of this section discusses each part of the main screen in more detail.

3.3 Main Menu Bar

The main menu bar has three icons. These icons are explained in the table below.

Table 7 Icons in the Main Menu Bar

ICON	DESCRIPTION
	The Help icon opens the help page for the current screen in Vantage Report.
	The About icon opens a screen with the version of Vantage Report.
	The Logout icon logs you out of Vantage Report.

3.3.1 The About Screen

Use this screen to get the current release and copyright for Vantage Report.

Figure 9 About



3.4 Device Window

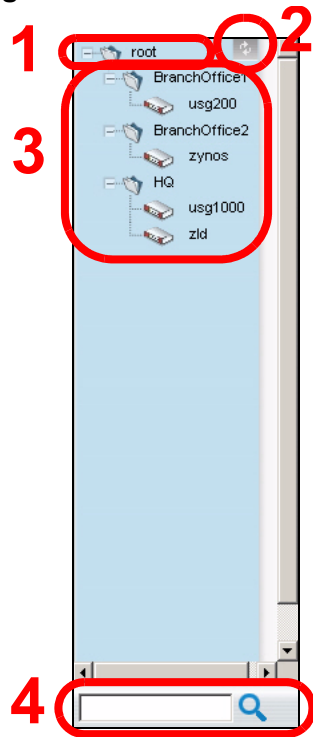
Use the device window to select which device(s) you want to include in a report, add devices to Vantage Report, and remove devices from Vantage Report.

Note: You have to add the device to the device window if you want Vantage Report to store log or traffic information from this device. If the Vantage Report server receives logs or traffic information from a device that is not in this list, it discards the logs.

In the device window, you can also look at basic information about each device, edit the information about the device, and search for devices in Vantage Report using this information. This chapter explains how to do these things.

The device window is located on the left side of the main screen in the web configurator. [Figure 10](#) shows an example.

Figure 10 Device Window



Each numbered section above is described in the following table.

Table 8 Device Window

SECTION	DESCRIPTION
1	To add a device to Vantage Report, - right click on root, and select Add Device. The Add Device screen appears in the device window. (See Figure 11.) To add a folder to Vantage Report, - right click on root, and select Add Folder. The Add Folder screen appears in the device window. (See Figure 11.)
2	To update the device window, click the Refresh button.

Table 8 Device Window

SECTION	DESCRIPTION
3	To move a device in the device tree, - right-click on the device, and select Cut it. Then right-click the destination folder and select Paste to. To select which device is included in a report, - click on the device. To look at the basic information about a device, - click on the device. The Device Information screen appears in the report and setting window. (See Figure 11.) To edit the basic information about a device, - right-click on the device, and select Edit Device. The Edit Device screen appears in the device window. (See Figure 11.) To edit the basic information about a folder, - right-click on the folder, and select Edit Folder. The Edit Folder screen appears in the device window. (See Figure 11.) To remove a device from Vantage Report, - right-click on the device, and select Delete Device. Vantage Report confirms you want to delete it before doing so. To remove a folder from Vantage Report, - right-click on the folder, and select Delete Folder. Vantage Report confirms you want to delete it before doing so.
4	To search for a device, type any part of the name, MAC address, or note and click the magnifying glass. If a match is found, Vantage Report highlights the device in the device window, but the report and setting window does not change. If a match is not found, you get a message. You can click the magnifying glass again to look for another match.

When you add a device to Vantage Report, you can specify the name, MAC address, type, and any notes for the device. When you click on the device, this information is displayed in the report and setting window (see [Section 3.6.1 on page 53](#)). When you edit a device, however, you can only edit the name and the notes. If you want to update the MAC address or device type, you have to delete

the current device and add it again. These screens are discussed in more detail together in [Figure 11 on page 40](#).

Figure 11 Add/Edit Device and Add/Edit Folder Screens

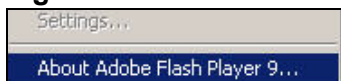
Each field is explained in the following table.

Table 9 Add/Edit Device and Add/Edit Folder Screen Fields

LABEL	DESCRIPTION
Name	Enter the name of the device or folder you want to add to Vantage Report. The device name can consist of alphanumeric characters, underscores(_), periods(.), or dashes(-), and it must be 1-28 characters long. This name is used to refer to the device (or folder) in Vantage Report, and it has to be different than other device (or folder) names in Vantage Report. You can use the system name of a device as the name for that device.
MAC	This field is not available in the Edit Device screen. Enter the LAN MAC address of the device you want to add. For the ZyWALL 1050, use the first (lowest) LAN MAC address. Once you add the device, you cannot change the MAC address anymore.
Type	This field is not available in the Edit Device screen. Select the model type of the device you want to add. Choices are: ZyNOS ZyWALL, ZyWALL 1050, USG 100, USG 200, USG 300, USG 1000, USG 2000, USG 20, USG 20W, USG 50, IDP 10 and Prestige. Not all reports (and fields in reports) are available with all models. See Table 267 on page 591 for a list of which items Vantage Report supports with various firmware versions of various devices.
Note	Enter any additional notes you want to make for the device or folder here.
Add	This field is available in the Add Device screen. Click this to add the device to Vantage Report. It takes time before Vantage Report displays information received from this device.
Save	This field is available in the Edit Device screen. Click this to save your changes to Vantage Report.

You can also right-click in the device window. If you do not right-click on a device or folder, the following menu appears. If you right-click on a device or folder, you can see the following menu items at the end of the menu.

Figure 12 Device Window Right-Click Menu



Click **About Adobe Flash Player 9...** to get information about the current version of Flash.

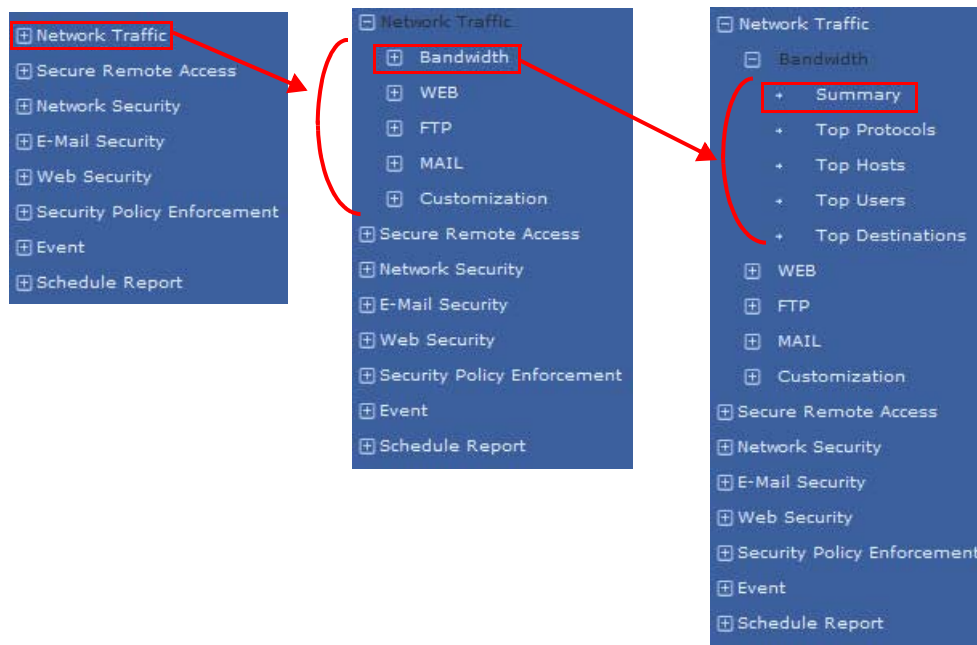
3.5 Menu Panel

Use the menu panel to select which monitor, statistical report, or screen you want to open.

Note: You have to select a device before you can open a monitor or statistical report.

These screens are organized into menus. Click on each top-level menu item to look at the second-level menu items. If a small triangle appears on the right side next to the menu item, then click on the second-level menu item to look at the third-level menu items. Otherwise, click on the monitor, statistical report, or screen you want to open. This is demonstrated in [Figure 13](#)

Figure 13 Menu Panel



Note: You can only open one second-level and one third-level menu at one time. If you open another one, the first one automatically closes.

[Table 10](#) expands the menu panel and introduces each monitor, statistical report, and screen. In addition, it also indicates if you can drill down into each statistical report.

Note: Not every report (or fields in a report) is available with every model of device and firmware version. See [Table 267 on page 591](#) for a list of which items Vantage Report supports with various firmware versions of various devices.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
Dashboard		
Monitor		Use monitors to check the status of ZyXEL devices.
Dashboard		The dashboard gives a quick top level summary of activity across devices that you pre-configured. The dashboard is available with the full version of Vantage Report.
Hardware Status		
	CPU Usage	Use this report to monitor the CPU usage on the selected device.
	Memory Usage	Use this report to monitor the memory usage on the selected device.
Network Traffic		
	Session Usage	Use this report to monitor the number of sessions change status on the selected device.
	Bandwidth	
	Port Usage	Use this report to monitor the throughput statistics on a selected device's port.
	Interface Usage	Use this report to monitor the throughput statistics on a selected device's interface.
	Web	Use this report to monitor the amount of traffic generated by web services in the selected device.
	FTP	Use this report to monitor the amount of traffic generated by FTP services in the selected device.
	Mail	Use this report to monitor the amount of traffic generated by mail services in the selected device.
Secure Remote Access		
	Site-to-site (IPSec)	Use this report to monitor the amount of traffic generated by site-to-site IPSec VPN services in the selected device.
	Client-to-site(IPSec)	Use this report to monitor the amount of traffic generated by client-to-site IPSec VPN services in the selected device.
	Client-to-site(SSL)	Use this report to monitor the amount of traffic generated by SSL VPN services in the selected device.
Network Security		
	Firewall Access Control	Use this report to monitor the number of occurrences of firewall access attempts.
	Attack	Use this report to monitor the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Intrusion Hits	Use this report to monitor the number of intrusions detected by the selected device's IDP feature.
	Antivirus	Use this report to monitor the number of virus occurrences prevented by the selected device.
E-Mail Security		
	Virus Found	Use this report to monitor the number of email virus occurrences prevented by the selected device.
	Spam	Use this report to monitor the number of spam messages stopped by the selected device.
	Intrusion Hits	Use this report to monitor the number of email intrusions detected by the selected device's IDP feature.
Web Security		
	Security Threat	Use this report to monitor the number of occurrences of web security related access attempts to web sites specified in the content filter.
	Virus Found	Use this report to monitor the number of web virus occurrences prevented by the selected device.
	Intrusion Hits	Use this report to monitor the number of web intrusions detected by the selected device's IDP feature.
Security Policy Enforcement		
	Content Filter	Use this report to monitor the number of occurrences of all access attempts to web sites specified in the content filter.
	App Patrol	Use this report to monitor the number of occurrences of applications allowed and blocked.
Report		Use reports to view various and detailed statistic report of ZyXEL devices.
Network Traffic		
	Bandwidth	
	Summary	Use this report to look at the amount of traffic handled by the selected device by time interval. You can also use this report to look at the top services in a specific time interval.
	Top Protocols	Use this report to look at the top services generating traffic through the selected device. You can also use this report to look at the top sources of traffic for any top service.
	Top Hosts	Use this report to look at the top sources of traffic in the selected device. You can also use this report to look at the top services for any top source.
	Top Users	Use this report to look at the top users generating traffic through the selected device. You can also use this report to look at the top services used by any top bandwidth user.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Top Destinations	Use this report to look at the top destinations of traffic in the selected device. You can also use this report to look at the services that were used the most to access the top destination IP addresses.
	WEB	
	Top Sites	Use this report to look at the top destinations of web traffic. You can also use this report to look at the top sources of web traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of web traffic. You can also use this report to look at the top destinations of web traffic for any top source.
	Top Users	Use this report to look at the top sources of web traffic by user. You can also use this report to look at the top destinations of web traffic for any top user.
	FTP	
	Top Sites	Use this report to look at the top destinations of FTP traffic. You can also use this report to look at the top sources of FTP traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of FTP traffic. You can also use this report to look at the top destinations of FTP traffic for any top source.
	Top Users	Use this report to look at the top sources of FTP traffic by user. You can also use this report to look at the top destinations of FTP traffic for any top user.
	MAIL	
	Top Sites	Use this report to look at the top destinations of mail traffic. You can also use this report to look at the top sources of mail traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of mail traffic. You can also use this report to look at the top destinations of mail traffic for any top source.
	Top Users	Use this report to look at the top sources of mail traffic by user. You can also use this report to look at the top destinations of mail traffic for any top user.
	Customization	
	Customization	Use this screen to select the ZyXEL firmware platform that the device uses.
	Top Destinations	Use this report to look at the top destinations of traffic for other services. You can also use this report to look at the top sources of traffic for other services for any top destination.
	Top Sources	Use this report to look at the top sources of traffic for other services. You can also use this report to look at the top destinations of traffic for other services for any top source.
	Top Users	Use this report to look at the top sources of traffic for other services. You can also use this report to look at the top destinations of other services' traffic for any top user. The service is selected in the main report.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
Secure Remote Access		
	Site-to-Site (IPSec)	
	Link Status	Use this report to see which of the device's VPN tunnels are connected.
	Traffic Monitor	Use this report to monitor the total amount of traffic handled by a device's VPN tunnels.
	Top Sites	Use this report to look at the peer IPSec routers with the most VPN traffic. You can also use this report to look at the top sources of VPN traffic for any top destination.
	Top Tunnels	Use this report to look at the VPN tunnels with the most VPN traffic. You can also use this report to look at the top senders or receivers of VPN traffic for a top VPN tunnel.
	Top Protocols	Use this report to look at the top services generating VPN traffic through the selected device. You can also use this report to look at the top senders or receivers of any top service through VPN.
	Top Hosts	Use this report to look at the top sources of VPN traffic. You can also use this report to look at the top destinations of VPN traffic for any top source.
	Top Users	Use this report to look at the users that send or receive the most VPN traffic. You can also use this report to look at the services sent through VPN from or to a top user.
	Top Destinations	Use this report to see to where the device sent the most VPN traffic. You can also use this report to look at the services sent through VPN from or to a top destination.
	Client-to-Site (IPSec)	
	User Status	Use this report to see which of the device's remote access users are connected.
	Top Protocols	Use this report to display which services the remote access users used the most. You can also use this report to look at the top remote access senders or receivers of any top service.
	Top Destinations	Use this report to look at where the remote VPN users sent the most traffic. You can also use this report to look at the remote access hosts that sent the most traffic to the selected top destination.
	Top Users	Use this report to look at the remote VPN users who sent the most VPN traffic. You can also use this report to look at the services sent through VPN from or to a top user.
	Client-to-Site (SSL)	

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	User Status	Use this report to see which of the device's remote access users are connected.
	Top Protocols	Use this report to display which services the remote access users used the most. You can also use this report to look at the top remote access senders or receivers of any top service.
	Top Destinations	Use this report to look at where the remote SSL VPN users sent the most traffic. You can also use this report to look at the remote access hosts that sent the most traffic to the selected top destination.
	Top Applications	Use this report to display which SSL VPN applications the remote access users accessed the most. You can also use this report to look at the top remote access senders or receivers of any top application.
	Top Users	Use this report to look at the users that send or receive the most VPN traffic. You can also use this report to look at the services sent through VPN from or to a top user.
	Xauth	
	Successful Login	Use this report to monitor the total number of users that have successfully logged in to use one of the device's VPN tunnels.
	Failed Login	Use this report to monitor the total number of users that have made unsuccessful attempts to log in to use one of the device's VPN tunnels.
Network Security		
	Firewall Access Control	
	Top Users Blocked	Use this report to look at the users from which the device blocked the most traffic.
	Top Packets Blocked	Use this report to look at the firewall rule that blocked the most packets.
	Attack	Use these reports to look at Denial-of-Service (DoS) attacks that were detected by the ZyXEL device's firewall.
	Summary	Use this report to look at the number of DoS attacks by time interval. You can also use this report to look at the top categories of DoS attacks in a specific time interval.
	Top Attacks	Use this report to look at the top kinds of DoS attacks by number of attacks. You can also use this report to look at the top categories of DoS attacks for any top source.
	Top Sources	Use this report to look at the top sources of DoS attacks by number of attacks. You can also use this report to look at the top categories of DoS attacks for any top source.
	By Type	Use this report to look at the top categories of DoS attacks by number of attacks. You can also use this report to look at the top sources of DoS attacks for any top category.
	Intrusion Hits	

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Summary	Use this report to look at the number of intrusions by time interval. You can also use this report to look at the top intrusion signatures in a specific time interval.
	Top Intrusions	Use this report to look at the top intrusion signatures by number of intrusions. You can also use this report to look at the top sources of intrusions for any top signature.
	Top Sources	Use this report to look at the top sources of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top source.
	Top Destinations	Use this report to look at the top destinations of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top destination.
	By Severity	Use this report to look at the top severities (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug. You can also use this report to look at the top intrusion signatures for any severity.
	Antivirus	
	Summary	Use this report to look at the number of virus occurrences by time interval. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
E-Mail Security		
	Virus Found	
	Summary	Use this report to look at the number of virus occurrences by time interval. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
	Spam	

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Summary	Use this report to look at the number of spam messages by time interval. You can also use this report to look at the top combinations of senders and first SMTP servers to which the spam was sent in a specific time interval.
	Top Senders	Use this report to look at the top combinations of senders and first SMTP servers to which the spam was sent by number of messages.
	Top Sources	Use this report to look at the top sources (last mail relay) of spam messages by number of messages.
	Intrusion Hits	
	Summary	Use this report to look at the number of intrusions by time interval. You can also use this report to look at the top intrusion signatures in a specific time interval.
	Top Intrusions	Use this report to look at the top intrusion signatures by number of intrusions. You can also use this report to look at the top sources of intrusions for any top signature.
	Top Sources	Use this report to look at the top sources of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top source.
	Top Destinations	Use this report to look at the top destinations of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top destination.
	By Severity	Use this report to look at the top severities (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug. You can also use this report to look at the top intrusion signatures for any severity.
Web Security		
	Security Threat	
	Summary	Use this report to look at the number of attempts to access unsafe web sites by time interval. You can also use this report to look at the top sources of attempts to access unsafe web sites in a specific time interval.
	Top Sites	Use this report to look at the top destinations of attempts to access unsafe web sites by number of attempts. You can also use this report to look at the top sources of attempts to access unsafe web sites for any top destination.
	Top Users	Use this report to look at the top users accessing unsafe web traffic. You can also use this report to look at the top destinations for any top source of unsafe web traffic.
	Top Hosts	Use this report to look at the top sources of attempts to access unsafe web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access unsafe web sites for any top source.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	By Category	Use this report to look at the top categories of destinations in attempts to access unsafe web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access unsafe web sites for any top category.
	Virus Found	
	Summary	Use this report to look at the number of virus occurrences by time interval. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
	Intrusion Hits	
	Summary	Use this report to look at the number of intrusions by time interval. You can also use this report to look at the top intrusion signatures in a specific time interval.
	Top Intrusions	Use this report to look at the top intrusion signatures by number of intrusions. You can also use this report to look at the top sources of intrusions for any top signature.
	Top Sources	Use this report to look at the top sources of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top source.
	Top Destinations	Use this report to look at the top destinations of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top destination.
	By Severity	Use this report to look at the top severities (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug. You can also use this report to look at the top intrusion signatures for any severity.
Security Policy Enforcement		
	EPS	
	EPS	Use this screen to see which users' computers complied or failed to comply with defined corporate policies before they can access the network.
	Content Filter(All)	

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Summary	Use this report to look at the number of attempts to access allowed and blocked web sites by time interval. You can also use this report to look at the top sources of attempts to access allowed and blocked web sites in a specific time interval.
	Top Sites	Use this report to look at the top destinations of attempts to access allowed and blocked web sites by number of attempts. You can also use this report to look at the top sources of attempts to access allowed and blocked web sites for any top destination.
	Top Users	Use this report to look at the top users for which the device forwarded or blocked web traffic. You can also use this report to look at the top destinations for any top source of allowed and blocked web traffic.
	Top Hosts	Use this report to look at the top sources of attempts to access allowed and blocked web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access allowed and blocked web sites for any top source.
	By Category	Use this report to look at the top categories of destinations in attempts to access allowed and blocked web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access allowed and blocked web sites for any top category.
	Content Filter(Blocked)	
	Summary	Use this report to look at the number of attempts to access blocked web sites by time interval. You can also use this report to look at the top sources of attempts to access blocked web sites in a specific time interval.
	Top Sites	Use this report to look at the top destinations in attempts to access blocked web sites by number of attempts. You can also use this report to look at the top sources of attempts to access blocked web sites for any top destination.
	Top Users	Use this report to look at the users for which the device blocked the most web site access attempts. You can also look at the top destinations for any user for which the device blocked the most web site access attempts.
	Top Hosts	Use this report to look at the top sources of attempts to access blocked web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access blocked web sites for any top source.
	By Category	Use this report to look at the top categories of destinations in attempts to access blocked web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access blocked web sites for any top category.
	Application Access Control	
	Top Applications Blocked	Use this report to look at the applications for which the device blocked the most connections.
	Top Users Blocked	Use this report to look at the users for which the device blocked the most connections.

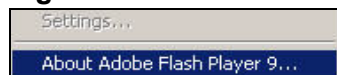
Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Top Applications Allowed	Use this report to look at the applications for which the device allowed the most connections.
Event		
	Login	
	Successful Login	Use this screen to look at who successfully logged into the ZyXEL device (for management or monitoring purposes).
	Failed Login	Use this screen to look at who tried to log in into the ZyXEL device (for management or monitoring purposes) but failed.
	Session Per Host	A device can limit a user's maximum number of NAT sessions. Use these screens to see who has exceeded the maximum number of NAT sessions the most often.
	Top Hosts	Use this screen to see which hosts have most frequently gone over the maximum number of NAT sessions per host.
	Top Users	Use this screen to see which users have most frequently gone over the maximum number of NAT sessions per host.
	Successful Login	Use this screen to look at who successfully logged into the ZyXEL device (for management or monitoring purposes).
Schedule Report		
	Summary	Use this screen to set up and maintain daily, weekly, and overtime (one-time) reports that Vantage Report sends by e-mail.
	Configure Template	Use this screen to add and edit report templates.
	Logo Template	Use this screen to configure the title name and logo shown on all reports.
Log		
Log Viewer		Use this screen to query and look at log entries for the selected ZyXEL device.
Log Receiver		Use these screens to look at the total number of logs that Vantage Report has received per day or per device.
VRPT System Logs		Use this screen to look at the Vantage Report's system logs.
Log Archiving		Use these screens to archive historical logs regularly and store in a preferred location. The location includes local directory in the Vantage Report server, an FTP server or a NAS (Network Archived Storage) device.
Log Remove		Use this screen to remove historical logs collected within a specified period.
System Setting		The root account can use all of the following screens. Other users can use the About screen and some features in User Management .

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
General Configuration		Use this screen to maintain global reporting settings, such as how many days of logs to keep and default chart type.
Server Configuration		Use this screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports.
Data Maintenance	Configuration	You can use this screen to backup or restore the settings in the General Configuration , and Server Configuration screens. (The format is XML.)
	Device List	You can use this screen to export the current device window to an XML file, or you can add devices stored in XML format to Vantage Report.
Upgrade		Use this screen to install new releases of Vantage Report. Do not use this screen to upgrade to the full version.
Registration		Use this screen to upgrade to the full version, or increase the number of devices Vantage Report supports.
Notification		Use this screen to allow the administrator or user to receive SMS notifications of rule based alerts and VRPT system alarms.
Rule-based Alert		Use this screen to monitor device behavior in real time according to customized conditions.
User Management		The Vantage Report supports multiple groups and users.
Group		Use this screen to manage (create, delete, edit) groups. You can also specify folders and devices this group users are allowed to view and manage.
Account		Use this screen to manage (create, delete, edit) user accounts.

You can also right-click in the menu panel. The following menu appears.

Figure 14 Menu Panel Right-Click Menu

Click **About Adobe Flash Player 9...** to get information about the current version of Flash.

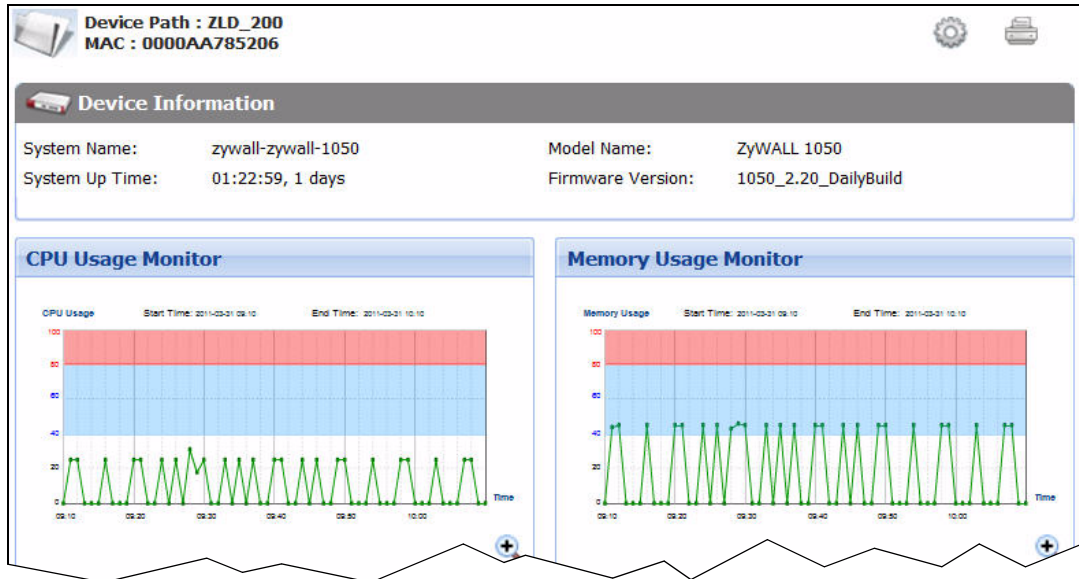
3.6 Report and Setting Window

The report and setting window displays the monitor, statistical report, or screen that you select in the device window and the menu panel.

3.6.1 Device Information Screen

When you first click on a device in the device window, the information you configured for the device displays in the report and setting window. See [Section 3.4 on page 37](#) for how to add and edit device information.

Figure 15 Device Information Screen



Each field is explained in the following table.

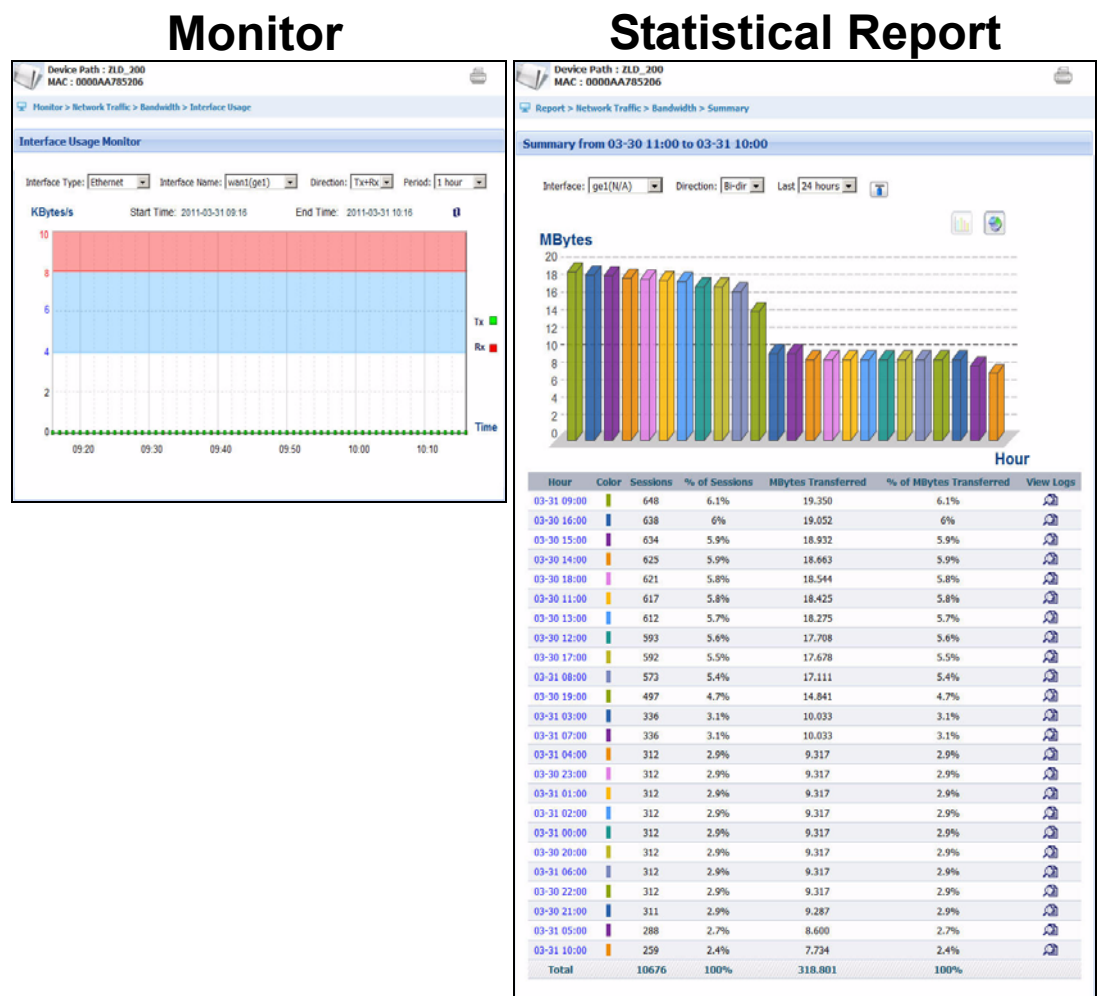
Table 11 Device Information Screen Fields

LABEL	DESCRIPTION
Device Path	You can create multiple layers of folders for devices. This field displays the name used to refer to the device in Vantage Report and the folders that the device is in. For example, if the device path is "folder1/folder2/myZW5", "folder1" is in the root folder, "folder2" is in folder1 and "myZW5" is the name of the device and it is in folder2.
MAC	This is the LAN MAC address of the device. For the ZyWALL 1050, this is the first (lowest) LAN MAC address.
System Name	This is the name of the device you configured.
System Up Time	This is the total amount of time the ZyXEL device has been running since it last restarted.
Model Name	This is the model type of the device. See Table 267 on page 591 for a list of which items Vantage Report supports with various firmware versions of various devices.
Firmware Version	This is the firmware version the ZyXEL device currently uses.

3.6.2 Monitors and Statistical Reports

The layout in the report and setting window is similar for all monitors. Similarly, the layout is similar for all statistical reports. For other screens, the layout is different for each one. Typical examples of monitors and statistical reports are shown in [Figure 16](#).

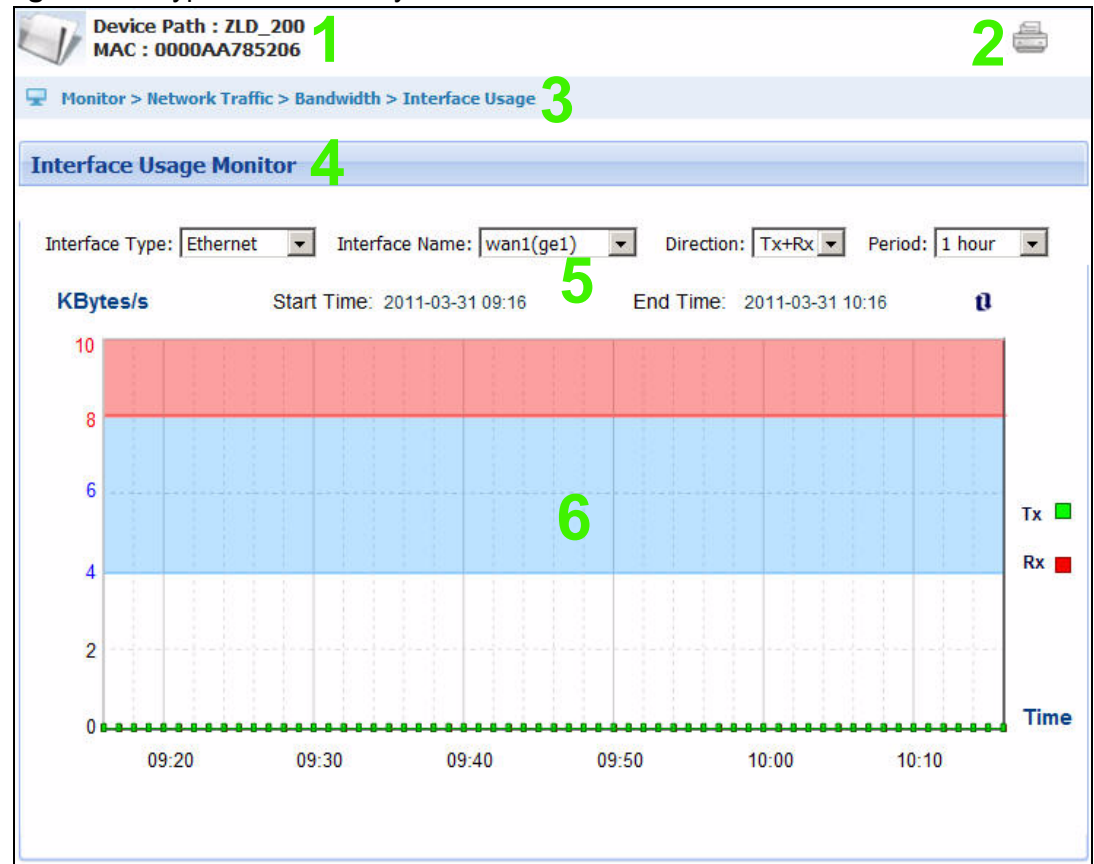
Figure 16 Report and Setting Window: Monitor and Statistical Report Examples



3.6.2.1 Monitor Layout

A typical monitor is shown in [Figure 10](#).

Figure 17 Typical Monitor Layout



Each numbered section above is described in the following table.

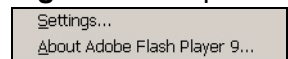
Table 12 Typical Monitor Features

SECTION	DESCRIPTION
1	Device Path, MAC: These fields display the path you added the ZyXEL device in the Vantage Report and the device's MAC address.
2	Print icon: Click this icon to print the current screen.
3	This field shows the menu items you selected to open this monitor.
4	This field displays the title of the monitor.

Table 12 Typical Monitor Features

SECTION	DESCRIPTION
5	Start Time: the time of the earliest traffic information in the graph End Time: the time of the latest traffic information in the graph. Refresh icon: Click this icon to update the screen immediately.
6	The graph shows how the status changes over time. The X-axis (horizontal) is time. See Section 2.3 on page 25 for more information about clock time in Vantage Report. The Y-axis (vertical) depends on the type of monitor you select. In Figure 17, the Y-axis is the amount of traffic in kilobytes the ge1 Ethernet interface has transmitted and received in the past one hour. See Section 2.6 on page 27 for more information about the source data used by the monitor.

You can also right-click on monitors. In some places, you see the standard browser menu. In other places (especially on graphs), the following menu appears.

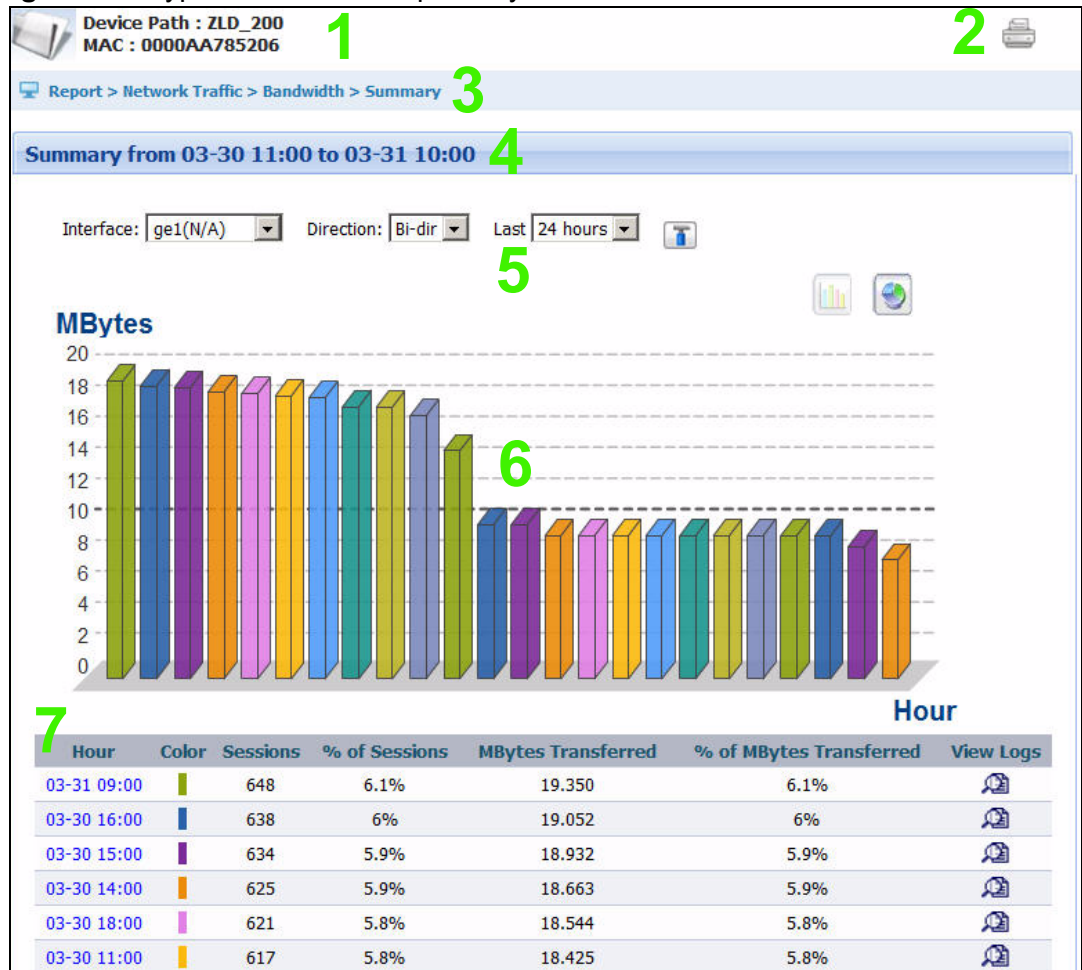
Figure 18 Report and Setting Window Right-Click Menu

Click **Settings...** if you want to change the Flash settings on the Vantage Report server. In most cases, this is unnecessary. Click **About Adobe Flash Player 9...** to get information about the current version of Flash.

3.6.2.2 Statistical Report Layout

A typical statistical report is shown in Figure 19.

Figure 19 Typical Statistical Report Layout



Each numbered section above is described in the following table.

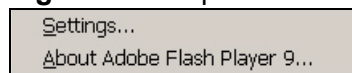
Table 13 Typical Statistical Report Features

SECTION	DESCRIPTION
1	Device Path, MAC: These fields display the path you added the ZyXEL device in the Vantage Report and the device's MAC address.
2	Print icon: Click this icon to print the current screen.
3	This field shows the menu items you selected to open this statistical report.
4	This field displays the title of the statistical report. The title includes the date(s) you specified in section 5.

Table 13 Typical Statistical Report Features

SECTION	DESCRIPTION
5	Last, Settings icon: Use one of these fields to specify what historical information is included in the report. - Select how many days, ending (and including today), in the Last field. - Click the Settings icon, the Report Display Settings screen appears. The date range can be up to 30 days long. You can select custom.. in the Last field and then select a specific Start Date and End Date. When you change any of these fields, the report updates automatically. Both the Last and Settings fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). They do not reset when you open or close drill-down reports. These fields are not available in drill-down reports because these reports use the same historical information as the main report. See Section 2.3 on page 25 for more information about time in Report screens.
6	The graph displays the specified report visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System Setting > General Configuration. See Section 14.1 on page 549. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little. See Section 2.6 on page 27 for more information about the source data used by the statistical report.
7	In the table, - Click on a link to drill down into the report. The current report is replaced by a detailed report for the selected record. The detailed report uses the same historical information you select in #5. - If DNS Reverse is enabled in System Setting > General Configuration, the table displays the domain name, if identifiable, with IP addresses (for example, "www.yahoo.com/200.100.20.10"). See Section 14.1 on page 549. - Some reports provide extra information (for example, number of traffic events) in the table. See each report for more information. - Click a view logs icon to display the logs related to the individual record. See Section 2.6 on page 27 for more information about the source data used by the statistical report.

You can also right-click on statistical reports. In some places, you see the standard browser menu. In other places (especially on graphs), the following menu appears.

Figure 20 Report and Setting Window Right-Click Menu

Click **Settings...** if you want to change the Flash settings on the Vantage Report server. In most cases, this is unnecessary. Click **About Adobe Flash Player 9...** to get information about the current version of Flash.

3.6.3 View Logs

The **Logs > Log Viewer** screen displays the logs related to an individual record in a statistical report. See [Appendix C on page 645](#) and [Appendix B on page 599](#) for information on the logs.

Figure 21 View Logs

Time	Source:Port	Destination:Port	User	Severity	Category	Message	Note
2011-03-31 10:55:54	0.0.0.0:0	0.0.0.0:0	unknown	Info	SSL VPN	file sharing my_cifs1 is accessed. sent=5029 rcvd=0	User: gary1
2011-03-31 10:55:54	0.0.0.0:0	0.0.0.0:0	unknown	Info	SSL VPN	web application owa9 is accessed. sent=233508 rcvd=430	User: gary9
2011-03-31 10:55:54	192.168.1.31:3434	218.104.52.178:80	user1	Info	Warning Web Sites	site14: Trusted Web site	WEB FORWARD
2011-03-31 10:55:54	0.0.0.0:0	0.0.0.0:0	unknown	Info	SSL VPN	web application owa8 is accessed. sent=325 rcvd=0	User: gary8
2011-03-31 10:55:54	192.168.1.31:3434	218.104.52.178:80	user1	Info	Warning Web Sites	site13: Trusted Web site	WEB FORWARD
2011-03-31 10:55:54	0.0.0.0:0	0.0.0.0:0	unknown	Info	SSL VPN	web application owa7 is accessed. sent=2308 rcvd=220	User: gary7
2011-03-31 10:55:54	192.168.1.31:3434	218.104.52.178:80	user1	Info	Warning Web Sites	site12: Trusted Web site	WEB FORWARD
2011-03-31 10:55:54	0.0.0.0:0	0.0.0.0:0	unknown	Info	SSL VPN	web application owa6 is accessed. sent=3245 rcvd=2220	User: gary6
2011-03-31 10:55:53	192.168.1.31:3434	218.104.52.178:80	user1	Info	Warning Web Sites	site11: Trusted Web site	WEB FORWARD
2011-03-31 10:55:53	0.0.0.0:0	0.0.0.0:0	unknown	Info	SSL VPN	web application owa5 is accessed. sent=2308 rcvd=50	User: gary5

Total Count:461,812 Total Page:46,182 First 1 2 3 4 5 6 7 8 9 10 Last Go

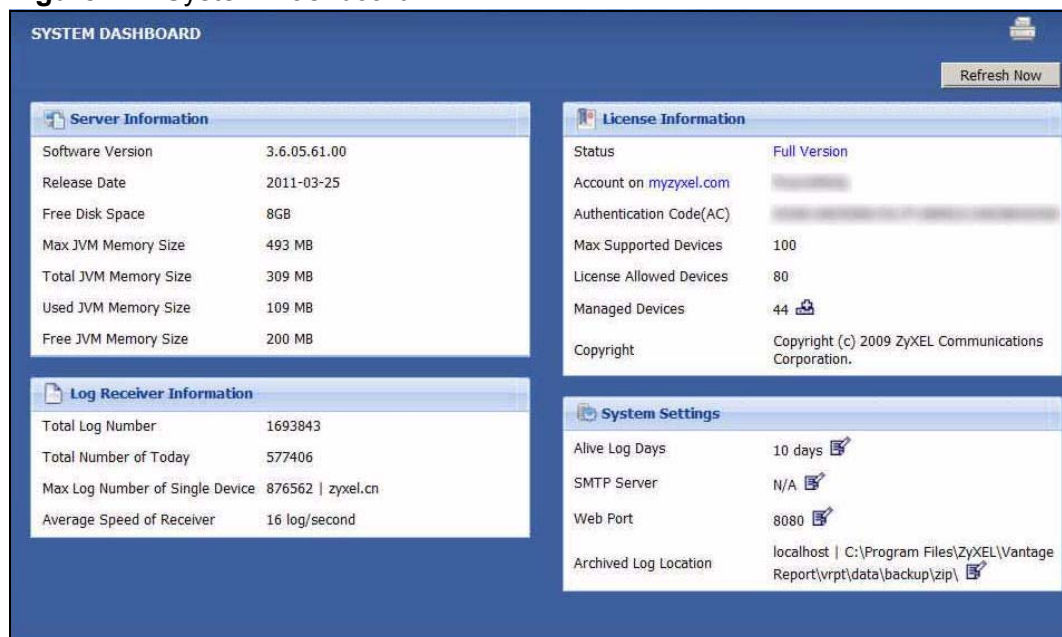
See [Table 227 on page 528](#) for the description of each field in this screen.

3.7 System Dashboard

When you log into the Vantage Report, the **System Dashboard** is the first screen displayed. The screen summarizes the Vantage Report system, license, log

received and system settings information. You can also click the Dashboard button at the right top corner to open this screen when you are in another screen.

Figure 22 System Dashboard



Each field is described in the following table.

Table 14 System Dashboard

LABEL	DESCRIPTION
Refresh Now	Click this to get this screen updated immediately.
Server Information	
Software Version	This field displays the Vantage Report version.
Release Date	This field displays the date the Vantage Report software version is released.
Free Disk Space	This field displays the available disk space in the computer your Vantage Report is installed.
Max JVM Memory Size	This field displays the maximum memory size the Vantage Report's Java Virtual Machine (JVM) can allocate on the computer where the Vantage Report is installed. You can configure the memory size according to the computer's RAM (Random Access Memory) size. Java applications request memory to the computer through the JVM.
Total JVM Memory Size	This field displays the total amount of memory the computer has allocated for the Vantage Report's JVM.
Used JVM Memory Size	This field displays the amount of memory size the Java applications are using.
Free JVM Memory Size	This field displays the amount of memory size available for Java applications.
Log Receiver Information	
Total Log Number	This field displays the total number of log entries the Vantage Report stores.

Table 14 System Dashboard

LABEL	DESCRIPTION
Total Number of Today	This field displays the total number of log entries the Vantage Report has received today.
Max Log Number of Single Device	This field displays the number of a device's log entries and the device's name which sends the most number of logs to the Vantage Report.
Average Speed of Receiver	This field displays the average time in seconds the Vantage Report received a log entry since it is last started.
License Information	
Status	This field displays the status or the version type (Full Version or Basic Version) of the Vantage Report license. Click the hyperlink to view more information about the license status in the System Setting > Registration screen.
Account on myzyxel.com	This field displays the user account you used to register your Vantage Report to the www.zyxel.com website. Click the myzyxel.com hyperlink to take you to the website. www.myzyxel.com is a central product registration website owned by ZyXEL.
Authentication Code	This field displays the string generated during the registration of your Vantage Report to www.zyxel.com.
Max Supported Devices	This field displays the maximum number of ZyXEL devices your Vantage Report version supports.
License Allowed Devices	This field displays the maximum ZyXEL devices you are allowed to manage in the Vantage Report. The number depends on the license you have entered in the System Setting > Registration . See Section 14.5.1 on page 559 .
Managed Devices	This field displays the number of ZyXEL devices you can manage in the Vantage Report. Click the Add Device icon to add more devices in the Vantage Report.
Copyright	This field displays the copyright of the Vantage Report.
System Settings	
Alive Log Days	This field displays the number of days the Vantage Report stores logs. The Vantage Report automatically deletes logs over this configured days.
SMTP Server	This field displays the mail server you configured for the Vantage Report to send reports through emails. Click the edit icon to take you to the System Setting > Server Configuration screen where you can configure the related settings.
Web Port	This field displays the port number the Vantage Report listens for user's web interface access. Click the edit icon to take you to the System Setting > Server Configuration screen where you can change the setting.
Archived Log Location	This field displays the location where the Vantage Report stores its archived logs currently. Click the edit icon to take you to the Logs > Log Archiving > File Archiving Settings screen where you can configure the related settings.

PART II

Monitors, Reports and Logs

Monitor (65)

Network Traffic (95)

Secure Remote Access (183)

Network Security (269)

Security Policy Enforcement (443)

Event (499)

EPS (459)

Schedule Report (509)

Logs (527)

Monitor

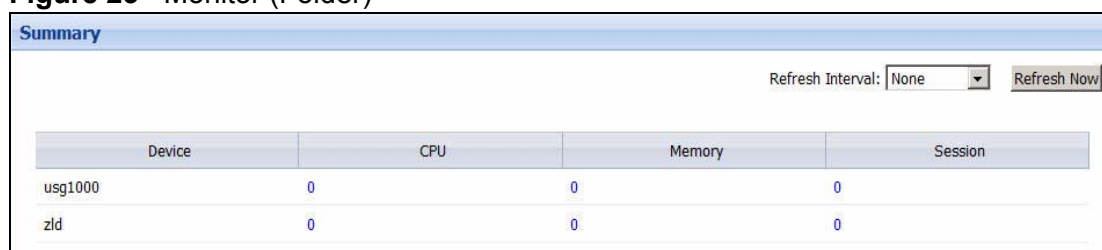
Use monitor screens to check the status of ZyXEL devices. See [Section 2.3 on page 25](#) for a related discussion about time.

Note: The available **Monitor** sub-menus may vary depending on your selected ZyXEL device model.

4.1 Monitor (Folder)

Click a folder () in the device window to open this screen. This screen provides a summary table to monitor the current CPU and memory usage, the number of sessions, total amount of traffic handled by each device under the folder.

Figure 23 Monitor (Folder)



Summary			
Refresh Interval: None Refresh Now			
Device	CPU	Memory	Session
usg1000	0	0	0
zld	0	0	0

Each field is described in the following table.

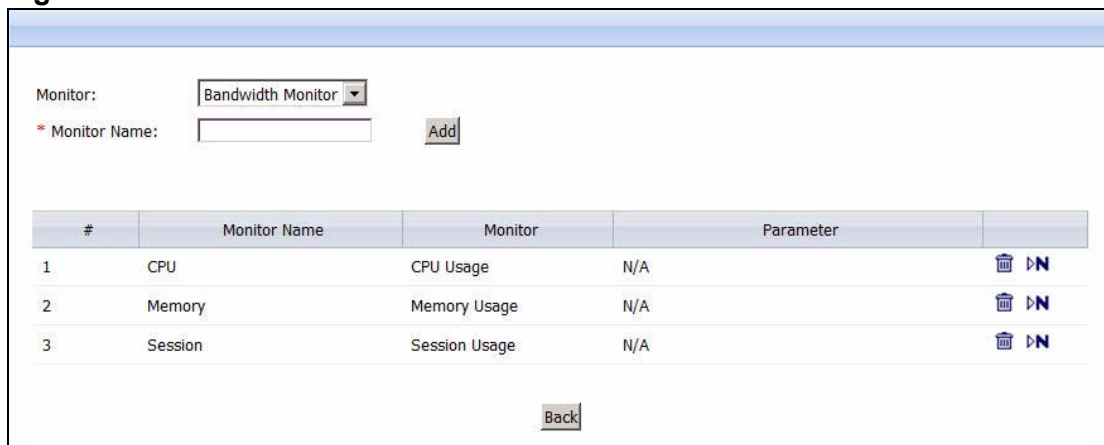
Table 15 Monitor (Folder)

LABEL	DESCRIPTION
Refresh Interval	Select how often (1 Minute , 5 Minutes , 10 Minutes) the Vantage Report updates the information in this screen. Select None to not to update this screen. Click Refresh Now to update the screen immediately.
Device	This field displays the name of a device under the selected folder configured when the device was registered in the Vantage Report.
CPU	This field displays the current CPU usage in percentage on the device.
Memory	This field displays the current memory usage in percentage on the device.
Session	This field displays the number of sessions the device is currently handling.

4.1.1 Customize the Column Fields

Click a folder and then click the **Setting**  icon at the top-right corner of the screen to open this screen. Use this screen to customize the column fields in the **Monitor (Folder)** screen (see [Figure 23 on page 65](#)). Vantage Report monitors the CPU usage, memory usage and the number of concurrent sessions by default for devices under a folder.

Figure 24 Customize the Column Fields



#	Monitor Name	Monitor	Parameter	
1	CPU	CPU Usage	N/A	
2	Memory	Memory Usage	N/A	
3	Session	Session Usage	N/A	

Each field is described in the following table.

Table 16 Customize the Column Fields

LABEL	DESCRIPTION
Monitor	Select a category to monitor device(s) under the folder.
Port	This field is available when you select Port Usage in the Monitor field. Select a port to monitor.
Direction	This field is available when you select Port Usage or Interface Usage in the Monitor field. Select transmission (Tx), receiving (Rx) or both (Tx+Rx) for the traffic direction to monitor.
Interface Type	This field is available when you select Interface Usage in the Monitor field. Select the type of the interface to monitor.
Interface	This field is available when you select Interface Usage in the Monitor field. The available options in this field may vary depending on the Interface Type you select. Select an interface to monitor.
Service	This field is available when you select Service Monitor in the Monitor field. Select a service type to monitor.
Monitor Name	Type up to 29 alphanumeric characters for the name of the monitor item. Underscore (_) is allowed.
Add	Click this to add the monitor item to the list table below and save the changes to the Vantage Report.
#	This field displays the index number of the monitor item.
Monitor Name	This field displays the name of the monitor item.
Monitor	This field displays the category of the monitor item.

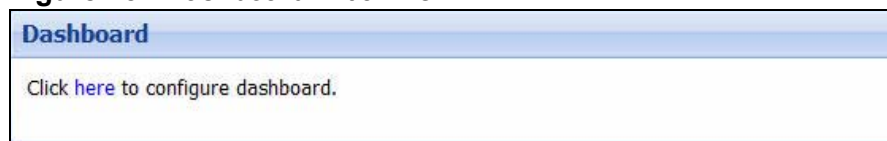
Table 16 Customize the Column Fields

LABEL	DESCRIPTION
Parameter	This field displays the additional parameters of the monitor item. N/A displays if no additional parameters for the monitor item.
Back	Click this to go back to the previous screen.

4.2 Dashboard

The dashboard gives a quick top level summary of activity for each device. Click a device and then click the **Monitor** menu to open the screen for the device. You get to pre-configure a list of reports or monitors you want the Vantage Report to display first. The dashboard is available with the full version of Vantage Report.

Click the **here** link if it is the first time you configure the dashboard for a device.

Figure 25 Dashboard Initial View

Then it takes you to the following screen where you can configure up to 4 monitors and/or reports shown in the device dashboard at one time.

Figure 26 Dashboard Configuration

Device Information

System Name:	zywall-zywall-1050	Model Name:	ZyWALL 1050
System Up Time:	01:22:59, 1 days	Firmware Version:	1050_2.20_DailyBuild

Monitor & Summary Report: CPU Usage	Monitor & Summary Report: Memory Usage
Period: 1 hour	Period: 1 hour
Footnotes:	Footnotes:

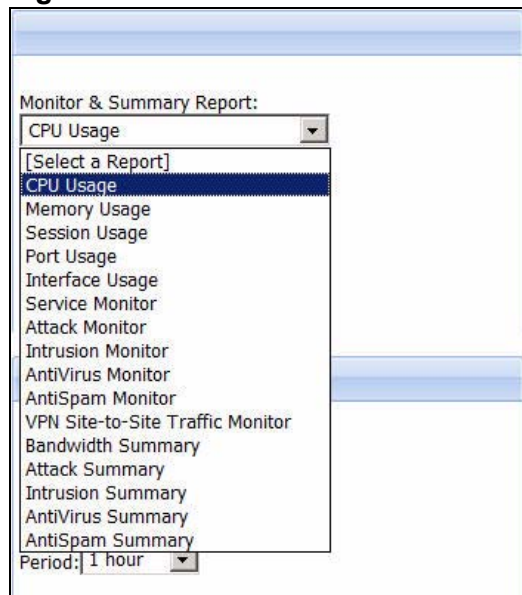
Monitor & Summary Report: Session Usage	Monitor & Summary Report: Port Usage
Period: 1 hour	Port: Port1
Footnotes:	Direction: Tx+Rx
	Period: 1 hour
	Footnotes:

Apply Reset

Select a monitor or summary report to display for each.

Note: The available monitor and summary report options shown in the list box may vary depending on the selected ZyXEL device.

Figure 27 Dashboard Select Device and Monitor or Summary



4.3 Dashboard

The dashboard looks as follows when you finish configuring it.

Click the magnifying glass icon at the right bottom of each monitor or report to go to the corresponding monitor screen. The dashboard is available with the full

version of Vantage Report. See [Section 3.6.1 on page 53](#) for the field descriptions shown in the screen.

Figure 28 Dashboard Configured



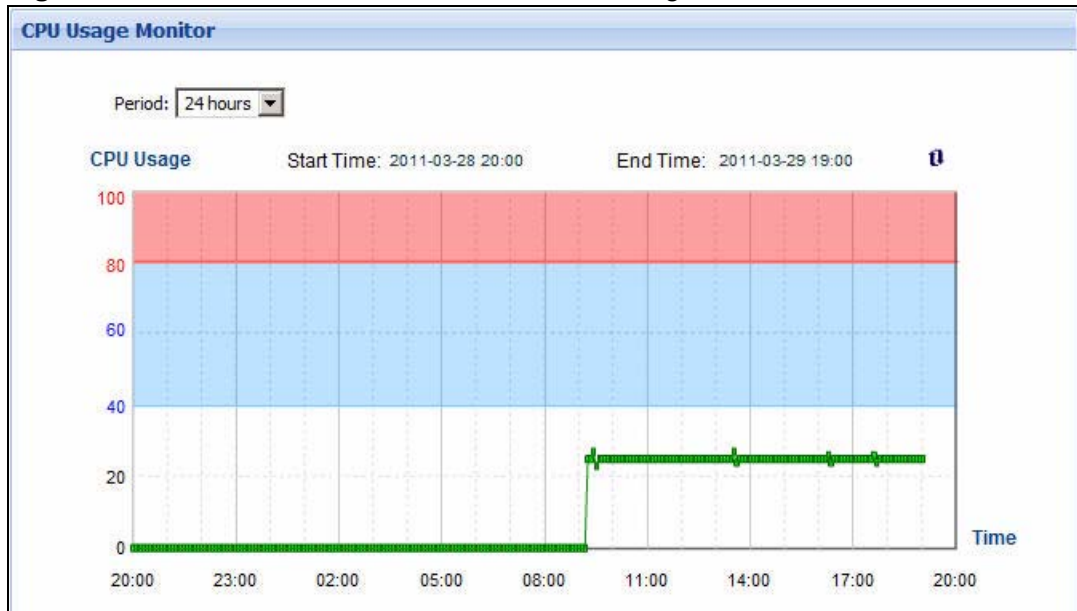
If you want to change a dashboard monitor or report, click the  icon at the top right corner. See [Figure 26 on page 68](#).

If you want to print the screen, click the  icon.

4.4 CPU Usage Monitor

Click **Monitor > Hardware Status > CPU Usage** to open this screen. Use this screen to monitor CPU usage in the selected device.

Figure 29 Monitor > Hardware Status > CPU Usage



Each field is described in the following table.

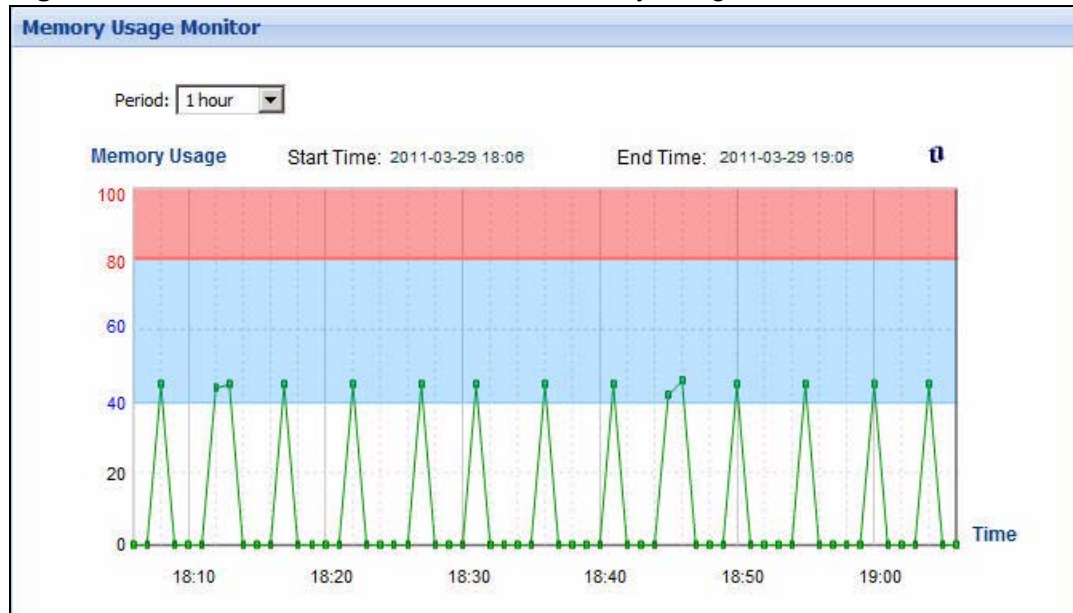
Table 17 Monitor > Hardware Status > CPU Usage

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. The Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the percentage of CPU usage on the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.5 Memory Usage Monitor

Click **Monitor > Hardware Status > Memory Usage** to open this screen. Use this screen to monitor memory usage in the selected device.

Figure 30 Monitor > Hardware Status > Memory Usage



Each field is described in the following table.

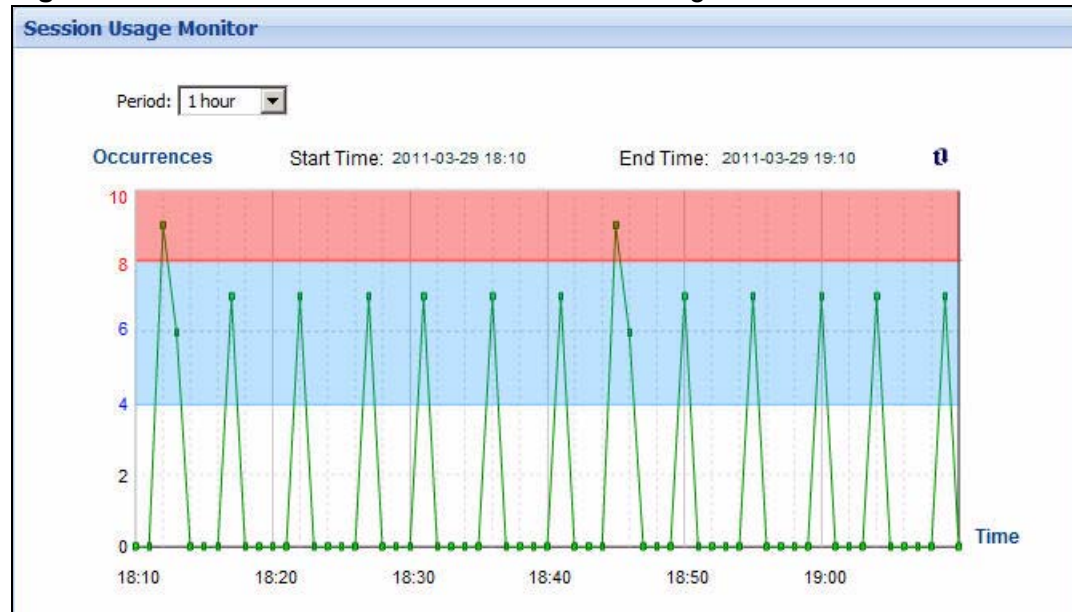
Table 18 Monitor > Hardware Status > Memory Usage

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. The Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the percentage of memory usage on the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.6 Session Usage Monitor

Click **Monitor > Network Traffic > Session Usage** to open this screen. Use this screen to monitor the number of sessions change at various times through the selected ZyXEL device. A session is a TCP/IP connection through the selected ZyXEL device.

Figure 31 Monitor > Network Traffic > Session Usage



Each field is described in the following table.

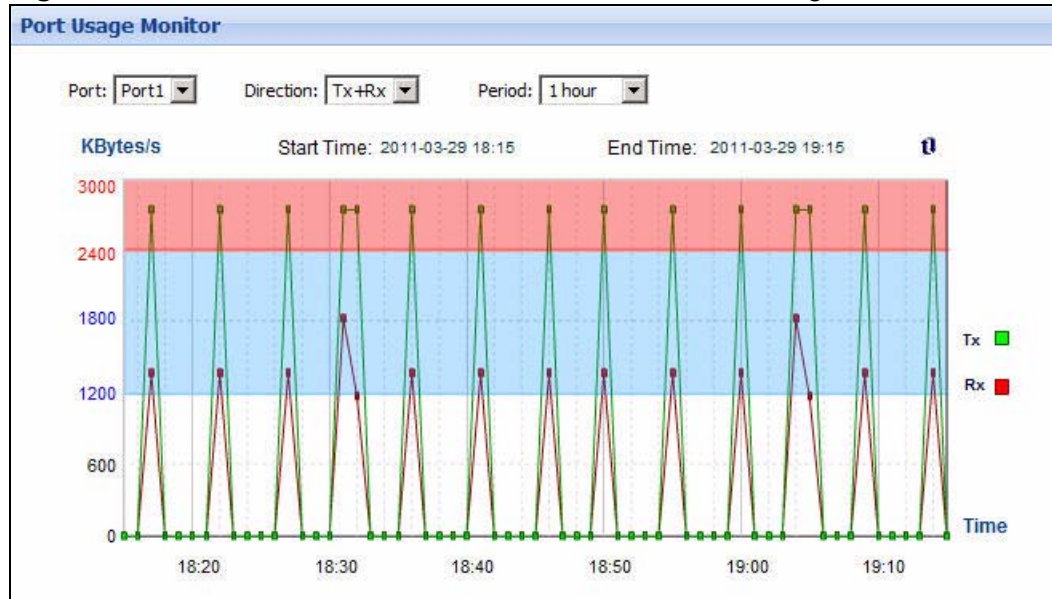
Table 19 Monitor > Network Traffic > Session Usage

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of sessions at a specific time or date. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.7 Port Usage Monitor

Click **Monitor > Network Traffic > Bandwidth > Port Usage** to open this screen. Use this screen to monitor the throughput statistics on a selected device's port.

Figure 32 Monitor > Network Traffic > Bandwidth > Port Usage



Each field is described in the following table.

Table 20 Monitor > Network Traffic > Bandwidth > Port Usage

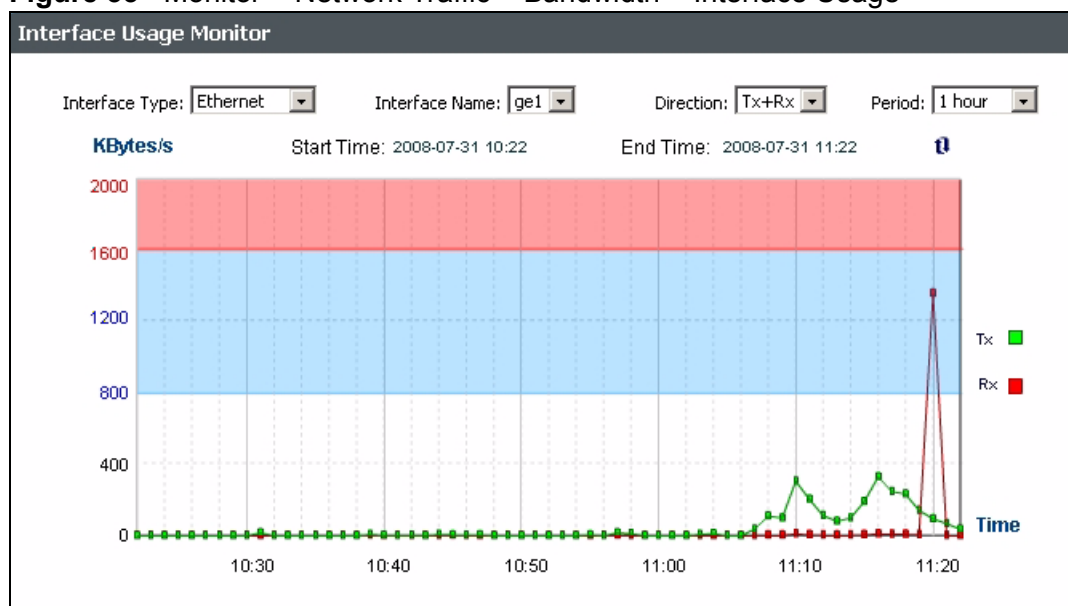
LABEL	DESCRIPTION
Port	Select a port to display the throughput statistics of the corresponding port.
Direction	Select the direction of the traffic for which you want to show throughput statistics in this graph. Select Tx to display transmitted traffic throughput statistics and select Rx to display received traffic throughput statistics in KBytes per second. Alternatively, select Tx-Rx to display both.
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. The Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.

Table 20 Monitor > Network Traffic > Bandwidth > Port Usage

LABEL	DESCRIPTION
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): the amount of traffic through the selected port. X-axis (horizontal): The X-axis displays a date or time depending on the length of time you choose in the Period field.

4.8 Interface Usage Monitor

Click **Monitor > Network Traffic > Bandwidth > Interface Usage** to open this screen. Use this screen to monitor the throughput statistics on a selected device's interface.

Figure 33 Monitor > Network Traffic > Bandwidth > Interface Usage

Each field is described in the following table.

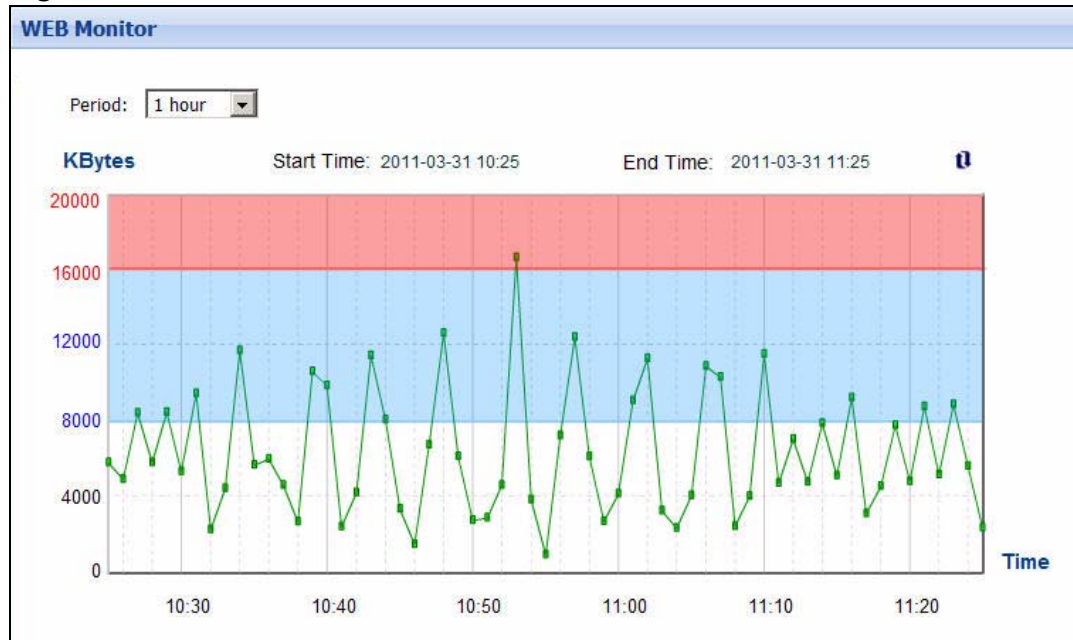
Table 21 Monitor > Network Traffic > Bandwidth > Interface Usage

LABEL	DESCRIPTION
Interface	Select a type of interfaces to display the throughput statistics of the corresponding interface type. The available options may vary depending on the selected device. The possible options are Ethernet, VLAN, PPP, bridge, dial-backup, 3G, Wireless.
Interface Name	Select an interface for which you want to display the throughput statistics of the corresponding interface. The available options of this field vary depending on the type of interface you selected in the Interface field. See the corresponding device's User's Guide for more information.
Direction	Select the direction of the traffic you want to show throughput statistics in this graph. Select Tx to display transmitted traffic throughput statistics and select Rx to display received traffic throughput statistics in KBytes per second. Alternatively, select Tx-Rx to display both.
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. The Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of traffic through the selected interface. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.9 Web Monitor

Click **Monitor > Network Traffic > Web** to open this screen. Use this screen to monitor the amount of traffic generated by web services in the selected device.

Figure 34 Monitor > Network Traffic > Web



Each field is described in the following table.

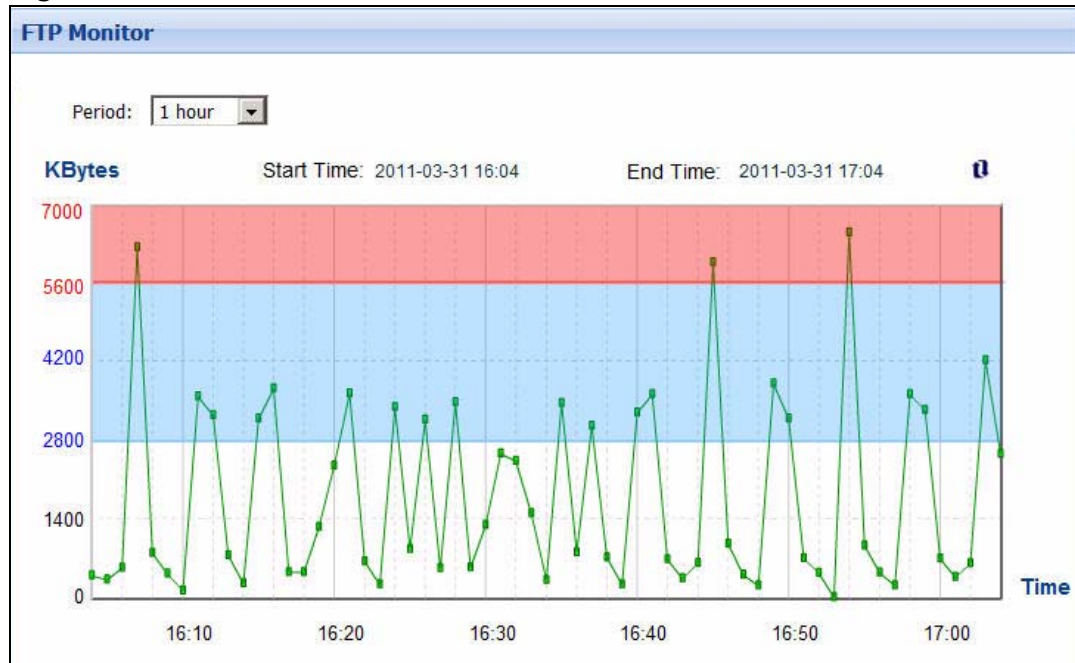
Table 22 Monitor > Network Traffic > Web

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of the selected service traffic that is handled by the selected device at various time. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.10 FTP Monitor

Click **Monitor > Network Traffic > FTP** to open this screen. Use this screen to monitor the amount of traffic generated by FTP services in the selected device.

Figure 35 Monitor > Network Traffic > FTP



Each field is described in the following table.

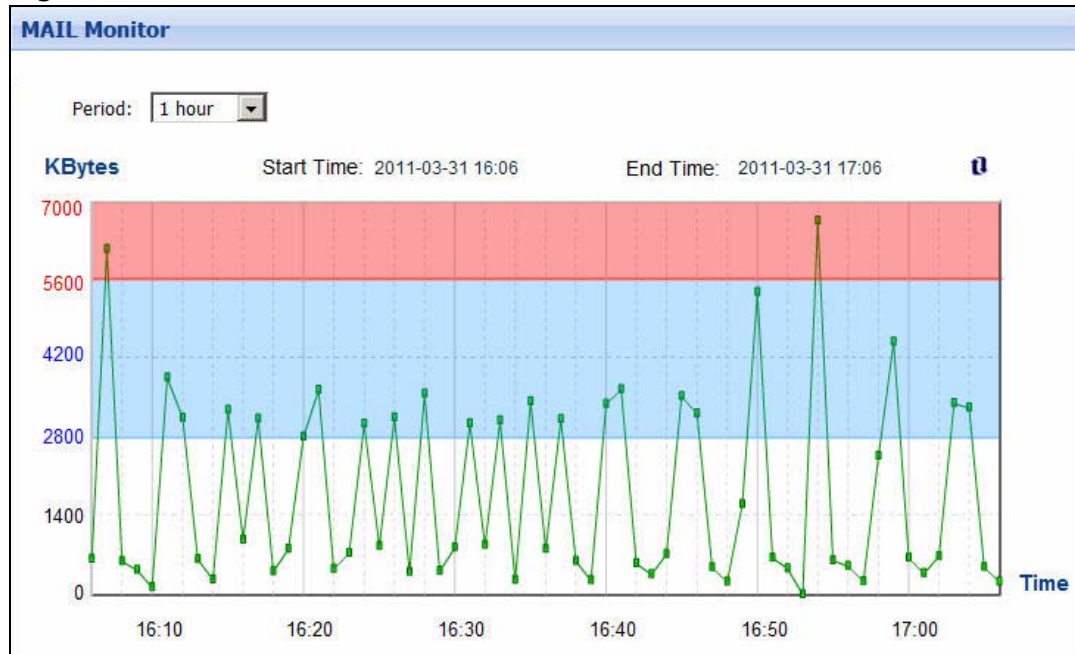
Table 23 Monitor > Network Traffic > FTP

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of the selected service traffic that is handled by the selected device at various time. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.11 E-Mail Monitor

Click **Monitor > Network Traffic > Mail** to open this screen. Use this screen to monitor the amount of traffic generated by E-Mail services in the selected device.

Figure 36 Monitor > Network Traffic > Mail



Each field is described in the following table.

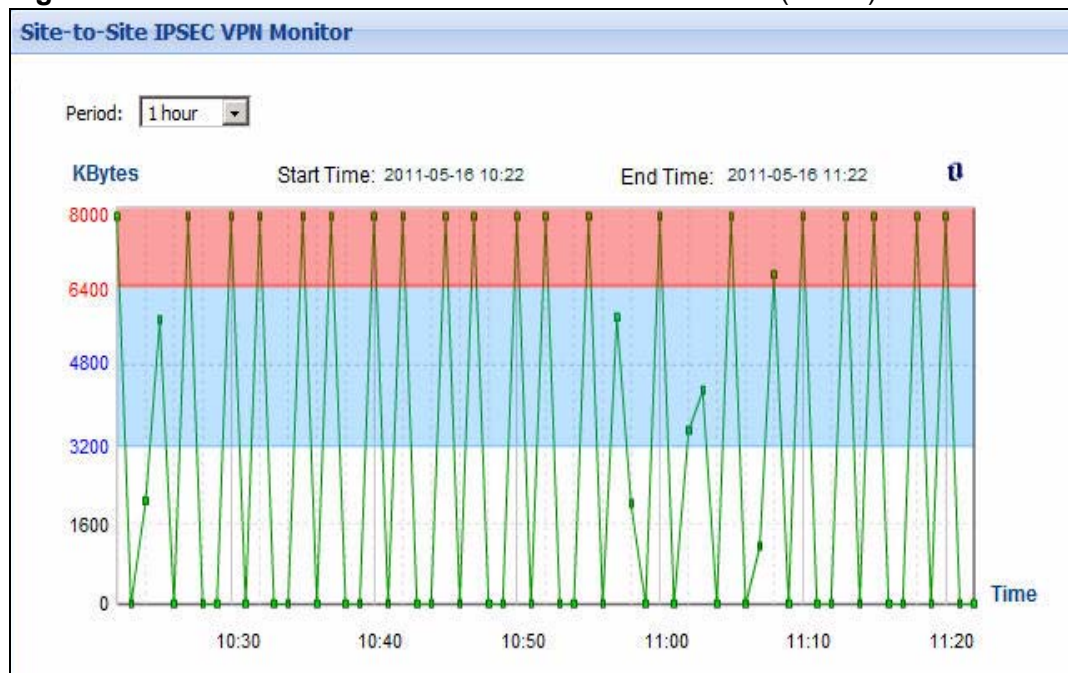
Table 24 Monitor > Network Traffic > Mail

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of the selected service traffic that is handled by the selected device at various time. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.12 Site to Site (IPSec) VPN Monitor

Click **Monitor > Secure Remote Access > Site-to-Site(IPSec)** to open this screen. Use this screen to monitor the amount of traffic generated by IPSec Secure Remote Access Site to Site services. in the selected device.

Figure 37 Monitor > Secure Remote Access > Site-to-Site(IPSec)



Each field is described in the following table.

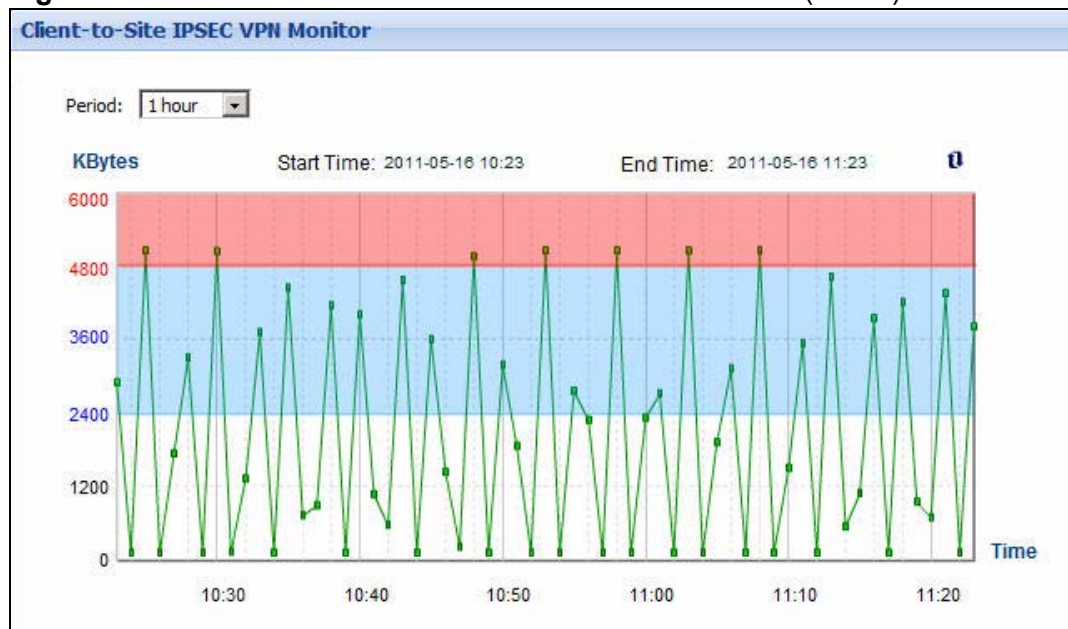
Table 25 Monitor > Secure Remote Access > Site-to-Site(IPSec)

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of the selected service traffic that is handled by the selected device at various time. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.13 Client to Site (IPSec) VPN Monitor

Click **Monitor > Secure Remote Access > Client-to-Site(IPSec)** to open this screen. Use this screen to monitor the amount of traffic generated by IPSec Secure Remote Access Client to Site in the selected device.

Figure 38 Monitor > Secure Remote Access > Client-to-Site(IPSec)



Each field is described in the following table.

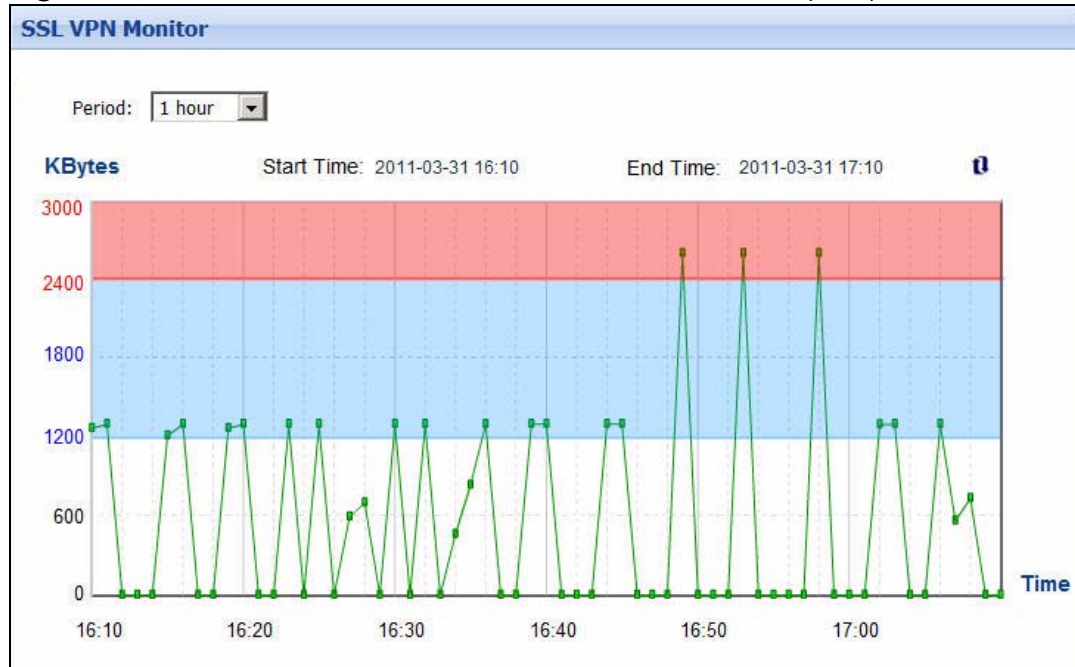
Table 26 Monitor > Secure Remote Access > Client-to-Site(IPSec)

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of the selected service traffic that is handled by the selected device at various time. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.14 Client to Site (SSL) VPN Monitor

Click **Monitor > Secure Remote Access > Client-to-Site(SSL)** to open this screen. Use this screen to monitor the amount of traffic generated by SSL Secure Remote Access in the selected device.

Figure 39 Monitor > Secure Remote Access > Client-to-Site(SSL)



Each field is described in the following table.

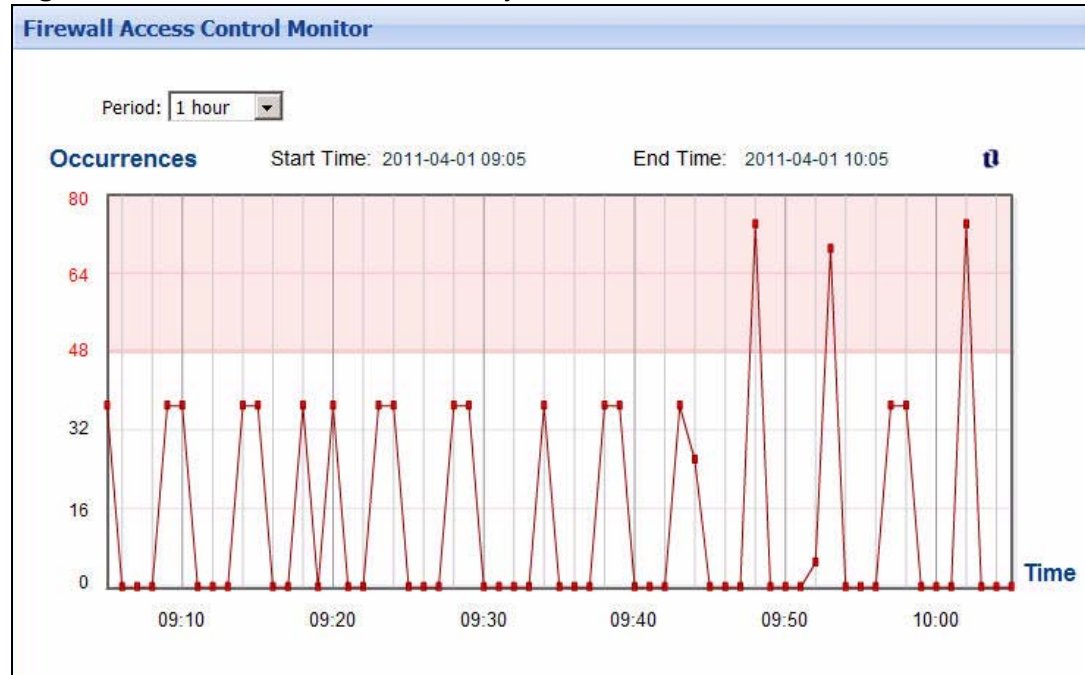
Table 27 Monitor > Secure Remote Access > Client-to-Site(SSL)

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the amount of the selected service traffic that is handled by the selected device at various time. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.15 Firewall Access Control Monitor

Click **Monitor > Network Security > Firewall Access Control** to open this screen. Use this screen to monitor the number of access attempts detected by the selected device's firewall feature.

Figure 40 Monitor > Network Security > Firewall Access Control



Each field is described in the following table.

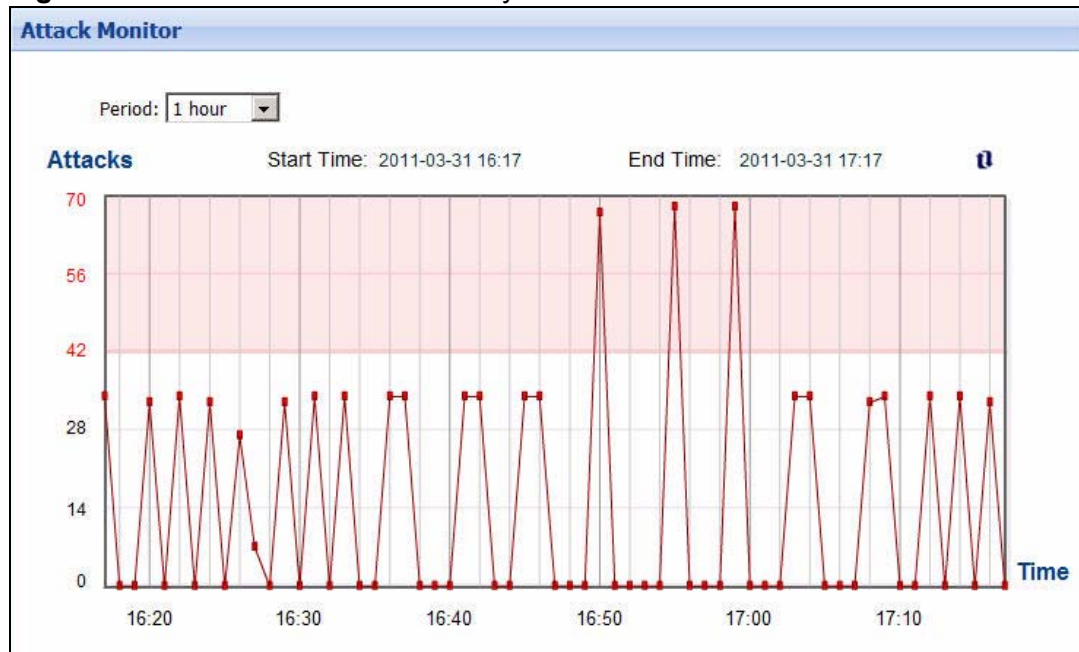
Table 28 Monitor > Network Security > Firewall Access Control

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of intrusions detected by the selected device's firewall feature at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.16 Attack Monitor

Click **Monitor > Network Security > Attack** to open this screen. Use this screen to monitor the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall.

Figure 41 Monitor > Network Security > Attack



Each field is described in the following table.

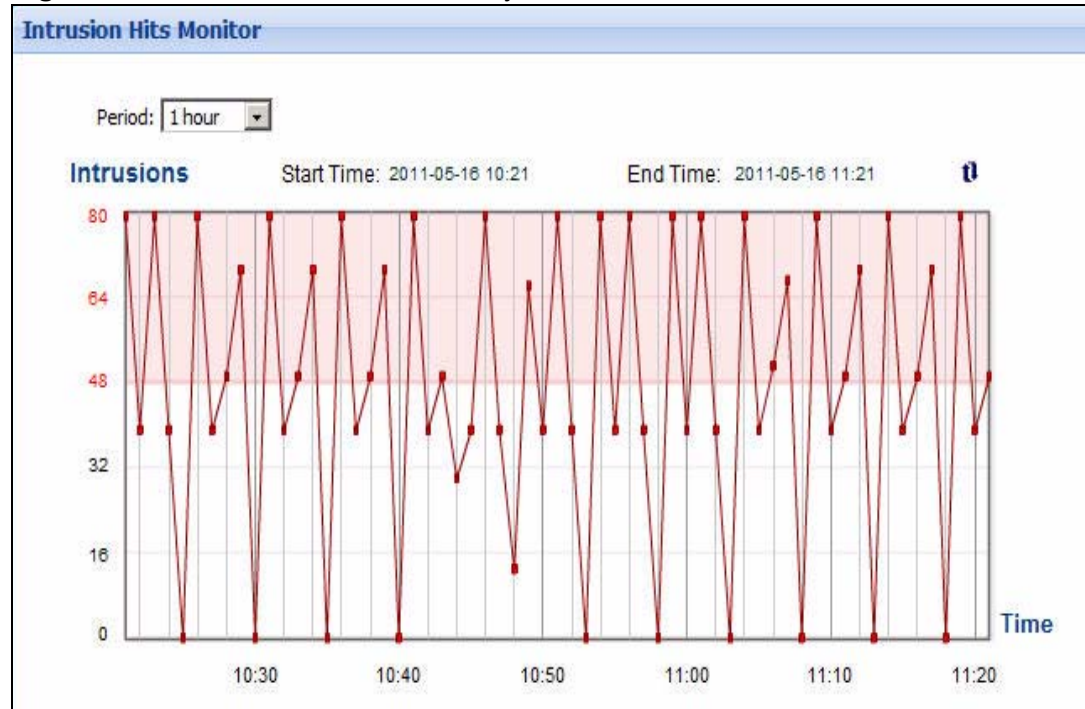
Table 29 Monitor > Network Security > Attack

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.17 Intrusion Hits

Click **Monitor > Network Security > Intrusion Hits** to open this screen. Use this screen to monitor the number of intrusions detected by the selected device's IDP feature.

Figure 42 Monitor > Network Security > Intrusion Hits



Each field is described in the following table.

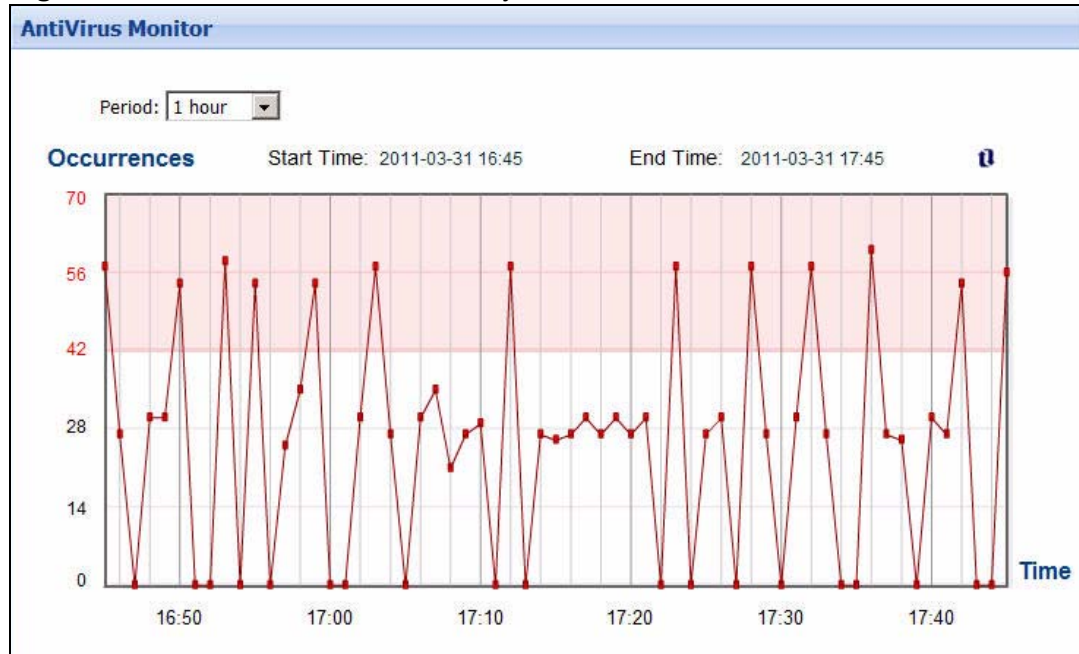
Table 30 Monitor > Network Security > Intrusion Hits

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of intrusions detected by the selected device's IDP feature at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.18 Anti-Virus Monitor

Click **Monitor** > **Network Security** > **AntiVirus** to open this screen. Use this screen to monitor the number of virus occurrences prevented by the selected device.

Figure 43 Monitor > Network Security > AntiVirus



Each field is described in the following table.

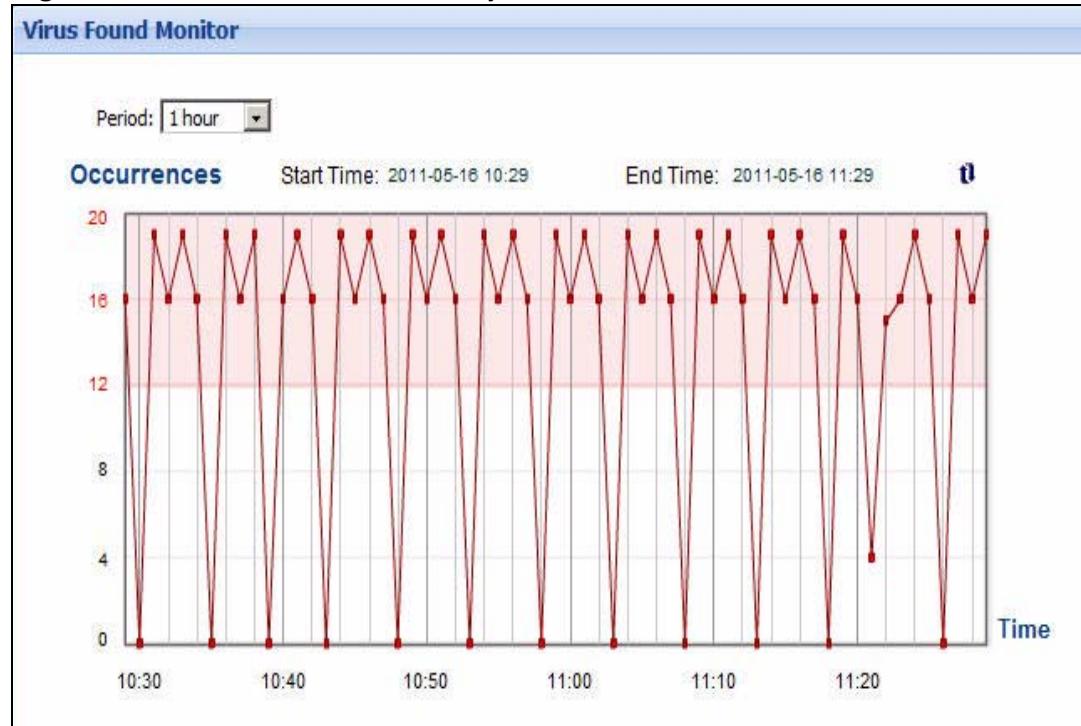
Table 31 Monitor > Network Security > AntiVirus

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of virus occurrences prevented by the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.19 E-Mail Virus Found Monitor

Click **Monitor > E-Mail Security > Virus Found** to open this screen. Use this screen to monitor the number of E-Mail virus occurrences prevented by the selected device.

Figure 44 Monitor > E-Mail Security > Virus Found



Each field is described in the following table.

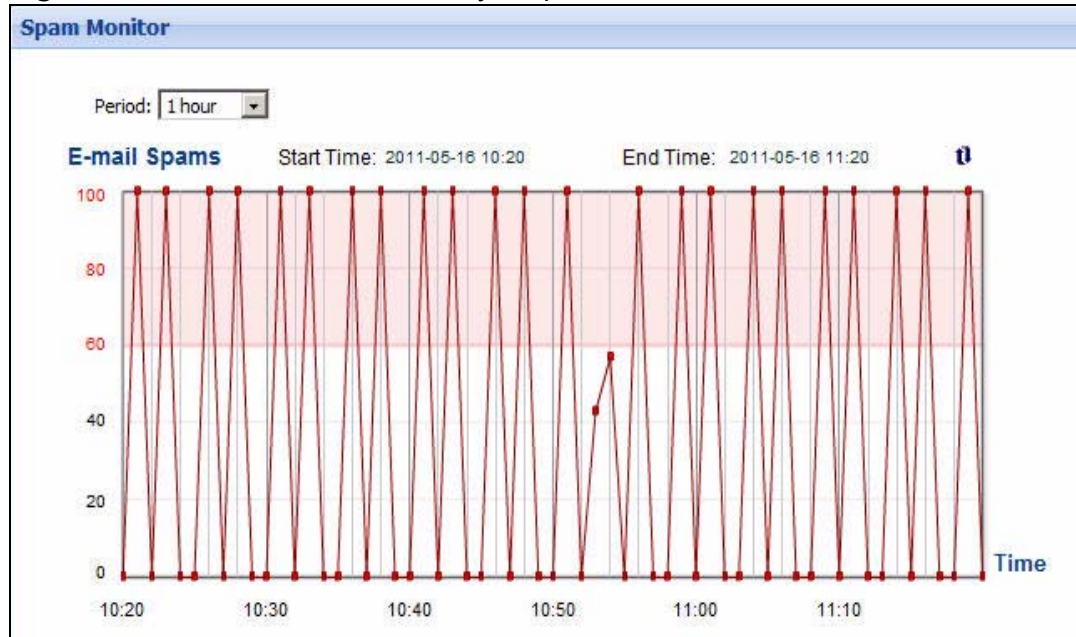
Table 32 Monitor > E-Mail Security > Virus Found

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of virus occurrences prevented by the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.20 Spam Monitor

Click **Monitor > E-Mail Security > Spam** to open this screen. Use this screen to monitor the number of spam messages stopped and recorded by the selected device.

Figure 45 Monitor > E-Mail Security > Spam



Each field is described in the following table.

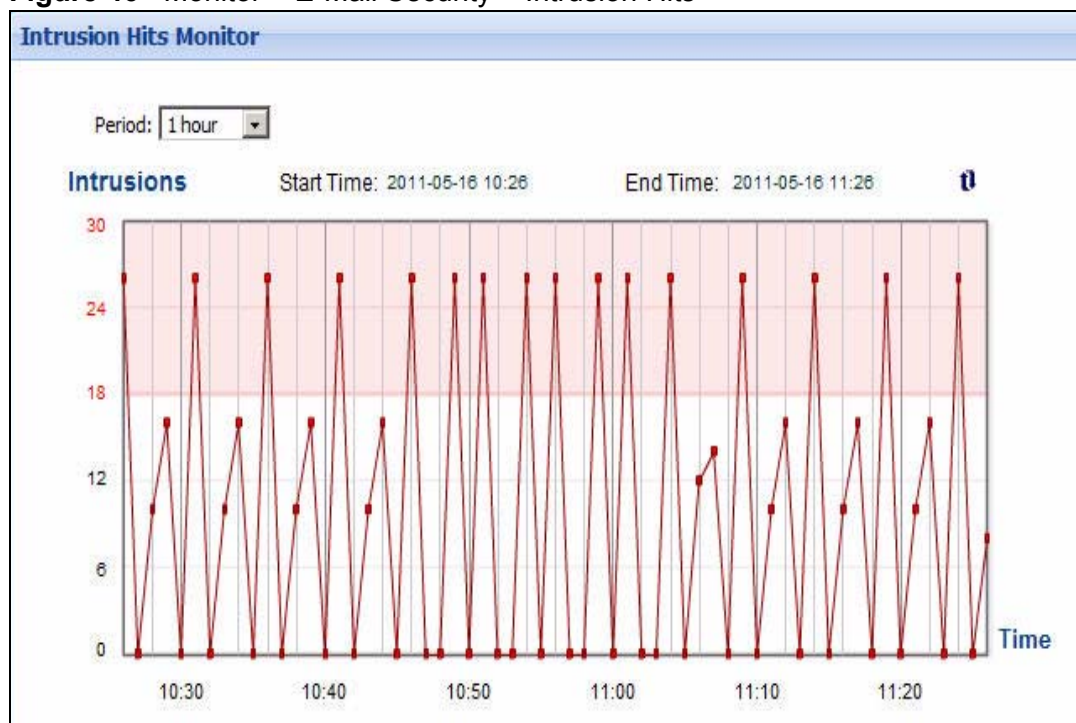
Table 33 Monitor > E-Mail Security > Spam

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of spam messages stopped by the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.21 E-Mail Intrusion Hits Monitor

Click **Monitor > E-Mail Security > Intrusion Hits** to open this screen. Use this screen to monitor the number of E-Mail intrusions detected by the selected device's IDP feature.

Figure 46 Monitor > E-Mail Security > Intrusion Hits



Each field is described in the following table.

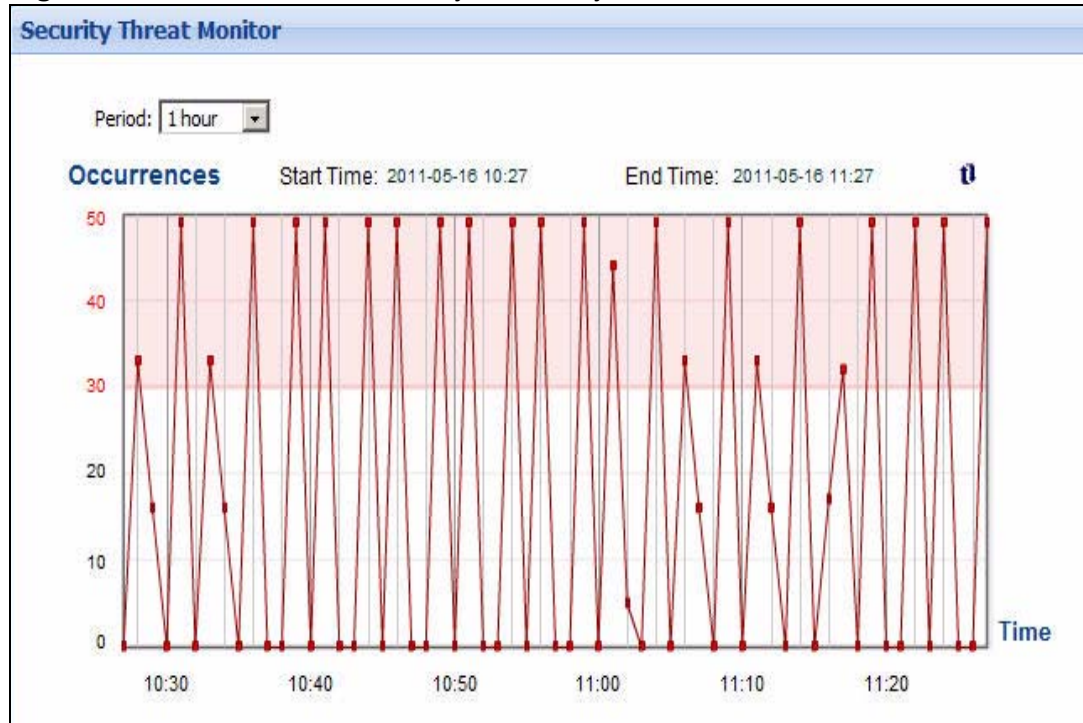
Table 34 Monitor > E-Mail Security > Intrusion Hits

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of intrusions detected by the selected device's IDP feature at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.22 Web Security - Security Threat Monitor

Click **Monitor > Web Security > Security Threat** to open this screen. Use this screen to monitor the number of web security related access attempts to web sites specified in the device's content filter feature.

Figure 47 Monitor > Web Security > Security Threat



Each field is described in the following table.

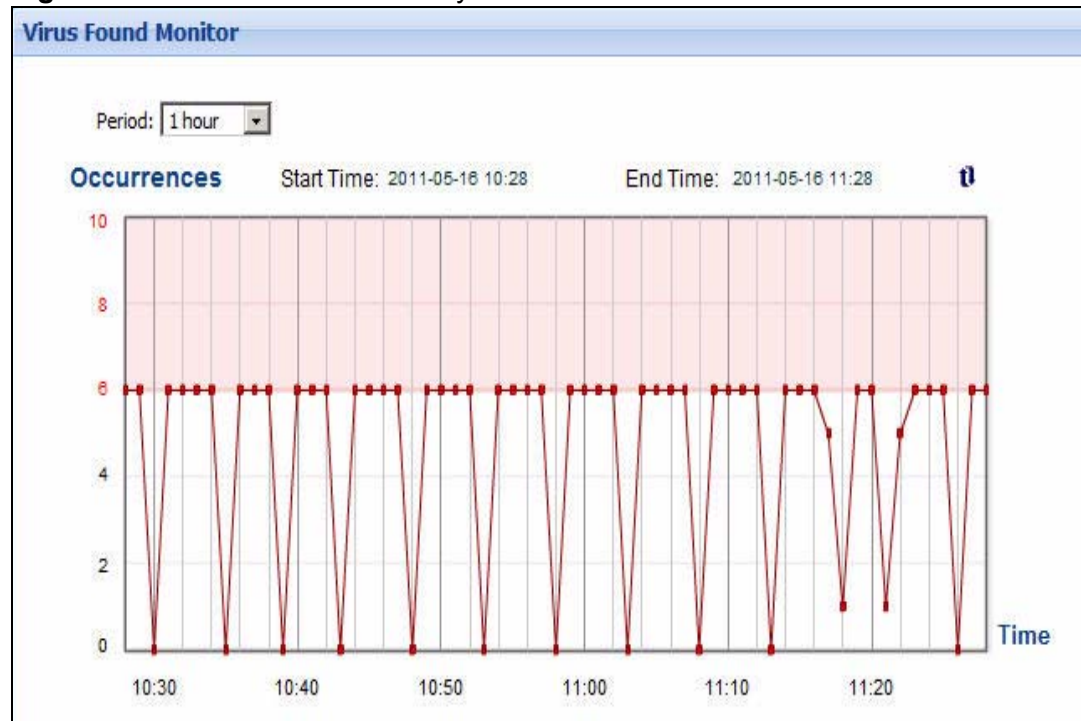
Table 35 Monitor > Web Security > Security Threat

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of web security related access attempts to specified web sites at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.23 Web Security Virus Found Monitor

Click **Monitor > Web Security > Virus Found** to open this screen. Use this screen to monitor the number of Web related virus occurrences prevented by the selected device.

Figure 48 Monitor > Web Security > Virus Found



Each field is described in the following table.

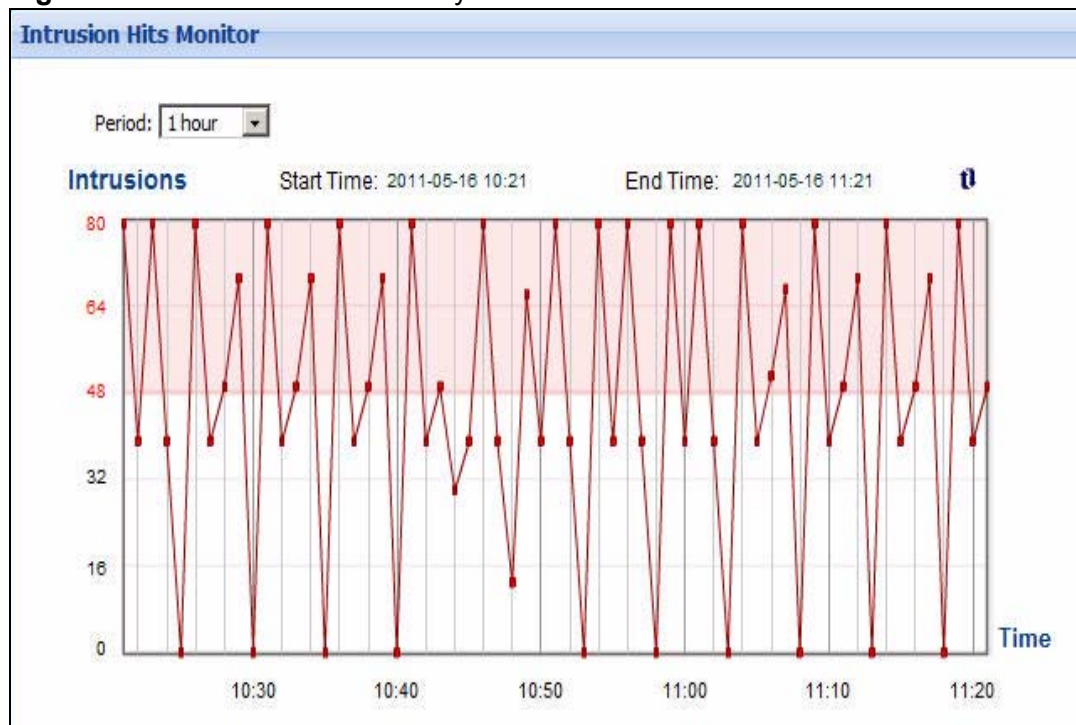
Table 36 Monitor > Web Security > Virus Found

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of virus occurrences prevented by the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.24 Web Security Intrusion Hits Monitor

Click **Monitor > Web Security > Intrusion Hits** to open this screen. Use this screen to monitor the number of web security related intrusions detected by the selected device's IDP feature.

Figure 49 Monitor > Web Security > Intrusion Hits



Each field is described in the following table.

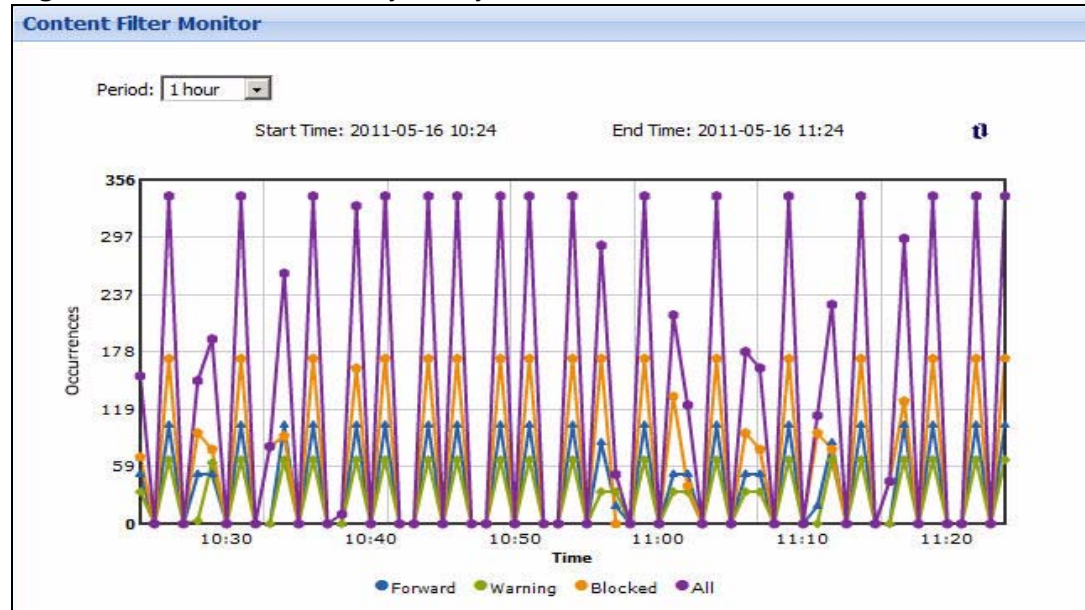
Table 37 Monitor > Web Security > Intrusion Hits

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of intrusions detected by the selected device's IDP feature at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.25 Content Filter Monitor

Click **Monitor > Security Policy Enforcement > Content Filter** to open this screen. Use this screen to monitor the number of access attempts to web sites specified in the device's content filter feature.

Figure 50 Monitor > Security Policy Enforcement > Content Filter



Each field is described in the following table.

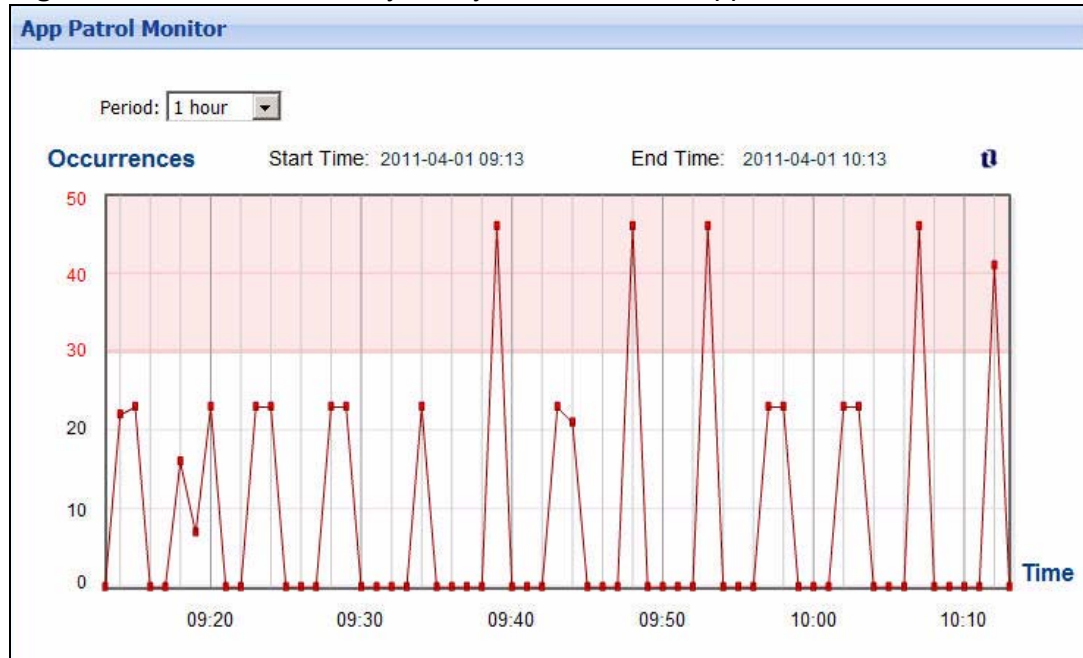
Table 38 Monitor > Security Policy Enforcement > Content Filter

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of access attempts to specified web sites at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

4.26 Application Patrol Monitor

Click **Monitor > Security Policy Enforcement > App Patrol** to open this screen. Use this screen to monitor the number of application access attempts detected by the selected device's App Patrol feature.

Figure 51 Monitor > Security Policy Enforcement > App Patrol



Each field is described in the following table.

Table 39 Monitor > Security Policy Enforcement > App Patrol

LABEL	DESCRIPTION
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the Period field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
	The Refresh icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of access attempts detected by the selected device's App Patrol feature at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the Period field.

Network Traffic

This chapter discusses how you can check the reports for the top sources and destinations of traffic for web, FTP, POP3/SMTP, and other protocols.

5.1 Bandwidth

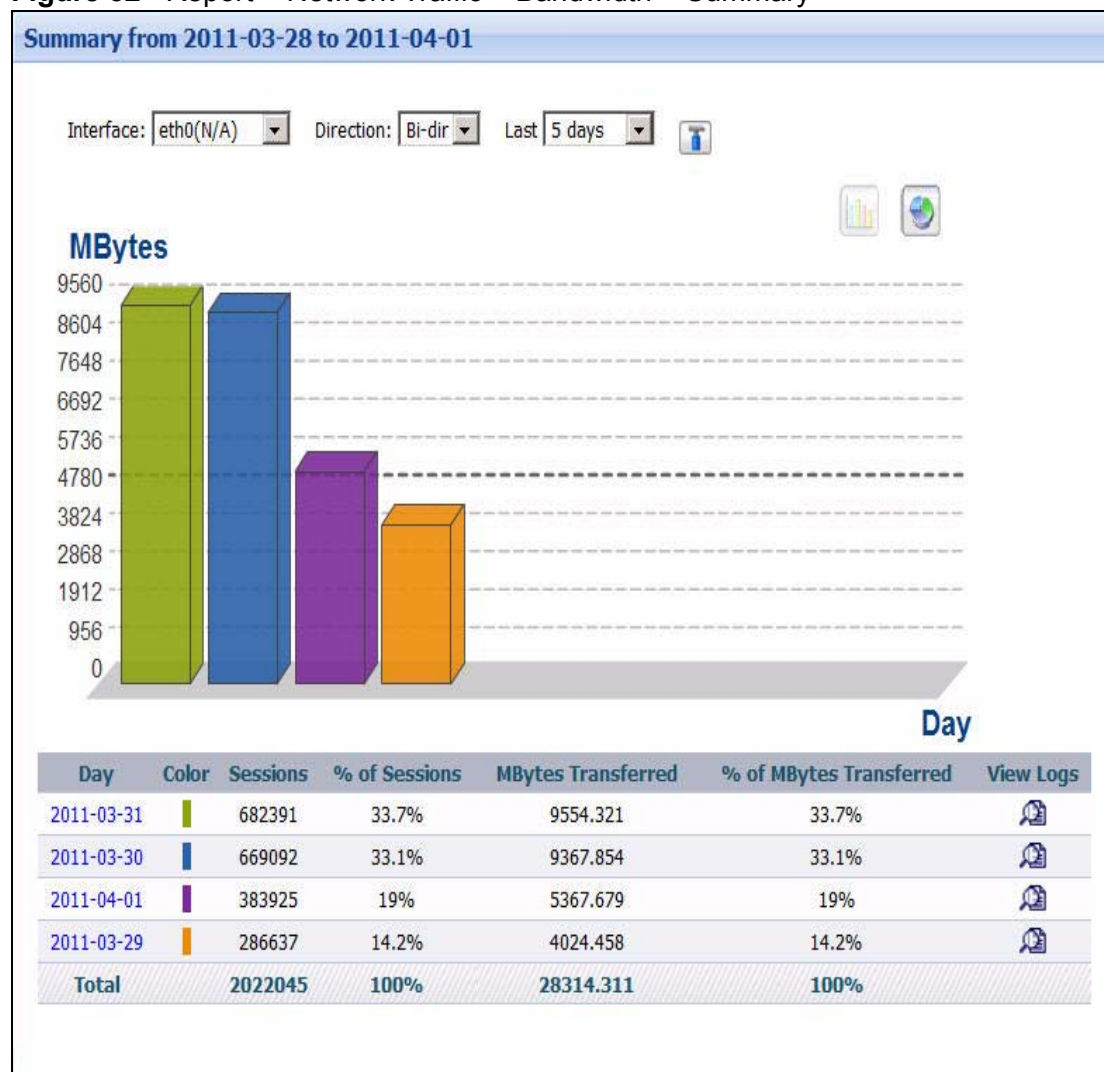
These reports look at how much traffic was handled by ZyXEL devices, who used the most bandwidth in a ZyXEL device, and which protocols were used. You can also look at traffic in various directions.

5.1.1 Bandwidth Summary

Use this report to look at the amount of traffic handled by the selected device by time interval.

Click **Report** > **Network Traffic** > **Bandwidth** > **Summary** to open this screen.

Figure 52 Report > Network Traffic > Bandwidth > Summary



Each field is described in the following table.

Table 40 Report > Network Traffic > Bandwidth > Summary

LABEL	DESCRIPTION
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. Bi-dir - all traffic, regardless of direction Rx - all traffic received on the device Tx - all traffic sent from the device For models where no Interface field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. All - all traffic, regardless of direction INBOUND - all traffic routed from the WAN OUTBOUND - all traffic routed to the WAN
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 40 Report > Network Traffic > Bandwidth > Summary

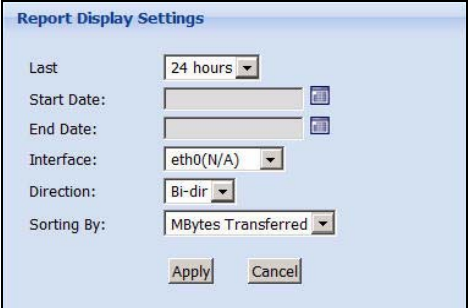
LABEL	DESCRIPTION
Settings	Use these fields or Last ... Days to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. The Interface and Direction fields are the same as in the main screen. You can display the report sorting by the MBytes Transferred, Sessions or Date/Time fields selected from the Sorting By field. These fields reset to their default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays the time intervals sorting by the amount of traffic transmitted in the period accordingly. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top services by amount of traffic in the selected time interval.
Color	This field displays what color represents each record (time interval) in the graph.
Sessions	This field displays the number of traffic events in each interval.
% of Sessions	This field displays what percentage each record's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled in each time interval.

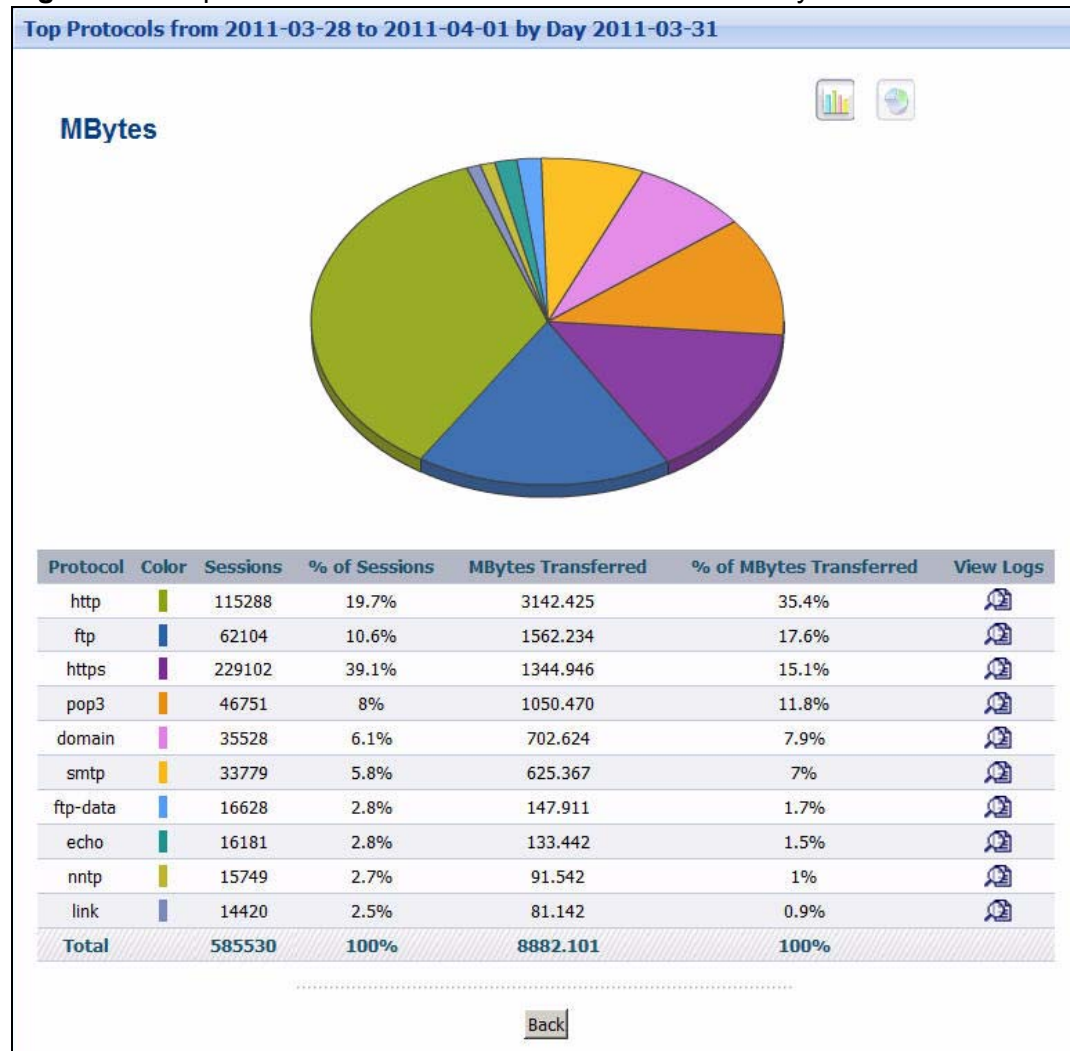
Table 40 Report > Network Traffic > Bandwidth > Summary

LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage each record's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the records above.

5.1.2 Bandwidth Summary Drill-Down

Use this report to look at the top services in a specific time interval.

Click on a specific time interval in **Report > Network Traffic > Bandwidth > Summary** to open this screen.

Figure 53 Report > Network Traffic > Bandwidth > Summary > Drill-Down

Each field is described in the following table.

Table 41 Report > Network Traffic > Bandwidth > Summary > Drill-Down

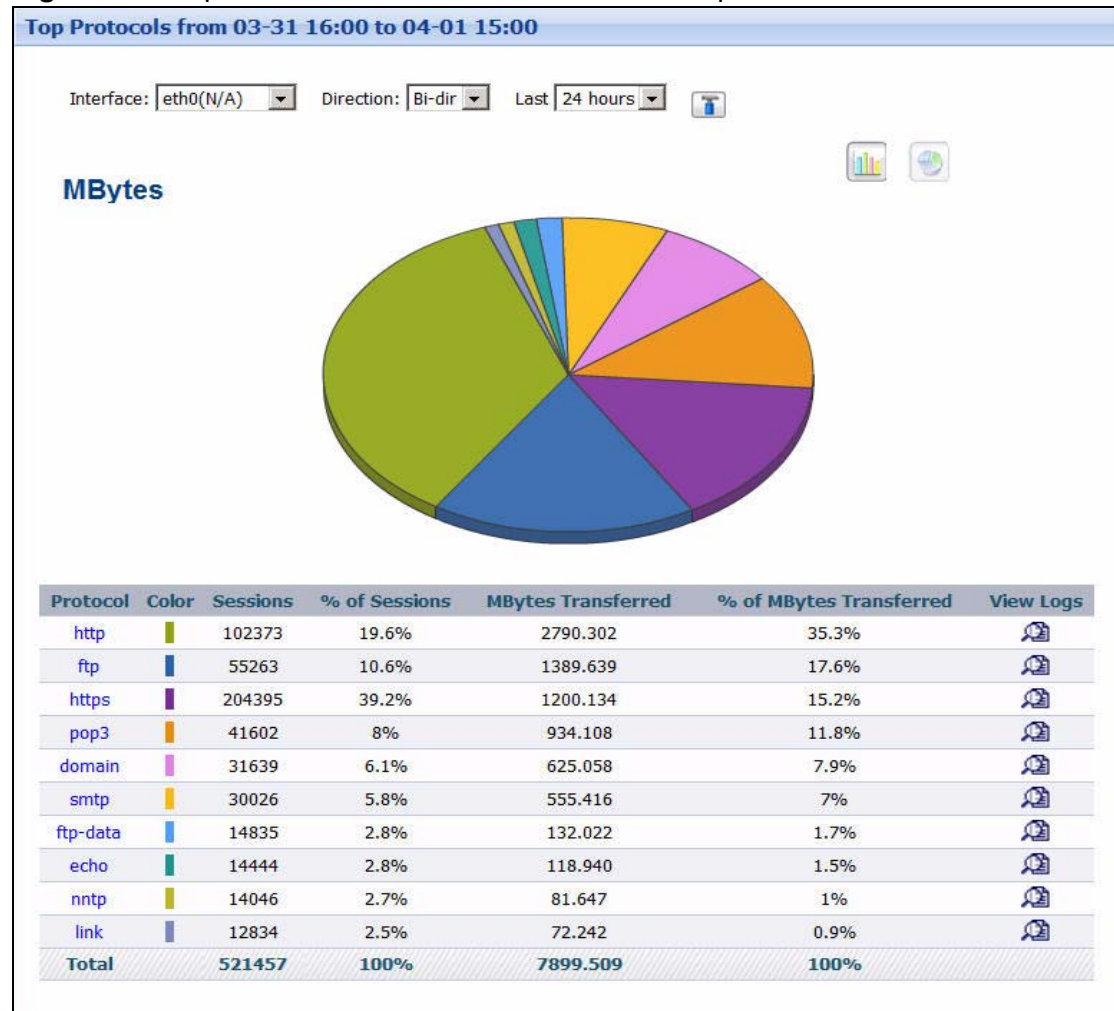
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services in the selected time interval, sorted by the amount of traffic attributed to each one. These services may be different than the ones you manage in the Service Settings screen.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service in the selected time interval.
% of Sessions	This field displays what percentage each service's number of traffic events makes out of the time interval's total number of traffic events.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each service in the selected time interval.
% of MBytes Transferred	This field displays what percentage of the time interval's total traffic belonged to each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. If the number of services in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.1.3 Bandwidth Top Protocols

Use this report to look at the top services generating traffic through the selected device.

Click **Report > Network Traffic > Bandwidth > Top Protocols** to open this screen.

Figure 54 Report > Network Traffic > Bandwidth > Top Protocols



Each field is described in the following table.

Table 42 Report > Network Traffic > Bandwidth > Top Protocols

LABEL	DESCRIPTION
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. Bi-dir - all traffic, regardless of direction Rx - all traffic received on the device Tx - all traffic sent from the device For models where no Interface field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. All - all traffic, regardless of direction INBOUND - all traffic routed from the WAN OUTBOUND - all traffic routed to the WAN
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 42 Report > Network Traffic > Bandwidth > Top Protocols

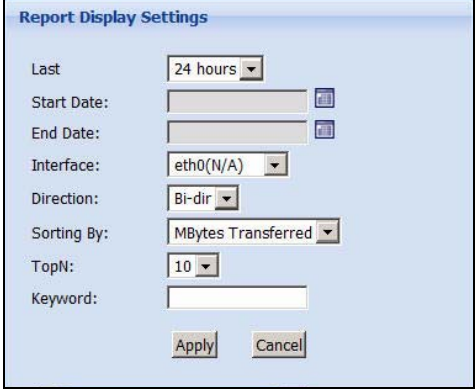
LABEL	DESCRIPTION
Settings	Use these fields or Last ... Days to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. The Interface and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Protocol field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services generating traffic through the selected device, sorted by the amount of traffic for each one. If the number of services is less than the maximum number of records displayed in this table, every service is displayed. These services may be different than the ones you manage in the Service Settings screen. Click on a service to look at the top sources of traffic for the selected service.

Table 42 Report > Network Traffic > Bandwidth > Top Protocols

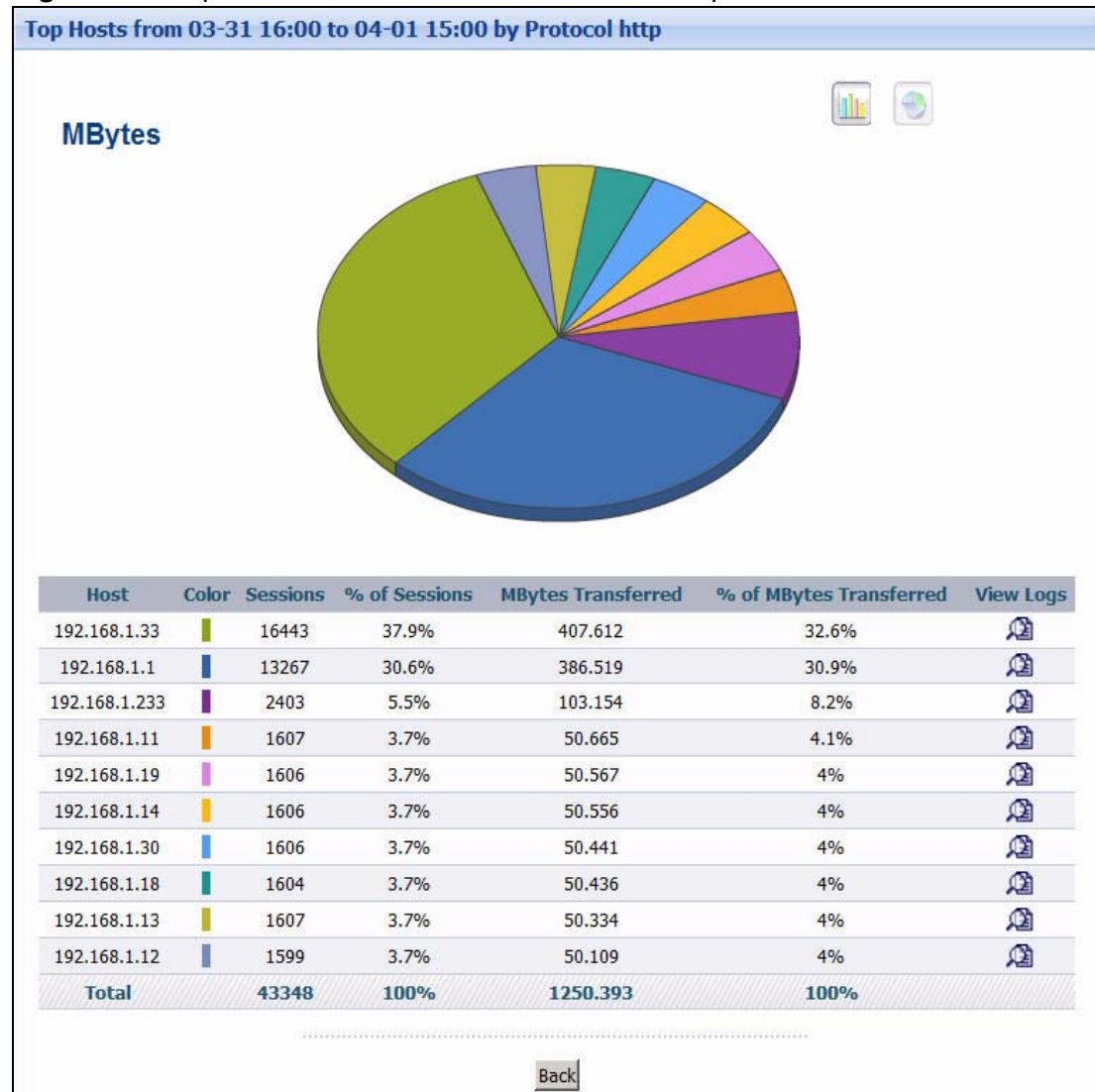
LABEL	DESCRIPTION
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service.
% of Sessions	This field displays what percentage each service's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each service generated through the selected device.
% of MBytes Transferred	This field displays what percentage each record's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above.

5.1.4 Bandwidth Top Protocols Drill-Down

Use this report to look at the top sources of traffic for any top service.

Click on a specific service in **Report > Network Traffic > Bandwidth > Top Protocols** to open this screen.

Figure 55 Report > Network Traffic > Bandwidth > Top Protocol > Drill-Down



Each field is described in the following table.

Table 43 Report > Network Traffic > Bandwidth > Top Protocol > Drill-Down

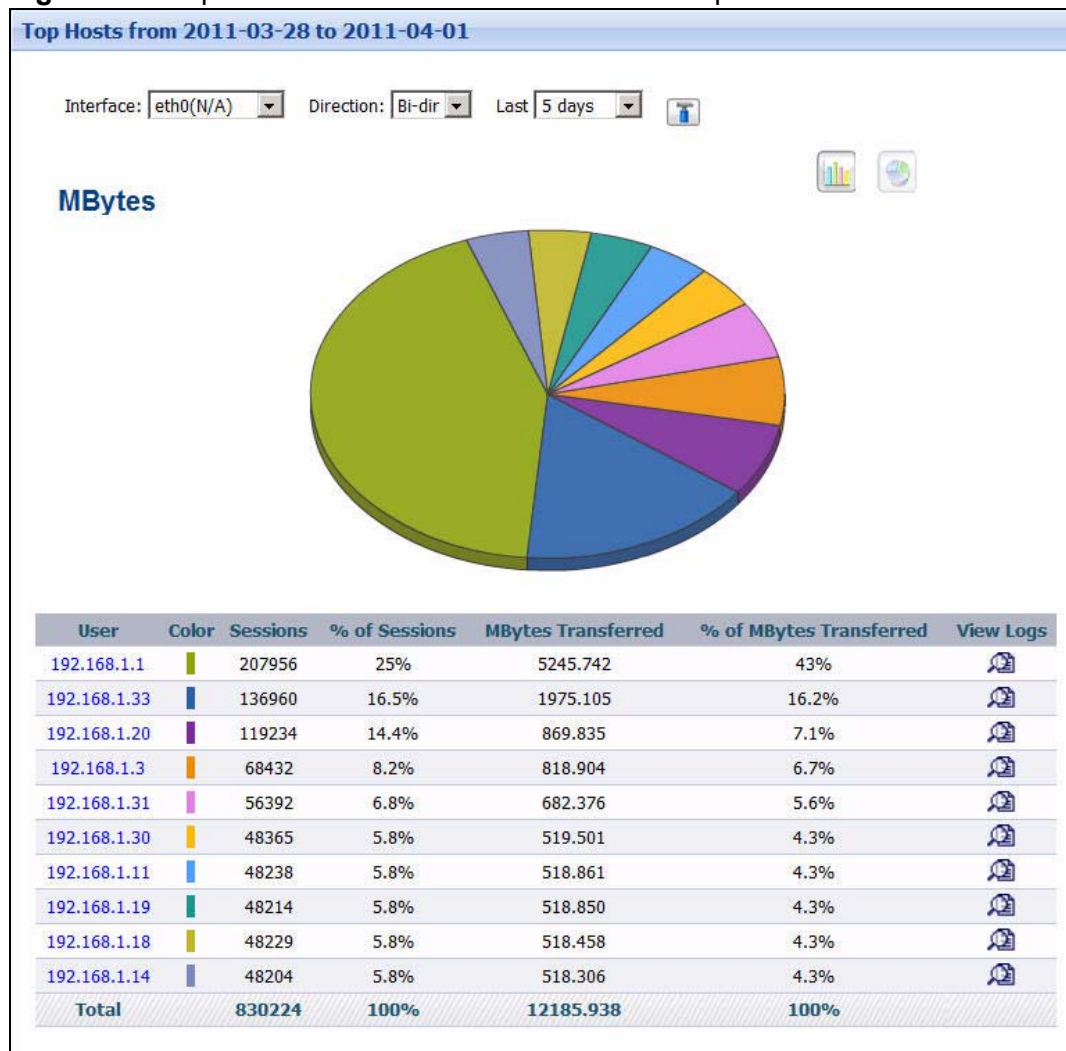
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of traffic for the selected service, sorted by the amount of traffic generated by each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events each source generated using the selected service.
% of Sessions	This field displays what percentage of the selected service's total number of traffic events came from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) each source generated using the selected service.
% of MBytes Transferred	This field displays what percentage of the selected service's total traffic came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources generating traffic using the selected service is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.1.5 Top Bandwidth Hosts

Use this report to look at the top sources of traffic in the selected device.

Click **Report > Network Traffic > Bandwidth > Top Hosts** to open this screen.

Figure 56 Report > Network Traffic > Bandwidth > Top Hosts



Each field is described in the following table.

Table 44 Report > Network Traffic > Bandwidth > Top Hosts

LABEL	DESCRIPTION
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. Bi-dir - all traffic, regardless of direction Rx - all traffic received on the device Tx - all traffic sent from the device For models where no Interface field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. All - all traffic, regardless of direction INBOUND - all traffic routed from the WAN OUTBOUND - all traffic routed to the WAN
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 44 Report > Network Traffic > Bandwidth > Top Hosts

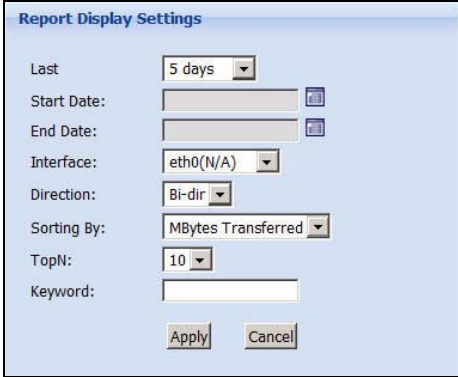
LABEL	DESCRIPTION
Settings	Use these fields or Last ... Days to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. The Interface and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 44 Report > Network Traffic > Bandwidth > Top Hosts

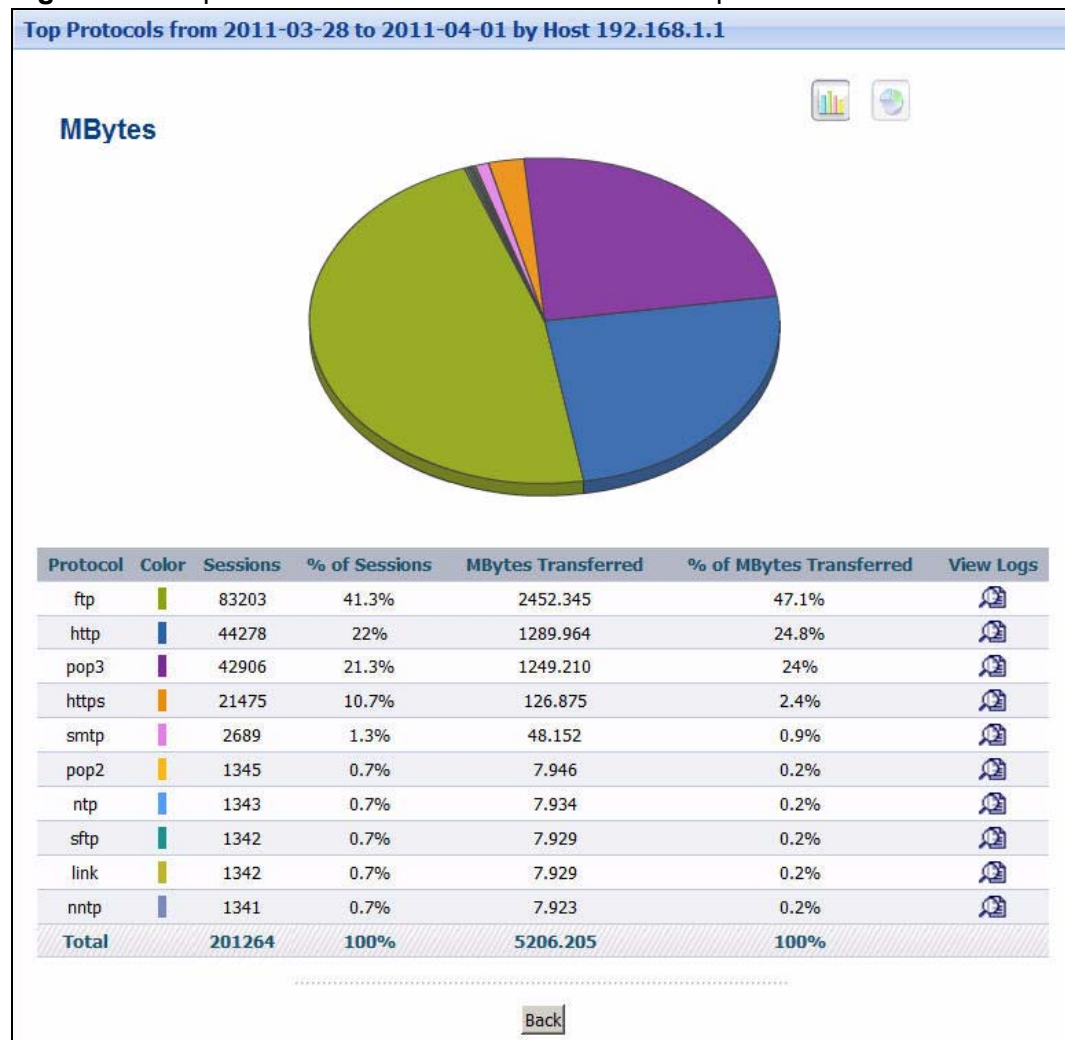
LABEL	DESCRIPTION
Host	This field displays the top sources of traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top services by amount of traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each source generated through the selected device.
% of MBytes Transferred	This field displays what percentage each record's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.1.6 Top Bandwidth Hosts Drill-Down

Use this report to look at the top services used by any top source.

Click on a specific source in **Report > Network Traffic > Bandwidth > Top Hosts** to open this screen.

Figure 57 Report > Network Traffic > Bandwidth > Top Hosts > Drill-Down



Each field is described in the following table.

Table 45 Report > Network Traffic > Bandwidth > Top Hosts > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services used by the selected source, sorted by the amount of traffic attributed to each one. These services may be different than the ones you manage in the Service Settings screen.

Table 45 Report > Network Traffic > Bandwidth > Top Hosts > Drill-Down

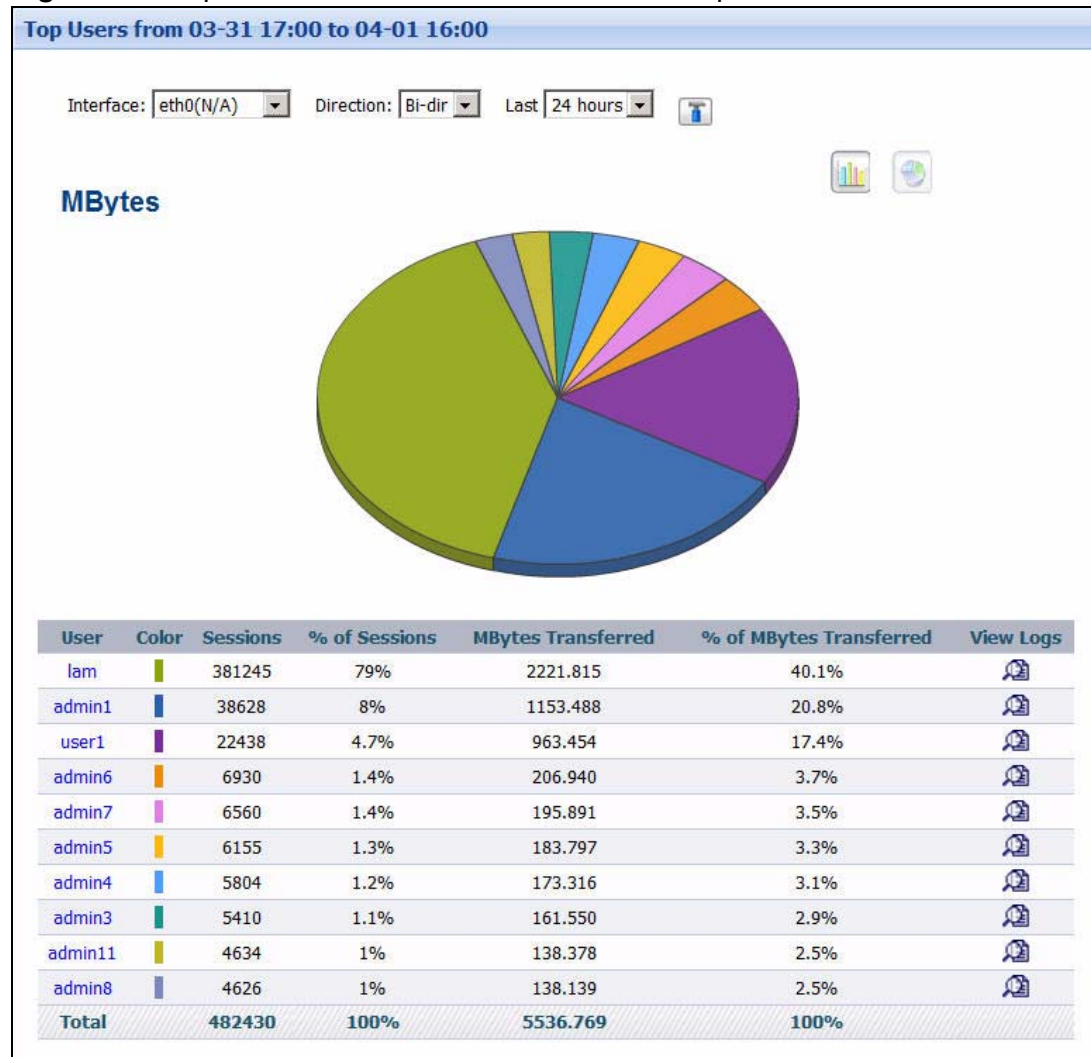
LABEL	DESCRIPTION
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events the selected source generated using each service.
% of Sessions	This field displays what percentage of the selected source's total number of traffic events belong to each service.
MBytes Transferred	This field displays how much traffic (in megabytes) the selected source generated using each service.
% of MBytes Transferred	This field displays what percentage of the selected source's total traffic belongs to each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. If the number of services used by the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.1.7 Top Bandwidth Users

Use this report to look at the selected device's logged-in users with the most traffic.

Click **Report > Network Traffic > Bandwidth > Top Users** to open this screen.

Figure 58 Report > Network Traffic > Bandwidth > Top Users



Each field is described in the following table.

Table 46 Report > Network Traffic > Bandwidth > Top Users

LABEL	DESCRIPTION
Interface	Select the logical interface for which you want to view bandwidth usage.
Direction	Select which kind of traffic, by direction, you want to look at. Bi-dir - all traffic, regardless of direction Rx - all traffic received on the device Tx - all traffic sent from the device

Table 46 Report > Network Traffic > Bandwidth > Top Users

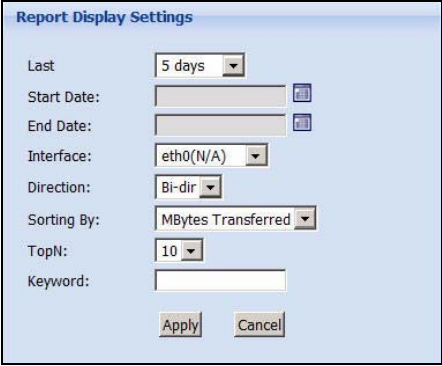
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. The Interface and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 46 Report > Network Traffic > Bandwidth > Top Users

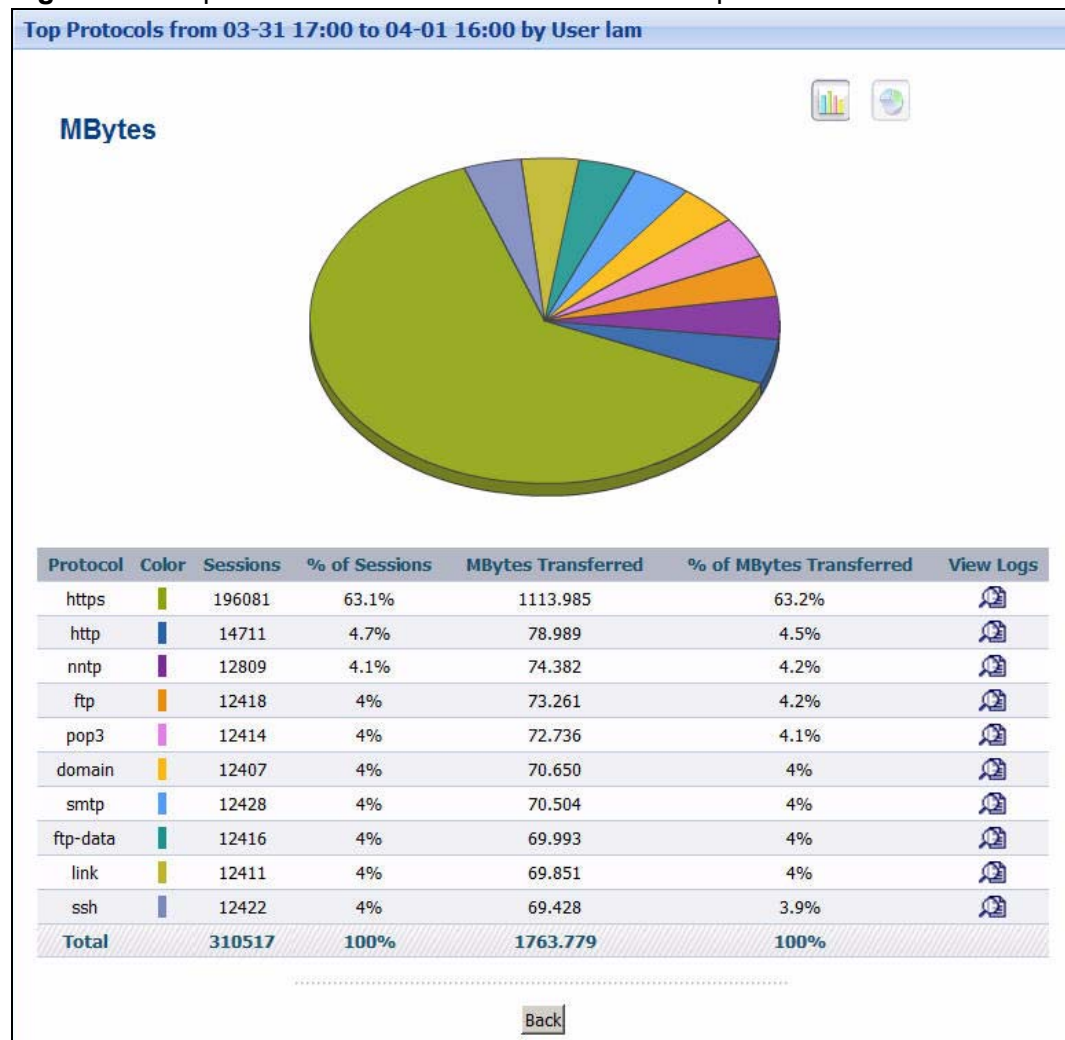
LABEL	DESCRIPTION
User	This field displays the users with the most traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click a user name to look at the top services by amount of traffic for the selected user.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each user generated through the selected device.
% of MBytes Transferred	This field displays what percentage each user's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

5.1.8 Top Bandwidth Users Drill-Down

Use this report to look at the top services used by any top bandwidth user.

Click on a specific user in **Report > Network Traffic > Bandwidth > Top Users** to open this screen.

Figure 59 Report > Network Traffic > Bandwidth > Top Users > Drill-Down



Each field is described in the following table.

Table 47 Report > Network Traffic > Bandwidth > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services used by the selected user, sorted by the amount of traffic attributed to each one. These services may be different than the ones you manage in the Service Settings screen.

Table 47 Report > Network Traffic > Bandwidth > Top Users > Drill-Down

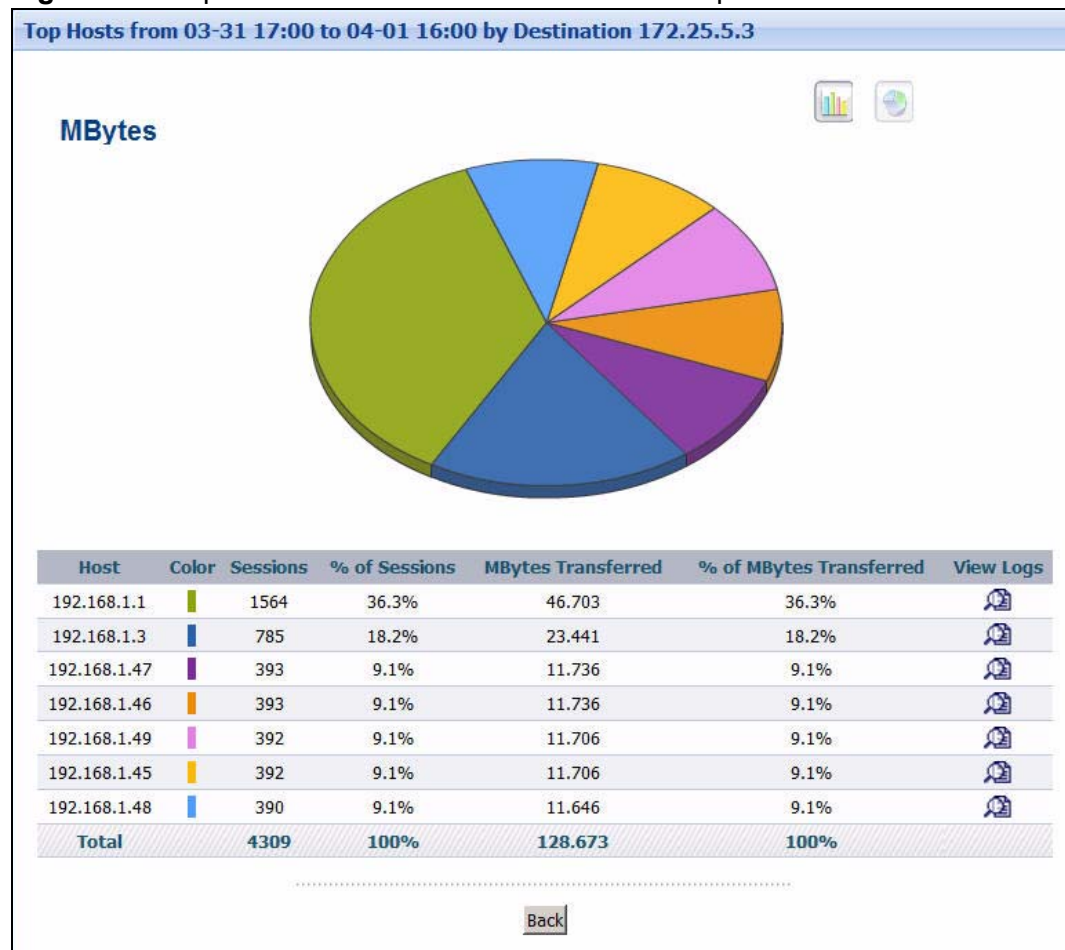
LABEL	DESCRIPTION
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events the selected user generated using each service.
% of Sessions	This field displays what percentage of the selected user's total number of traffic events was generated using each service.
MBytes Transferred	This field displays how much traffic (in megabytes) the selected user generated using each service.
% of MBytes Transferred	This field displays what percentage of the selected user's total traffic belonged to each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. If the number of services used by the selected user is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.1.9 Top Bandwidth Destinations

Use this report to look at the destination IP addresses to which the selected device sent the most traffic.

Click **Report > Network Traffic > Bandwidth > Top Destinations** to open this screen.

Figure 60 Report > Network Traffic > Bandwidth > Top Destinations



Each field is described in the following table.

Table 48 Report > Network Traffic > Bandwidth > Top Destinations

LABEL	DESCRIPTION
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. Bi-dir - all traffic, regardless of direction Rx - all traffic received on the device Tx - all traffic sent from the device For models where no Interface field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. All - all traffic, regardless of direction INBOUND - all traffic routed from the WAN OUTBOUND - all traffic routed to the WAN
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 48 Report > Network Traffic > Bandwidth > Top Destinations

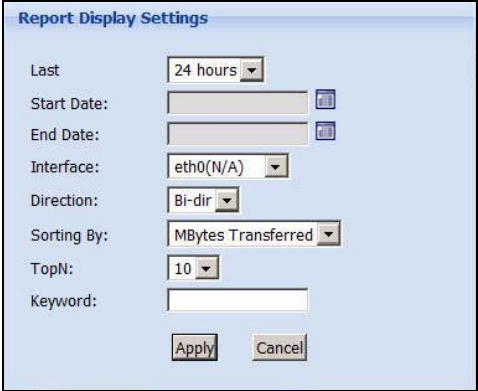
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. The Interface and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 48 Report > Network Traffic > Bandwidth > Top Destinations

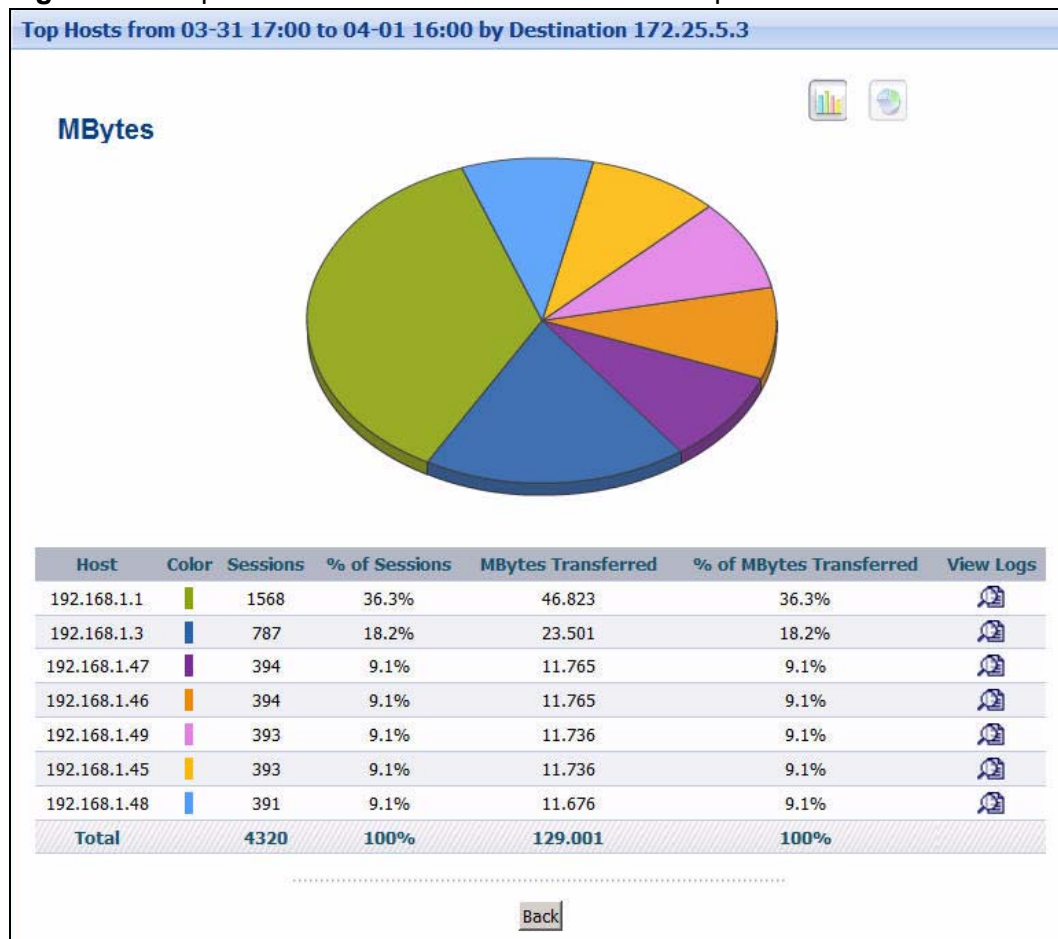
LABEL	DESCRIPTION
Destination	This field displays the destinations to which the selected device sent the most traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top sources of web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the selected device handled for each destination.
% of MBytes Transferred	This field displays what percentage of the traffic went to each destination out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

5.1.10 Top Bandwidth Destinations Drill-Down

Use this report to look at the services that were used the most (on the selected device) to access the top destination IP addresses.

Click on the link in an entry in **Report > Network Traffic > Bandwidth > Top Destinations** to open this screen.

Figure 61 Report > Network Traffic > Bandwidth > Top Destinations > Drill-Down



Each field is described in the following table.

Table 49 Report > Network Traffic > Bandwidth > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources that sent traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.

Table 49 Report > Network Traffic > Bandwidth > Top Destinations > Drill-Down

LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events was sent from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) there was for the selected destination from each source.
% of MBytes Transferred	This field displays what percentage of a destination's traffic came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. If the number of services used by the selected user is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.2 Web Traffic

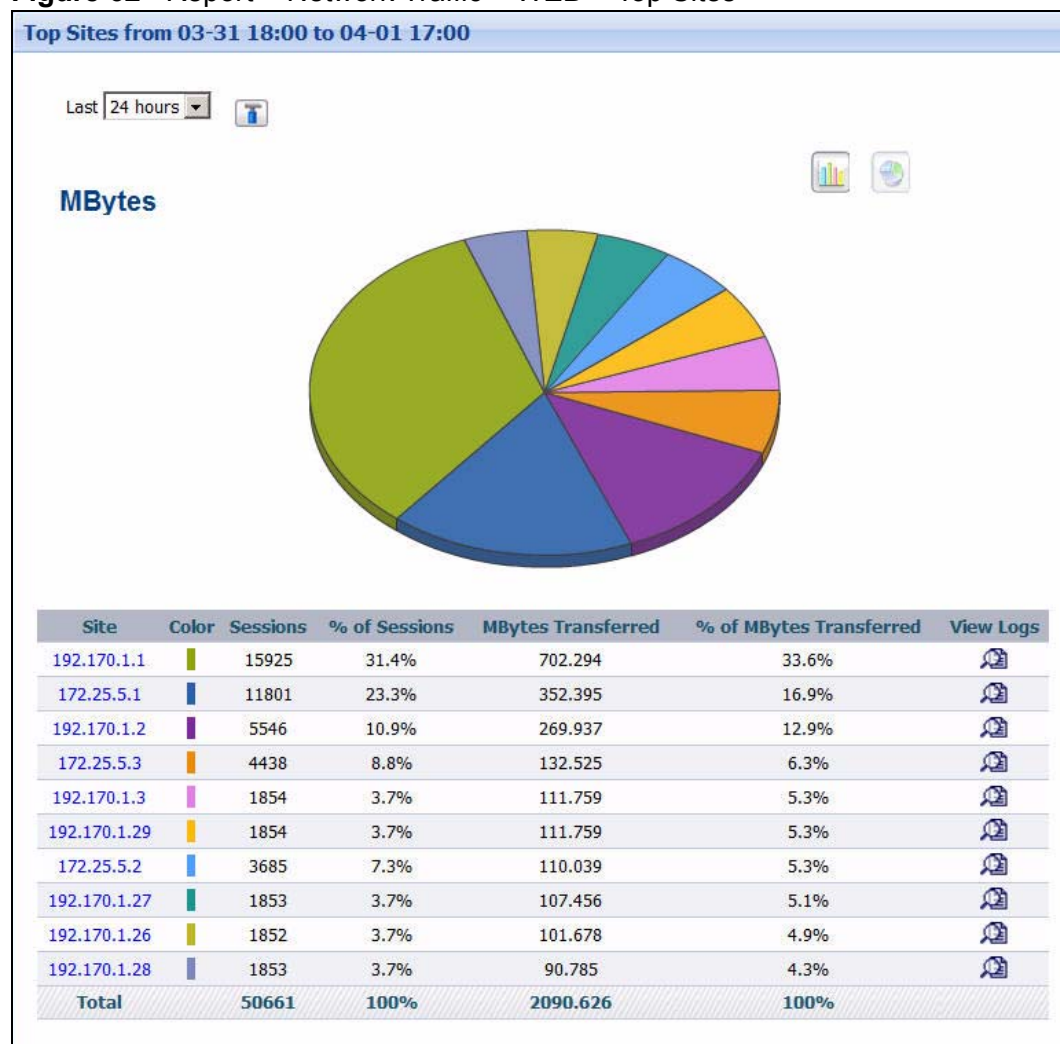
These reports look at the top destinations and sources of web traffic.

5.2.1 Top Web Sites

Use this report to look at the top destinations of web traffic.

Click **Report > Network Traffic > WEB > Top Sites** to open this screen.

Figure 62 Report > Network Traffic > WEB > Top Sites



Each field is described in the following table.

Table 50 Report > Network Traffic > WEB > Top Sites

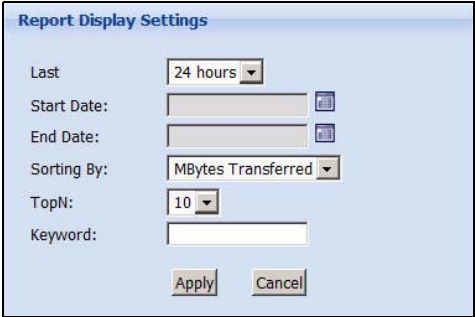
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 50 Report > Network Traffic > WEB > Top Sites

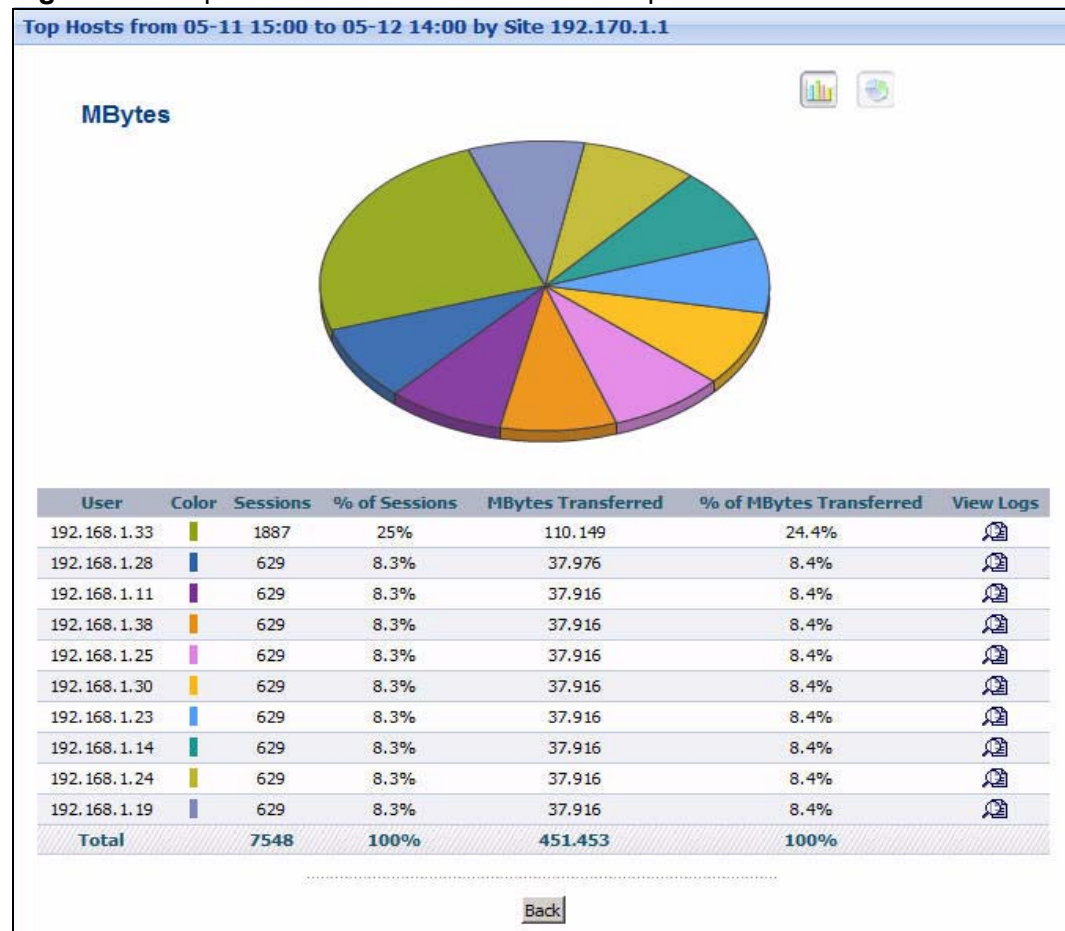
LABEL	DESCRIPTION
Site	This field displays the top destinations of web traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top sources of web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of the traffic went to each destination out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.2.2 Top Web Sites Drill-Down

Use this report to look at the top sources of web traffic for any top destination.

Click on a specific destination in **Report > Network Traffic > WEB > Top Sites** to open this screen.

Figure 63 Report > Network Traffic > WEB > Top Sites > Drill-Down



Each field is described in the following table.

Table 51 Report > Traffic > WEB > Top Sites > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.

Table 51 Report > Traffic > WEB > Top Sites > Drill-Down

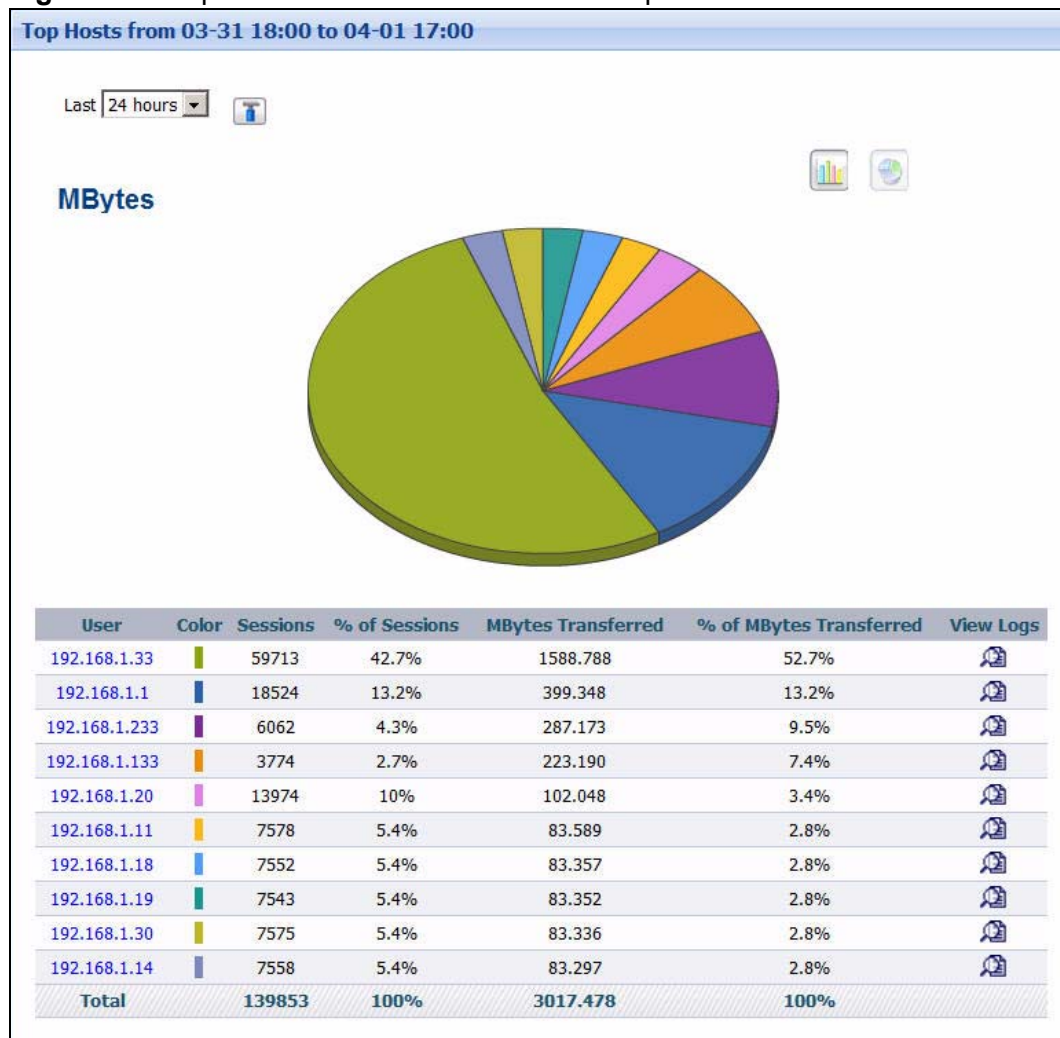
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events was sent from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's traffic was generated from each source.
Total	This entry displays the totals for the sources above. If the number of sources of web traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.2.3 Top Web Hosts

Use this report to look at the top sources of web traffic.

Click **Report > Network Traffic > WEB > Top Hosts** to open this screen.

Figure 64 Report > Network Traffic > WEB > Top Hosts



Each field is described in the following table.

Table 52 Report > Network Traffic > WEB > Top Hosts

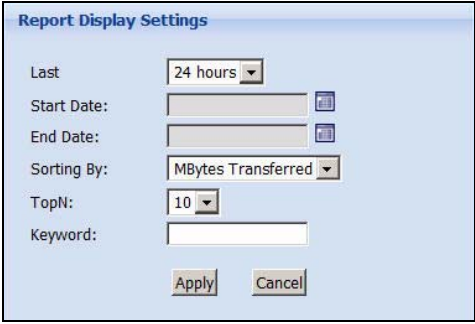
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 52 Report > Network Traffic > WEB > Top Hosts

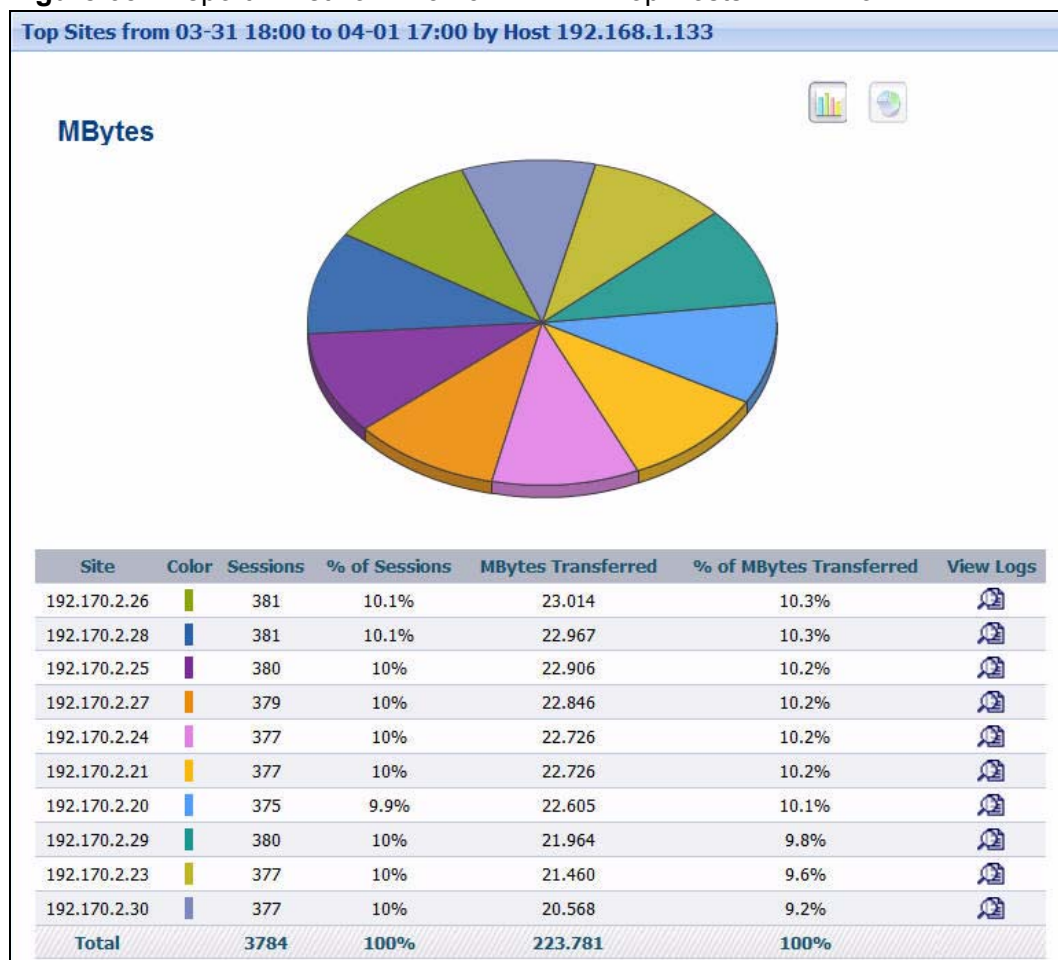
LABEL	DESCRIPTION
Host	This field displays the top sources of web traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of web traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of web traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.2.4 Top Web Hosts Drill-Down

Use this report to look at the top destinations of web traffic for any top source.

Click on a specific source in **Report > Network Traffic > WEB > Top Hosts** to open this screen.

Figure 65 Report > Network Traffic > WEB > Top Hosts > Drill-Down



Each field is described in the following table.

Table 53 Report > Network Traffic > WEB > Top Hosts > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic from the selected source, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").

Table 53 Report > Network Traffic > WEB > Top Hosts > Drill-Down

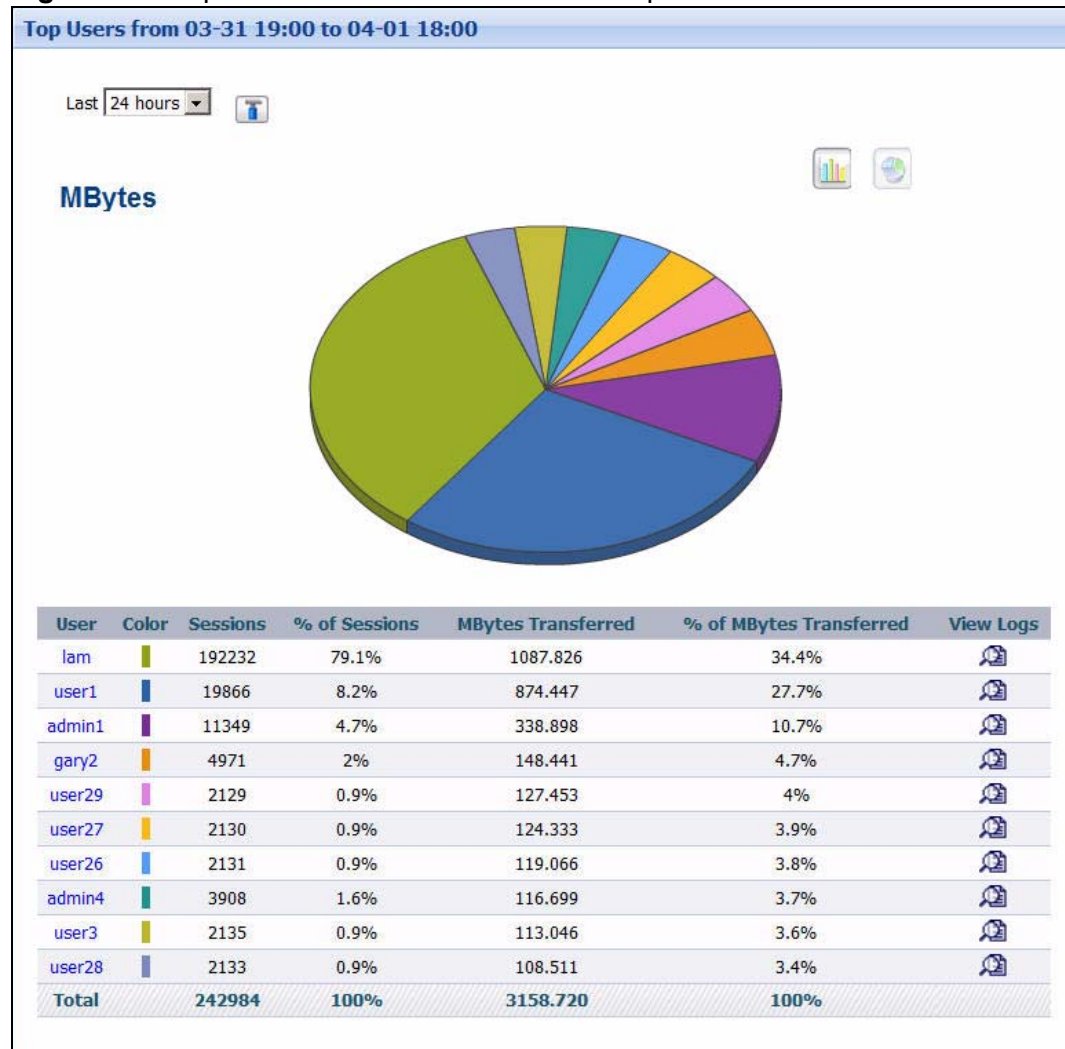
LABEL	DESCRIPTION
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected source to each destination.
% of Sessions	This field displays what percentage of the selected source's total number of traffic events was sent to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes Transferred	This field displays what percentage of the selected source's traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of web traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.2.5 Top Web Users

Use this report to look at the users that send the most web traffic.

Click **Report > Network Traffic > WEB > Top Users** to open this screen.

Figure 66 Report > Network Traffic > WEB > Top Users



Each field is described in the following table.

Table 54 Report > Network Traffic > WEB > Top Users

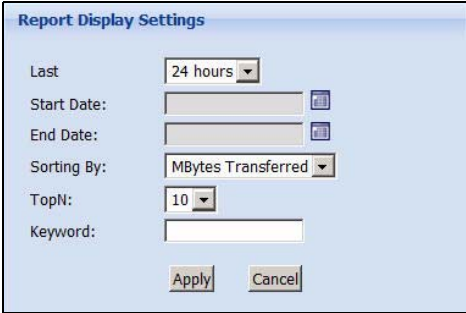
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 54 Report > Network Traffic > WEB > Top Users

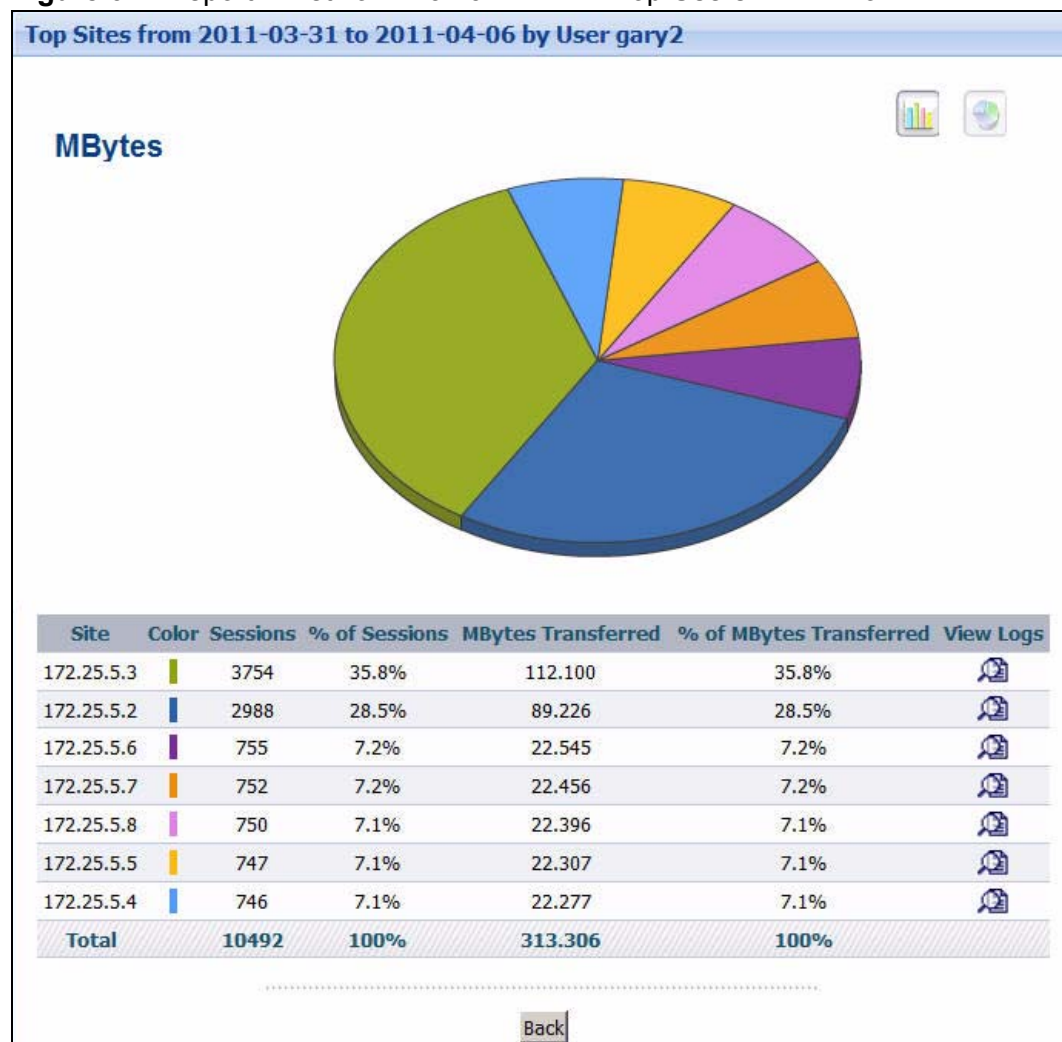
LABEL	DESCRIPTION
User	This field displays the users that send the most web traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.2.6 Top Web Users Drill-Down

Use this report to look at the top destinations of web traffic for any top user.

Click on a specific source in **Report > Network Traffic > WEB > Top Users** to open this screen.

Figure 67 Report > Network Traffic > WEB > Top Users > Drill-Down



Each field is described in the following table.

Table 55 Report > Network Traffic > WEB > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic from the selected user, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected user to each destination.
% of Sessions	This field displays what percentage of the selected user's total number of traffic events went to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected user to each destination.
% of MBytes Transferred	This field displays what percentage of the selected user's total traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.3 FTP Traffic

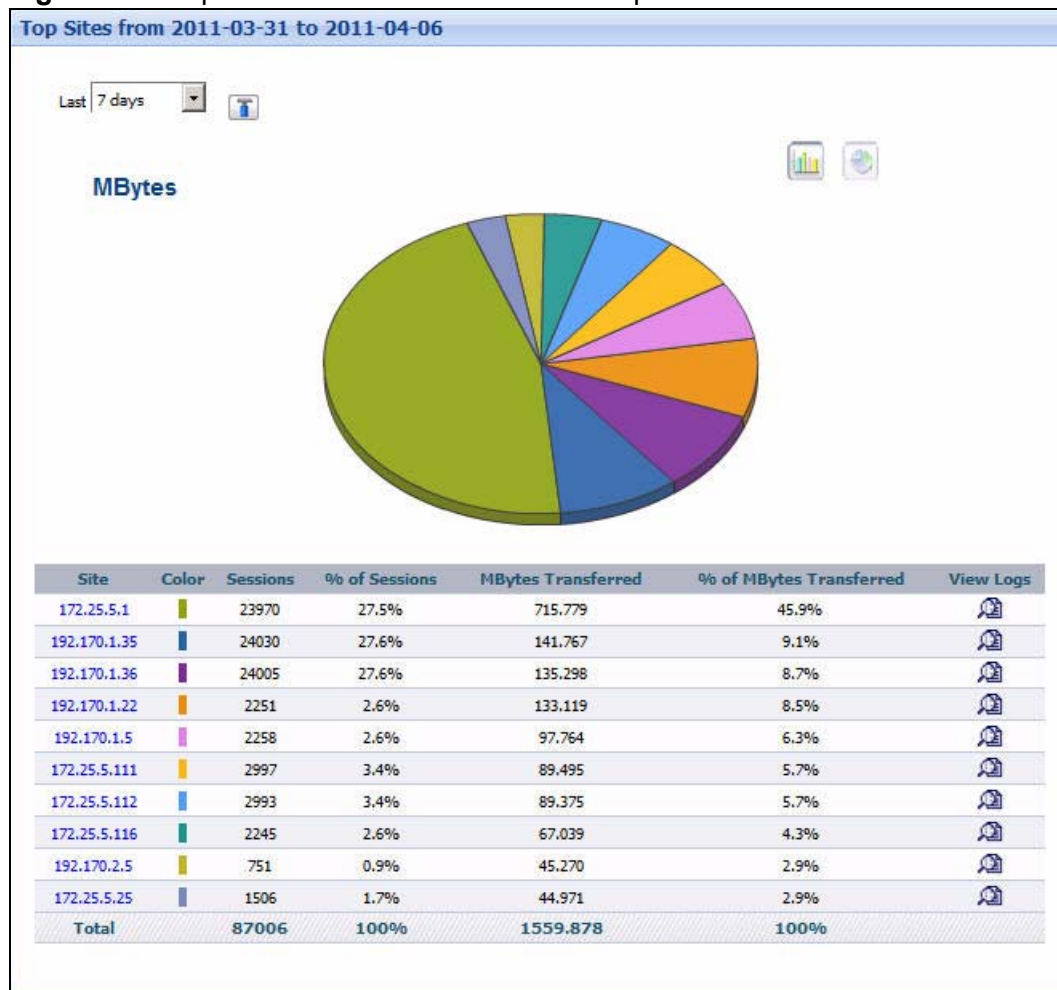
These reports look at the top destinations and sources of FTP traffic.

5.3.1 Top FTP Sites

Use this report to look at the top destinations of FTP traffic.

Click **Report > Network Traffic > FTP > Top Sites** to open this screen.

Figure 68 Report > Network Traffic > FTP > Top Sites



Each field is described in the following table.

Table 56 Report > Network Traffic > FTP > Top Sites

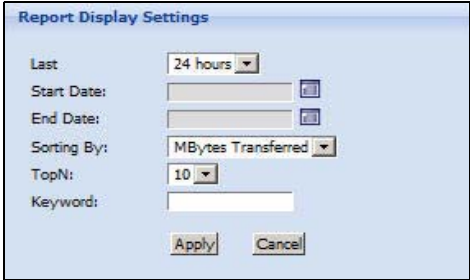
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 56 Report > Network Traffic > FTP > Top Sites

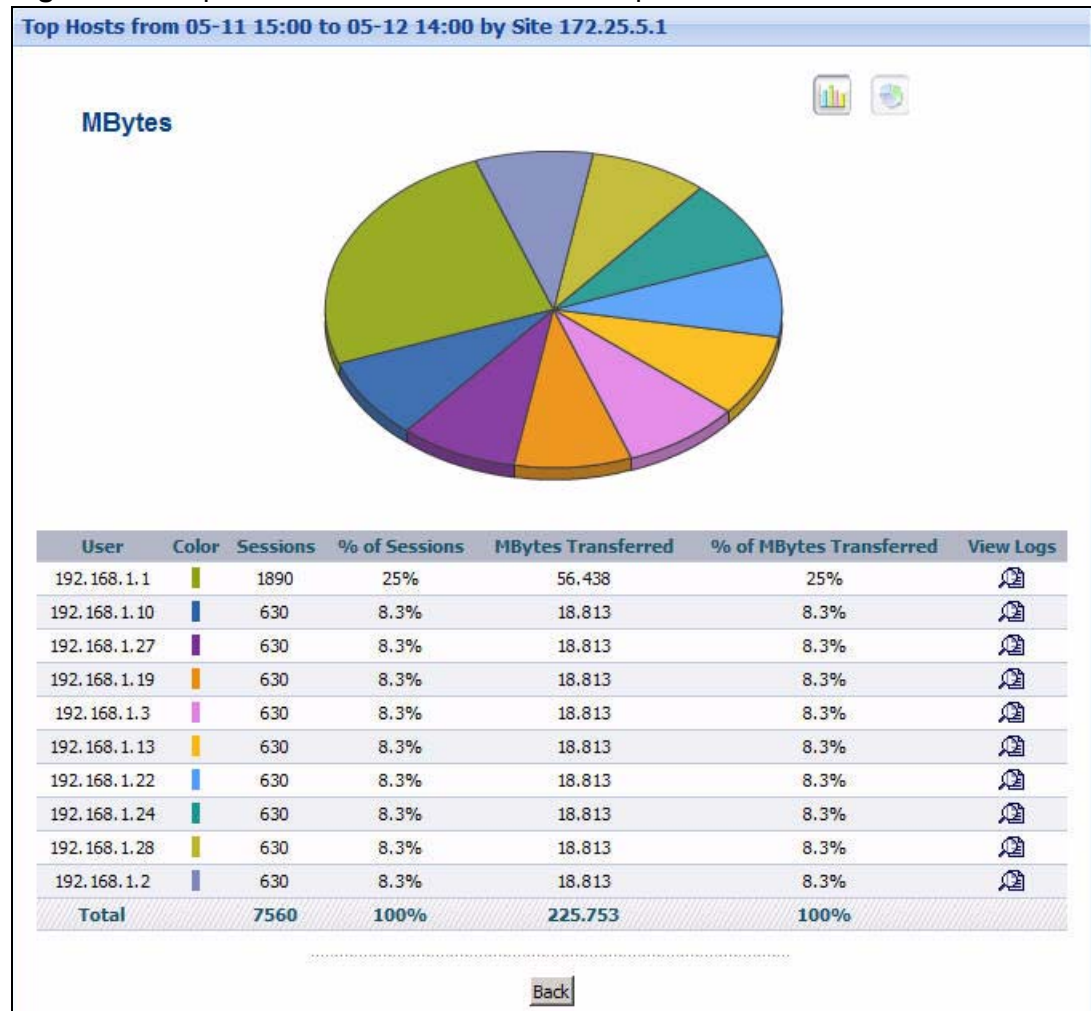
LABEL	DESCRIPTION
Site	This field displays the top destinations of FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top sources of FTP traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.3.2 Top FTP Sites Drill-Down

Use this report to look at the top sources of FTP traffic for any top destination.

Click on a specific destination in **Report > Network Traffic > FTP > Top Sites** to open this screen.

Figure 69 Report > Network Traffic > FTP > Top Sites > Drill-Down



Each field is described in the following table.

Table 57 Report > Network Traffic > FTP > Top Sites > Drill-Down

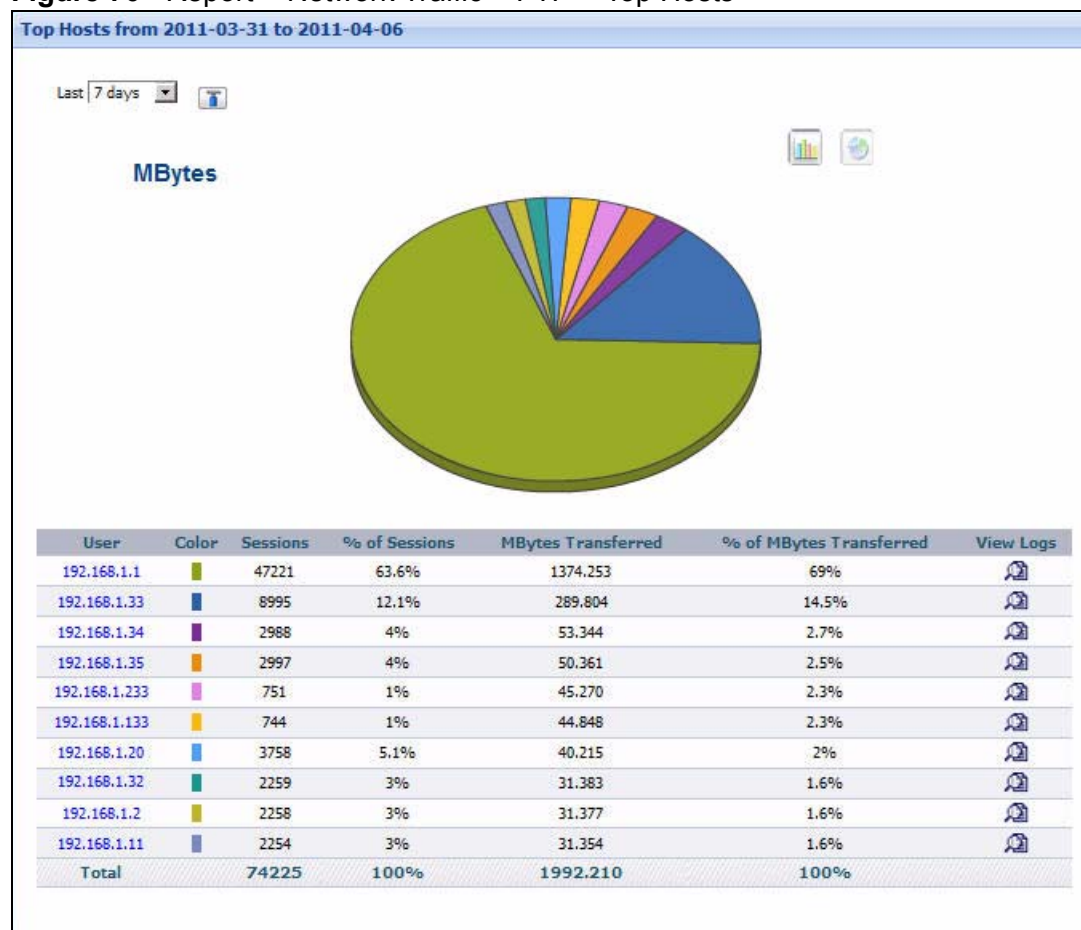
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of FTP traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events came from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's FTP traffic came from each source.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.3.3 Top FTP Hosts

Use this report to look at the top sources of FTP traffic.

Click **Report > Network Traffic > FTP > Top Hosts** to open this screen.

Figure 70 Report > Network Traffic > FTP > Top Hosts



Each field is described in the following table.

Table 58 Report > Network Traffic > FTP > Top Hosts

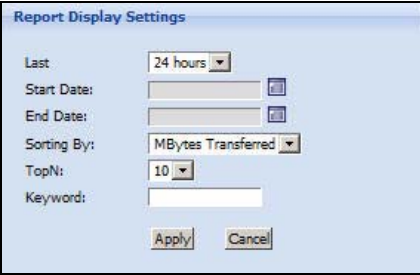
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 58 Report > Network Traffic > FTP > Top Hosts

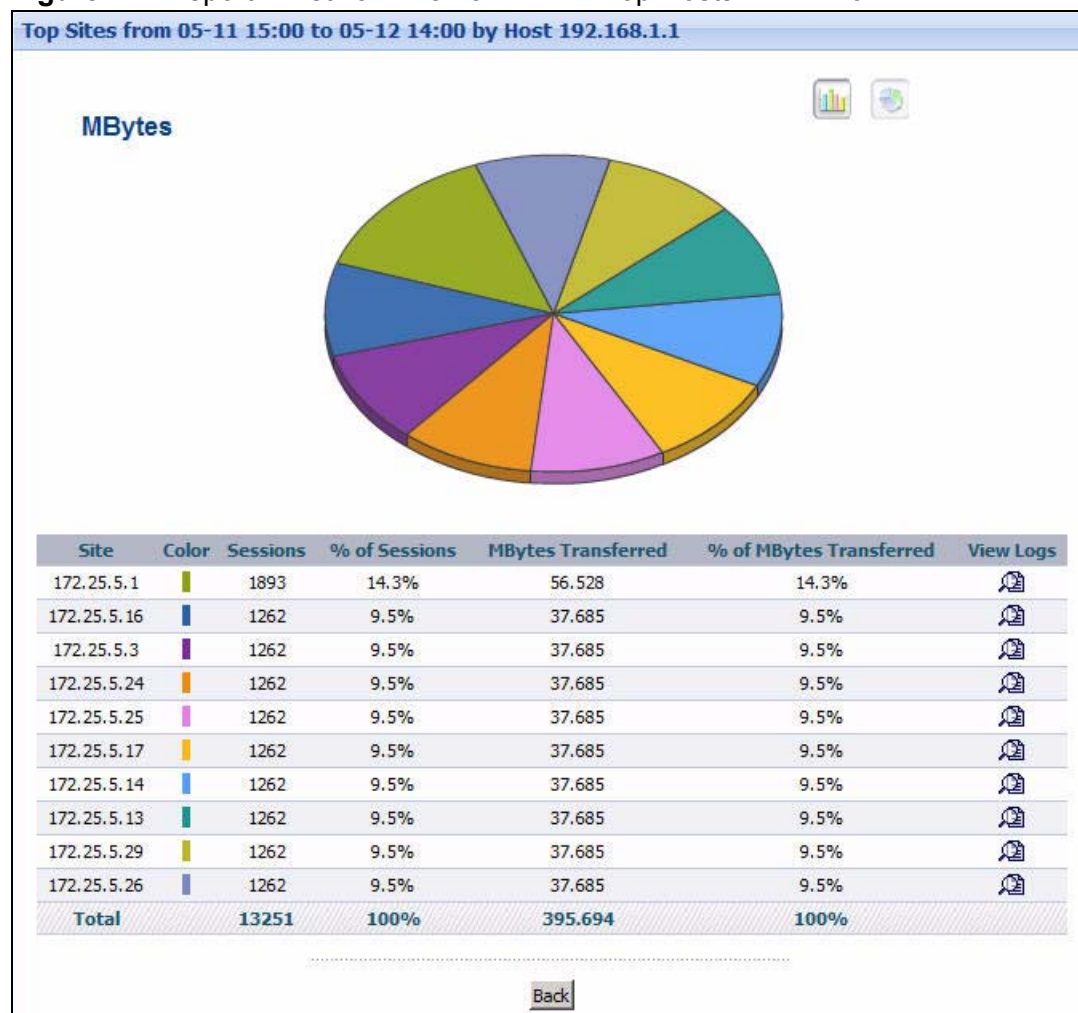
LABEL	DESCRIPTION
Host	This field displays the top sources of FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of FTP traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.3.4 Top FTP Hosts Drill-Down

Use this report to look at the top destinations of FTP traffic for any top source.

Click on a specific source in **Report > Network Traffic > FTP > Top Hosts** to open this screen.

Figure 71 Report > Network Traffic > FTP > Top Hosts > Drill-Down



Each field is described in the following table.

Table 59 Report > Network Traffic > FTP > Top Hosts > Drill-Down

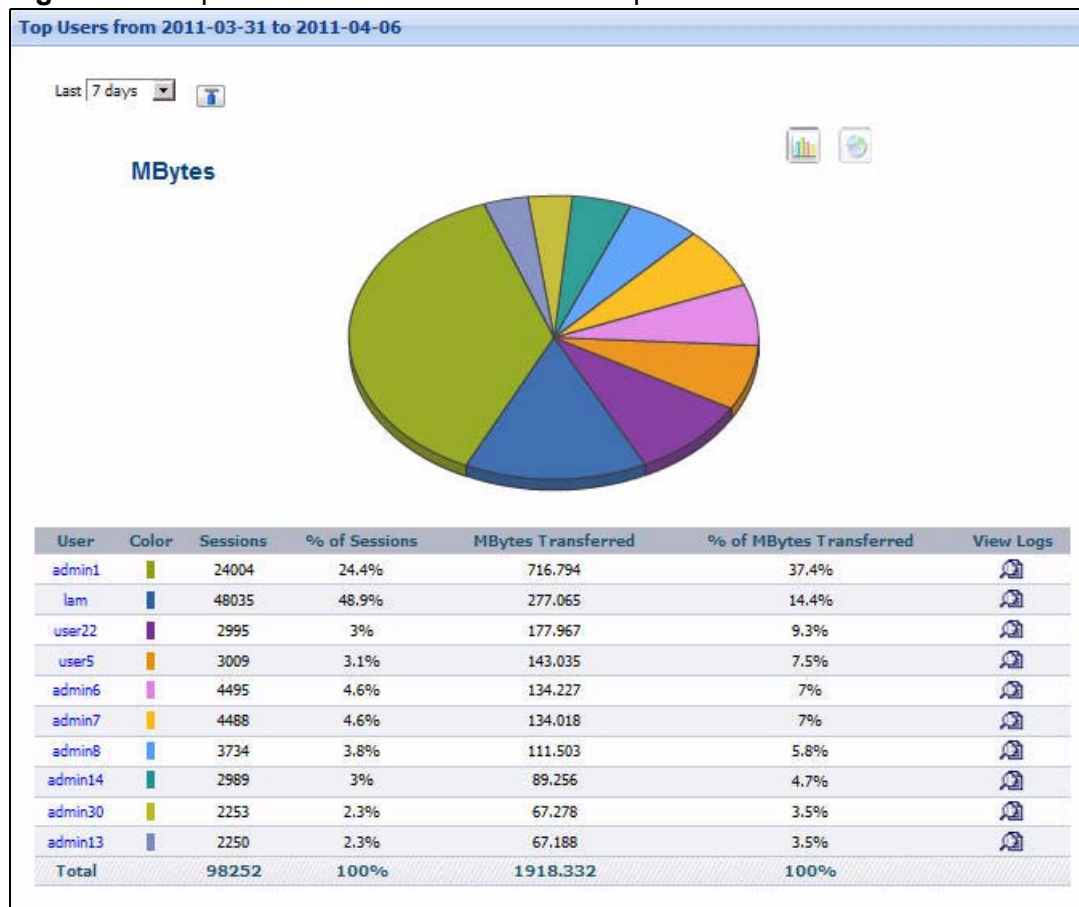
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of FTP traffic from the selected source, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected source to each destination.
% of Sessions	This field displays what percentage of the selected source's total number of traffic events went to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes Transferred	This field displays what percentage of the selected source's traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.3.5 Top FTP Users

Use this report to look at the users that send the most FTP traffic.

Click **Report > Network Traffic > FTP > Top Users** to open this screen.

Figure 72 Report > Network Traffic > FTP > Top Users



Each field is described in the following table.

Table 60 Report > Network Traffic > FTP > Top Users

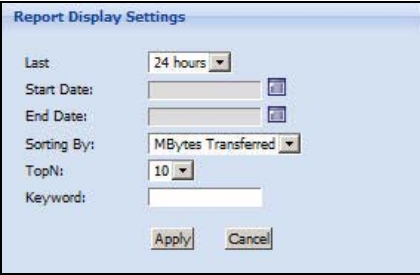
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 60 Report > Network Traffic > FTP > Top Users

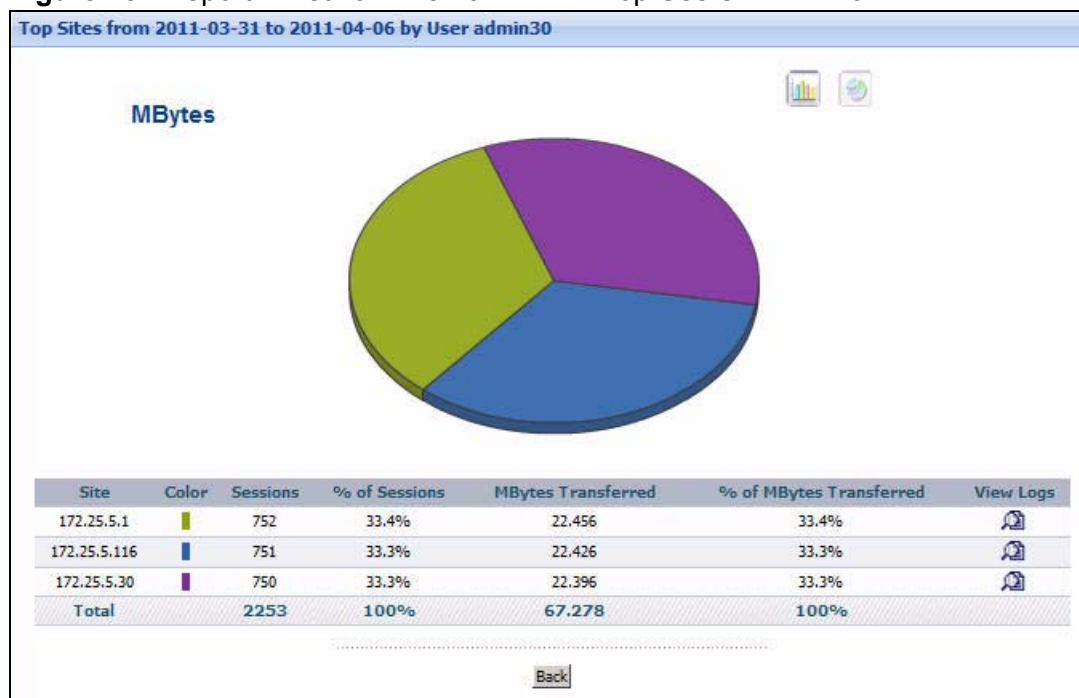
LABEL	DESCRIPTION
User	This field displays the users that sent the most FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click a user name to look at the top destinations of FTP traffic for the selected user.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.3.6 Top FTP Users Drill-Down

Use this report to look at the top destinations of FTP traffic for any top user.

Click on a specific source in **Report > Network Traffic > FTP > Top Users** to open this screen.

Figure 73 Report > Network Traffic > FTP > Top Users > Drill-Down



Each field is described in the following table.

Table 61 Report > Network Traffic > FTP > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of FTP traffic from the selected user, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected user to each destination.
% of Sessions	This field displays what percentage of the selected user's total number of traffic events went to each destination.

Table 61 Report > Network Traffic > FTP > Top Users > Drill-Down

LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected user to each destination.
% of MBytes Transferred	This field displays what percentage of the selected user's total traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected user is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.4 Mail Traffic

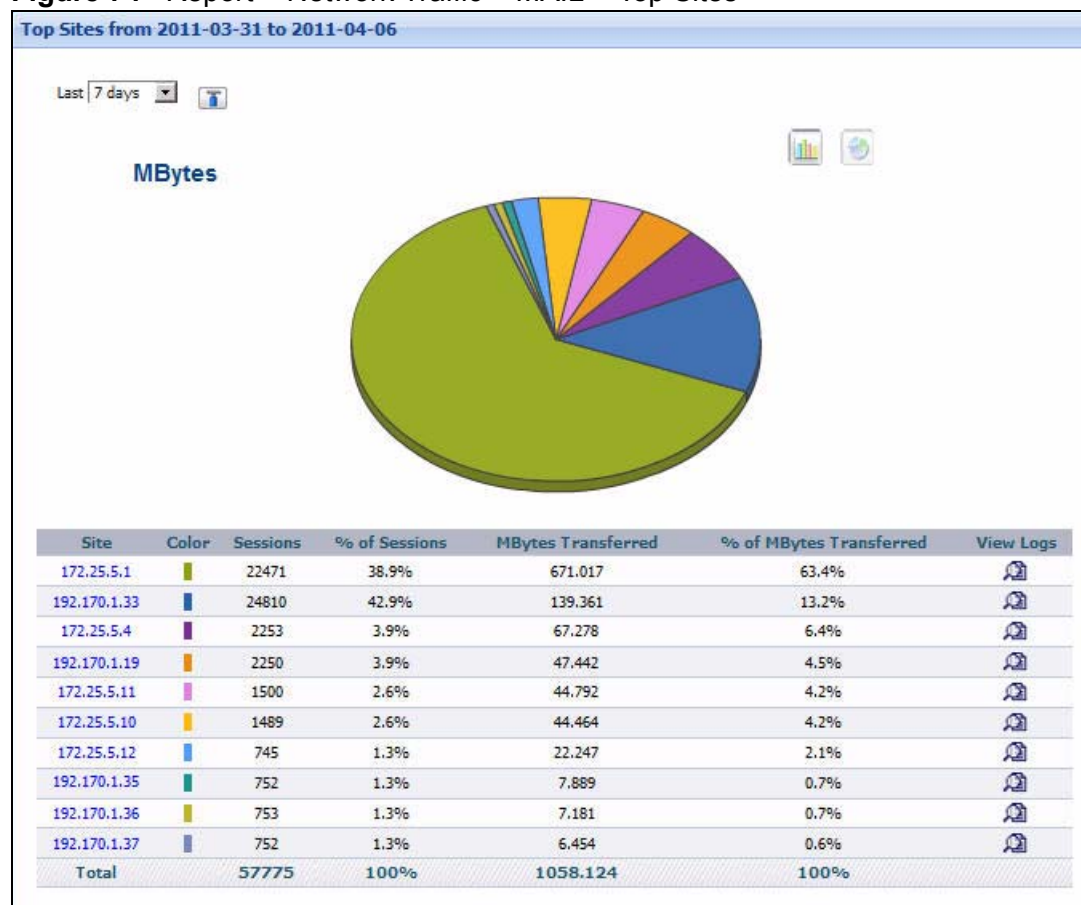
These reports look at the top destinations and sources of mail traffic.

5.4.1 Top Mail Sites

Use this report to look at the top destinations and sources of mail traffic.

Click **Report > Network Traffic > MAIL > Top Sites** to open this screen.

Figure 74 Report > Network Traffic > MAIL > Top Sites



Each field is described in the following table.

Table 62 Report > Traffic > MAIL > Top Sites

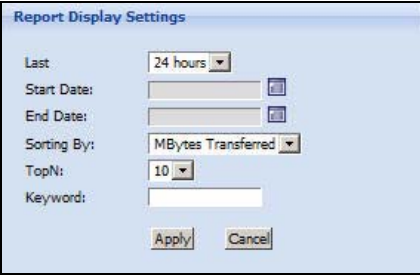
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 62 Report > Traffic > MAIL > Top Sites

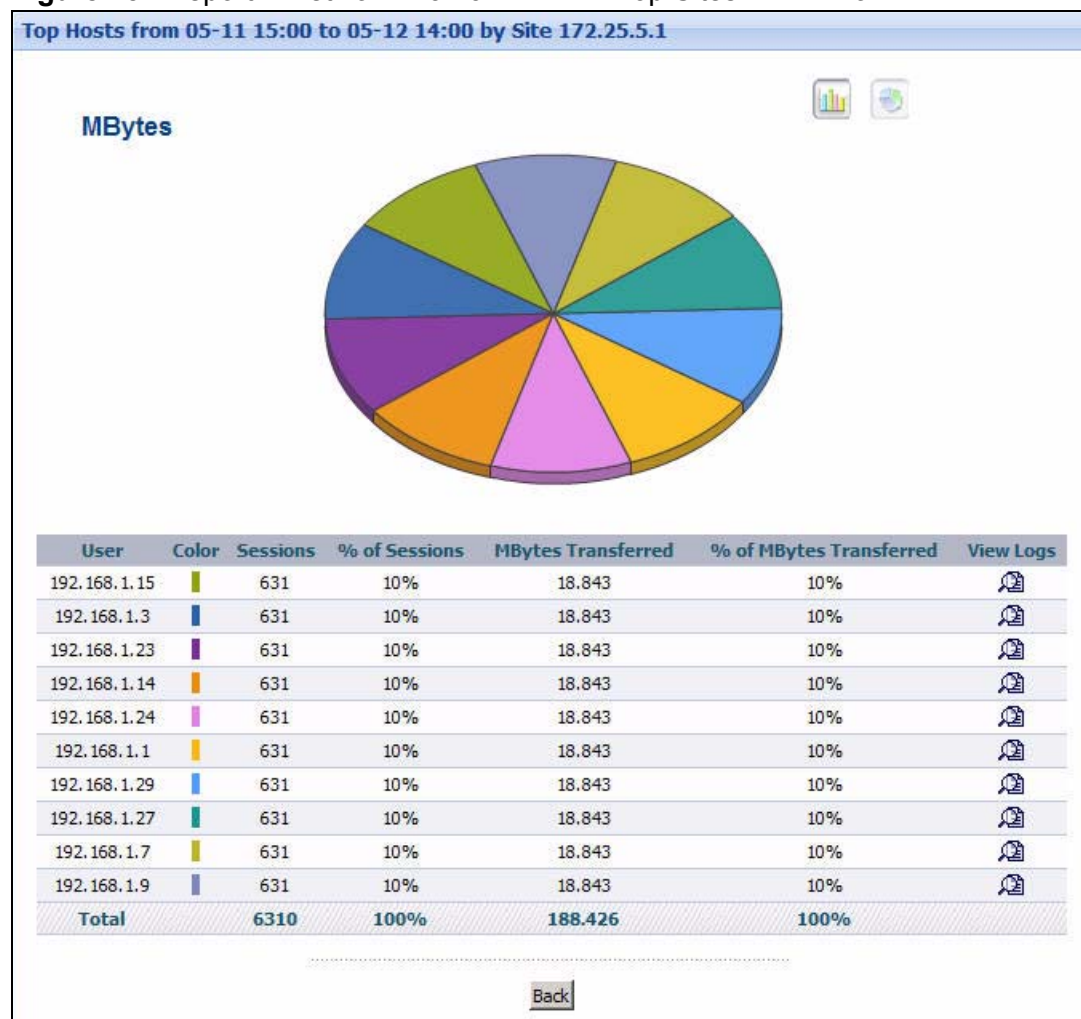
LABEL	DESCRIPTION
Site	This field displays the top destinations of mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top sources of mail traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.4.2 Top Mail Sites Drill-Down

Use this report to look at the top sources of mail traffic for any top destination.

Click on a specific destination in **Report > Network Traffic > MAIL > Top Sites** to open this screen.

Figure 75 Report > Network Traffic > MAIL > Top Sites > Drill-Down



Each field is described in the following table.

Table 63 Report > Network Traffic > MAIL > Top Sites > Drill-Down

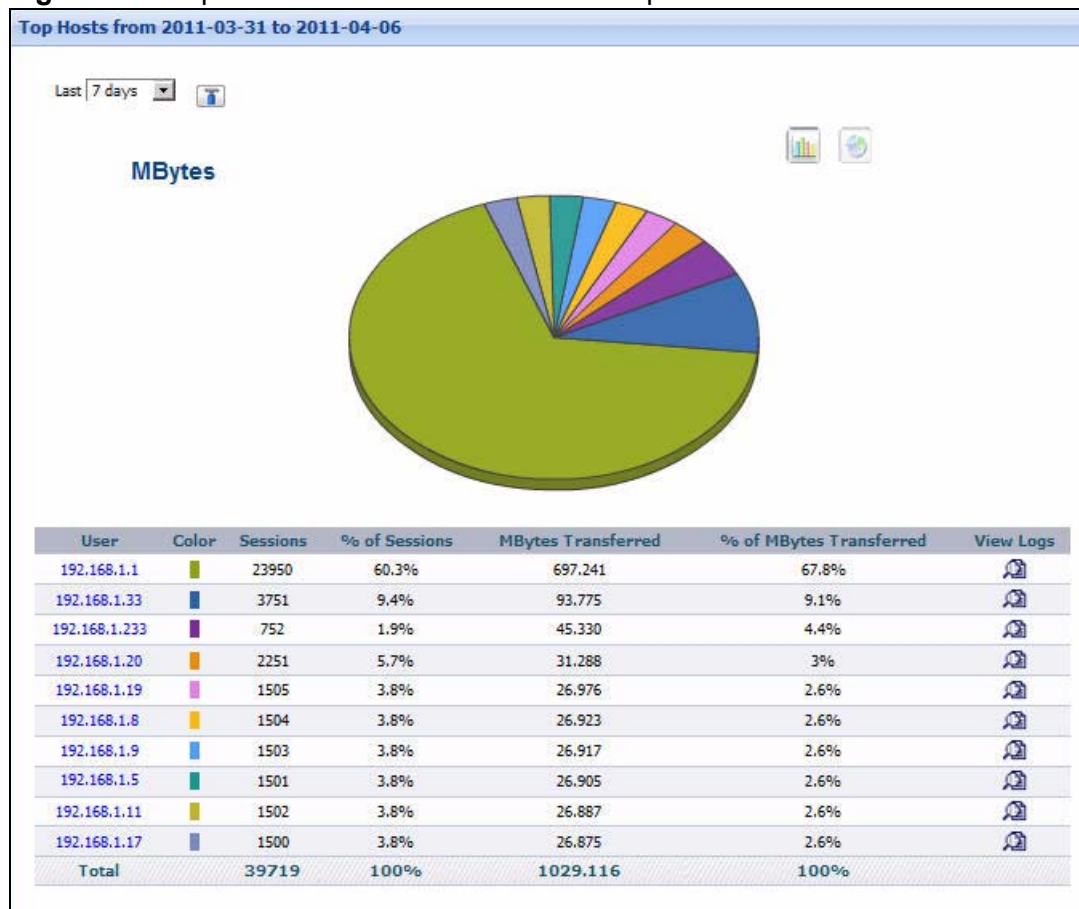
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of mail traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events came from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) came from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's mail traffic came from each source.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.4.3 Top Mail Hosts

Use this report to look at the top sources of mail traffic.

Click **Report > Network Traffic > MAIL > Top Hosts** to open this screen.

Figure 76 Report > Network Traffic > MAIL > Top Hosts



Each field is described in the following table.

Table 64 Report > Network Traffic > MAIL > Top Hosts

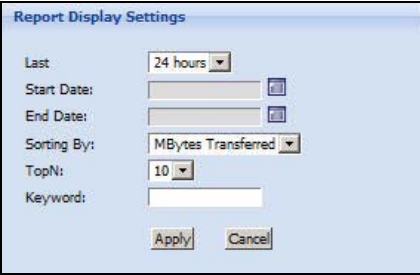
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 64 Report > Network Traffic > MAIL > Top Hosts

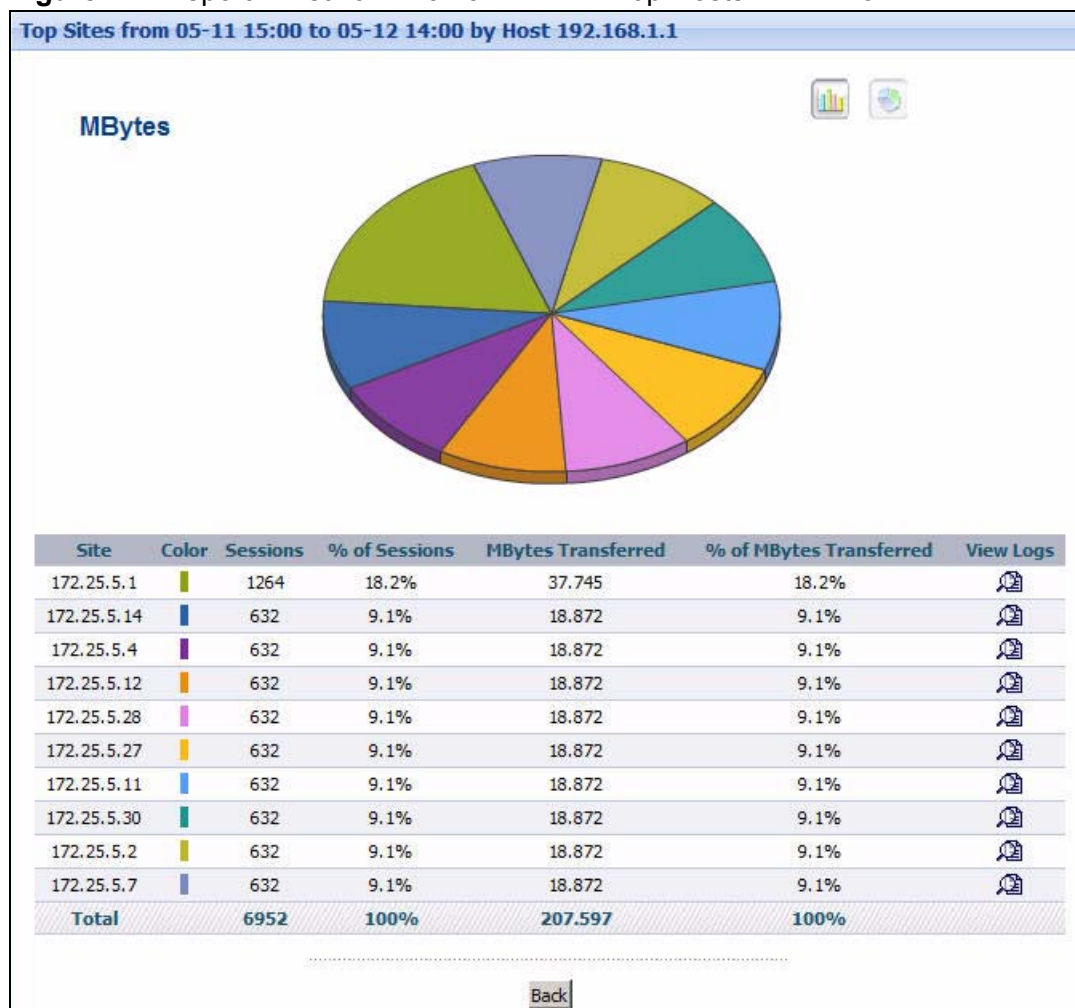
LABEL	DESCRIPTION
Host	This field displays the top sources of mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of mail traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.4.4 Top Mail Hosts Drill-Down

Use this report to look at the top destinations of mail traffic for any top source.

Click on a specific source in **Report > Network Traffic > MAIL > Top Hosts** to open this screen.

Figure 77 Report > Network Traffic > MAIL > Top Hosts > Drill-Down



Each field is described in the following table.

Table 65 Report > Network Traffic > MAIL > Top Hosts > Drill-Down

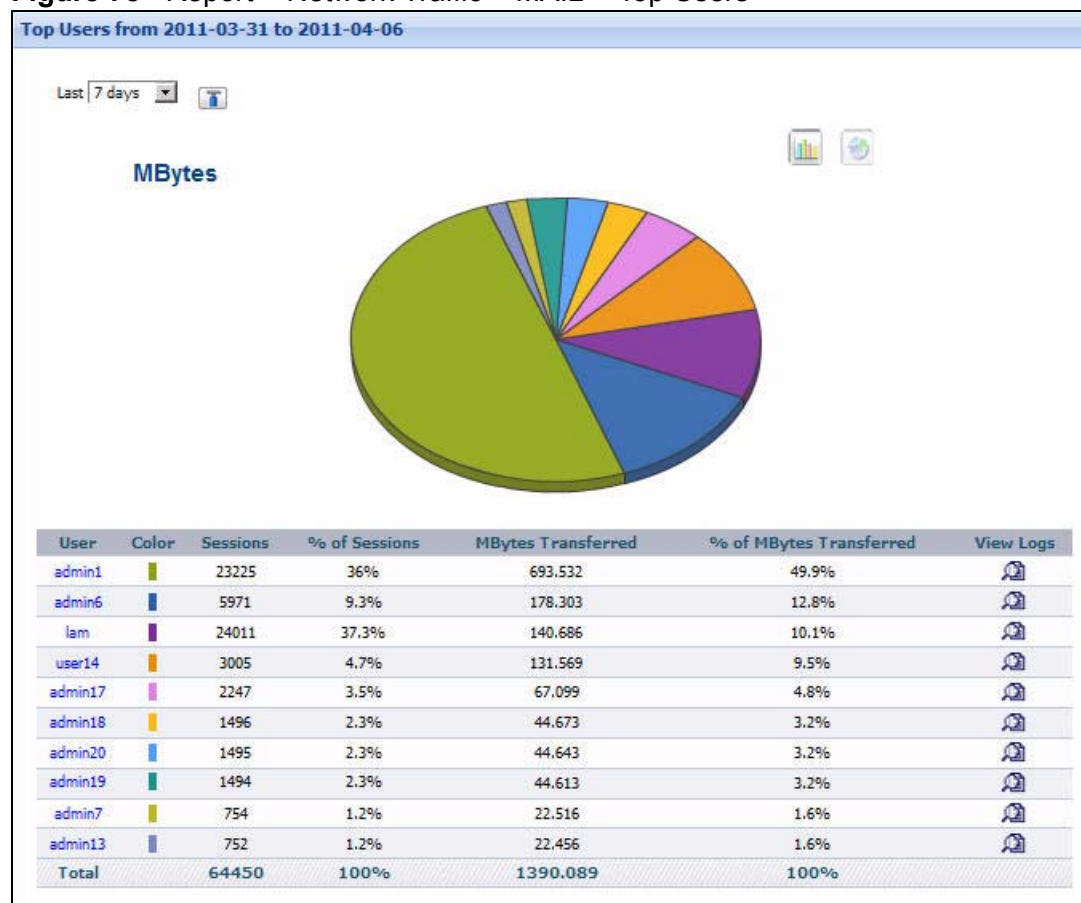
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of mail traffic from the selected source, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected source to each destination.
% of Sessions	This field displays what percentage of the selected source's total number of traffic events went to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes Transferred	This field displays what percentage of the selected source's total traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.4.5 Top Mail Users

Use this report to look at the users that send the most mail traffic.

Click **Report > Network Traffic > MAIL > Top Users** to open this screen.

Figure 78 Report > Network Traffic > MAIL > Top Users



Each field is described in the following table.

Table 66 Report > Network Traffic > MAIL > Top Users

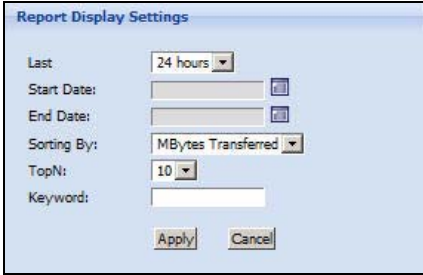
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 66 Report > Network Traffic > MAIL > Top Users

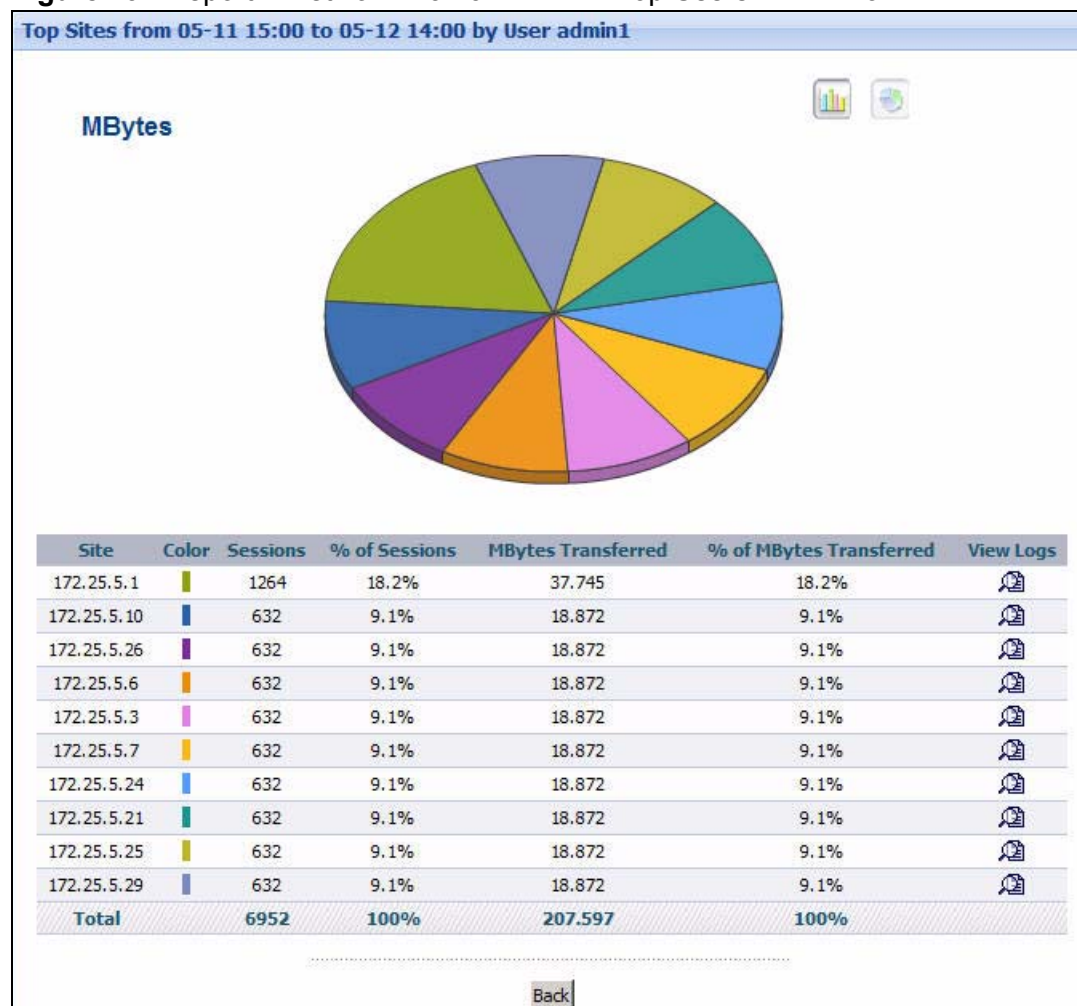
LABEL	DESCRIPTION
User	This field displays the users that send the most mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of mail traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.4.6 Top Mail Users Drill-Down

Use this report to look at the top destinations of mail traffic for any top user.

Click on a specific source in **Report > Network Traffic > MAIL > Top Users** to open this screen.

Figure 79 Report > Network Traffic > MAIL > Top Users > Drill-Down



Each field is described in the following table.

Table 67 Report > Network Traffic > MAIL > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of mail traffic from the selected user, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected user to each destination.
% of Sessions	This field displays what percentage of the selected user's total number of traffic events went to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected user to each destination.
% of MBytes Transferred	This field displays what percentage of the selected user's total traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.5 Other Traffic

These reports look at the top sources and destinations of any kind of traffic.

5.5.1 Platform Selection

Click **Report > Network Traffic > Customization > Customization** to open the **Platform Selection** screen.

Figure 80 Report > Network Traffic > Customization > Customization (Platform Selection)

The screenshot shows a web interface titled "Platform Selection". It contains two radio button options for selecting a ZyXEL firmware platform. The first option is "ZyNOS (Including Prestige, ZyWALL IDP 10, ZyWALL Series except ZyWALL 1050)". The second option is "ZLD (Including ZyWALL USG Series & ZyWALL 1050)". At the bottom right, there is a "Next" button.

Use this screen to select the ZyXEL firmware platform that the device uses.

Then click **Next**.

5.5.2 Service Settings

The following screen displays after you select the ZyXEL firmware platform. Use this screen to add, edit, or remove services that you can view in **Other Traffic** reports. These services appear in the **Customized Services** drop-down box.

You can use services that are pre-defined in Vantage Report, or you can create new services. If you create new services, you have to specify the protocol and port number(s) for the service.

Figure 81 Report > Network Traffic > Customization > Customization (Service Settings)

The screenshot shows a web interface titled "Service Settings". It has two main sections: "Add a Known Service" and "Add a Customized Service". The "Add a Known Service" section has a dropdown menu currently showing "[Customized Service]". The "Add a Customized Service" section has input fields for "Name:", "Port Range (1-65535):", and "Protocol:" (with a dropdown menu showing "tcp"). To the right of these fields is a large empty box labeled "Customized Service:". At the bottom, there are "Add" and "Delete" buttons.

Each field is described in the following table.

Table 68 Report > Network Traffic > Customization > Customization (Service Settings)

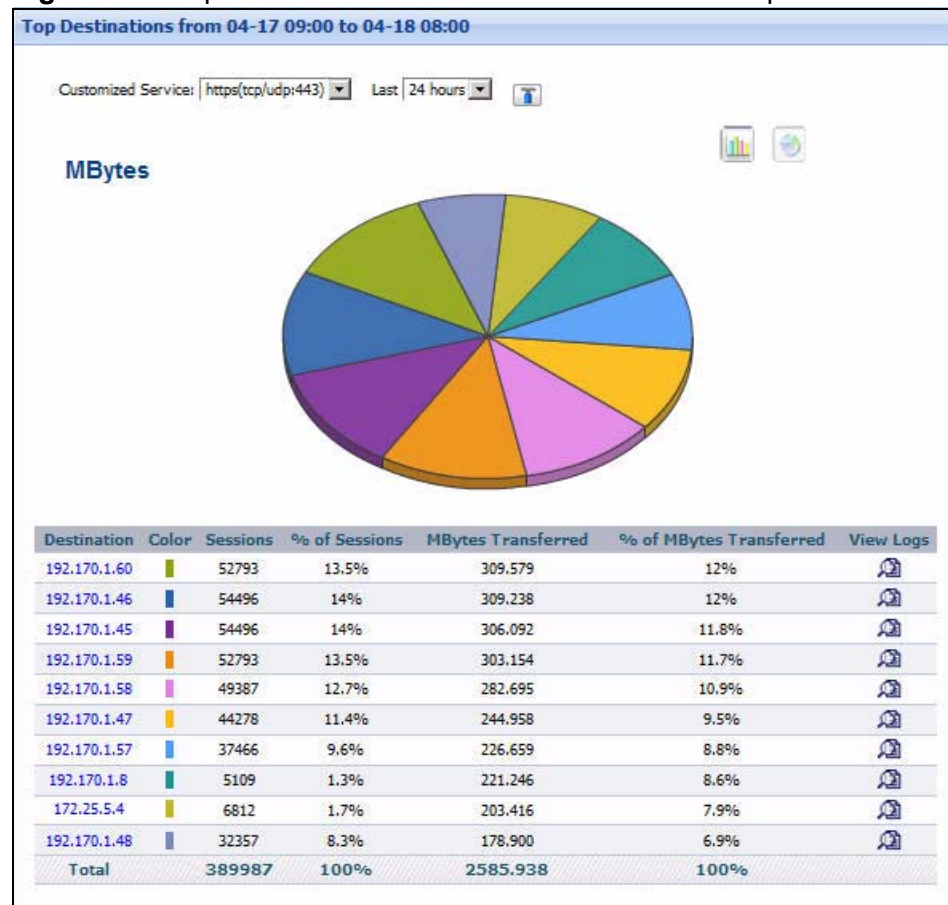
LABEL	DESCRIPTION
Add a Known Service	Use this drop-down box to add a service to the Customized Service drop-down box. - Select a pre-defined service from the drop-down list box, and click the Add button; or - Select [Customized Service], fill in the Add a Customized Service section, and click the Add button. This drop-down box does not include web, mail, or FTP services.
Add a Customized Service	Use this section to create new TCP/UDP services that are not in the pre-defined list. You cannot edit pre-defined services.
Name	Enter a name to identify the new customized service. It does not have to be unique. This name is used when the service is displayed in the Customized Service drop-down box.
Port Range	Enter a port range (start port to end port, in ascending order) that is not already in use to define your service. Use the same start and end port if the service is only defined by one port.
Protocol	Select the protocol used by the service. Choices are tcp , udp and tcp/udp .
Customized Service	This list box lists all the services that appear in the Customized Service drop-down box. You can use this list box to remove services from the drop-down box or to edit services you create. To remove a service from the Customized Service drop-down box, click on the service in this list box, and click the Delete button. To edit any service you created, click on the service in the list box, edit the settings in the Add a Customized Service section, and click the Apply button.
Add	Click this button to add the pre-defined service (in the Add a Known Service drop-down box) or new service (in the Add a Customized Service section) the Customized Service drop-down box.
Delete	Click this button to remove the selected service (in the Customized Service list box) from the Customized Service drop-down box. If you delete a service you created, you have to create the service again later, if you need it.

5.5.3 Top Destinations of Other Traffic

Use this report to look at the top destinations of other services' traffic.

Click **Report > Network Traffic > Customization > Top Destinations** to open this screen.

Figure 82 Report > Network Traffic > Customization > Top Destinations



Each field is described in the following table.

Table 69 Report > Network Traffic > Customization > Top Destinations

LABEL	DESCRIPTION
Customized Service	Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the Service Settings screen.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 69 Report > Network Traffic > Customization > Top Destinations

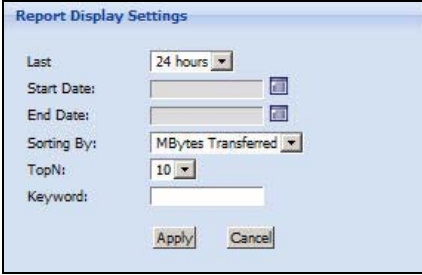
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the top sources of the selected service's traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

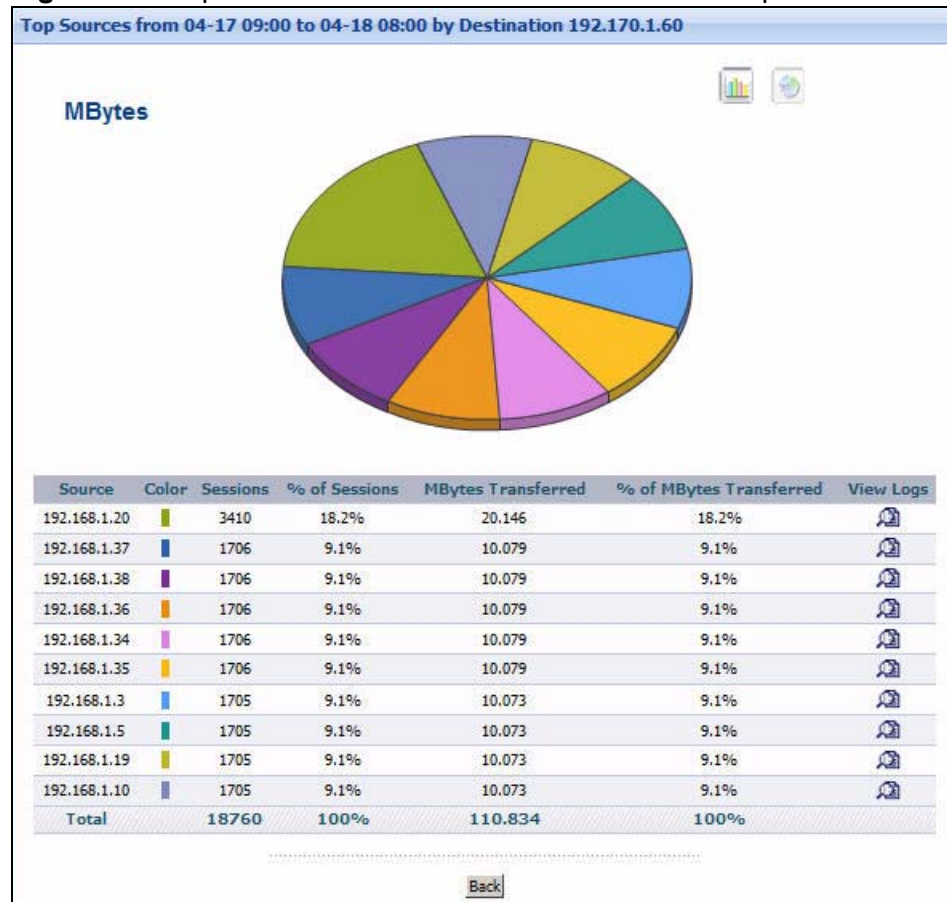
Table 69 Report > Network Traffic > Customization > Top Destinations

LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.5.4 Top Destinations of Other Traffic Drill-Down

Use this report to look at the top sources of other services' traffic for any top destination. The service is selected in the main report.

Click on a specific destination in **Report > Network Traffic > Customization > Top Destinations** to open this screen.

Figure 83 Report > Network Traffic > Customization > Top Destinations > Drill-Down

Each field is described in the following table.

Table 70 Report > Network Traffic > Customization > Top Destinations > Drill-Down

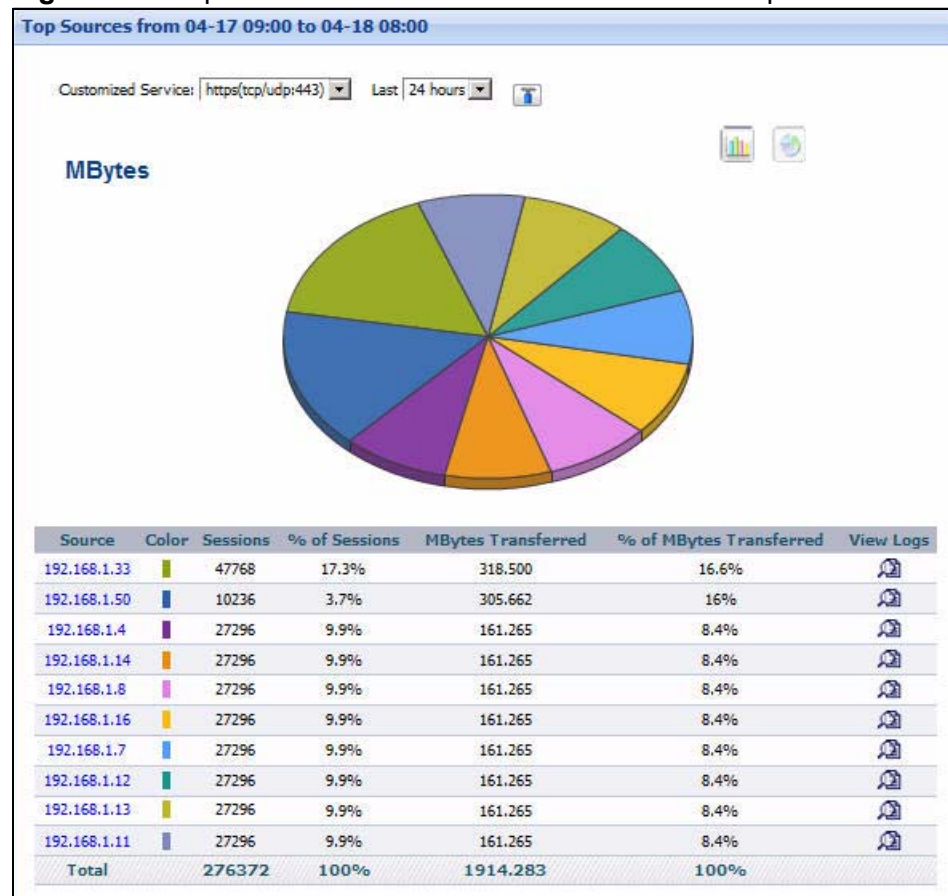
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected service's traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events for the selected destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was sent from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's traffic came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.5.5 Top Sources of Other Traffic

Use this report to look at the top sources of other services' traffic.

Click **Report > Network Traffic > Customization > Top Sources** to open this screen.

Figure 84 Report > Network Traffic > Customization > Top Sources



Each field is described in the following table.

Table 71 Report > Network Traffic > Customization > Top Sources

LABEL	DESCRIPTION
Customized Service	Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the Service Settings screen.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 71 Report > Network Traffic > Customization > Top Sources

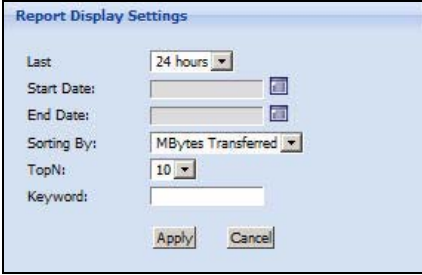
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of the selected service's traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.

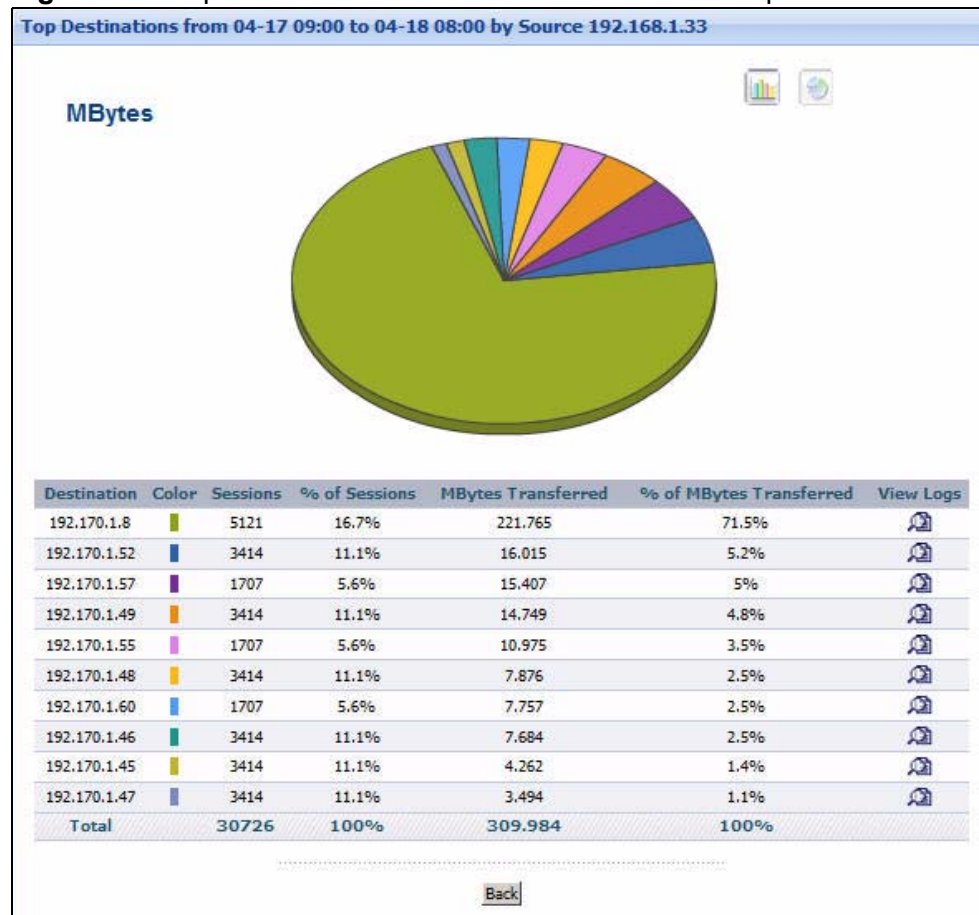
Table 71 Report > Network Traffic > Customization > Top Sources

LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.5.6 Top Sources of Other Traffic Drill-Down

Use this report to look at the top destinations of other services' traffic for any top source. The service is selected in the main report.

Click on a specific source in **Report > Network Traffic > Customization > Top Sources** to open this screen.

Figure 85 Report > Network Traffic > Customization > Top Sources > Drill-Down

Each field is described in the following table.

Table 72 Report > Network Traffic > Customization > Top Sources > Drill-Down

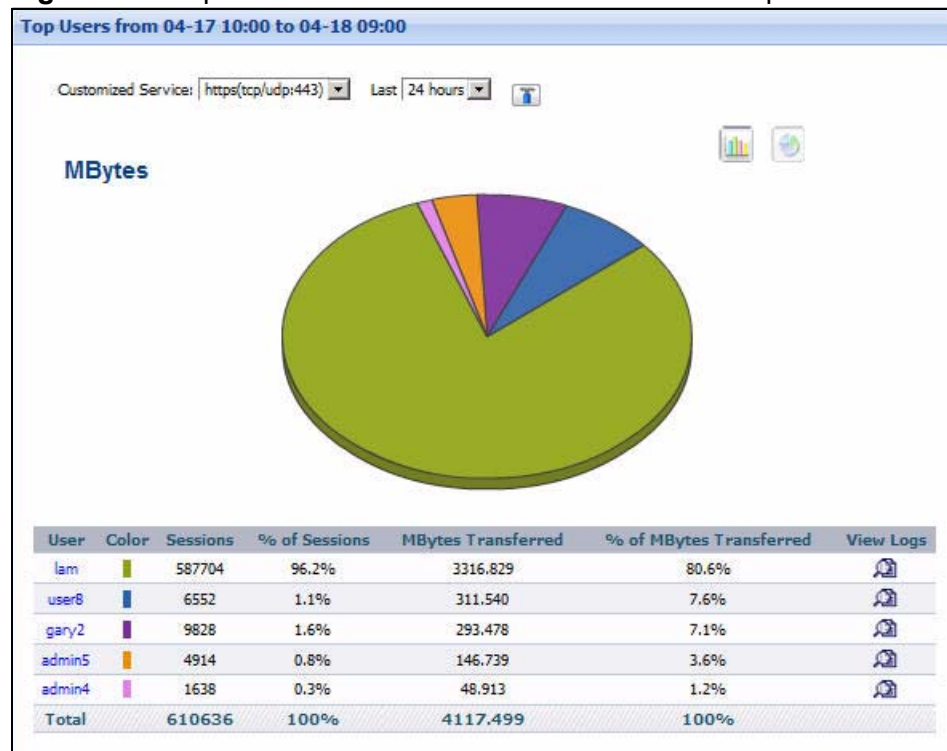
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of the selected service's traffic from the selected source, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected source to each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events for the selected source.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes Transferred	This field displays what percentage of the selected source's traffic using the selected service was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.5.7 Top Other Traffic Users

Use this report to look at the users that send the most other services' traffic.

Click **Report > Network Traffic > Customization > Top Users** to open this screen.

Figure 86 Report > Network Traffic > Customization > Top Users



Each field is described in the following table.

Table 73 Report > Network Traffic > Customization > Top Users

LABEL	DESCRIPTION
Customized Service	Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the Service Settings screen.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 73 Report > Network Traffic > Customization > Top Users

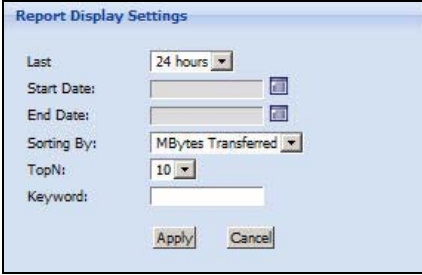
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: Enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that sent the most of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of the selected service's traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events for the time range of the report.

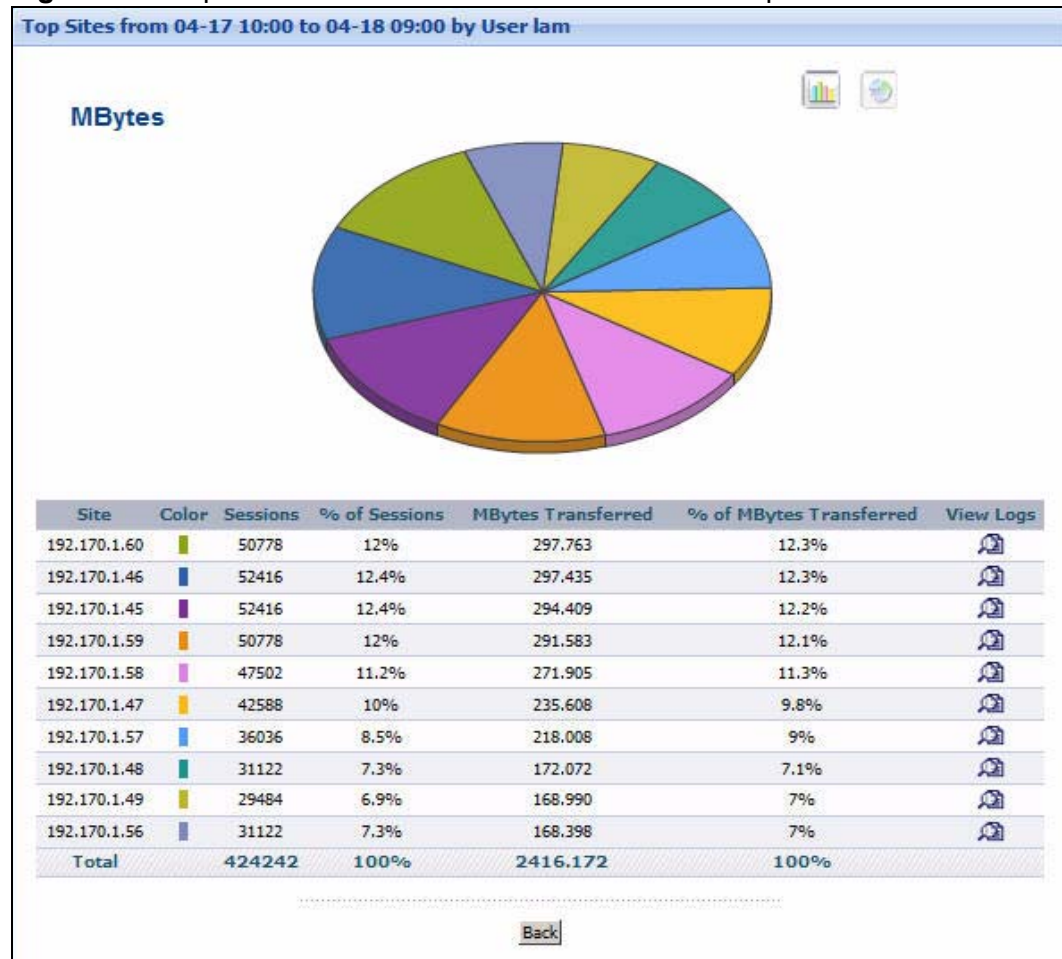
Table 73 Report > Network Traffic > Customization > Top Users

LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.5.8 Top Users of Other Traffic Drill-Down

Use this report to look at the top destinations of other services' traffic for any top user. The service is selected in the main report.

Click on a specific user in **Report > Network Traffic > Customization > Top Users** to open this screen.

Figure 87 Report > Network Traffic > Customization > Top Users > Drill-Down

Each field is described in the following table.

Table 74 Report > Network Traffic > Customization > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of the selected service's traffic from the selected user, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected user to each destination.
% of Sessions	This field displays what percentage of the selected user's total number of traffic events went to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected user to each destination.
% of MBytes Transferred	This field displays what percentage of the selected user's mail traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

Secure Remote Access

6.1 Secure Remote Access - Site-to-Site (IPSec)

This chapter discusses how you can check the reports to look at the top sources and destinations of traffic in Secure Remote Access tunnels. Site-to-site refers to static Secure Remote Access tunnels between two IPSec devices. Each end must be identified by an IP address, domain name or dynamic domain name. More detailed site-to-site Secure Remote Access analysis is also available for devices using the ZLD firmware platform (like the ZyWALL 1050).

Note: To look at Secure Remote Access usage reports, each ZyXEL device must record forwarded IPSec Secure Remote Access traffic in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **IPSec** is enabled.

6.1.1 Secure Remote Access Link Status

Use this report to see which of the device's Secure Remote Access tunnels are connected.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Link Status** to open this screen.

Figure 88 Report > Secure Remote Access > Site-to-Site (IPSec) > Link Status

Site	Tunnel
IKE_1	
IKE_10	
IKE_11	
IKE_12	
IKE_13	
IKE_14	
IKE_15	
IKE_16	
IKE_17	
IKE_18	

Number per Page: 10

Total Count: 31 Total Page: 4 First 1 2 3 4 Last Go

Each field is described in the following table.

Table 75 Report > Secure Remote Access > Site-to-Site (IPSec) > Link Status

LABEL	DESCRIPTION
Site	This column displays the names of peer IPSec routers. Each IPSec router is identified by the name of the phase 1 IKE SA (also known as the gateway policy). A site's status icon is green when all of the configured Secure Remote Access tunnels between the device and the peer IPSec router are connected. A site's status icon is yellow when some of the configured Secure Remote Access tunnels between the device and the peer IPSec router are connected. A site's status icon is red when none of the configured Secure Remote Access tunnels between the device and the peer IPSec router are connected.
Tunnel	This column displays the names of the device's Secure Remote Access tunnels. A tunnel's status icon is green when the Secure Remote Access tunnel is connected. A tunnel's status icon is red when the Secure Remote Access tunnel is not connected.
Total Count	This field displays how many sites are recorded.
Total Page	This field displays how many screens it takes to display all the sites.

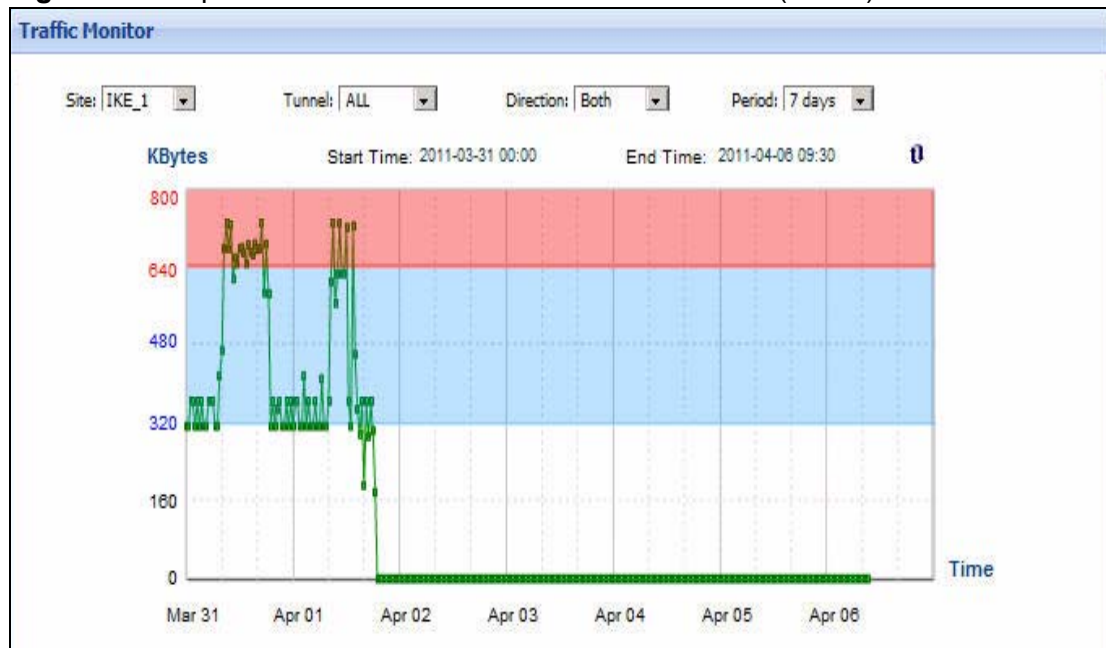
Table 75 Report > Secure Remote Access > Site-to-Site (IPSec) > Link Status

LABEL	DESCRIPTION
First .. Last	Click First , Last , or a specific page number to look at the sites on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .

6.1.2 Secure Remote Access Traffic Monitor

Use this report to monitor the total amount of traffic handled by a device's Secure Remote Access tunnels.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Traffic Monitor** to open this screen.

Figure 89 Report > Secure Remote Access > Site-to-Site (IPSec) > Traffic Monitor

Each field is described in the following table.

Table 76 Report > Secure Remote Access > Site-to-Site (IPSec) > Traffic Monitor

LABEL	DESCRIPTION
Site	Select a peer IPSec router.
Tunnel	Select a Secure Remote Access tunnel. Select All to display the total traffic for the device's Secure Remote Access tunnels with the selected site.

Table 76 Report > Secure Remote Access > Site-to-Site (IPSec) > Traffic Monitor

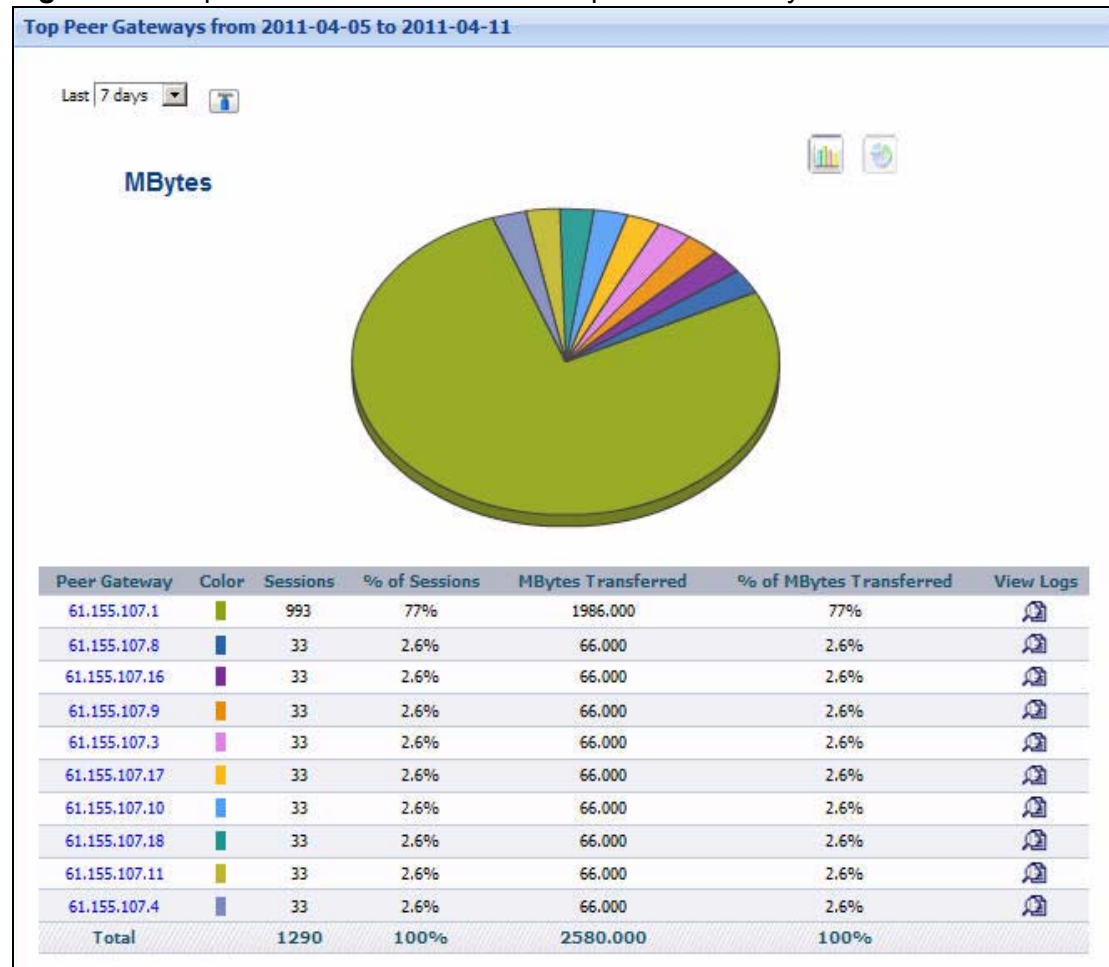
LABEL	DESCRIPTION
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
Period	Choose the time interval you want to view in this field.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
refresh	Click this to update the screen immediately.
graph	The graph shows how the status changes over time. Y-axis (vertical): how much traffic is handled by the device each minute X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the Start Time and End Time.

6.1.3 Top VPN Peer Gateways

Use this report to look at the top destinations of VPN traffic. The device must be a ZyNOS based ZyWALL in order to view this report.

Click **Report > VPN > Site-to-Site > Top Peer Gateways** to open this screen.

Figure 90 Report > VPN > Site-to-Site > Top Peer Gateways



Each field is described in the following table.

Table 77 Report > VPN > Site-to-Site > Top Peer Gateways

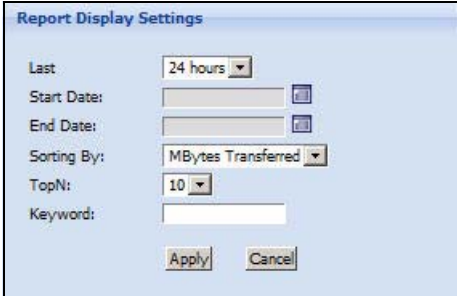
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Peer Gateway field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 77 Report > VPN > Site-to-Site > Top Peer Gateways

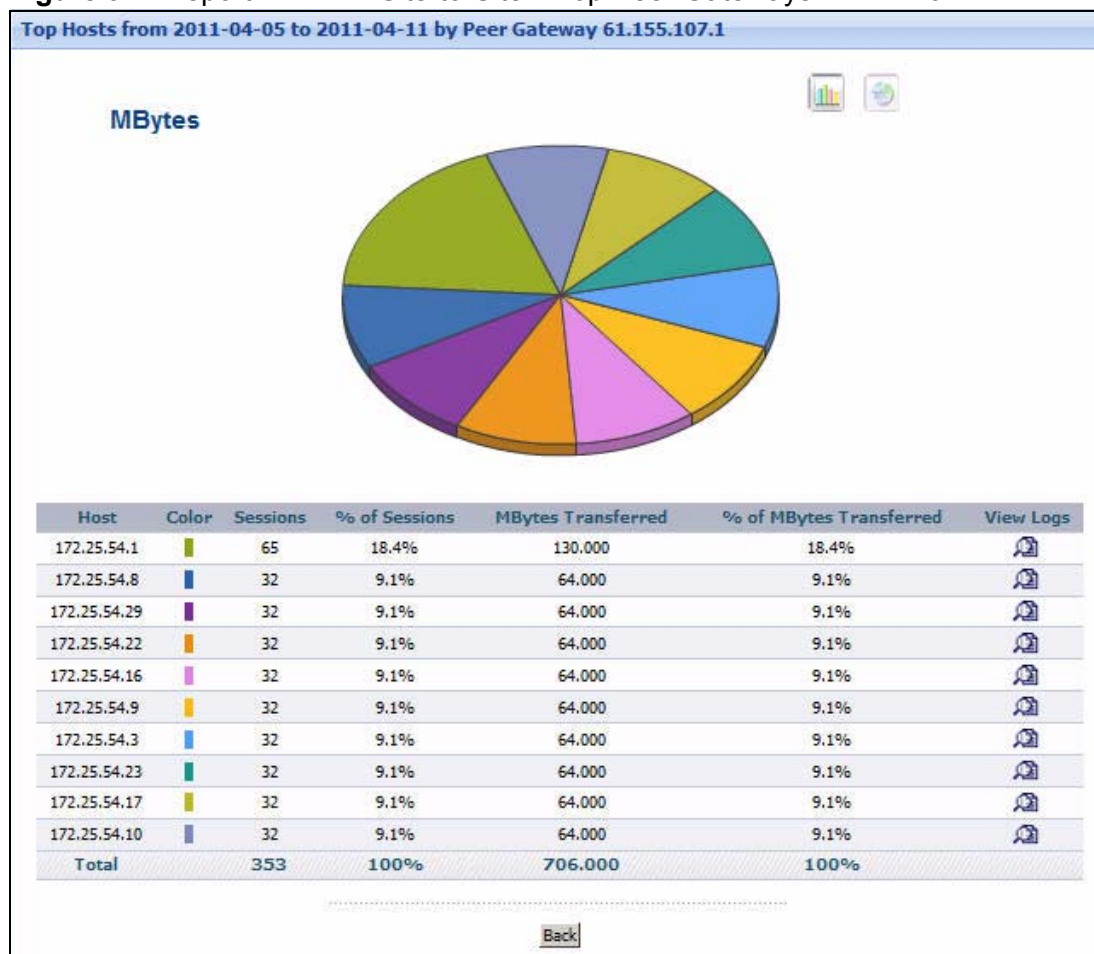
LABEL	DESCRIPTION
Peer Gateway	This field displays the top destinations of VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by the IP address of the remote gateway. Click on a destination to look at the top sender hosts that sent the most VPN traffic to the selected host.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.4 Top VPN Peer Gateways Drill-Down

Use this report to look at the top sources of VPN traffic for any top destination.

Click on a specific destination in **Report > VPN > Site-to-Site > Top Peer Gateways** to open this screen.

Figure 91 Report > VPN > Site-to-Site > Top Peer Gateways > Drill-Down



Each field is described in the following table.

Table 78 Report > VPN > Site-to-Site > Top Peer Gateways > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of VPN traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.

Table 78 Report > VPN > Site-to-Site > Top Peer Gateways > Drill-Down

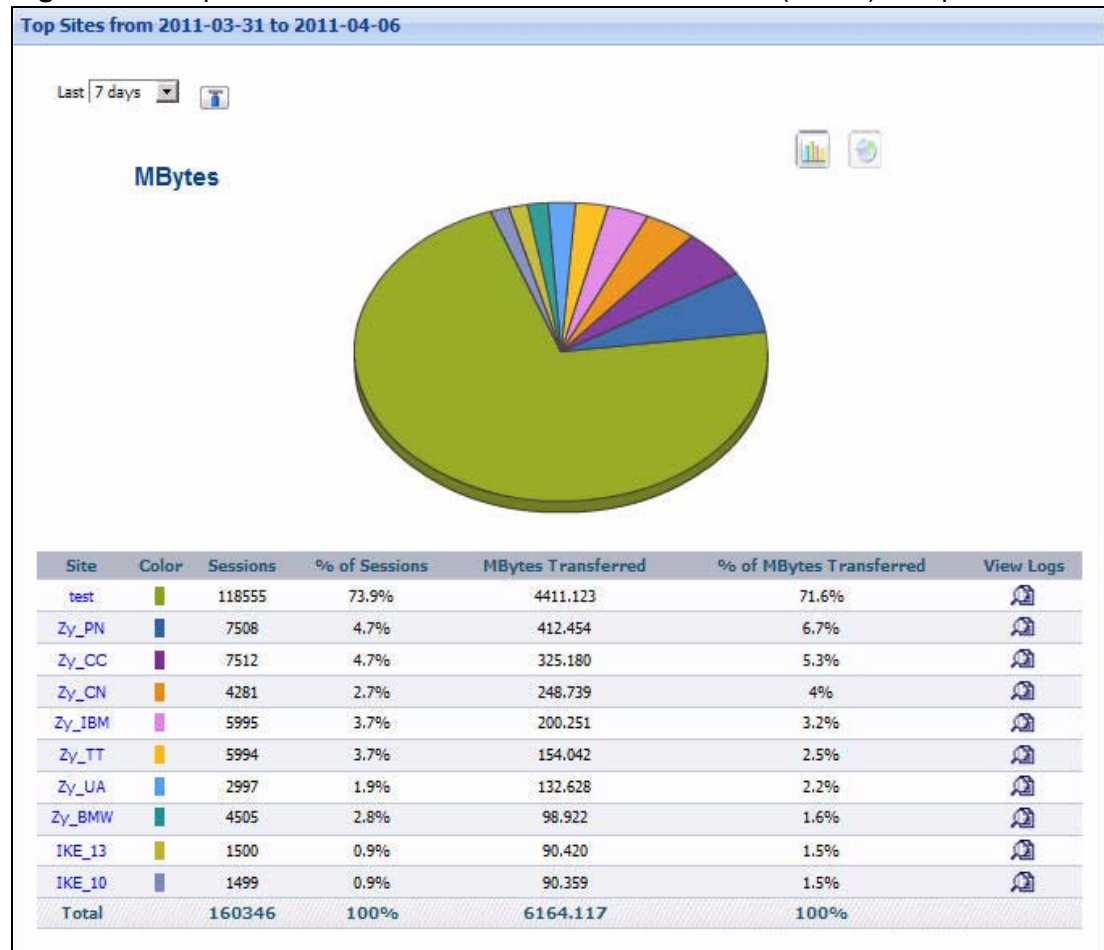
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events for the selected destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's VPN traffic was generated from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. It only displays the top 10 sources in the screen.
Back	Click this to return to the main report.

6.1.5 Top Secure Remote Access Sites

Use this report to look at the peer IPSec routers with the most Secure Remote Access traffic.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites** to open this screen.

Figure 92 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites



Each field is described in the following table.

Table 79 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites

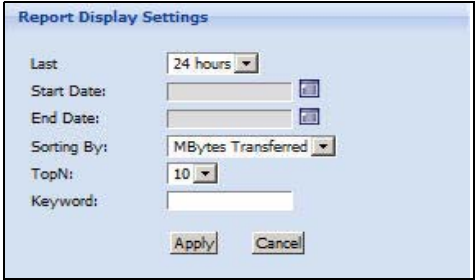
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 79 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites

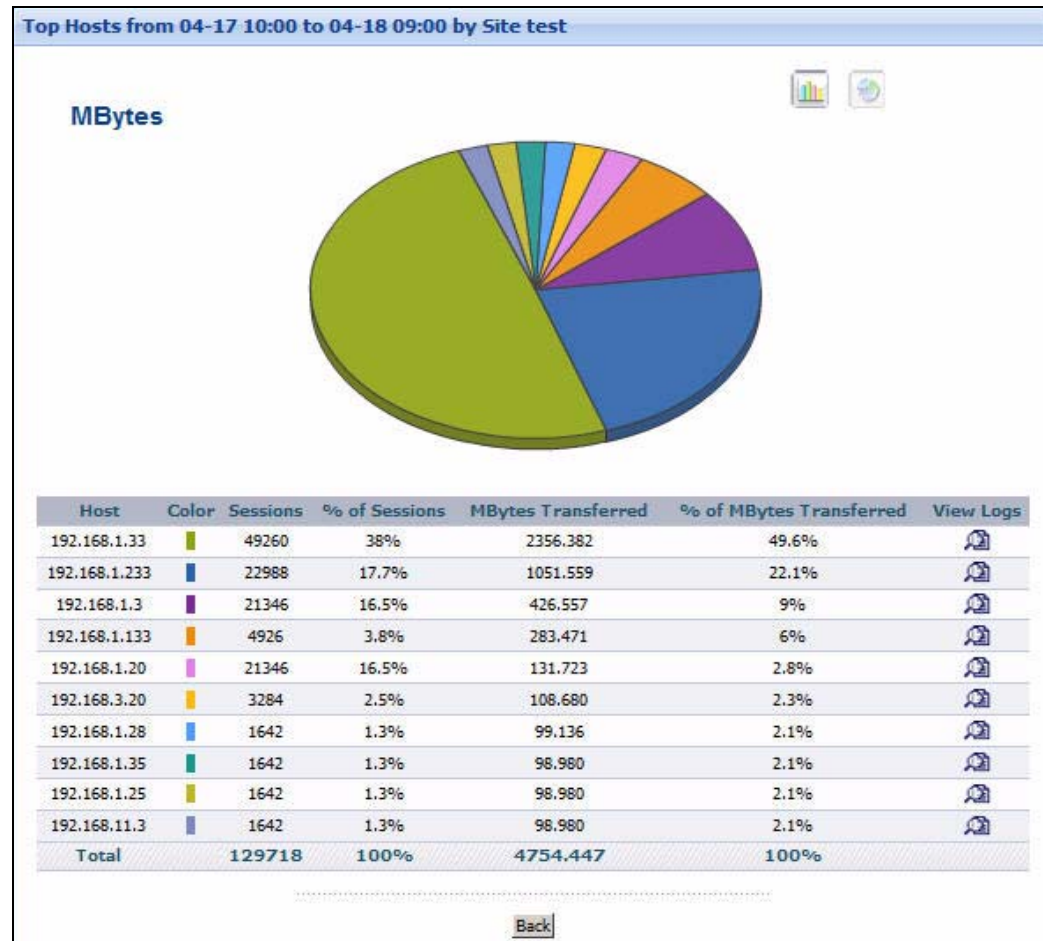
LABEL	DESCRIPTION
Site	This field displays the peer IPSec routers with the most Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of peer IPSec routers is less than the maximum number of records displayed in this table, every peer IPSec router is displayed. Each peer IPSec router is identified by the name of the phase 1 IKE SA (also known as the gateway policy). Click on a name to look at the top sources of Secure Remote Access traffic for the selected site.
Color	This field displays what color represents each site in the graph.
Sessions	This field displays the number of traffic events for each site.
% of Sessions	This field displays what percentage each site's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each site.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each site.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.6 Top Secure Remote Access Sites Drill-Down

Use this report to look at the top sources of Secure Remote Access traffic for any top destination.

Click on a specific destination in **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites** to open this screen.

Figure 93 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites > Drill-Down



Each field is described in the following table.

Table 80 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites > Drill-Down

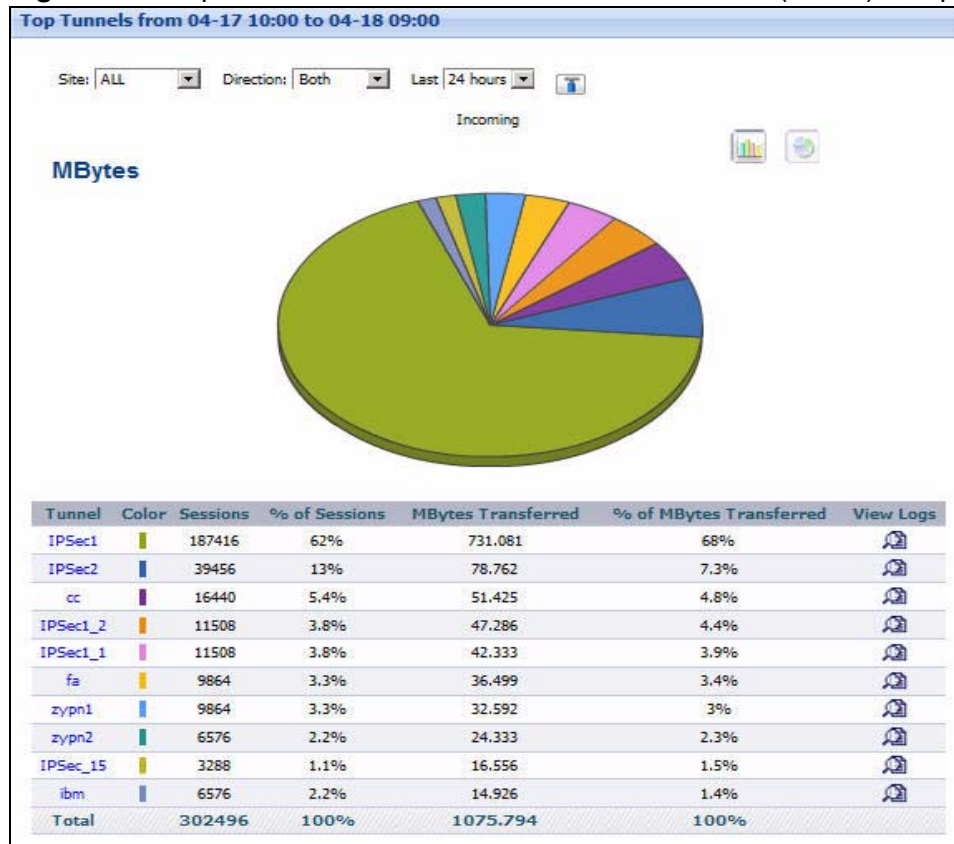
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of Secure Remote Access traffic to the selected peer IPSec router, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events for the selected destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's Secure Remote Access traffic was generated from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

6.1.7 Top Secure Remote Access Tunnels

Use this report to look at the Secure Remote Access tunnels with the most Secure Remote Access traffic.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels** to open this screen.

Figure 94 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels



Each field is described in the following table.

Table 81 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels

LABEL	DESCRIPTION
Site	Select a peer IPSec router. Select All to display the device's Secure Remote Access tunnels with the most traffic, regardless of which peer IPSec router they use.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 81 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels

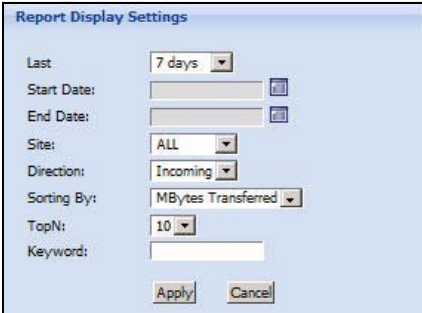
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Site and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Tunnel field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 81 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels

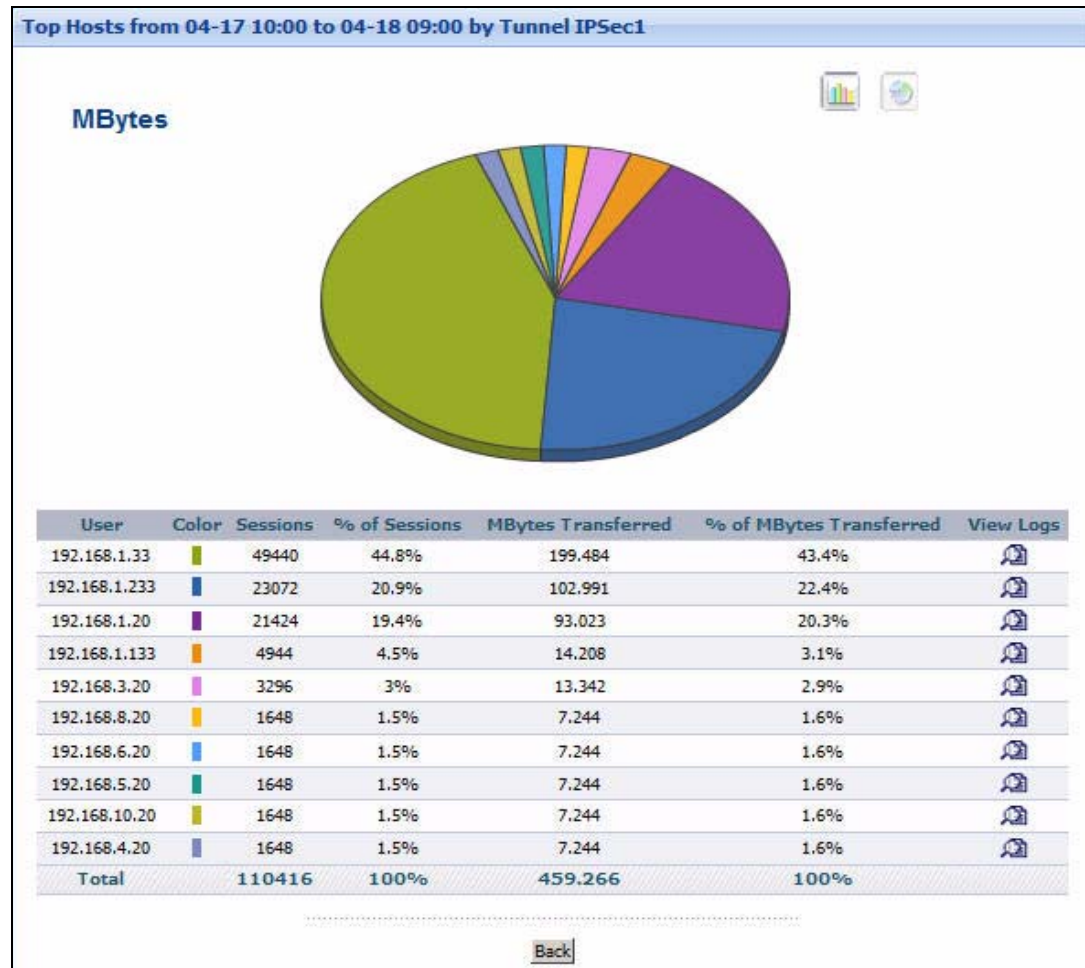
LABEL	DESCRIPTION
Tunnel	This field displays the phase 2 IPSec tunnels with the most Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of tunnels is less than the maximum number of records displayed in this table, every tunnel is displayed. Each tunnel is identified by the name of the phase 2 IPSec SA (also known as the network policy). Click on a name to look at the top sources of Secure Remote Access traffic for the selected tunnel.
Color	This field displays what color represents each tunnel in the graph.
Sessions	This field displays the number of traffic events for each tunnel.
% of Sessions	This field displays what percentage each tunnel's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each tunnel.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each tunnel.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.8 Top Secure Remote Access Tunnels Drill-Down

Use this report to look at the top senders or receivers of Secure Remote Access traffic for a top Secure Remote Access tunnel.

Click on a specific destination in **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels** to open this screen.

Figure 95 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels > Drill-Down



Each field is described in the following table.

Table 82 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels > Drill-Down

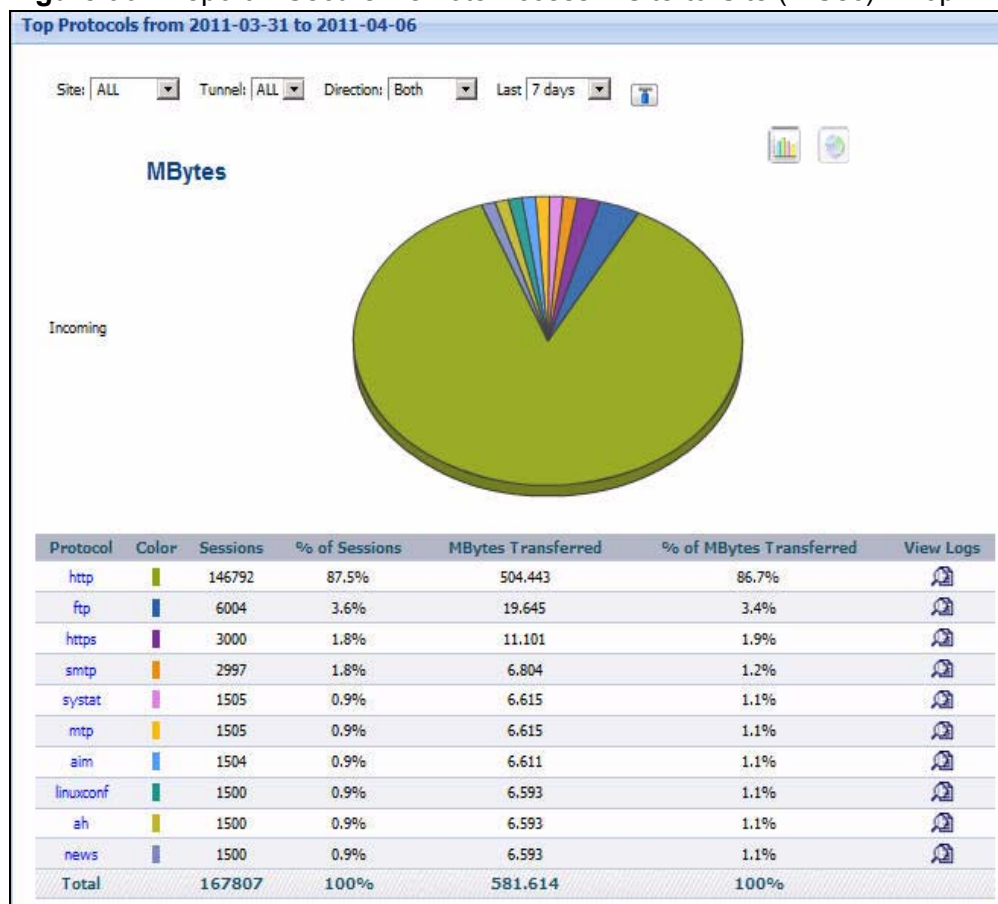
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of Secure Remote Access traffic for the selected Secure Remote Access tunnel, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events from each host to the selected Secure Remote Access tunnel.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access tunnel.
MBytes Transferred	This field displays how much traffic (in megabytes) went through the Secure Remote Access tunnel for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access tunnel's traffic was for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above. By default, only the top 10 hosts are displayed. You can change the number of hosts to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.1.9 Top Secure Remote Access Protocols

Use this report to look at the top services generating Secure Remote Access traffic through the selected device.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols** to open this screen.

Figure 96 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols



Each field is described in the following table.

Table 83 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols

LABEL	DESCRIPTION
Site	Select a peer IPSec router. Select All to display the device's Secure Remote Access tunnels with the most traffic, regardless of which peer IPSec router they use.
Tunnel	Select a Secure Remote Access tunnel. Select All to display the total traffic for the device's Secure Remote Access tunnels with the selected site (or all sites).
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 83 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols

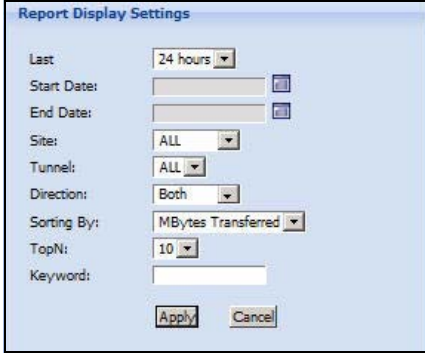
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Site, Tunnel and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Protocol field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 83 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols

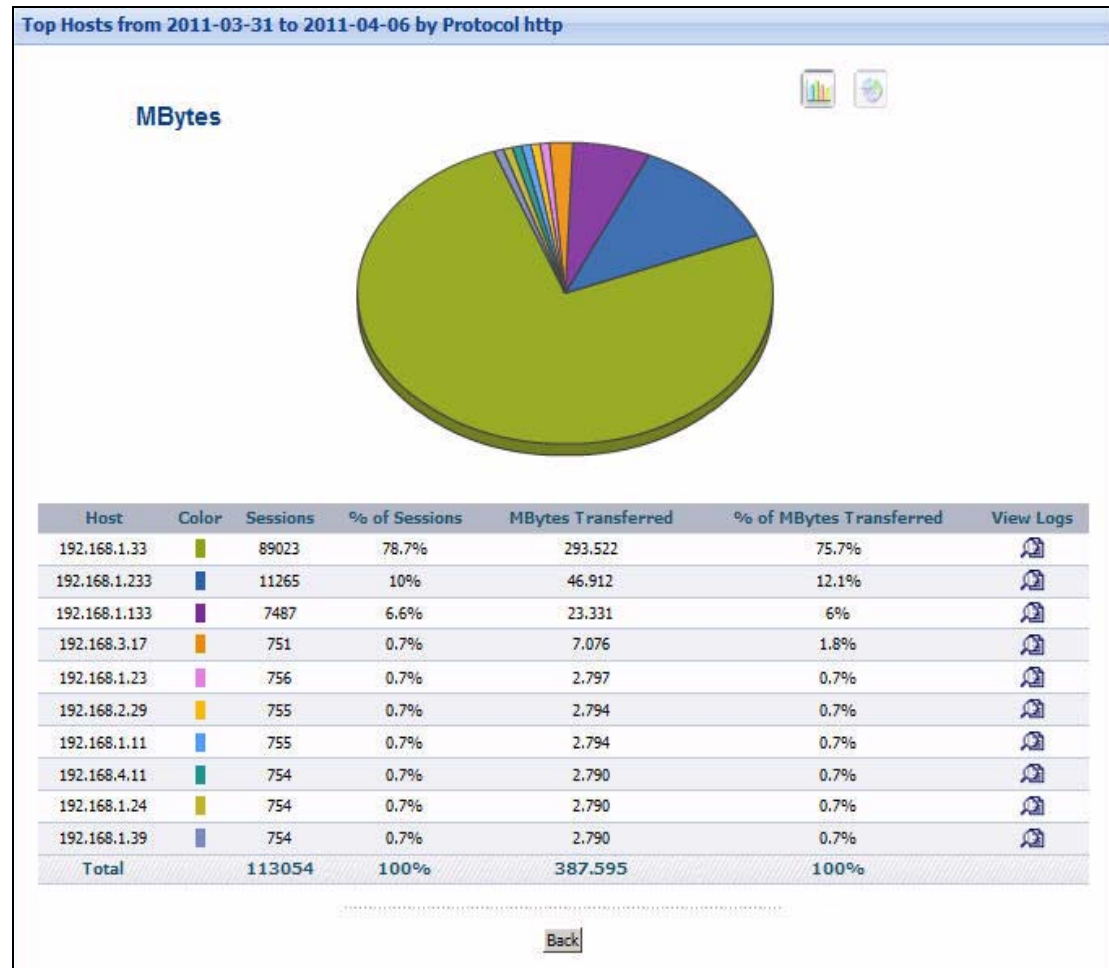
LABEL	DESCRIPTION
Protocol	This field displays the services most used by Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through Secure Remote Access.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the protocols above.

6.1.10 Top Secure Remote Access Protocols Drill-Down

Use this report to look at the top senders or receivers of any top service through Secure Remote Access.

Click on a specific service in **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols** to open this screen.

Figure 97 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols > Drill-Down



Each field is described in the following table.

Table 84 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols > Drill-Down

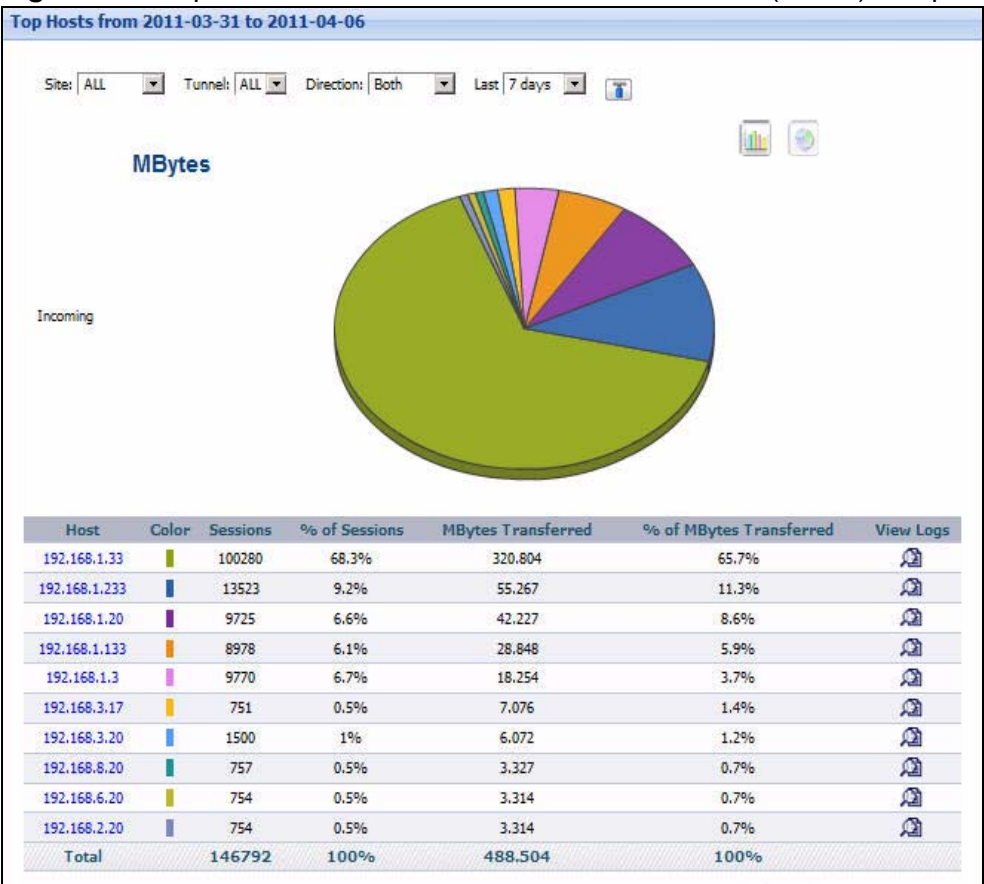
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of Secure Remote Access traffic using the selected service, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above. By default, only the top 10 hosts are displayed. You can change the number of hosts to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.1.11 Top Secure Remote Access Hosts

Use this report to look at the top senders or receivers of Secure Remote Access traffic.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts** to open this screen.

Figure 98 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts



Each field is described in the following table.

Table 85 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts

LABEL	DESCRIPTION
Site	Select a peer IPSec router. Select All to display the device's Secure Remote Access tunnels with the most traffic, regardless of which peer IPSec router they use. This field is not available with all models.
Tunnel	Select a Secure Remote Access tunnel. Select All to display the total traffic for the device's Secure Remote Access tunnels with the selected site (or all sites). This field is not available with all models.

Table 85 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts

LABEL	DESCRIPTION
Direction	Select which direction of traffic, you want to view statistics. This field is not available with all models. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.

Table 85 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts

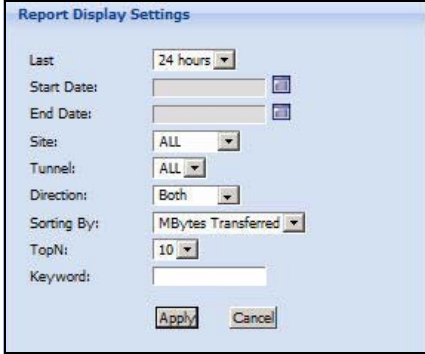
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Site, Tunnel and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 85 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts

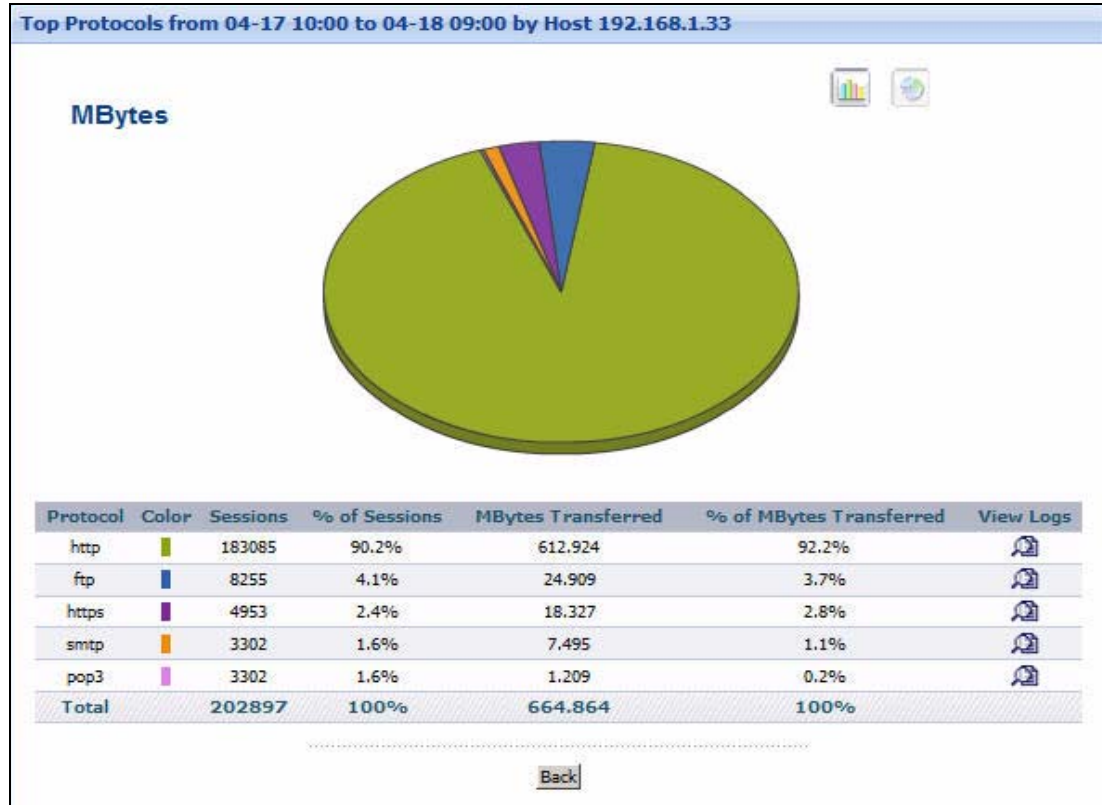
LABEL	DESCRIPTION
Host	This field displays the top senders or receivers of Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of hosts is less than the maximum number of records displayed in this table, every host is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a host to look at the top protocols of Secure Remote Access traffic for the selected host.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each host.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above.

6.1.12 Top Secure Remote Access Hosts Drill-Down

Use this report to look at the services sent through Secure Remote Access from a top sender or to a top receiver.

Click on a specific source in **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts** to open this screen.

Figure 99 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts > Drill-Down



Each field is described in the following table.

Table 86 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services of Secure Remote Access traffic from the selected host, sorted by the amount of traffic attributed to each one. Each service is identified by its IP address.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events of each protocol.

Table 86 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts > Drill-Down

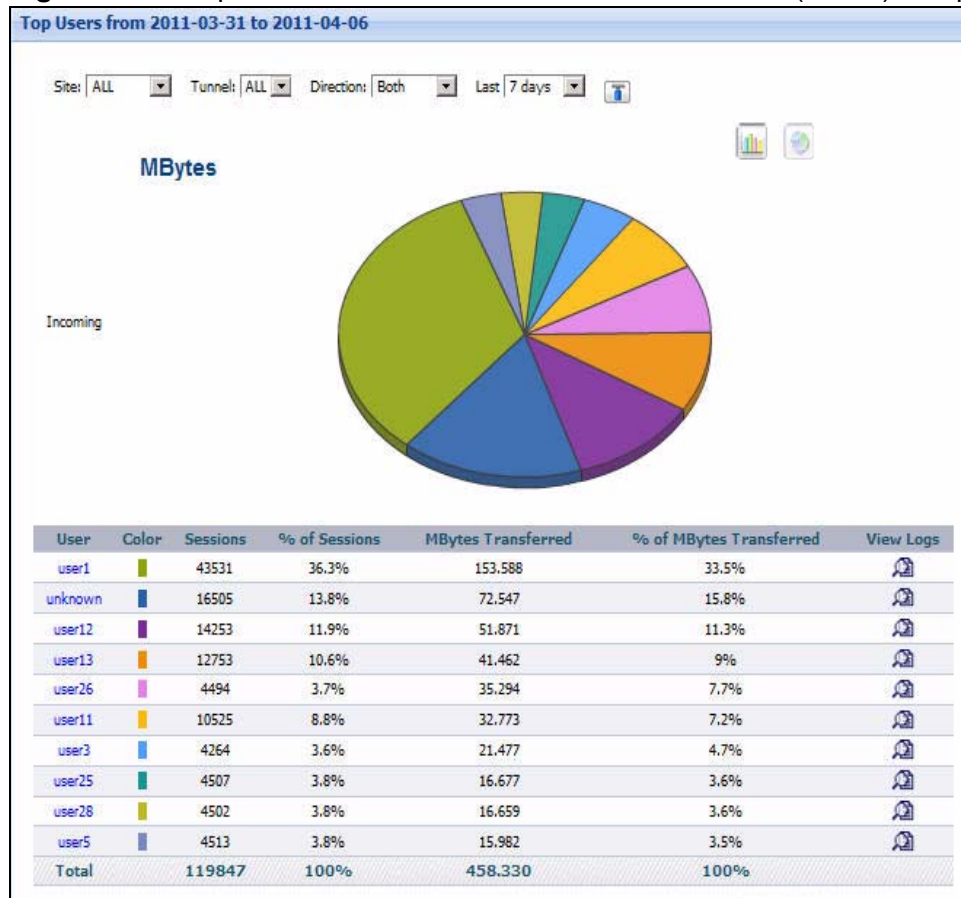
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the Secure Remote Access tunnels for each protocol.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic belonged to each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.1.13 Top Secure Remote Access Users

Use this report to look at the users that send or receive the most Secure Remote Access traffic.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users** to open this screen.

Figure 100 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users



Each field is described in the following table.

Table 87 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users

LABEL	DESCRIPTION
Site	Select a peer IPSec router. Select All to display the device's Secure Remote Access tunnels with the most traffic, regardless of which peer IPSec router they use.
Tunnel	Select a Secure Remote Access tunnel. Select All to display the total traffic for the device's Secure Remote Access tunnels with the selected site (or all sites).
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 87 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users

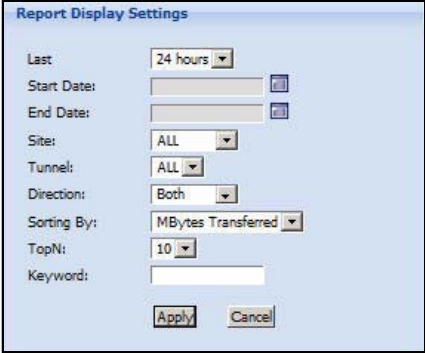
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Site, Tunnel and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 87 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users

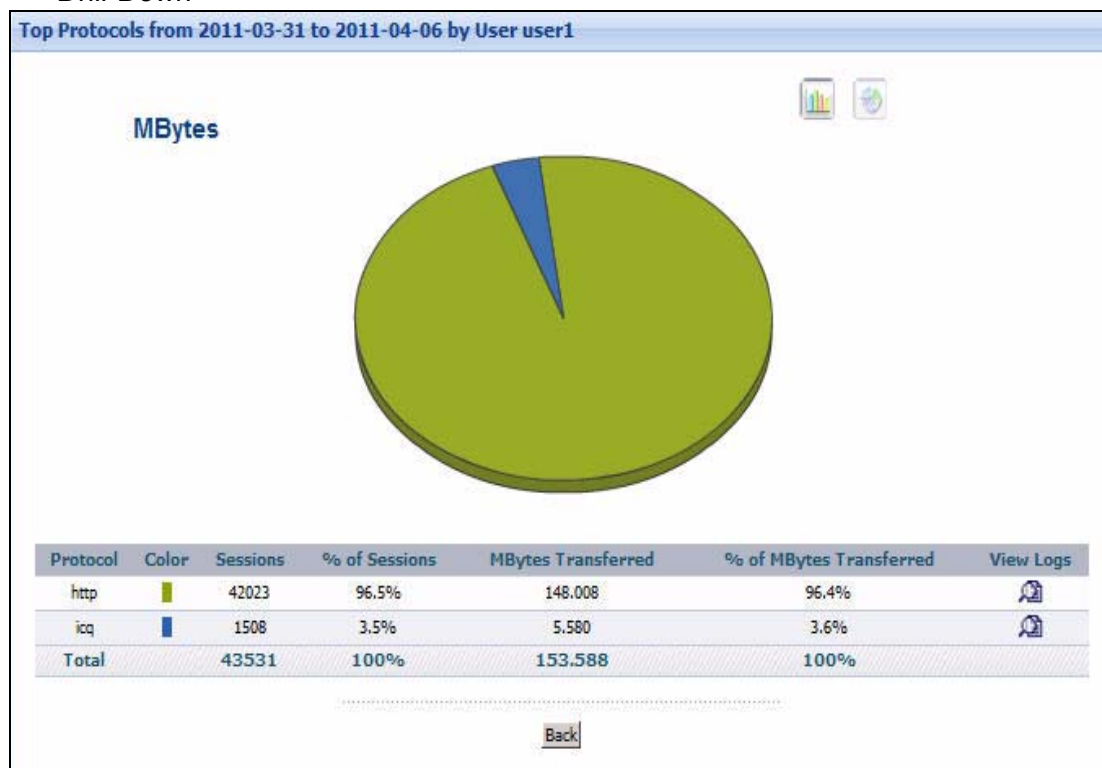
LABEL	DESCRIPTION
User	This field displays the top senders or receivers of Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user to look at where the user sent the most Secure Remote Access traffic.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

6.1.14 Top Secure Remote Access Users Drill-Down

Use this report to look at the services sent through Secure Remote Access from or to a top user.

Click on a specific source in **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users** to open this screen.

Figure 101 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users > Drill-Down



Each field is described in the following table.

Table 88 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services of Secure Remote Access traffic from the selected user, sorted by the amount of traffic attributed to each one.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events of each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.

Table 88 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users > Drill-Down

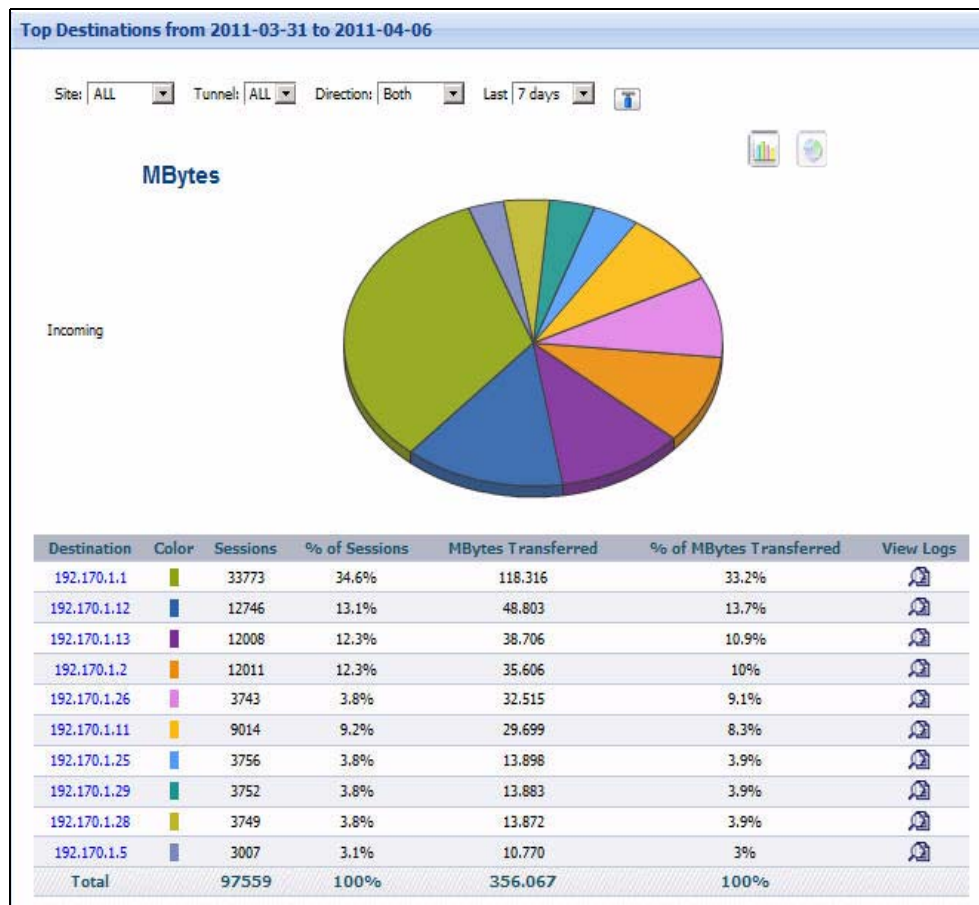
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the Secure Remote Access tunnels for each protocol.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic belonged to each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.1.15 Top Secure Remote Access Destinations

Use this report to look at the destinations with the most Secure Remote Access traffic.

Click **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations** to open this screen.

Figure 102 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations



Each field is described in the following table.

Table 89 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations

LABEL	DESCRIPTION
Site	Select a peer IPSec router. Select All to display the device's Secure Remote Access tunnels with the most traffic, regardless of which peer IPSec router they use.
Tunnel	Select a Secure Remote Access tunnel. Select All to display the total traffic for the device's Secure Remote Access tunnels with the selected site (or all sites).

Table 89 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations

LABEL	DESCRIPTION
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Site, Tunnel and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.

Table 89 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations

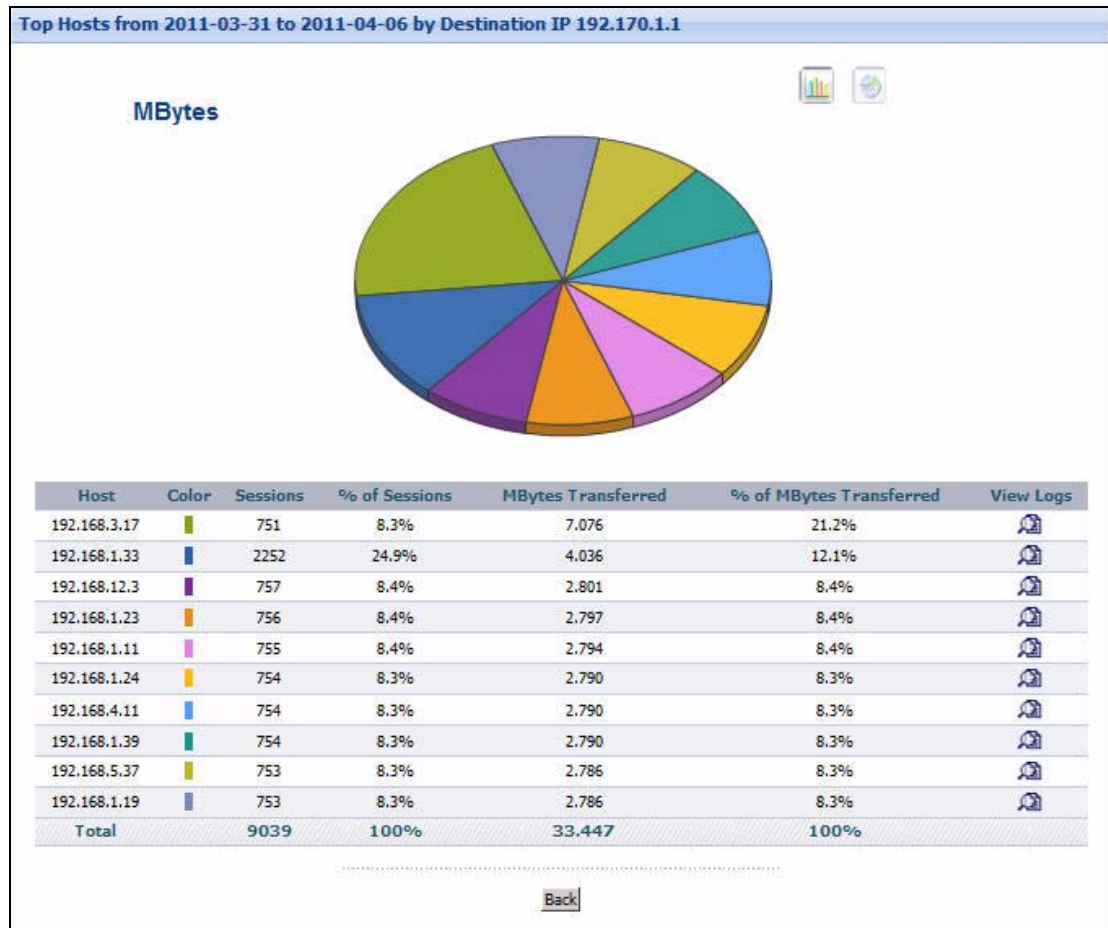
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the where the device sent the most Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the sender hosts that sent the most Secure Remote Access traffic to the selected host.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.16 Top Secure Remote Access Destinations Drill-Down

Use this report to look at the services sent through Secure Remote Access from or to a top destination.

Click on a specific destination in **Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations** to open this screen.

Figure 103 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations > Drill-Down



Each field is described in the following table.

Table 90 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of Secure Remote Access traffic using the selected service, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events of each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the Secure Remote Access tunnels for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic belonged to each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. By default, only the top hosts are displayed. You can change the number of hosts to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.2 Secure Remote Access - Client-to-Site (IPSec)

Secure Remote Access tunnels with the remote gateway set as any are called dynamic tunnels (only the remote device can initiate a dynamic IPSec Secure Remote Access tunnel). Devices can use xauth to authenticate remote users (by username and password) when they try to initiate a dynamic Secure Remote Access tunnel. The Secure Remote Access remote access screens display statistics for remote users that use dynamic Secure Remote Access tunnels and have been authenticated by xauth.

6.2.1 Secure Remote Access User Status

Use this report to see statistics about the device's remote Secure Remote Access users.

Click **Report > Secure Remote Access > Client-to-Site (IPSec) > User Status** to open this screen.

Figure 104 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status

User Status from 2011-03-15 to 2011-04-13

User Status: Number per Page: Last:

User Name	Status	Login Time	Logout Time	Duration	IP	Incoming Traffic(MBytes)	Outgoing Traffic(MBytes)
Ian		2011-03-29 09:09:09		15 days 2 hours	172.25.21.7	2048,000	2048,000
Ping		2011-03-29 09:09:09		15 days 2 hours	172.25.21.7	61.489	25,068
Windy		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	63.858	28,315
Sunny		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	4,746	1,022
Rain		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	6,044	0,873
Jiji		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	7,355	0,582
Jimmy		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	0,797	4,392
Poka		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	0,799	0,583
Sam		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	1,064	0,043
Luse		2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	0,551	0,205

Total Count:18 Total Page:2 First 1 2 Last Go

Each field is described in the following table.

Table 91 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status

LABEL	DESCRIPTION
User Status	Select which status of users, you want to view statistics. ALL - to display for both connected and disconnected users. Online - to display information for connected users. Offline - to display information for disconnected users.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
User Name	This field displays the top remote access senders or receivers of Secure Remote Access traffic in the selected device. Click the title of this column to sort the list of users in alphabetical or reverse-alphabetical order. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Status	This column displays the current status of users who have logged in. A user's status icon is green when the user is currently connected. A user's status icon is red when the user has already logged out.

Table 91 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status

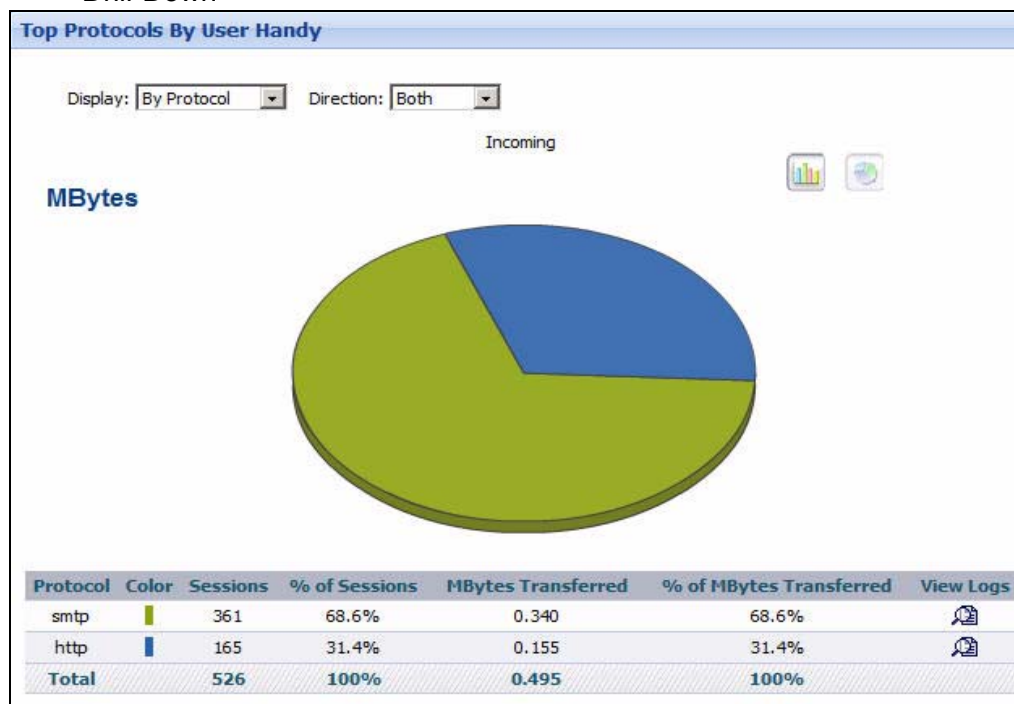
LABEL	DESCRIPTION
Login Time	This column displays when the remote access user last logged in. Click the title of this column to sort the list of users by the time they last logged in.
Logout Time	This column displays when the remote access user last logged out. The field is empty if the remote access user is still logged in. Click the title of this column to sort the list of users by the time they last logged out.
Duration	This field displays current length (duration) of the login if the remote access user is still logged in. Click the title of this column to sort the list of users by how long they have been logged in.
IP	This field displays the user's IP address. Click the title of this column to sort the list of users by IP address.
Incoming Traffic (MBytes)	This field displays the amount of traffic received by the user through the device. Click the title of this column to sort the list of users by the amount of traffic routed through the device.
Outgoing Traffic (MBytes)	This field displays the amount of traffic sent by the user through the device. Click the title of this column to sort the list of users by the amount of traffic routed from the device.
Total	This entry displays the total number of users on each page of the report.

6.2.2 Secure Remote Access User Status Drill-Down

Use this report to look at the services transferred through the device by any top users.

Click on a specific user in **Report > Secure Remote Access > Client-to-Site (IPSec) > User Status** to open this screen.

Figure 105 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status > Drill-Down



Each field is described in the following table.

Table 92 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status > Drill-Down

LABEL	DESCRIPTION
Display	Select how you want the report to show statistics. By Protocol - all services sent or received by the specific user. By Destination - all destination hosts the user sent traffic to.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 92 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status > Drill-Down

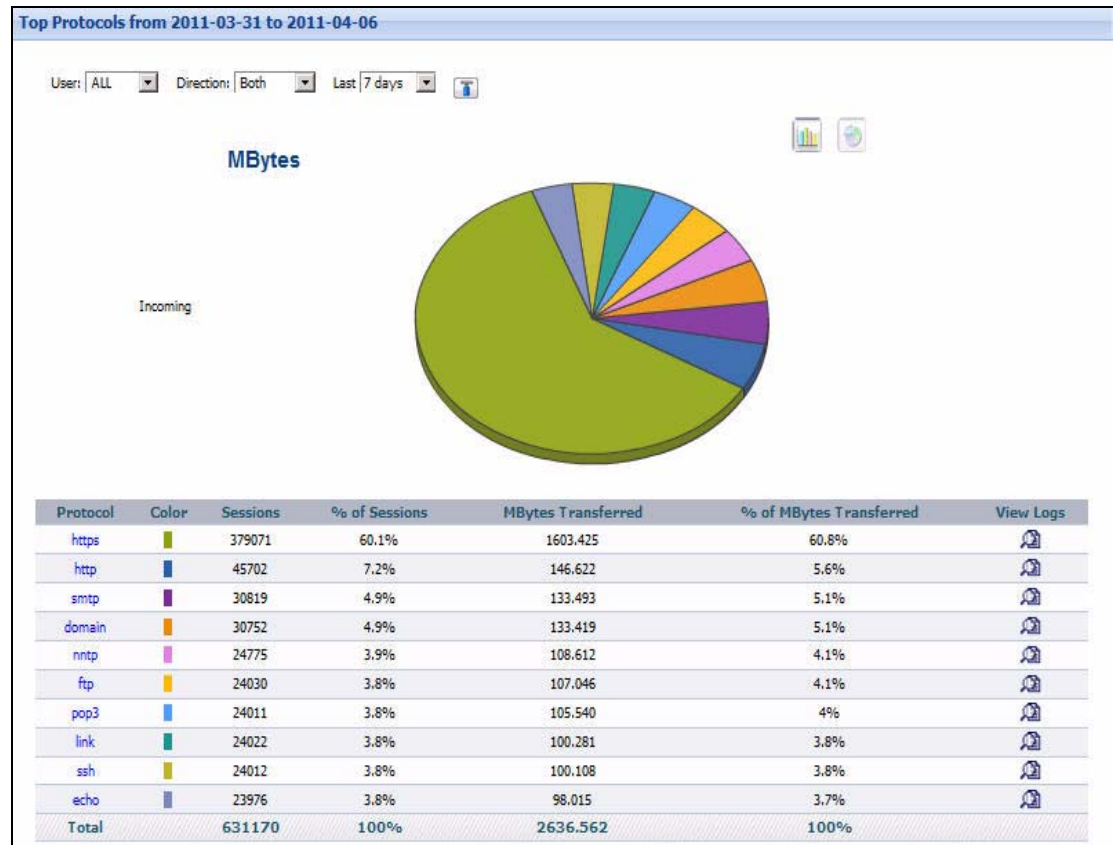
LABEL	DESCRIPTION
Protocol	This field displays the services most used by the selected user, sorted by the amount of traffic for each one. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings . Each protocol is identified by its service type name.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service.
% of Sessions	This field displays what percentage each service's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each service.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.2.3 Top Secure Remote Access Protocols

Use this report to display which services the remote access users sent or received the most.

Click **Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols** to open this screen.

Figure 106 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols



Each field is described in the following table.

Table 93 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols

LABEL	DESCRIPTION
User	Select a remote access user. Select ALL to display the protocols with the most traffic sent through the remote access Secure Remote Access tunnels.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 93 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols

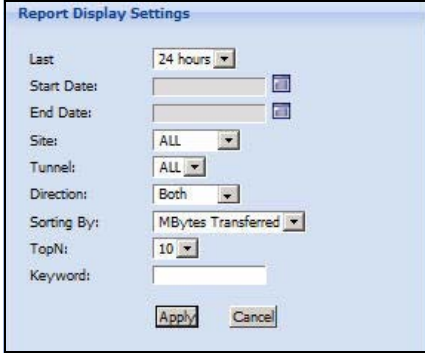
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The User and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Protocol field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 93 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols

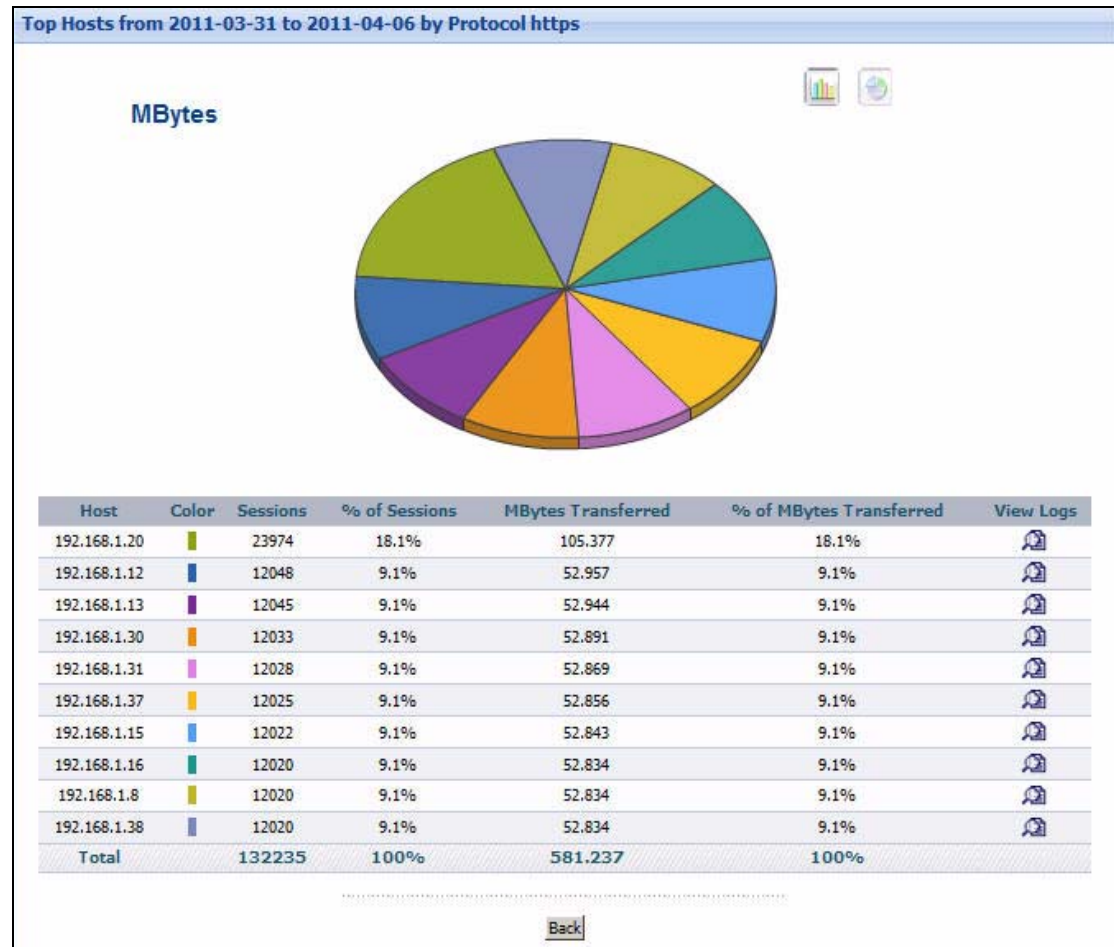
LABEL	DESCRIPTION
Protocol	This field displays the services most used by remote access Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through Secure Remote Access.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

6.2.4 Top Secure Remote Access Protocols Drill-Down

Use this report to look at the top remote access senders or receivers of any top service.

Click on a specific service in **Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols** to open this screen.

Figure 107 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols > Drill-Down



Each field is described in the following table.

Table 94 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols > Drill-Down

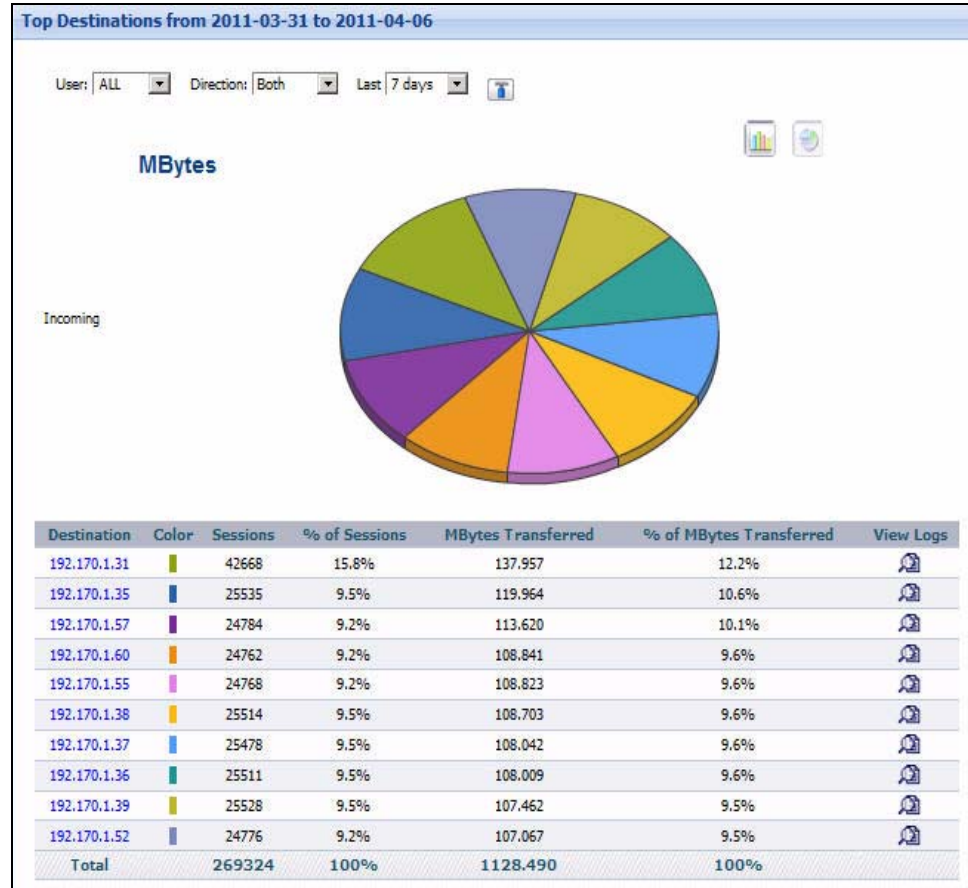
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of Secure Remote Access traffic using the selected service, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above. By default, only the top 10 hosts are displayed. You can change the number of hosts to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.2.5 Top Secure Remote Access Destinations

Use this report to look at the destinations with the most remote access Secure Remote Access traffic.

Click **Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations** to open this screen.

Figure 108 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations



Each field is described in the following table.

Table 95 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations

LABEL	DESCRIPTION
User	Select a remote access user. Select ALL to display the destinations with the most traffic sent through the remote access Secure Remote Access tunnels.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 95 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations

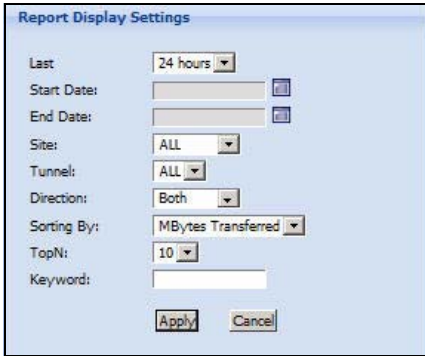
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The User and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 95 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations

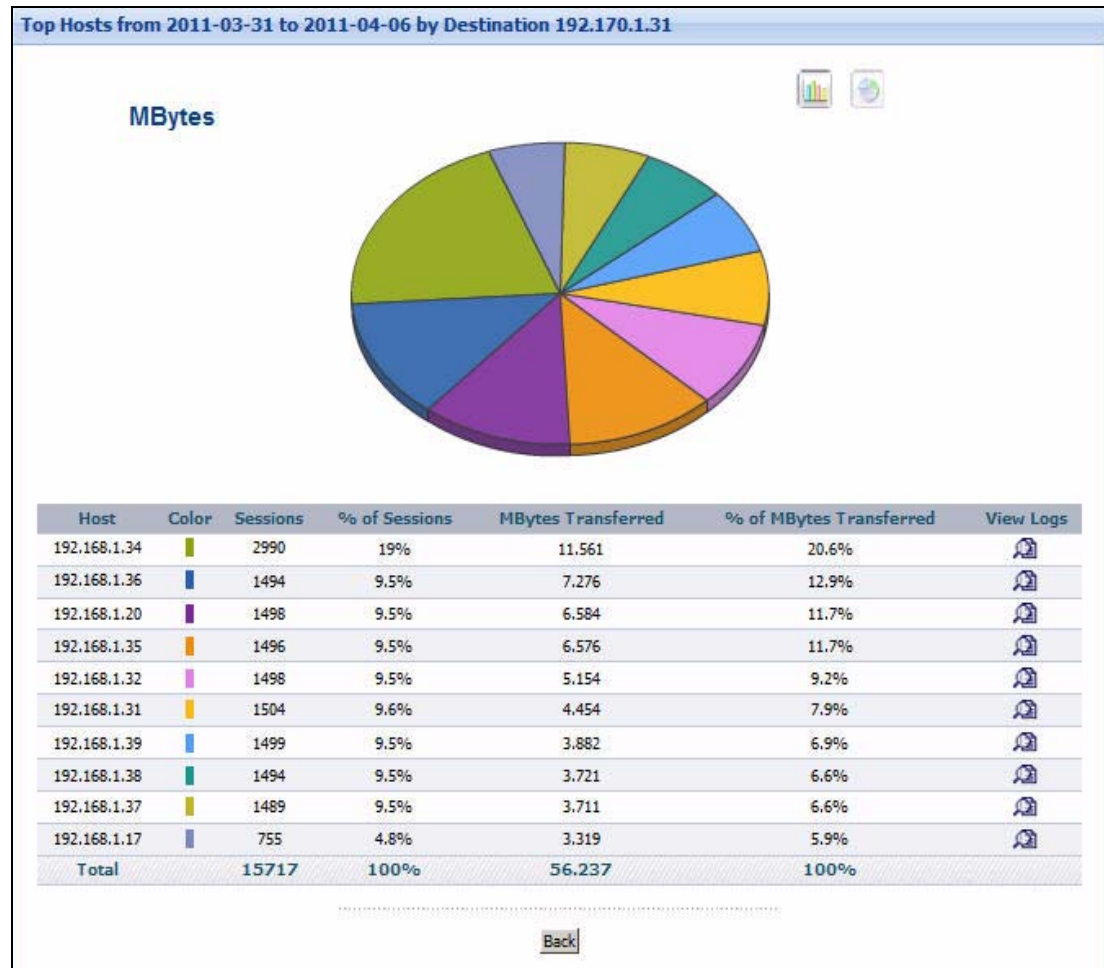
LABEL	DESCRIPTION
Destination	This field displays the IP addresses to which the selected device sent the most remote access Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the sender hosts that send the most Secure Remote Access traffic to the selected host.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.2.6 Top Secure Remote Access Destinations Drill-Down

Use this report to look at the remote access hosts that sent the most traffic to the selected top destination.

Click on a specific destination in **Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations** to open this screen.

Figure 109 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations > Drill-Down



Each field is described in the following table.

Table 96 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations > Drill-Down

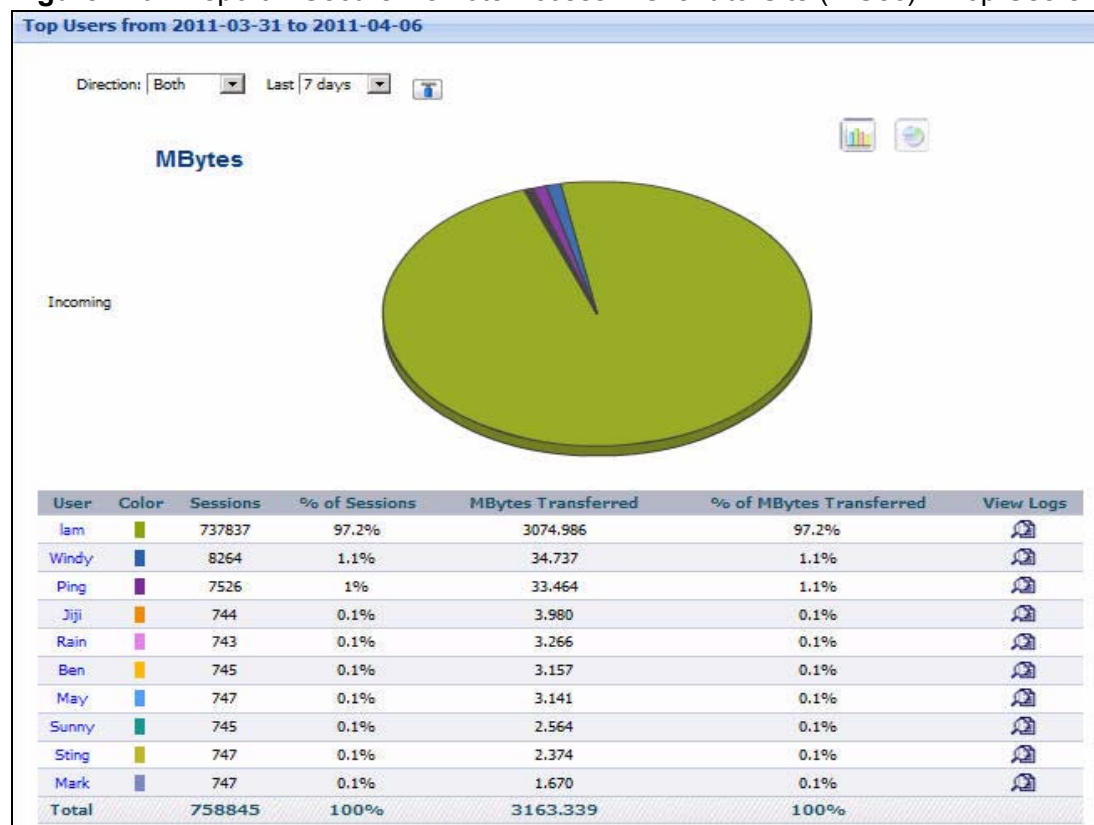
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources that sent remote access Secure Remote Access traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events of each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the Secure Remote Access tunnels for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic belonged to each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above. By default, only the top 10 hosts are displayed. You can change the number of hosts to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.2.7 Secure Remote Access Top Users

Use this report to look at the users that send or receive the most Secure Remote Access traffic.

Click **Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users** to open this screen.

Figure 110 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users



Each field is described in the following table.

Table 97 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users

LABEL	DESCRIPTION
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.

Table 97 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users

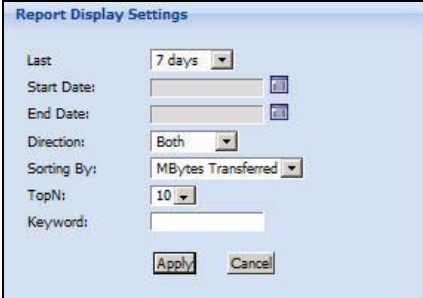
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the Settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Direction field is the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most remote access Secure Remote Access traffic. Click on a user to look at the services of Secure Remote Access traffic sent or received the most by the selected user.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 97 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users

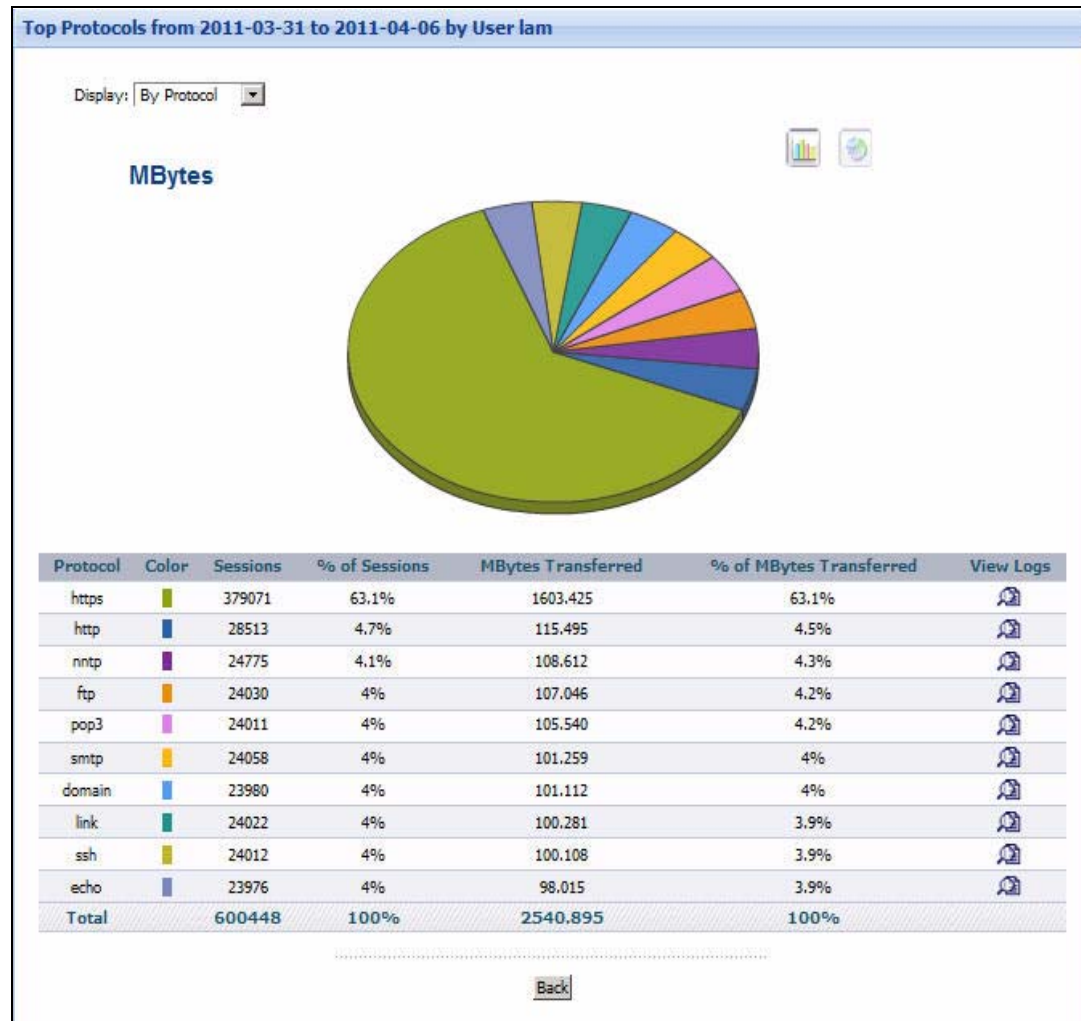
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.2.8 Secure Remote Access Top Users Drill-Down

Use this report to look at the services transferred the most through Secure Remote Access remote access by any top users.

Click on a specific user in **Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users** to open this screen.

Figure 111 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users > Drill-Down



Each field is described in the following table.

Table 98 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users > Drill-Down

LABEL	DESCRIPTION
Display	Select how you want the report to show statistics. By Protocol - all services sent or received by the specific user. By Destination - all destination hosts the user sent traffic to.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most used by the selected user, sorted by the amount of traffic for each one. By default, only the top 10 services are displayed. You can change the number of hosts to be displayed through the TopN setting in Settings . Each protocol is identified by its name.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.3 Secure Remote Access - Client-to-Site (SSL)

SSL Secure Remote Access tunnels are HTTPS connections via the ZyXEL devices. Only remote hosts can initiate SSL Secure Remote Access tunnels. Devices authenticates remote users (by username and password) when they try to initiate a SSL Secure Remote Access tunnel. The Secure Remote Access remote access screens display statistics for remote users that use SSL Secure Remote Access tunnels and have been authenticated.

6.3.1 Secure Remote Access User Status

Use this report to see statistics about the device's remote Secure Remote Access users.

Click **Report > Secure Remote Access > Client-to-Site (SSL) > User Status** to open this screen.

Figure 112 Report > Secure Remote Access > Client-to-Site (SSL) > User Status

User Status from 2011-03-15 to 2011-04-13

User Status: Number per Page: Last

User Name	Status	Login Time	Logout Time	Duration	IP	Incoming Traffic(MBytes)	Outgoing Traffic(MBytes)
gary0		2011-03-29 09:08:57		15 days 2 hours	0.0.0.0	0	0

Total Count:1 Total Page:1 First 1 Last

Each field is described in the following table.

Table 99 Report > Secure Remote Access > Client-to-Site (SSL) > User Status

LABEL	DESCRIPTION
User Status	Select which status of users, you want to view statistics. ALL - to display for both connected and disconnected users. Online - to display information for connected users. Offline - to display information for disconnected users.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.

Table 99 Report > Secure Remote Access > Client-to-Site (SSL) > User Status

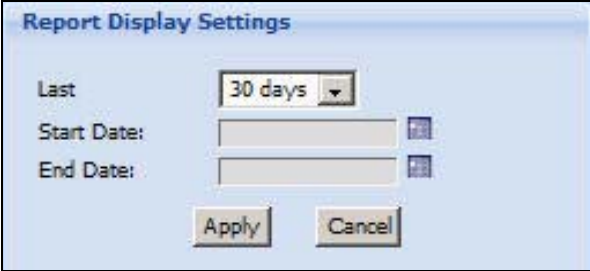
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen.
User Name	This field displays the top remote access senders or receivers of Secure Remote Access traffic in the selected device. Click the title of this column to sort the list of users in alphabetical or reverse-alphabetical order. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Status	This column displays the current status of users who have logged in. A user's status icon is green when the user is currently connected. A user's status icon is red when the user has already logged out.
Login Time	This column displays when the remote access user last logged in. Click the title of this column to sort the list of users by the time they last logged in.
Logout Time	This column displays when the remote access user last logged out. The field is empty if the remote access user is still logged in. Click the title of this column to sort the list of users by the time they last logged out.
Duration	This field displays current length (duration) of the login if the remote access user is still logged in. Click the title of this column to sort the list of users by how long they have been logged in.
IP	This field displays the user's IP address. Click the title of this column to sort the list of users by IP address.
Incoming Traffic (MBytes)	This field displays the amount of Secure Remote Access traffic sent or received by the user and routed through the device. Click the title of this column to sort the list of users by the amount of traffic routed through the device.

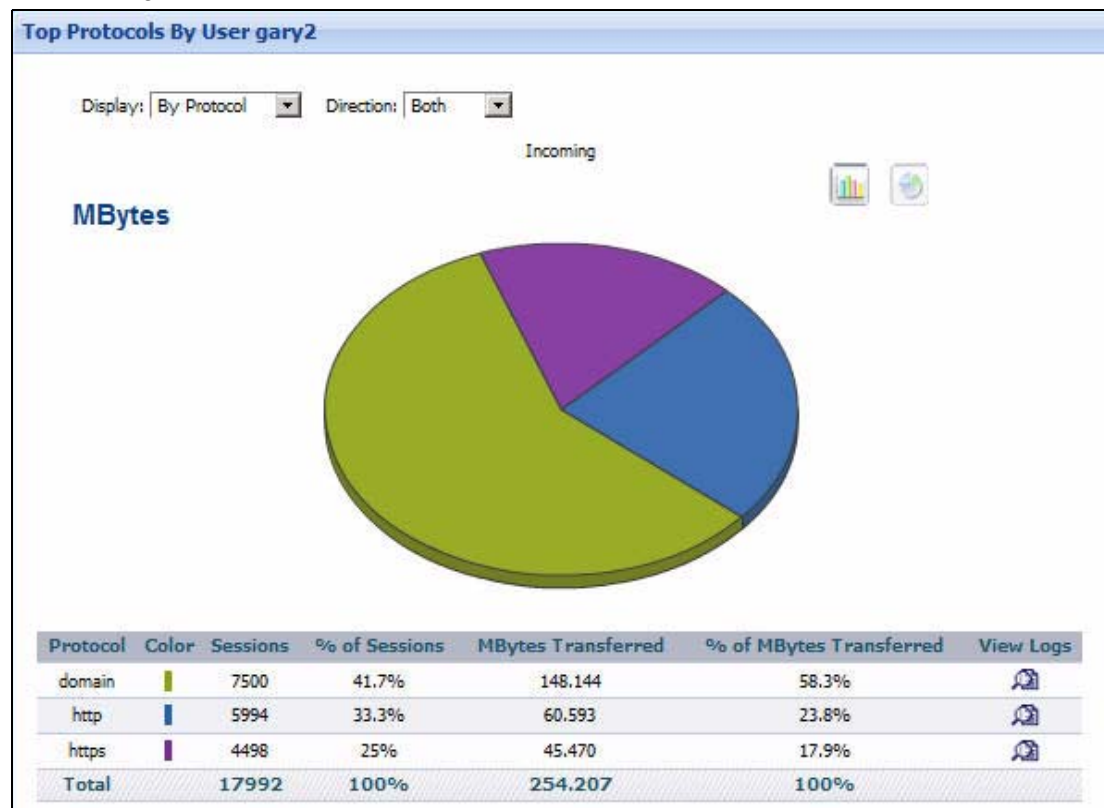
Table 99 Report > Secure Remote Access > Client-to-Site (SSL) > User Status

LABEL	DESCRIPTION
Outgoing Traffic (MBytes)	This field displays the amount of Secure Remote Access traffic sent or received by the user and routed by the device. Click the title of this column to sort the list of users by the amount of traffic routed from the device.
Total	This entry displays the total number of users on each page of the report.

6.3.2 Secure Remote Access User Status Drill-Down

Use this report to look at the services transferred through the device by any top users.

Click on a specific user in **Report > Secure Remote Access > Client-to-Site (SSL) > User Status** to open this screen.

Figure 113 Report > Secure Remote Access > Client-to-Site (SSL) > User Status > Drill-Down

Each field is described in the following table.

Table 100 Report > Secure Remote Access > Client-to-Site (SSL) > User Status > Drill-Down

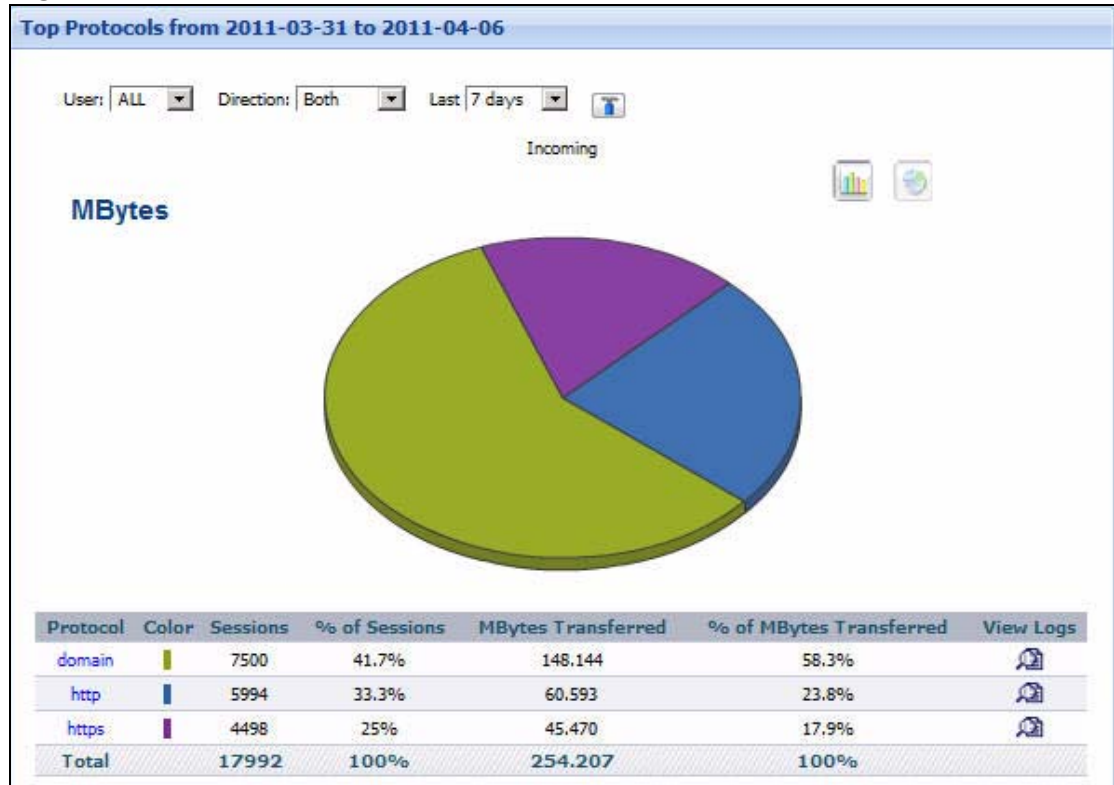
LABEL	DESCRIPTION
Display	Select how you want the report to show statistics. By Protocol - all services sent or received by the specific user. By Destination - all destination hosts the user sent traffic to. By Application - all internal services the user accessed to.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most used by the selected user, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected user.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each service.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the service above. The entry is just for top 10 services for the selected user.
Back	Click this to return to the main report.

6.3.3 Top Secure Remote Access Protocols

Use this report to display which services the remote access users used the most.

Click **Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols** to open this screen.

Figure 114 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols



Each field is described in the following table.

Table 101 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols

LABEL	DESCRIPTION
User	Select a remote access user. Select ALL to display the protocols with the most traffic sent through the remote access Secure Remote Access tunnels.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 101 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols

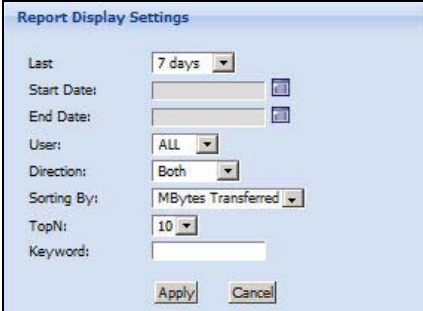
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The User and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Protocol field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 101 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols

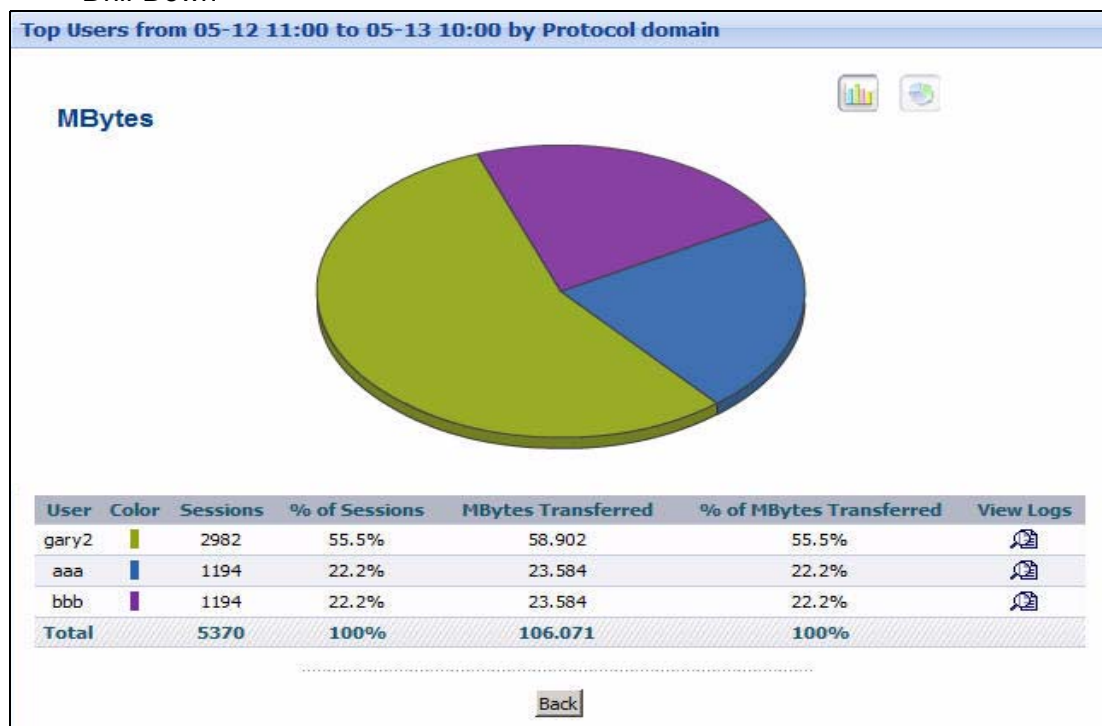
LABEL	DESCRIPTION
Protocol	This field displays the services most transferred through SSL Secure Remote Access tunnel in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through Secure Remote Access.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

6.3.4 Top Secure Remote Access Protocols Drill-Down

Use this report to look at the remote access senders or receivers who sent the most traffic for a specific service.

Click on a specific service in **Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols** to open this screen.

Figure 115 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols > Drill-Down



Each field is described in the following table.

Table 102 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most Secure Remote Access traffic using the selected service.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.

Table 102 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols > Drill-Down

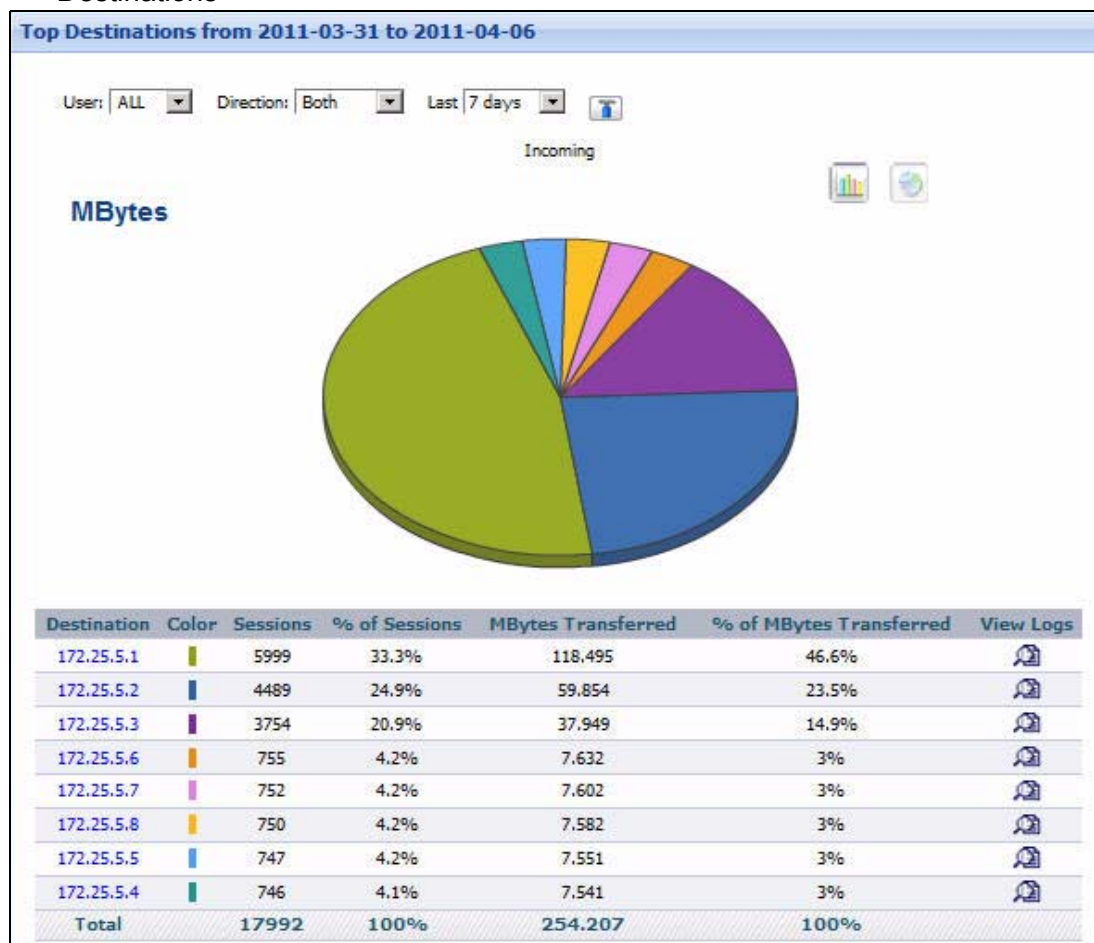
LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.3.5 Top Secure Remote Access Destinations

Use this report to look at the destinations with the most remote access Secure Remote Access traffic.

Click **Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations** to open this screen.

Figure 116 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations



Each field is described in the following table.

Table 103 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations

LABEL	DESCRIPTION
User	Select a remote access user. Select ALL to display the destinations with the most traffic sent through the remote access Secure Remote Access tunnels.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.

Table 103 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations

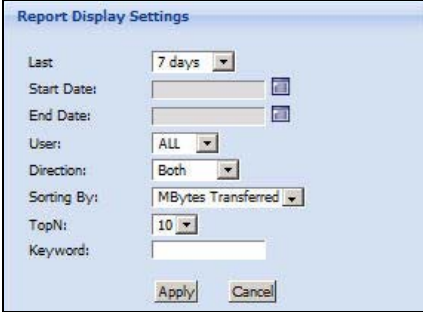
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The User and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 103 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations

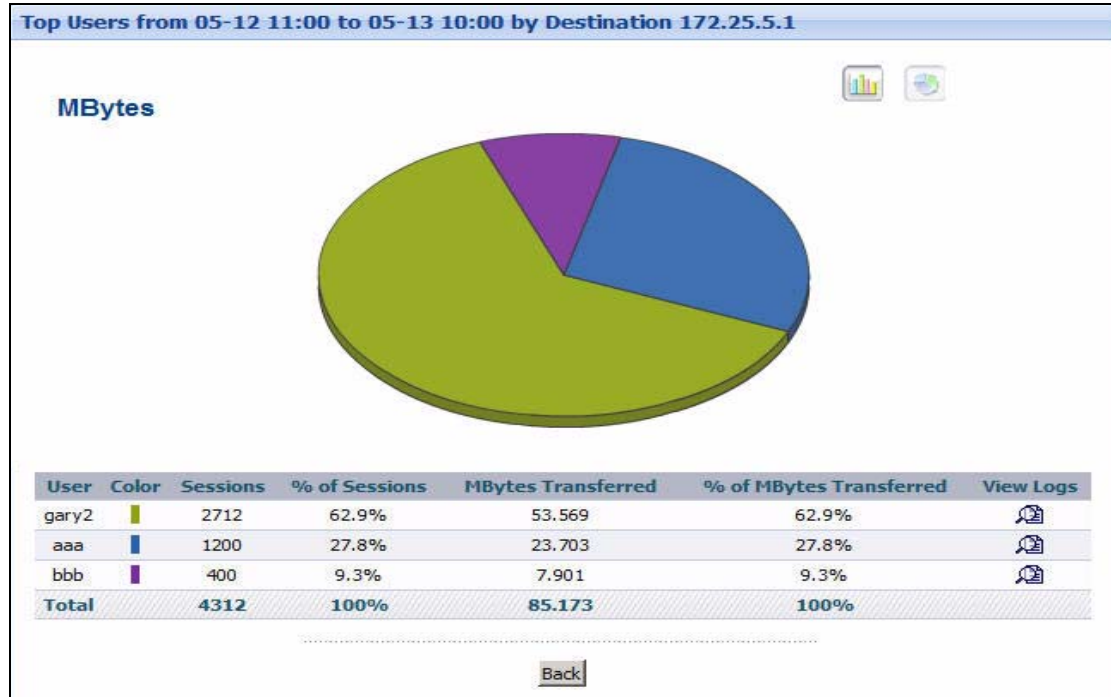
LABEL	DESCRIPTION
Destination	This field displays where the remote user sent the most Secure Remote Access traffic, sorted by the amount of traffic for each destination. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the sender hosts that sent the most SSL Secure Remote Access traffic to the selected host.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the traffic summary for the destination hosts.

6.3.6 Top Secure Remote Access Destinations Drill-Down

Use this report to look at the remote access hosts that sent the most traffic to the selected top destination.

Click on a specific destination in **Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations** to open this screen.

Figure 117 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations > Drill-Down



Each field is described in the following table.

Table 104 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most Secure Remote Access traffic to the selected destination host.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each user.

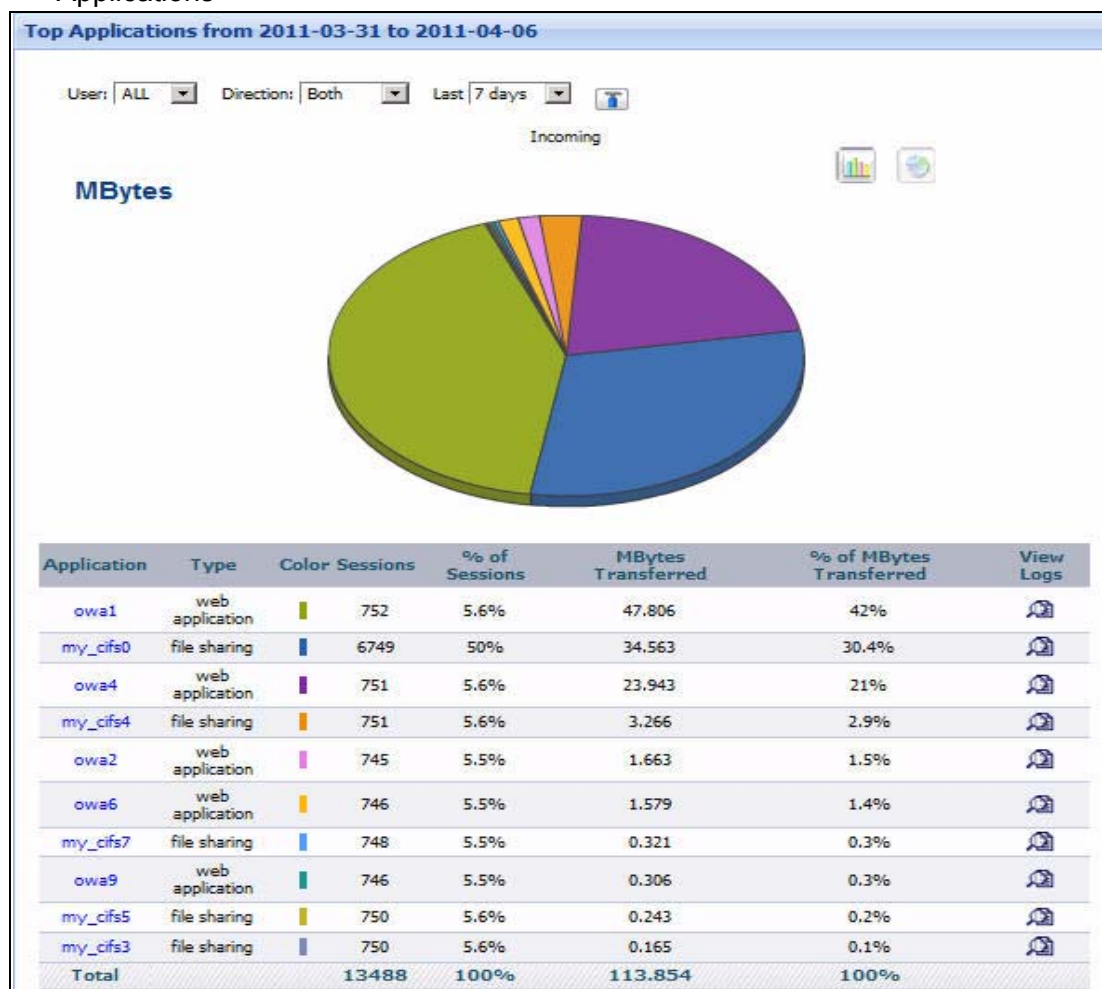
Table 104 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations > Drill-Down

LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.3.7 Top Secure Remote Access Applications

Use this report to look at the applications with the most remote access Secure Remote Access traffic.

Click **Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications** to open this screen.

Figure 118 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications

Each field is described in the following table.

Table 105 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications

LABEL	DESCRIPTION
User	Select a remote access user. Select ALL to display the applications with the most traffic sent through the remote access Secure Remote Access tunnels.
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.

Table 105 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications

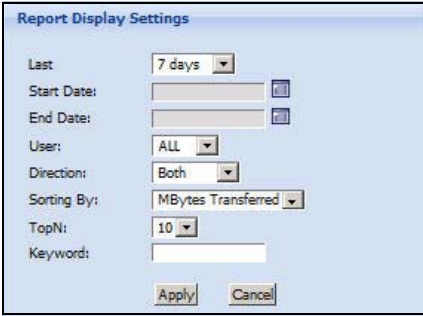
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The User and Direction fields are the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Application field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the internal services the remote users access the most through SSL Secure Remote Access, sorted by the amount of traffic for each one. If the number of applications is less than the maximum number of records displayed in this table, every application is displayed. Each application is identified by its name. Click on an application to look at the top remote user's hosts of Secure Remote Access traffic for the selected application.
Type	This field displays what kind of service the internal server provides.

Table 105 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications

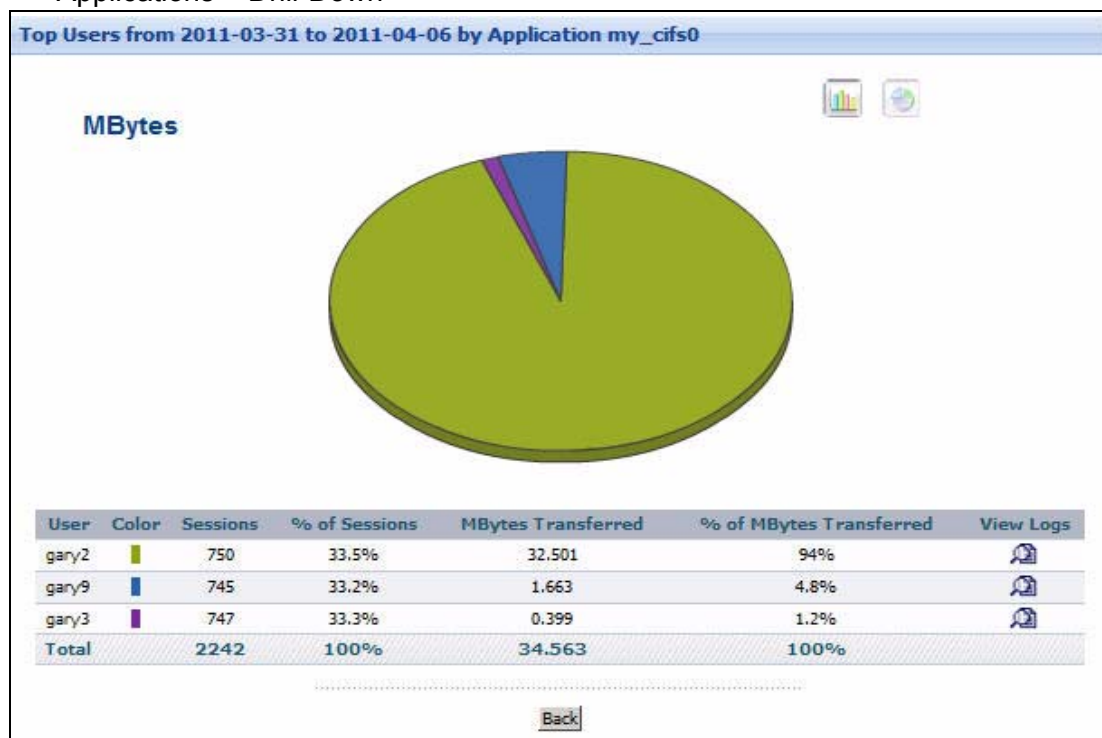
LABEL	DESCRIPTION
Color	This field displays what color represents each application in the graph.
Sessions	This field displays the number of traffic events for each application.
% of Sessions	This field displays what percentage each application's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each application.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each application.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the traffic summary for the application servers. By default, only the top 10 application servers are displayed. You can change the number of application servers to be displayed through the TopN setting in Settings .

6.3.8 Top Secure Remote Access Applications Drill-Down

Use this report to look at the remote access hosts that sent the most traffic to the selected Secure Remote Access application.

Click on a specific application in **Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications** to open this screen.

Figure 119 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications > Drill-Down



Each field is described in the following table.

Table 106 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most Secure Remote Access traffic to access the selected application service.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.

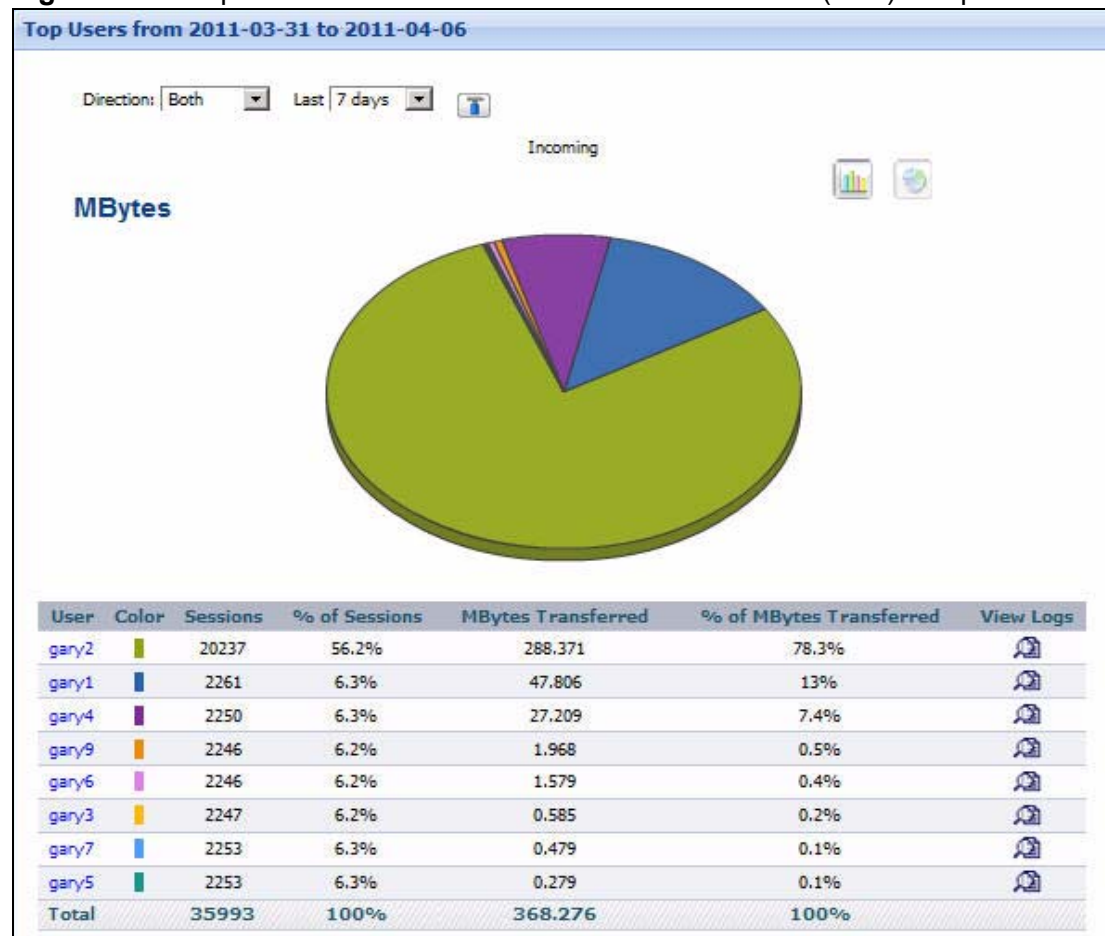
Table 106 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications > Drill-Down

LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.3.9 Secure Remote Access Top Users

Use this report to look at the users that send or receive the most Secure Remote Access traffic.

Click **Report > Secure Remote Access > Client-to-Site (SSL) > Top Users** to open this screen.

Figure 120 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users

Each field is described in the following table.

Table 107 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users

LABEL	DESCRIPTION
Direction	Select which direction of traffic, you want to view statistics. Both - all Secure Remote Access traffic the devices sent or received. Incoming - all traffic the devices received through Secure Remote Access tunnel. Outgoing - all traffic the devices sent out through Secure Remote Access tunnel.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. The Direction field is the same as in the main screen. Select MBytes Transferred to sort the records by the amount of traffic. Select Sessions to sort by the number of sessions. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click Apply to update the report immediately, or click Cancel to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.

Table 107 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users

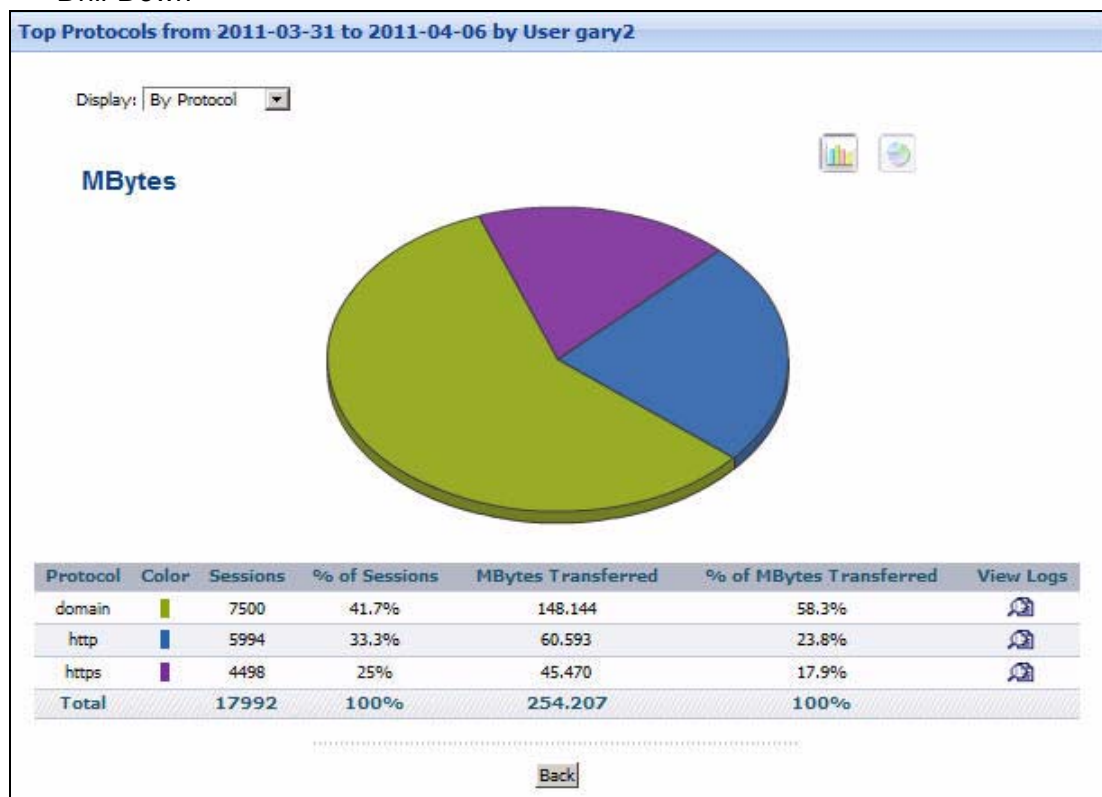
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most Secure Remote Access traffic. Click on a user to look at the services of Secure Remote Access traffic sent or received the most by the selected user.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .

6.3.10 Secure Remote Access Top Users Drill-Down

Use this report to look at the services sent the most through Secure Remote Access by the selected user.

Click on a specific user in **Report > Secure Remote Access > Client-to-Site (SSL) > Top Users** to open this screen.

Figure 121 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users > Drill-Down



Each field is described in the following table.

Table 108 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users > Drill-Down

LABEL	DESCRIPTION
Display	Select how you want the report to show statistics. By Protocol - all services sent or received by the specific user. By Destination - all destination hosts the user sent traffic to. By Application - all internal services the user accessed to.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 108 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users > Drill-Down

LABEL	DESCRIPTION
Protocol	This field displays the services for which the selected user sent or received the most traffic, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected Secure Remote Access traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each host.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the traffic summary for the services. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the TopN setting in Settings .
Back	Click this to return to the main report.

6.4 Xauth

Devices can use xauth to authenticate remote users (by username and password) when they try to initiate a dynamic IPsec Secure Remote Access tunnel. Use these screens to display records of successful and unsuccessful logins to the device's IPsec Secure Remote Access tunnels.

6.4.1 Secure Remote Access Successful Login

Use this report to monitor the total number of users that have successfully logged in to use one of the device's Secure Remote Access tunnels.

Click **Report > Secure Remote Access > Xauth > Successful Login** to open this screen.

Figure 122 Report > Secure Remote Access > Xauth> Successful Login

Time	Login User	Source IP
2011-04-01 18:47:16	Sting	172.25.21.7
2011-04-01 18:47:15	Ada	172.25.21.7
2011-04-01 18:47:15	Dom	172.25.21.7
2011-04-01 18:47:15	Ben	172.25.21.7
2011-04-01 18:47:15	Pong	172.25.21.7
2011-04-01 18:47:15	Handy	172.25.21.7
2011-04-01 18:47:14	Mark	172.25.21.7
2011-04-01 18:47:14	Senddy	172.25.21.7
2011-04-01 18:47:14	Pary	172.25.21.7
2011-04-01 18:47:14	Hen	172.25.21.7

Each field is described in the following table.

Table 109 Report > Secure Remote Access > Xauth> Successful Login

LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen.
Time	This column displays when the user last logged in. The entries are sorted in chronological order.

Table 109 Report > Secure Remote Access > Xauth> Successful Login

LABEL	DESCRIPTION
Login User	This field displays the user name of a user that logged into one of the device's Secure Remote Access tunnels. Each user is identified by user name.
Source IP	This is the IP address from which the user logged into one of the device's Secure Remote Access tunnels.
Total	This entry displays the total number of users on the current page of the report. If you want to see a different page of the report, type the number of the page in the field.

6.4.2 Secure Remote Access Failed Login

Use this report to monitor the total number of users that have made unsuccessful attempts to log in to use one of the device's Secure Remote Access tunnels.

Click **Report > Secure Remote Access > Xauth> Failed Login** to open this screen.

Figure 123 Report > Secure Remote Access > Xauth> Failed Login

Logs per Page: 10	Last 7 days	
Time	Login User	Source IP
2011-04-01 18:47:17	Xbi	172.25.21.7
2011-04-01 18:47:17	Huanhuan	172.25.21.7
2011-04-01 18:47:17	CuiCui	172.25.21.7
2011-04-01 18:47:17	Yingying	172.25.21.7
2011-04-01 18:47:17	Lingling	172.25.21.7
2011-04-01 18:47:16	Qingqing	172.25.21.7
2011-04-01 18:47:16	Weiwei	172.25.21.7
2011-04-01 18:47:16	Pangpang	172.25.21.7
2011-04-01 18:47:16	Dengdeng	172.25.21.7
2011-04-01 18:47:16	Wangwang	172.25.21.7
Total Count:17993 Total Page:1800 First 1 2 3 4 5 6 7 8 9 10 Last Go		

Each field is described in the following table.

Table 110 Report > Secure Remote Access > Xauth> Failed Login

LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen.
Time	This column displays when the user last failed to log in. The entries are sorted in chronological order.
Login User	This field displays the user name of a user that failed to log into one of the device's Secure Remote Access tunnels. Each user is identified by user name.
Source IP	This is the IP address from which the user attempted to log into one of the device's Secure Remote Access tunnels.
Total	This entry displays the total number of users on the current page of the report. If you want to see a different page of the report, type the number of the page in the field.

Network Security

This chapter discusses how to use reports to look at Denial-of-Service (DoS) attacks that were detected by the ZyXEL device's firewall.

7.1 Firewall Access Control

These screens display which users and packets were blocked based on the firewall configuration.

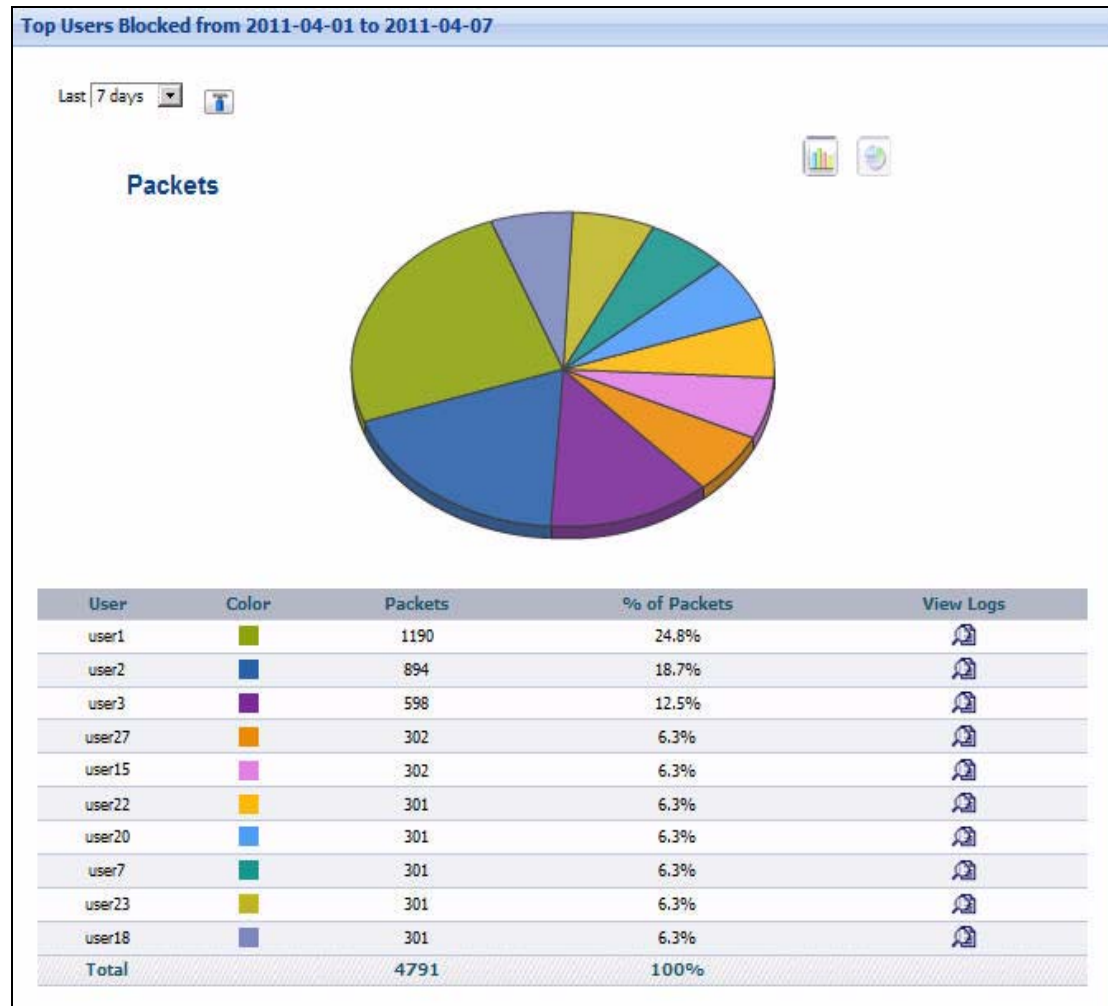
Note: To look at firewall access control reports, each ZyXEL device must record blocked packets and users in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Access Control** is enabled.

7.1.1 Top Users Blocked

Use this report to look at the users from which the device blocked the most traffic.

Click **Report > Network Security > Firewall Access Control > Top Users Blocked** to open this screen.

Figure 124 Report > Network Security > Firewall Access Control > Top Users Blocked



Each field is described in the following table.

Table 111 Report > Network Security > Firewall Access Control > Top Users Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields. It does not include the Direction you select.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 111 Report > Network Security > Firewall Access Control > Top Users Blocked

LABEL	DESCRIPTION
User	This field displays the users from which the selected device blocked the most traffic, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Packets	This field displays the number of packets the device blocked from each user.
% of Packets	This field displays what percentage each user's number of blocked packets makes out of the total number of blocked packets that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

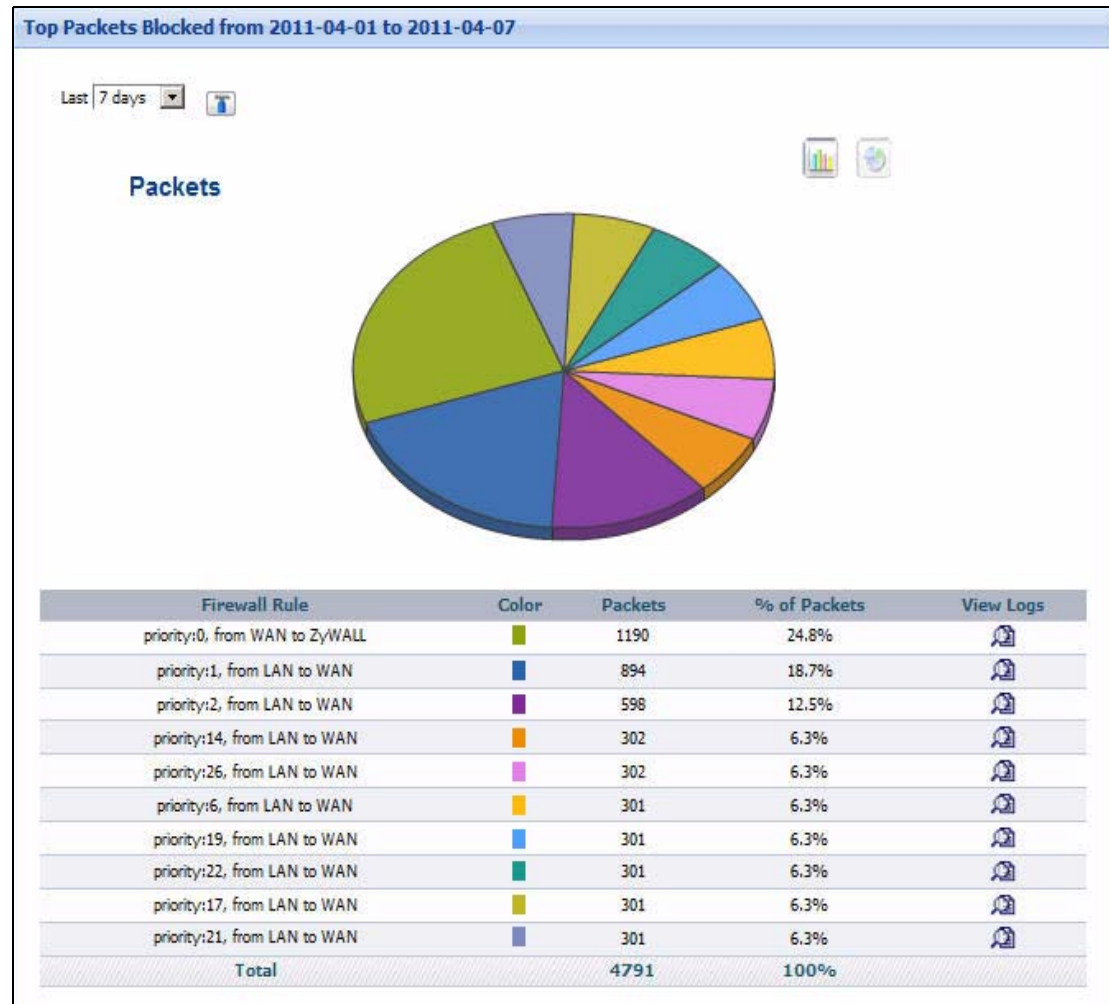
7.1.2 Top Packets Blocked

Use this report to look at the firewall rule that blocked the most packets.

Note: To look at firewall access control reports, each ZyXEL device must record blocked packets and users in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Access Control** is enabled.

Click **Report > Network Security > Firewall Access Control > Top Packets Blocked** to open this screen.

Figure 125 Report > Network Security > Firewall Access Control > Top Packets Blocked



Each field is described in the following table.

Table 112 Report > Network Security > Firewall Access Control > Top Packets Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields. It does not include the Direction you select.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Firewall Rule field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 112 Report > Network Security > Firewall Access Control > Top Packets Blocked

LABEL	DESCRIPTION
Firewall Rule	This field displays the name of the firewall rule on the selected device that blocked packets, sorted by the number of packets for each one. Each firewall rule is identified by priority in the firewall rule list and the traffic direction to which it applies.
Color	This field displays what color represents each firewall rule in the graph.
Packets	This field displays the number of packets the firewall rule blocked from each user.
% of Packets	This field displays what percentage each firewall rule's number of blocked packets makes out of the total number of blocked packets that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the firewall rules above.

7.2 Attack

These reports look at the number of DoS attacks by time interval, top sources and by category.

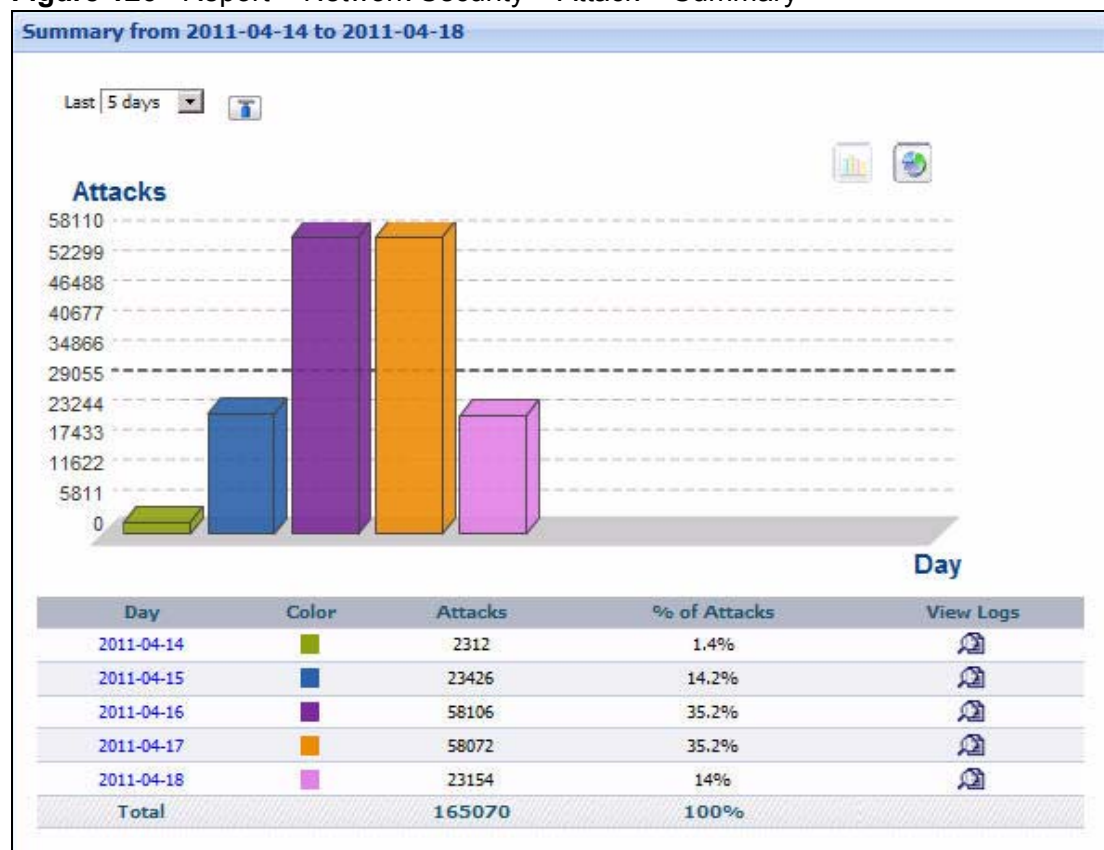
7.2.1 Attack Summary

Use this report to look at the number of DoS attacks by time interval.

Note: To look at attack reports, each ZyXEL device must record DoS attacks in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Attacks** is enabled.

Click **Report > Network Security > Attack > Summary** to open this screen.

Figure 126 Report > Network Security > Attack > Summary



Each field is described in the following table.

Table 113 Report > Network Security > Attack > Summary

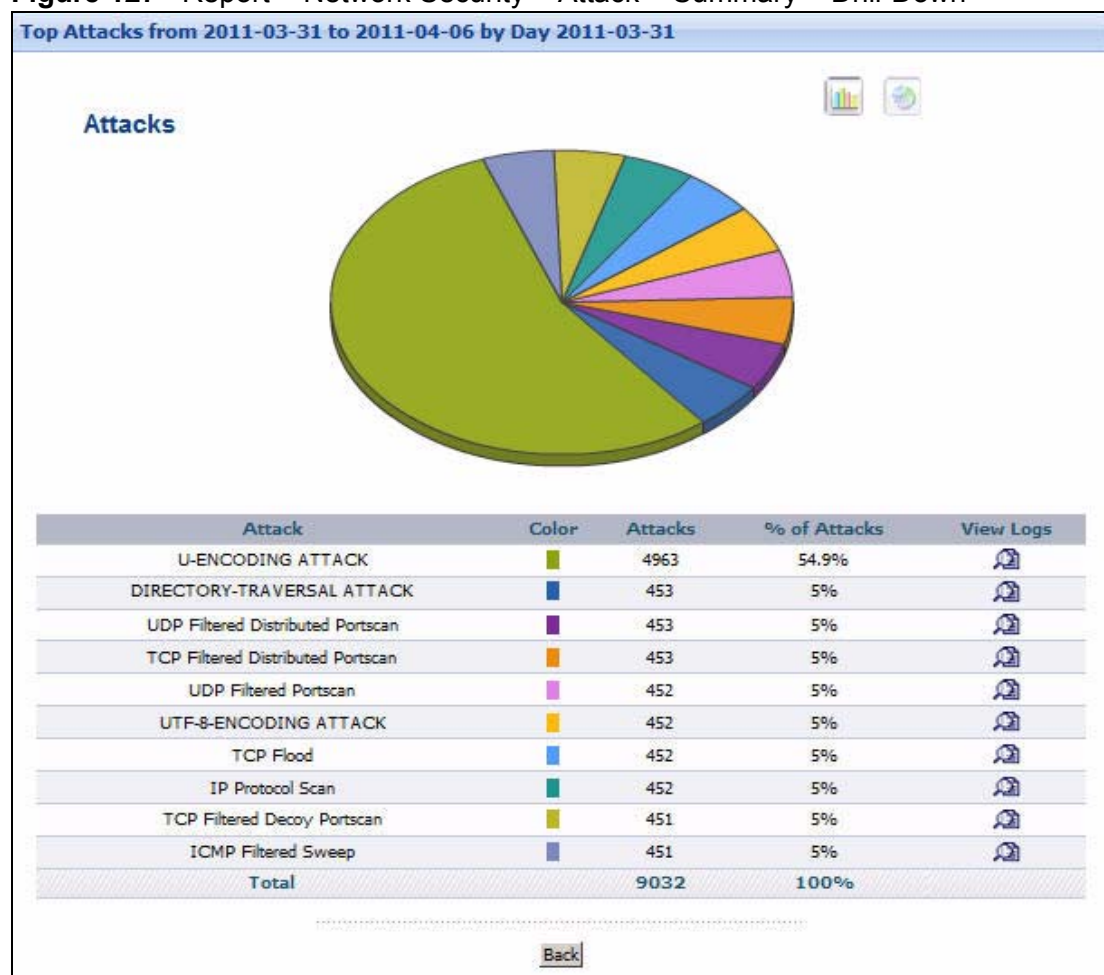
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top categories of attacks in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attacks	This field displays the number of DoS attacks in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.2.2 Attack Summary Drill-Down

Use this report to look at the top categories of DoS attacks in a specific time interval.

Click on a specific time interval in **Report > Network Security > Attack > Summary** to open this screen.

Figure 127 Report > Network Security > Attack > Summary > Drill-Down



Each field is described in the following table.

Table 114 Report > Network Security > Attack > Summary > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks in the selected time interval, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks by each category occurred in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks in the selected time interval comes from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above. If the number of categories in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

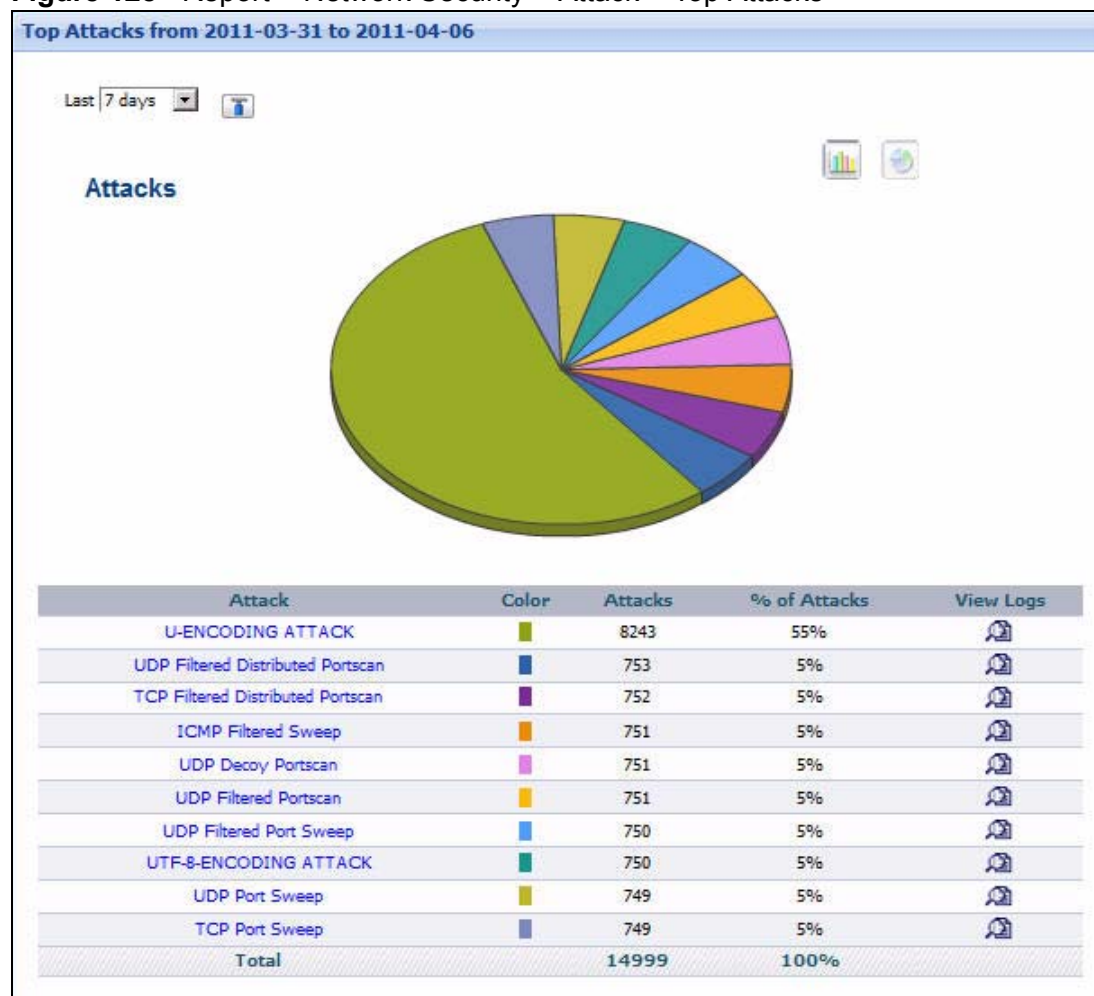
7.2.3 Top Attacks

Use this report to look at the top kinds of DoS attacks by number of attacks.

Note: To look at attack reports, each ZyXEL device must record DoS attacks in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Attacks** is enabled.

Click **Report > Network Security > Attack > Top Attacks** to open this screen.

Figure 128 Report > Network Security > Attack > Top Attacks



Each field is described in the following table.

Table 115 Report > Network Security > Attack > Top Attacks

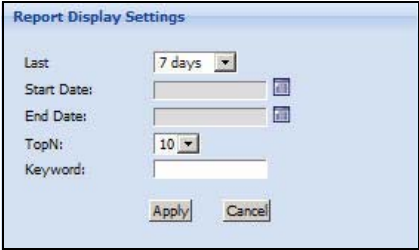
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Attack field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks in the selected time interval, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks from each category occurred in the selected time interval.

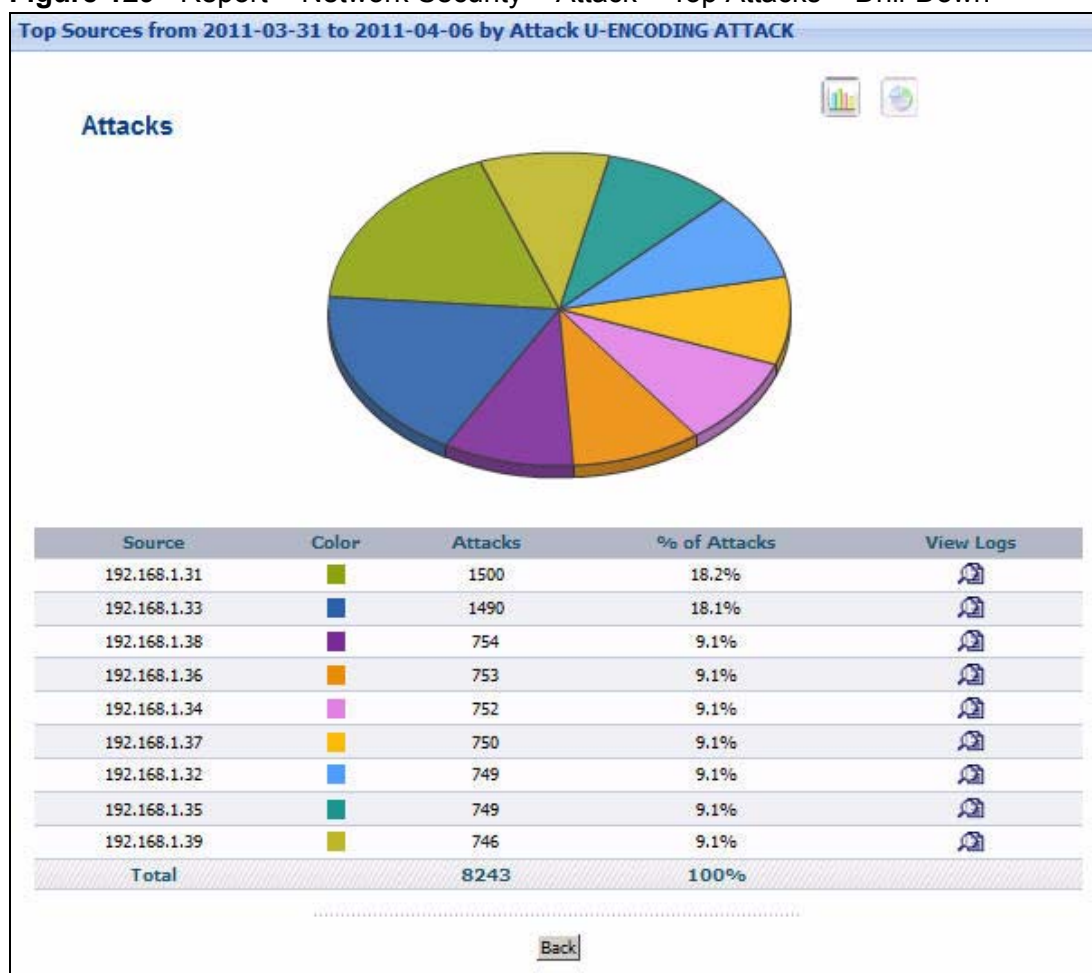
Table 115 Report > Network Security > Attack > Top Attacks

LABEL	DESCRIPTION
% of Attacks	This field displays what percentage of all DoS attacks in the selected time interval comes from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above. If the number of categories in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.

7.2.4 Top Attacks Drill-Down

Use this report to look at the top categories of DoS attacks for any top source.

Click on a specific source in **Report > Network Security > Attack > Top Attacks** to open this screen.

Figure 129 Report > Network Security > Attack > Top Attacks > Drill-Down

Each field is described in the following table.

Table 116 Report > Network Security > Attack > Top Attacks > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected category of DoS attacks.
Color	This field displays what color represents each source in the graph.
Attacks	This field displays the number of DoS attacks in the selected category that came from each source.
% of Attacks	This field displays what percentage of all DoS attacks in the selected category came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected category of DoS attacks is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

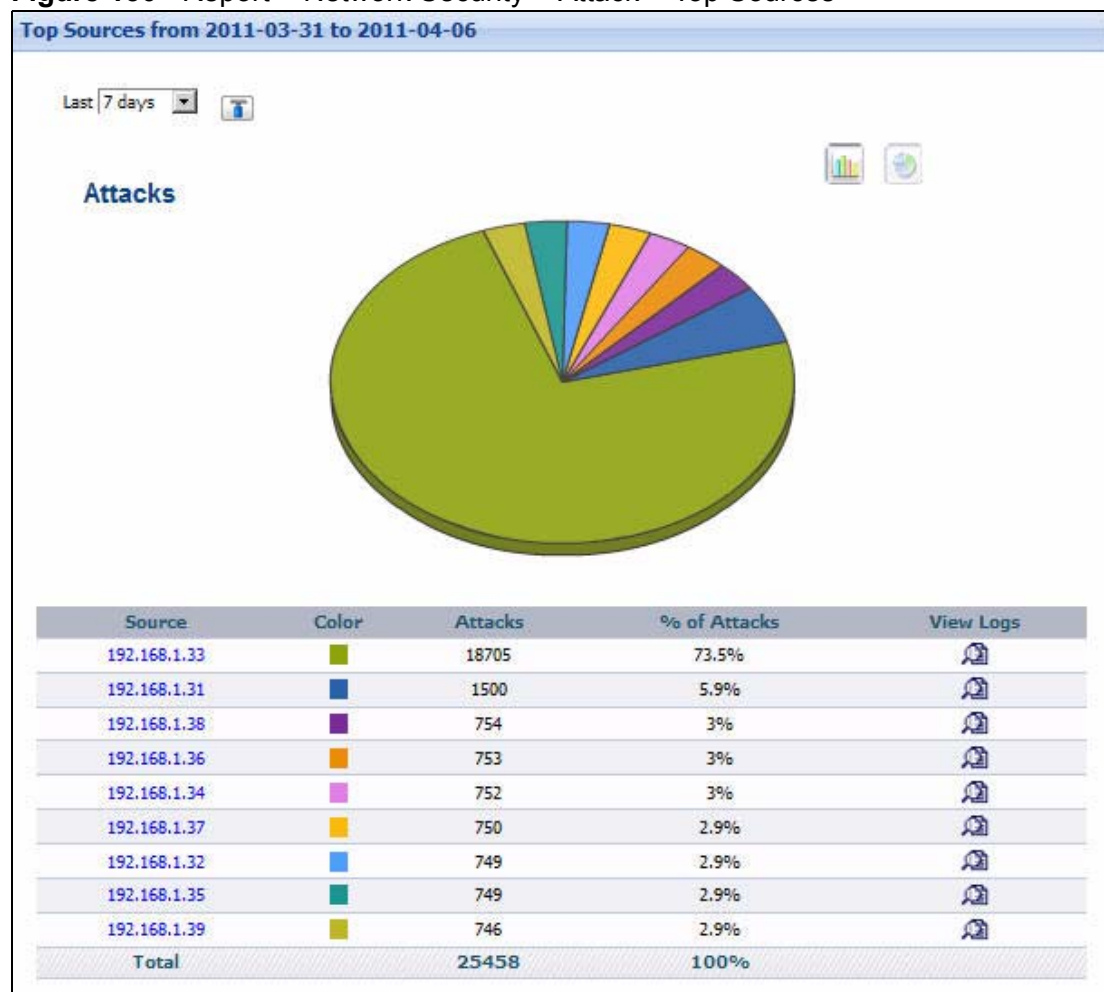
7.2.5 Top Attack Sources

Use this report to look at the top sources of DoS attacks by number of attacks.

Note: To look at attack reports, each ZyXEL device must record DoS attacks in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Attacks** is enabled.

Click **Report > Network Security > Attack > Top Sources** to open this screen.

Figure 130 Report > Network Security > Attack > Top Sources



Each field is described in the following table.

Table 117 Report > Network Security > Attack > Top Sources

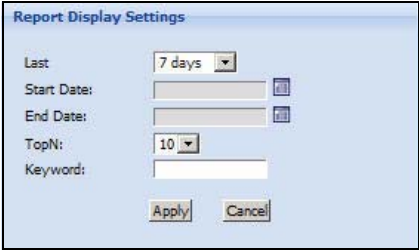
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 117 Report > Network Security > Attack > Top Sources

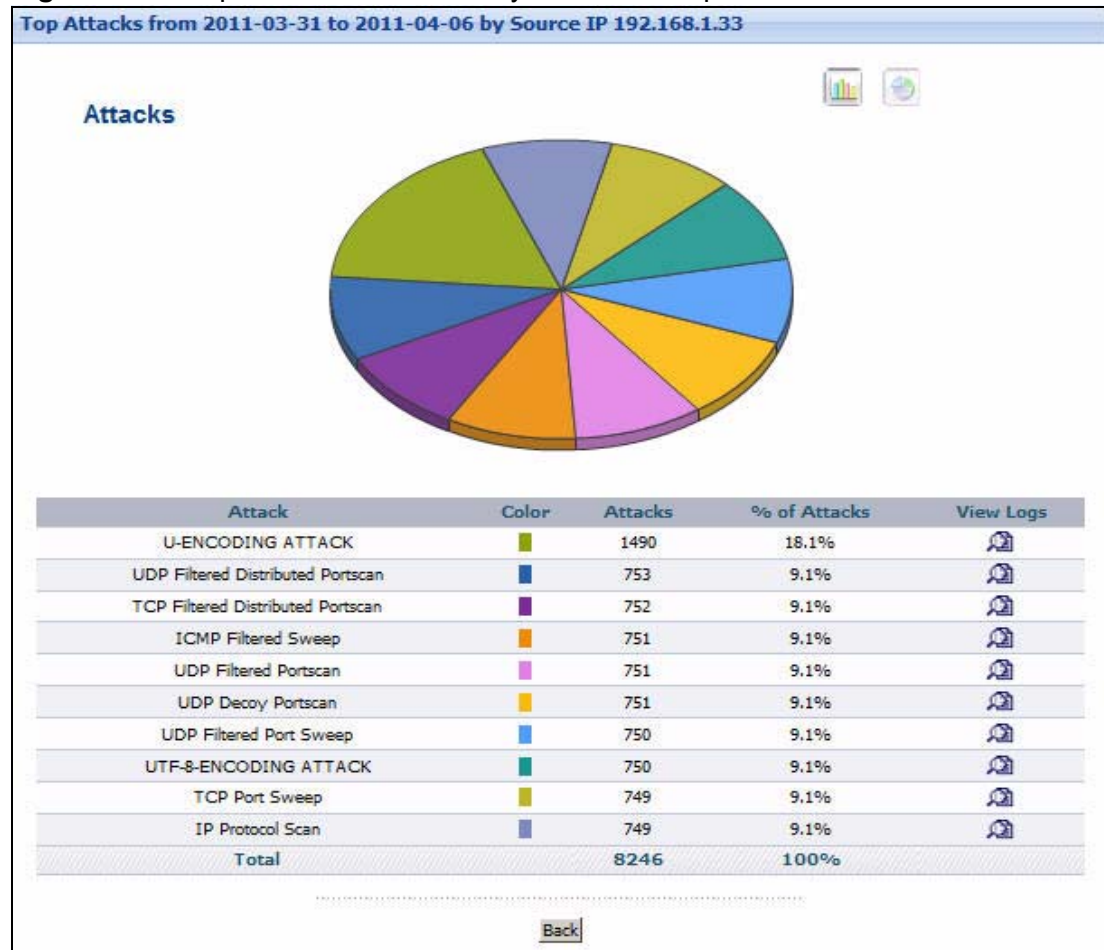
LABEL	DESCRIPTION
Source	This field displays the top sources of DoS attacks in the selected device, sorted by the number of attacks by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top categories of DoS attacks by the selected source.
Color	This field displays what color represents each source in the graph.
Attacks	This field displays the number of DoS attacks by each source.
% of Attacks	This field displays what percentage of all DoS attacks was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.2.6 Top Attack Sources Drill-Down

Use this report to look at the top categories of DoS attacks for any top source.

Click on a specific source in **Report > Network Security > Attack > Top Sources** to open this screen.

Figure 131 Report > Network Security > Attack > Top Sources > Drill-Down



Each field is described in the following table.

Table 118 Report > Network Security > Attack > Top Sources > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks from the selected source, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays the number of DoS attacks from each category that occurred from the selected source.

Table 118 Report > Network Security > Attack > Top Sources > Drill-Down

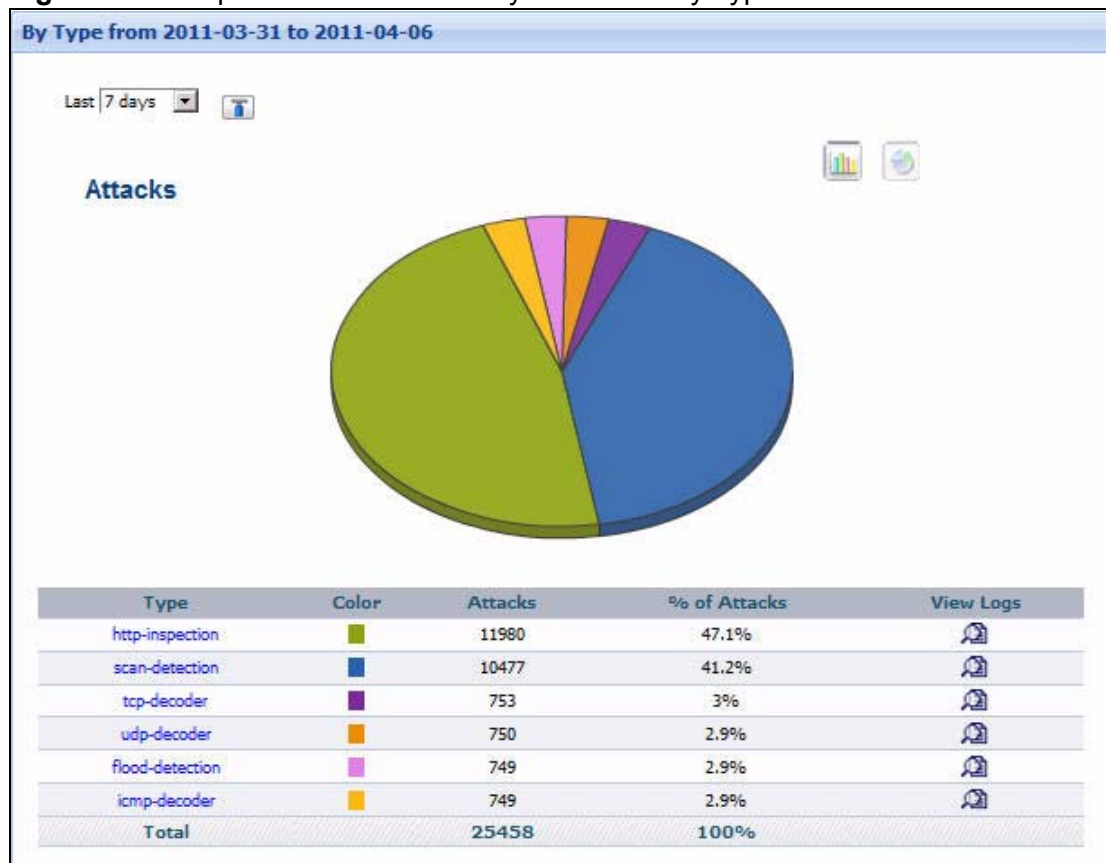
LABEL	DESCRIPTION
% of Attacks	This field displays what percentage of all DoS attacks from the selected source comes from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above. If the number of categories of DoS attacks from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.2.7 Attack Types

Use this report to look at the categories of DoS attacks by number of attacks.

Note: To look at attack reports, each ZyXEL device must record DoS attacks in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Attacks** is enabled.

Click **Report > Network Security > Attack > By Type** to open this screen.

Figure 132 Report > Network Security > Attack > By Type

Each field is described in the following table.

Table 119 Report > Network Security > Attack > By Type

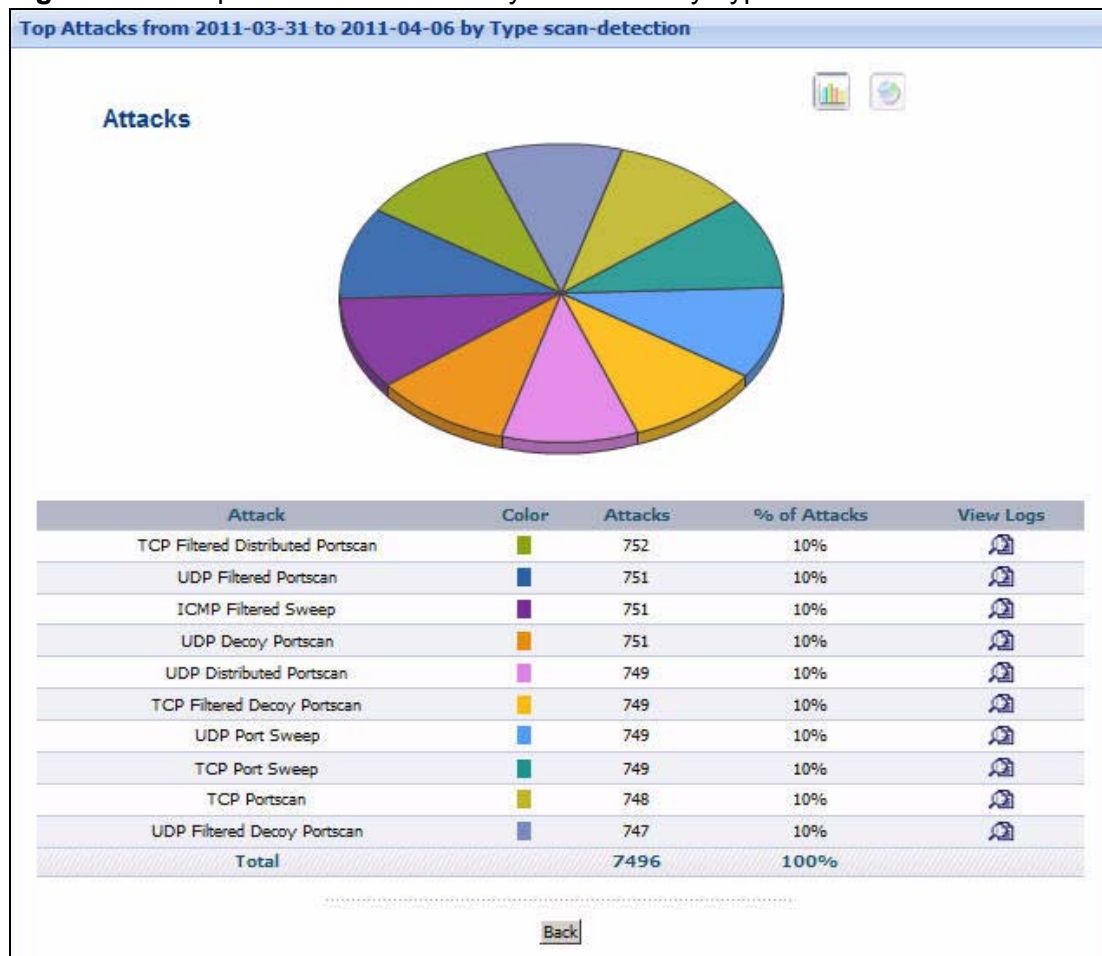
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Type	This field displays the categories of DoS attacks in the selected device, sorted by the number of attacks by each one. Click on a category to look at the DoS attacks in the selected category.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks from each category the device stopped.
% of Attacks	This field displays what percentage of all DoS attacks come from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

7.2.8 Attack Types Drill-Down

Use this report to look at the sources of DoS attacks for any top category.

Click on a specific category in **Report > Network Security > Attack > By Type** to open this screen.

Figure 133 Report > Network Security > Attack > By Type > Drill-Down



Each field is described in the following table.

Table 120 Report > Network Security > Attack > By Type > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the DoS attacks in the selected category, sorted by the number of each. Each source is identified by its IP address.
Color	This field displays what color represents each attack in the graph.
Attacks	This field displays the number of each DoS attack type.
% of Attacks	This field displays what percentage of all DoS attacks in the selected category belonged to each type.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the attacks above.
Back	Click this to return to the main report.

7.3 Intrusion Hits

These reports look at intrusion signatures, types of intrusions, severity of intrusions, and the top sources and destinations of intrusions that are logged on the selected ZyXEL device. **Intrusions** are caused by malicious or suspicious packets sent with the intent of causing harm, illegally accessing resources or interrupting service. They are detected by the selected device's IDP feature.

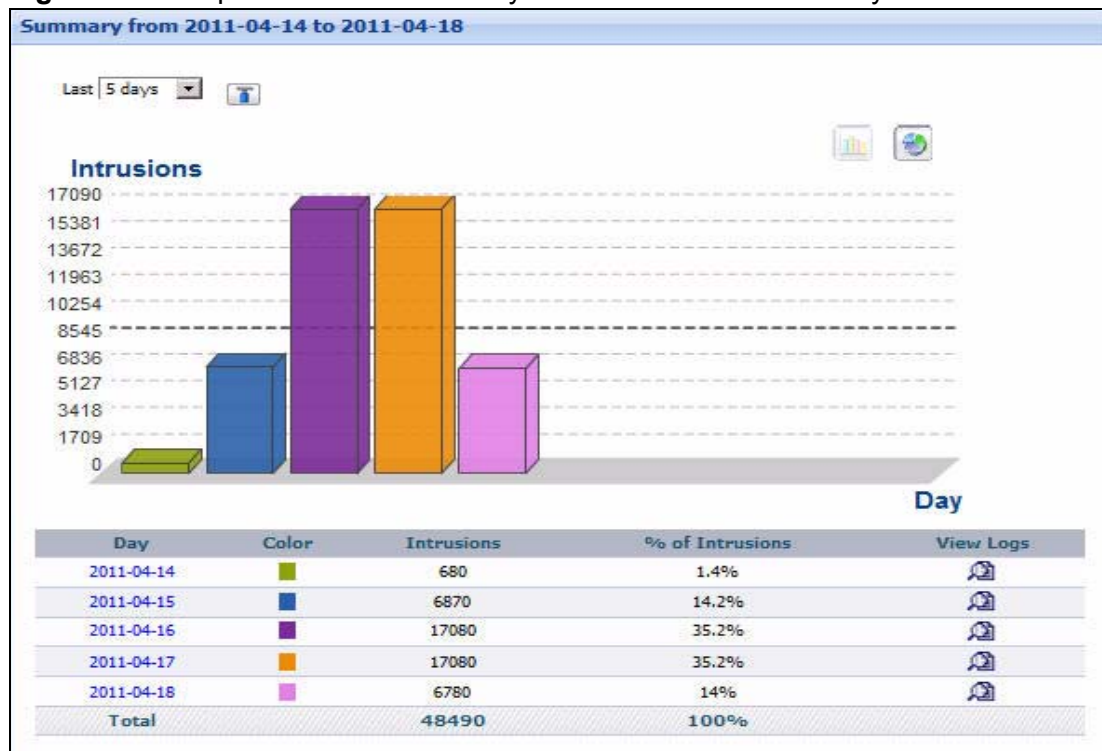
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP > Signature**, and make sure the ZyXEL device logs each **Attack Type** you want to see in Vantage Report.

7.3.1 Intrusion Hits Summary

Use this report to look at the number of intrusions by time interval.

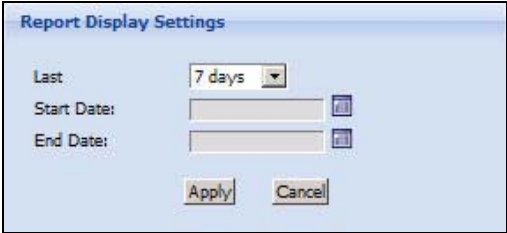
Click **Report > Network Security > Intrusion Hits > Summary** to open this screen.

Figure 134 Report > Network Security > Intrusion Hits > Summary



Each field is described in the following table.

Table 121 Report > Network Security > Intrusion Hits > Summary

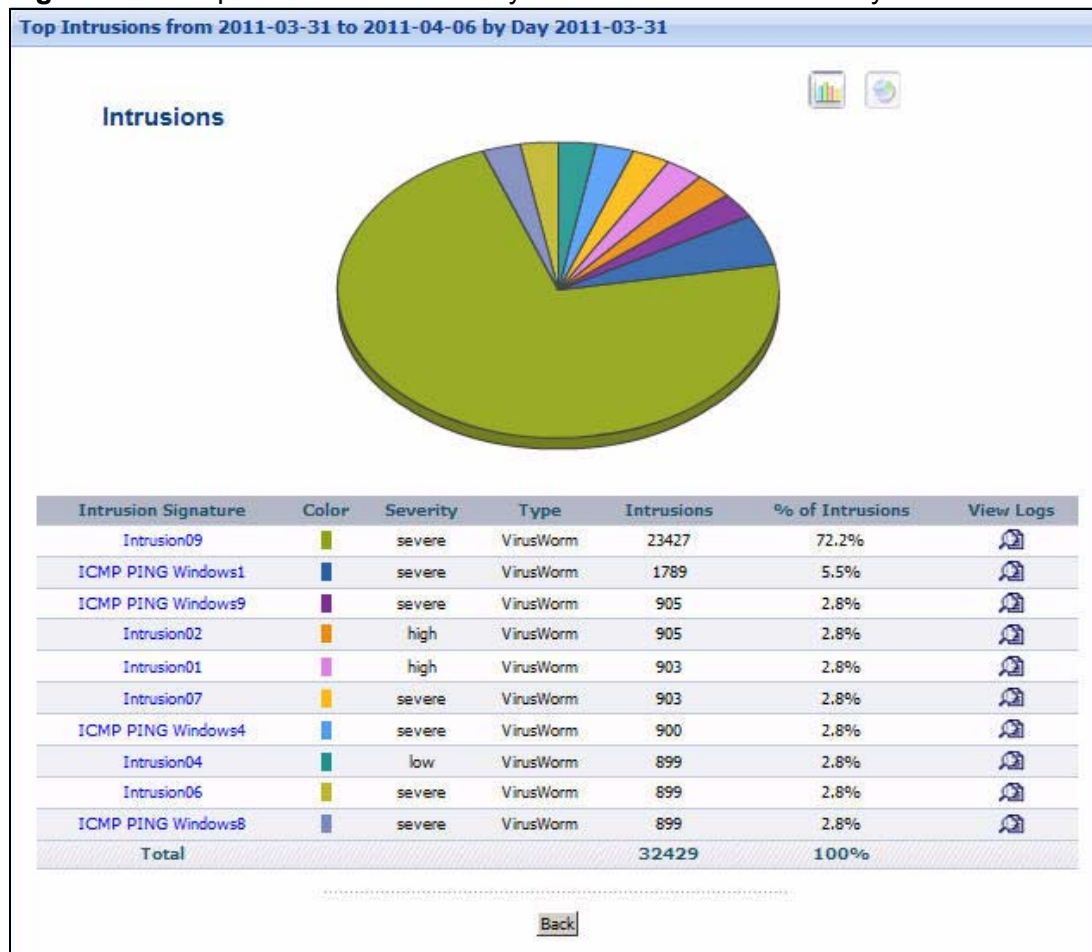
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the intrusion signatures in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Intrusions	This field displays the number of intrusions in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.3.2 Intrusion Hits Summary Drill-Down

Use this report to look at the intrusion signatures in a specific time interval.

Click on a specific time interval in **Report > Network Security > Intrusion Hits > Summary** to open this screen.

Figure 135 Report > Network Security > Intrusion Hits > Summary > Drill-Down



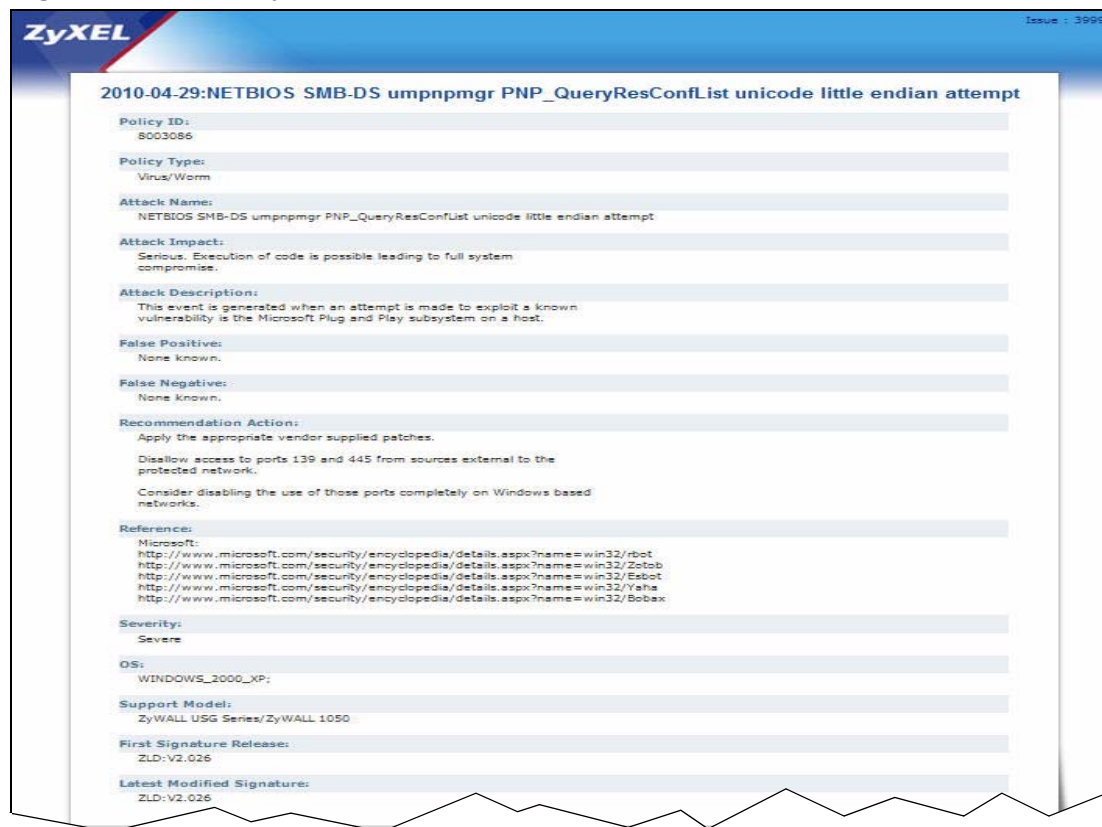
Each field is described in the following table.

Table 122 Report > Network Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 136 on page 296).
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

Note: Clicking on some linked entries in the Intrusion screen will open a new window that provides details on the security issue encountered by the devices. The following screen is displayed.

Figure 136 Security Issue Details

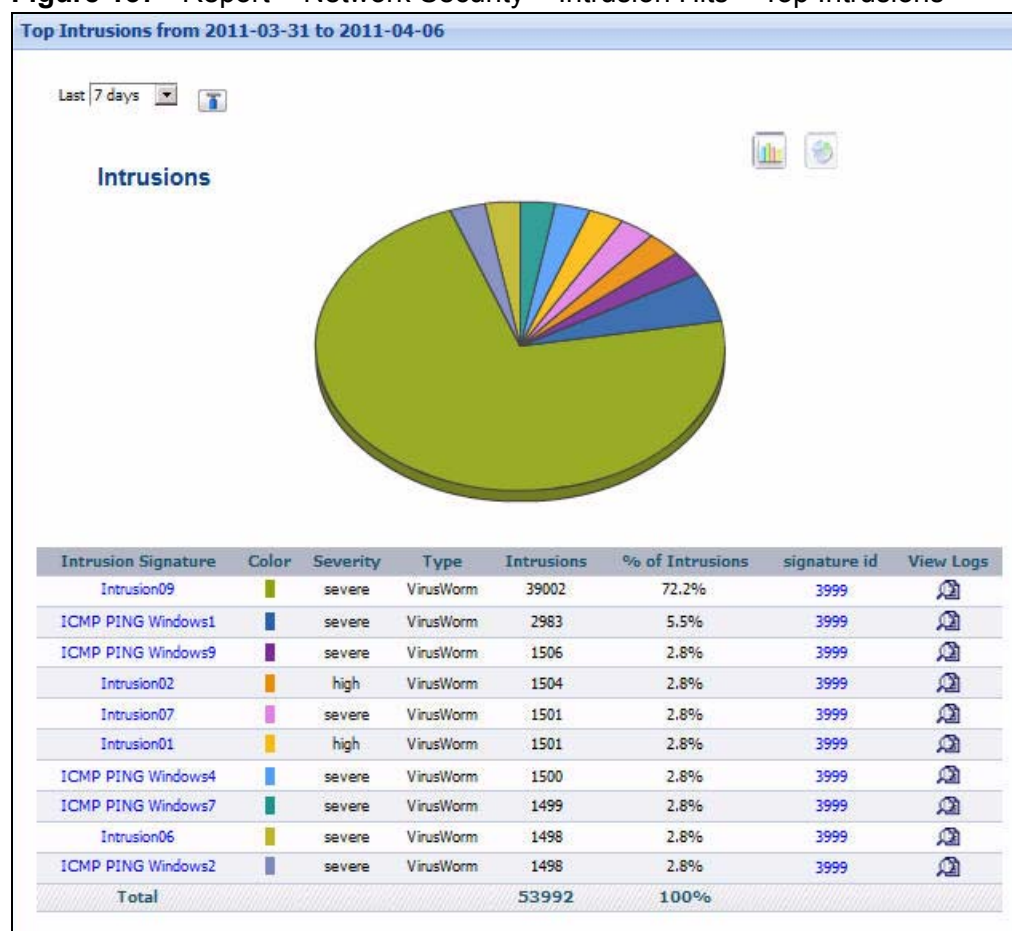


7.3.3 Top Intrusion Hits Signatures

Use this report to look at the top intrusion signatures by number of intrusions.

Click **Report > Network Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 137 Report > Network Security > Intrusion Hits > Top Intrusions



Each field is described in the following table.

Table 123 Report > Network Security > Intrusion Hits > Top Intrusions

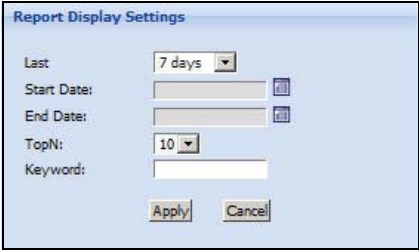
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Intrusion Signature field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature.
Color	This field displays what color represents each intrusion signature in the graph.

Table 123 Report > Network Security > Intrusion Hits > Top Intrusions

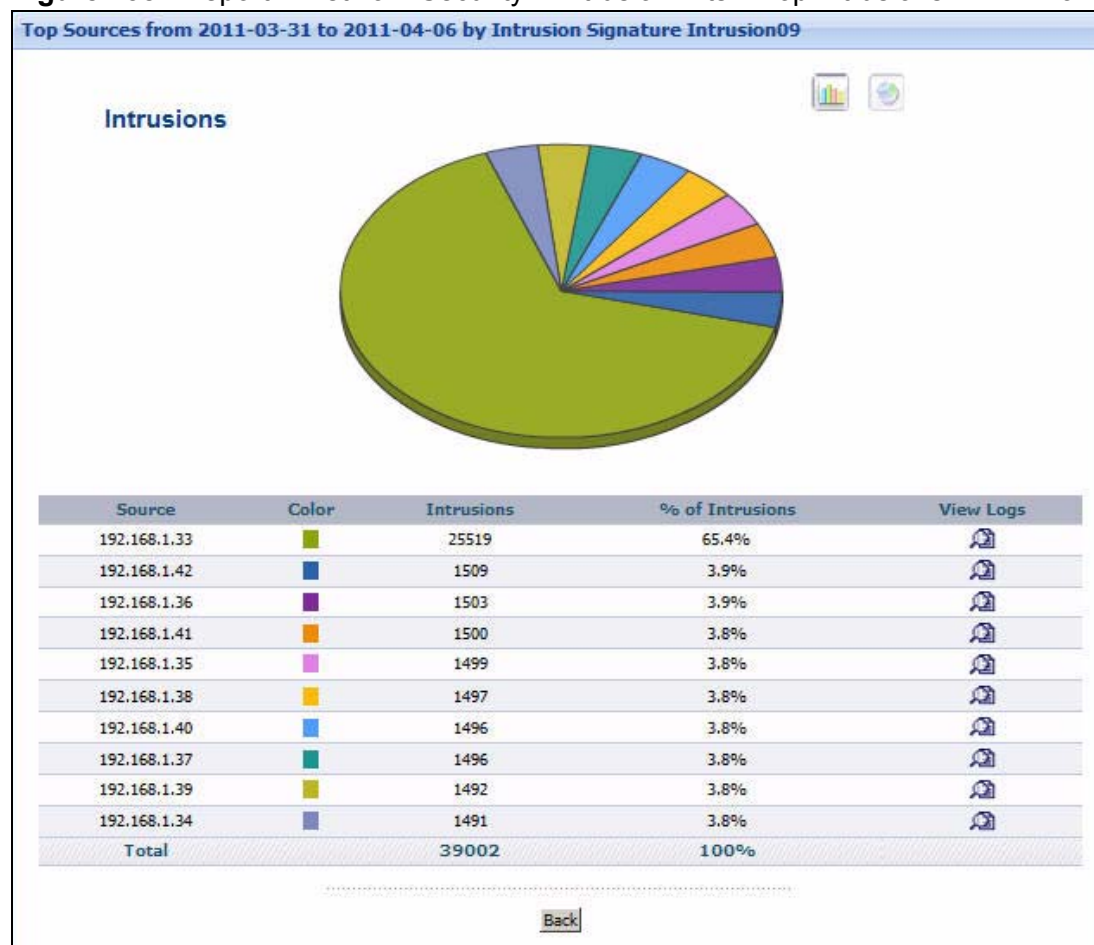
LABEL	DESCRIPTION
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
signature id	This is the security issue identification number. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 136 on page 296).
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

7.3.4 Top Intrusion Hits Signatures Drill-Down

Use this report to look at the top sources of intrusions for any top signature.

Click on a specific intrusion signature in **Report > Network Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 138 Report > Network Security > Intrusion Hits > Top Intrusions > Drill-Down



Each field is described in the following table.

Table 124 Report > Network Security > Intrusion Hits > Top Intrusions > Drill-Down

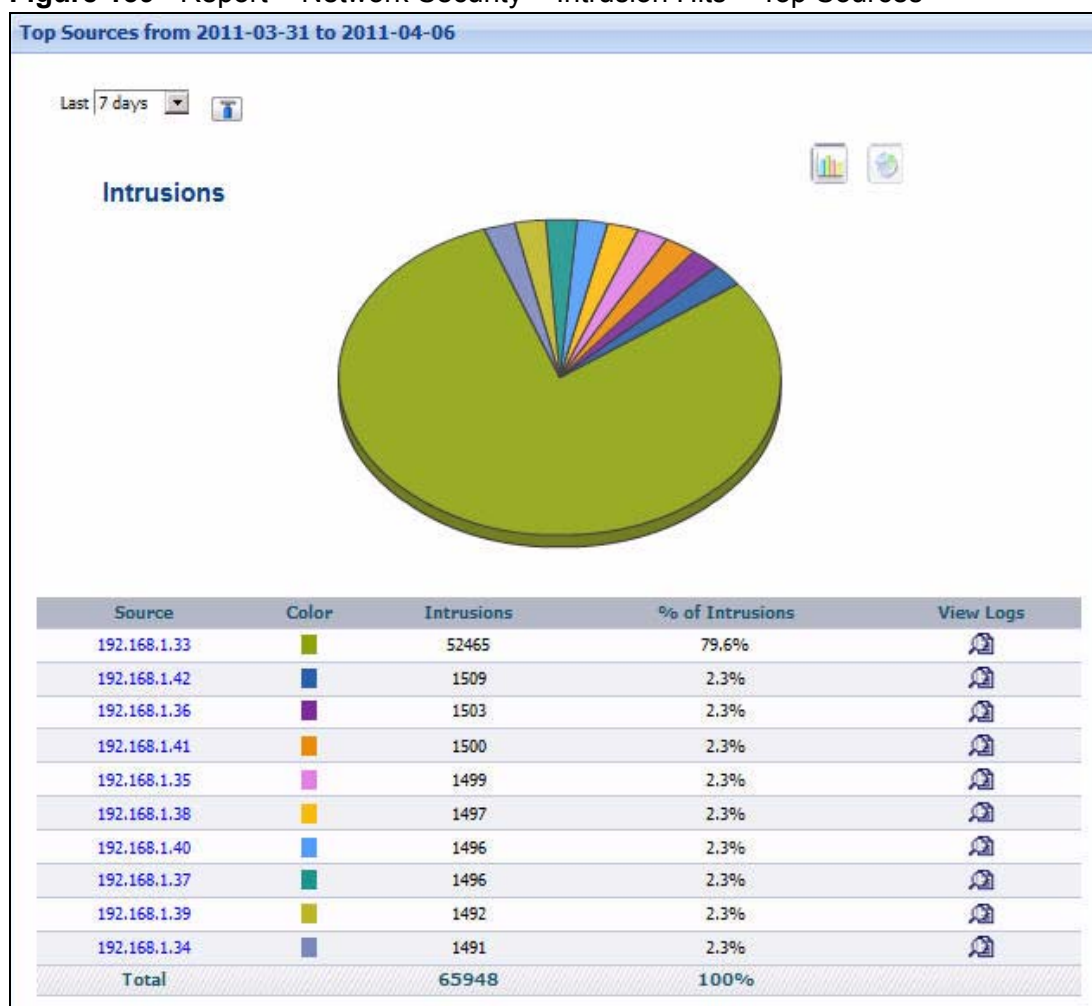
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected intrusion signature, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions using the selected intrusion signature was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected intrusion signature is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.3.5 Top Intrusion Hits Sources

Use this report to look at the top sources of intrusions by number of intrusions.

Click **Report > Network Security > Intrusion Hits > Top Sources** to open this screen.

Figure 139 Report > Network Security > Intrusion Hits > Top Sources



Each field is described in the following table.

Table 125 Report > Network Security > Intrusion Hits > Top Sources

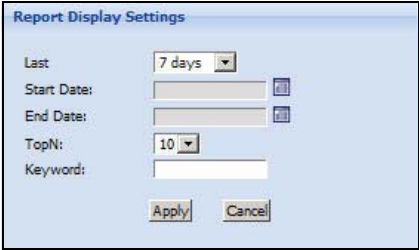
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 125 Report > Network Security > Intrusion Hits > Top Sources

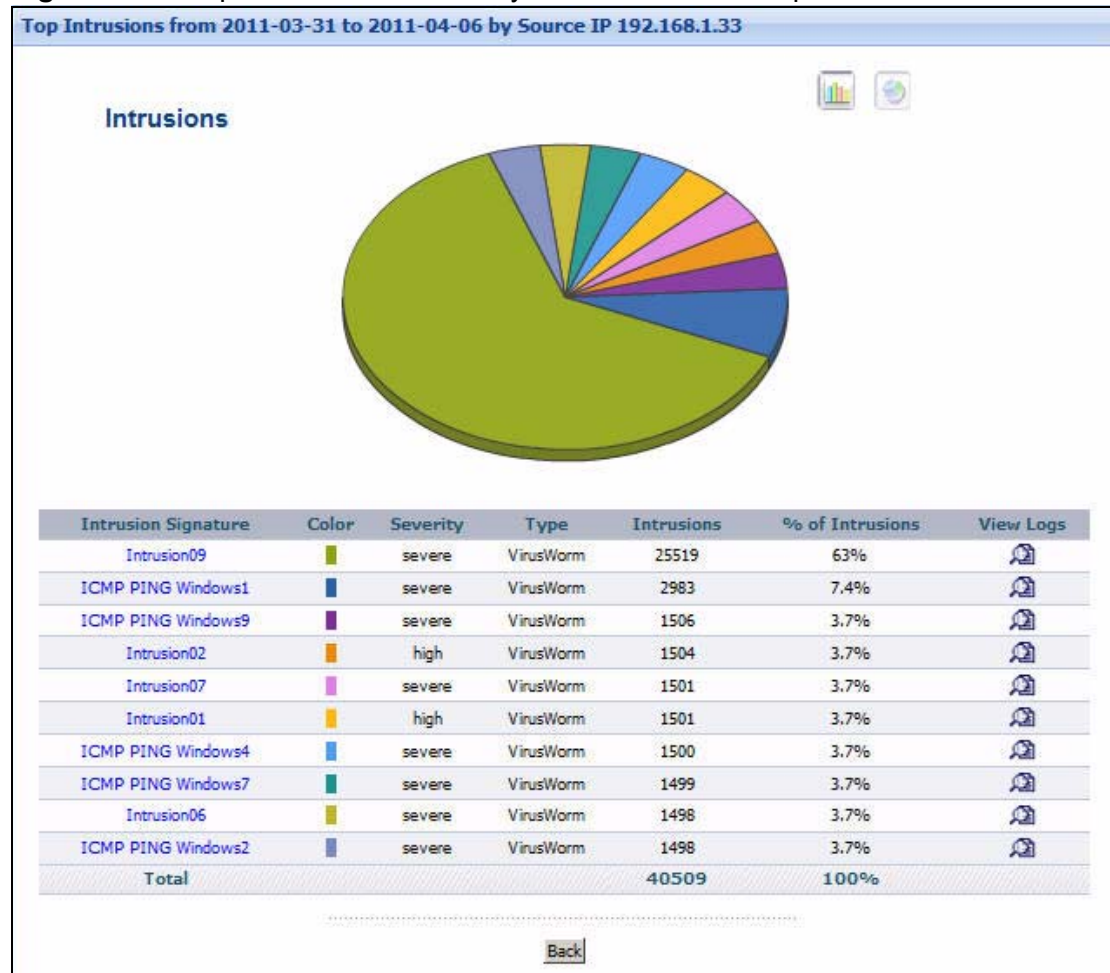
LABEL	DESCRIPTION
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top intrusion signatures for the selected source.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.3.6 Top Intrusion Hits Sources Drill-Down

Use this report to look at the top intrusion signatures for any top source.

Click on a specific source in **Report > Network Security > Intrusion Hits > Top Sources** to open this screen.

Figure 140 Report > Network Security > Intrusion Hits > Top Sources > Drill-Down



Each field is described in the following table.

Table 126 Report > Network Security > Intrusion Hits > Top Sources > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures from the selected source, sorted by the number of intrusions by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.

Table 126 Report > Network Security > Intrusion Hits > Top Sources > Drill-Down

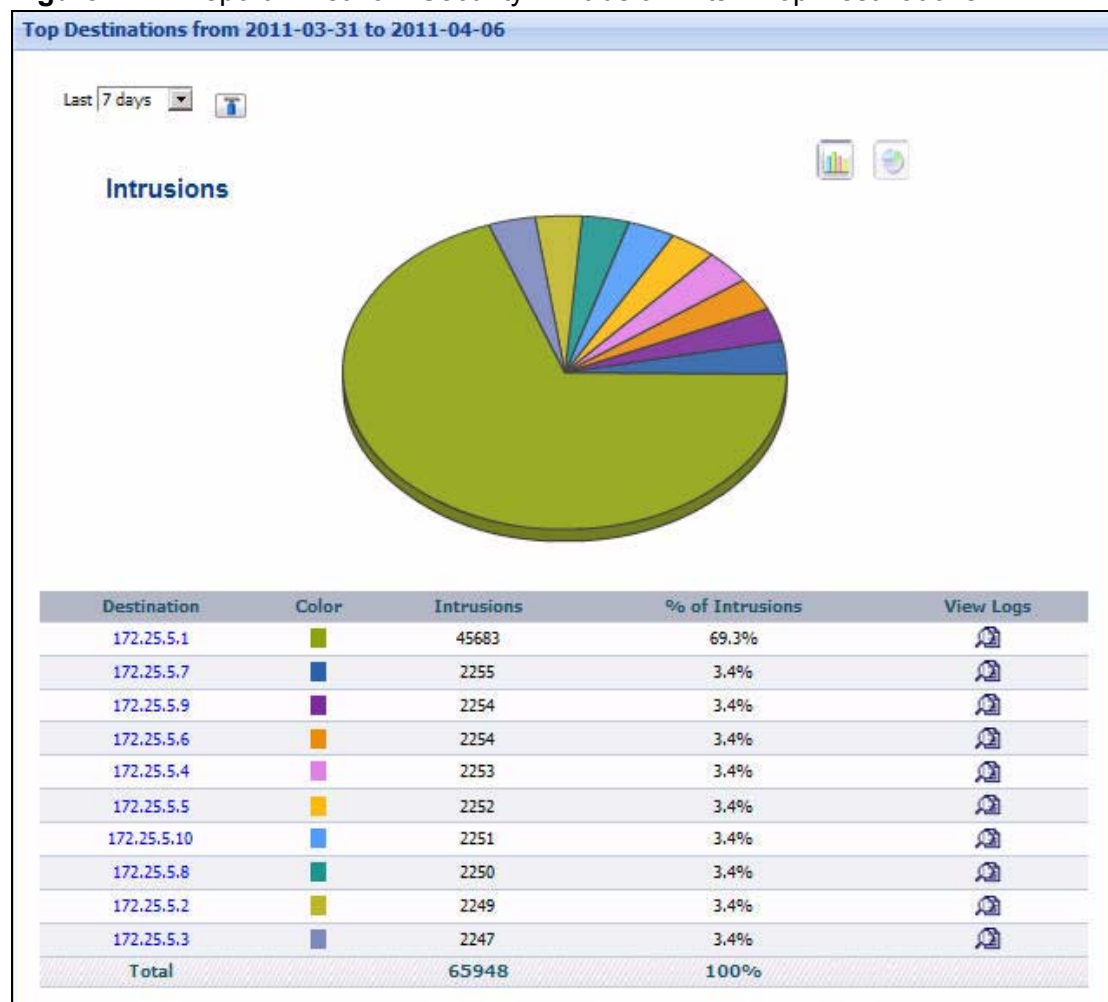
LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by the selected source using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions by the selected source was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.3.7 Top Intrusion Hits Destinations

Use this report to look at the top destinations of intrusions by number of intrusions.

Click **Report > Network Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 141 Report > Network Security > Intrusion Hits > Top Destinations



Each field is described in the following table.

Table 127 Report > Network Security > Intrusion Hits > Top Destinations

LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 127 Report > Network Security > Intrusion Hits > Top Destinations

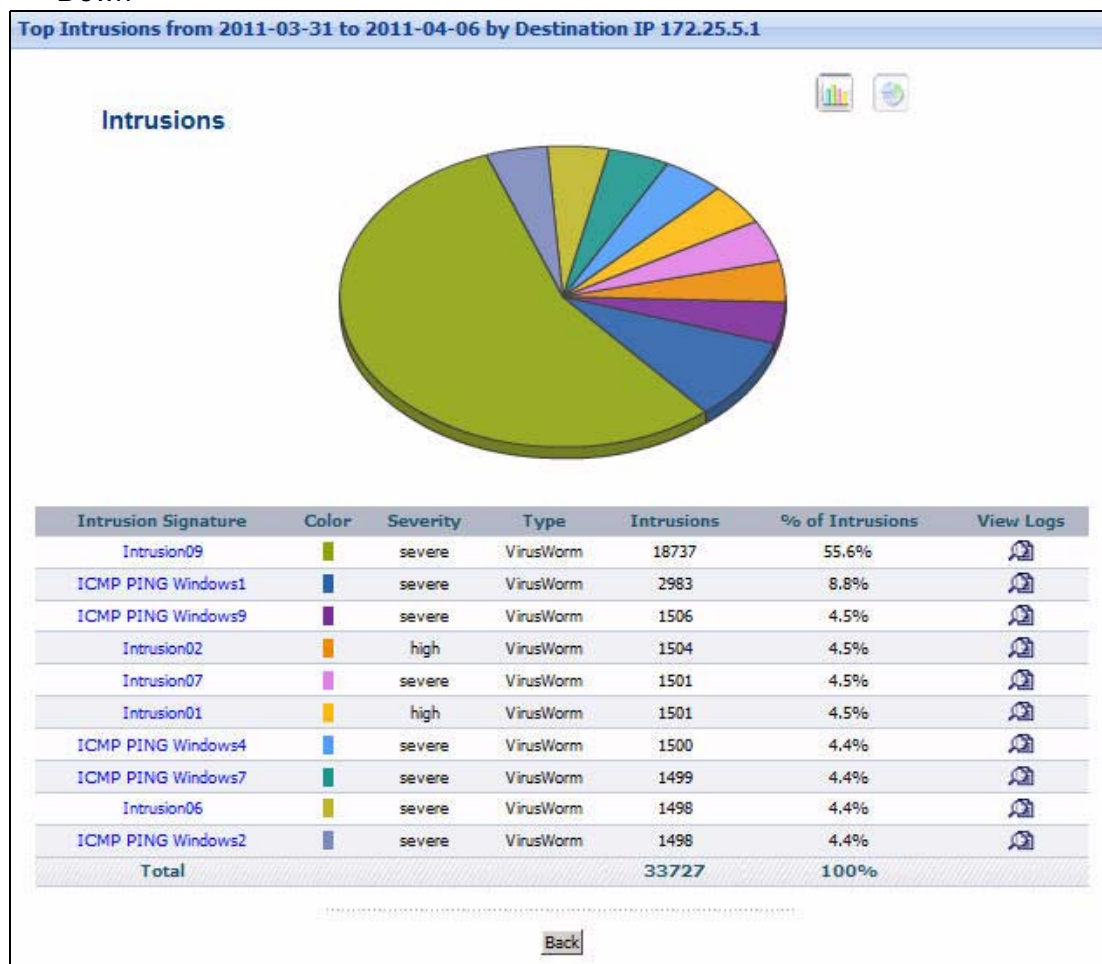
LABEL	DESCRIPTION
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top intrusion signatures for the selected destination.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

7.3.8 Top Intrusion Hits Destinations Drill-Down

Use this report to look at the top intrusion signatures for any top destination.

Click on a specific destination in **Report > Network Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 142 Report > Network Security > Intrusion Hits > Top Destinations > Drill-Down



Each field is described in the following table.

Table 128 Report > Network Security > Intrusion Hits > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures sent to the selected destination, sorted by the number of intrusions at each one.
Color	This field displays what color represents each intrusion signature in the graph.

Table 128 Report > Network Security > Intrusion Hits > Top Destinations > Drill-Down

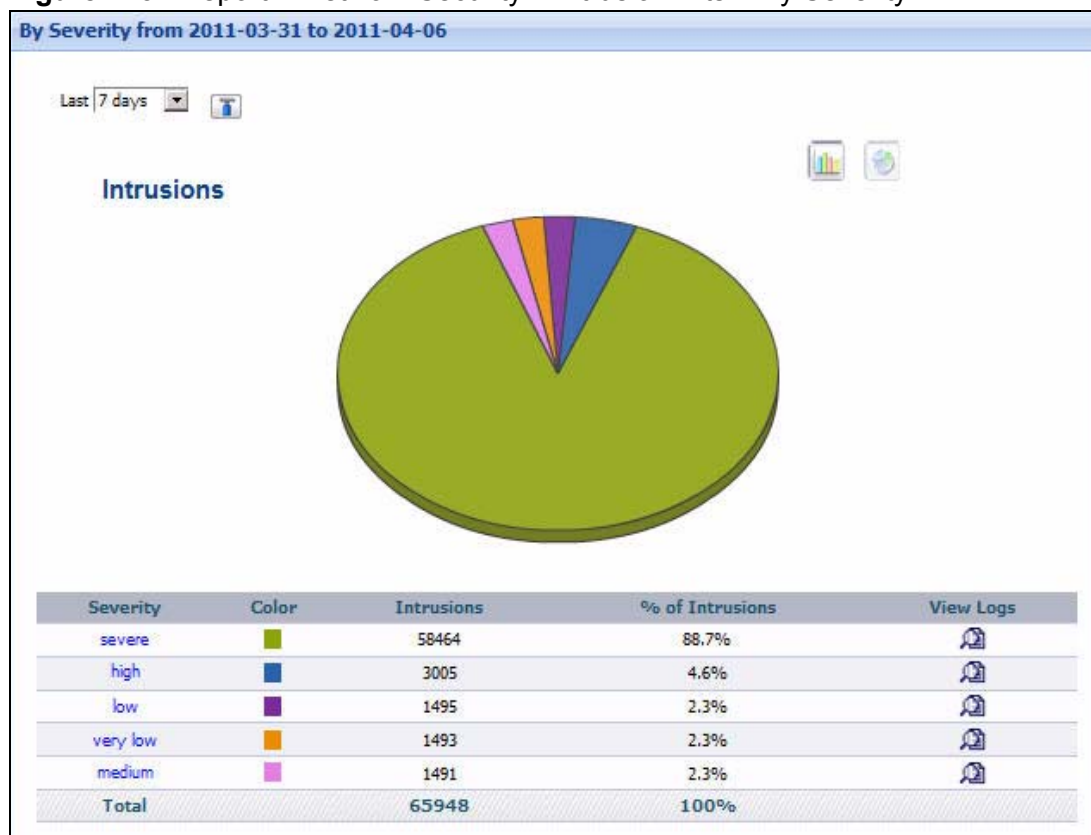
LABEL	DESCRIPTION
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of each intrusion signature sent to the selected destination.
% of Intrusions	This field displays what percentage of all intrusions sent to the selected destination belong to each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.3.9 Intrusion Hits Severities

Use this report to look at the severity (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug.

Click **Report > Network Security > Intrusion Hits > By Severity** to open this screen.

Figure 143 Report > Network Security > Intrusion Hits > By Severity



Each field is described in the following table.

Table 129 Report > Network Security > Intrusion Hits > By Severity

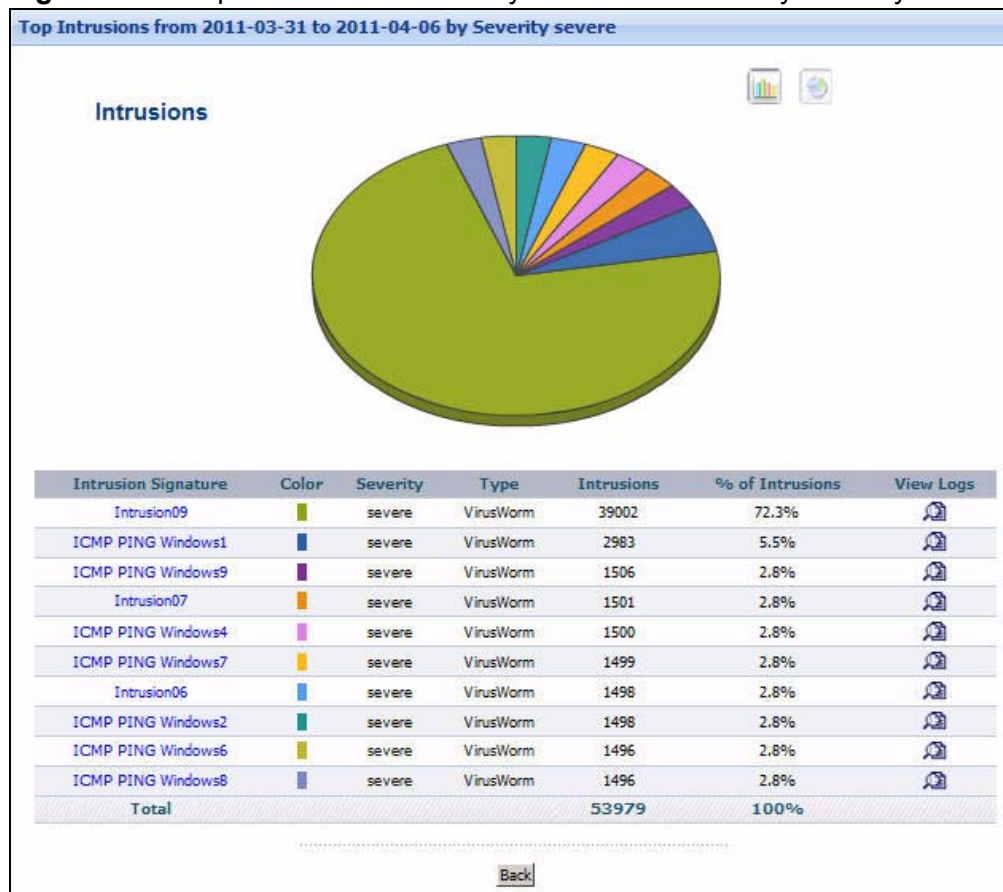
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

7.3.10 Intrusion Hits Severities Drill-Down

Use this report to look at the intrusion signatures for any severity.

Click on a specific severity in **Report > Network Security > Intrusion Hits > By Severity** to open this screen.

Figure 144 Report > Network Security > Intrusion Hits > By Severity > Drill-Down



Each field is described in the following table.

Table 130 Report > Network Security > Intrusion Hits > By Severity > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the intrusion signatures of the selected severity, sorted by the number of intrusions by each one.

Table 130 Report > Network Security > Intrusion Hits > By Severity > Drill-Down

LABEL	DESCRIPTION
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of the selected severity using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions of the selected severity was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

7.4 Antivirus

These reports look at viruses that were detected by the ZyXEL device's anti-virus feature.

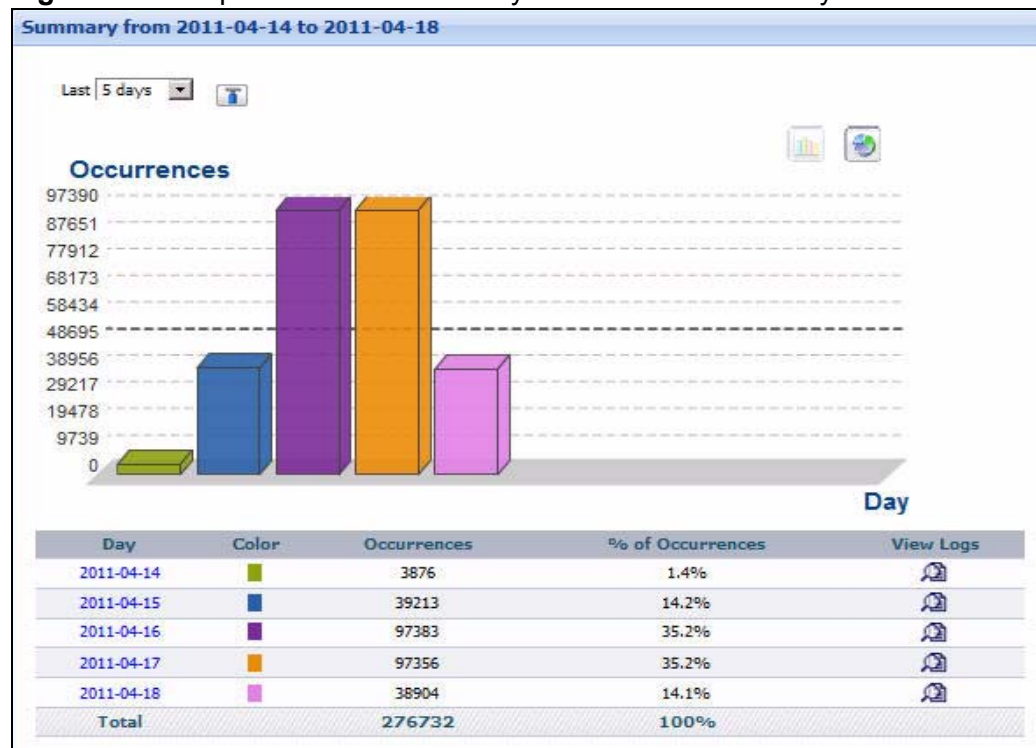
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus > General**. ZyXEL devices can log viruses based on the **Service** the virus was using. Make sure the ZyXEL device logs viruses you want to include in Vantage Report.

7.4.1 Antivirus Summary

Use this report to look at the number of virus occurrences by time interval.

Click **Report > Network Security > AntiVirus > Summary** to open this screen.

Figure 145 Report > Network Security > AntiVirus > Summary



Each field is described in the following table.

Table 131 Report > Network Security > AntiVirus > Summary

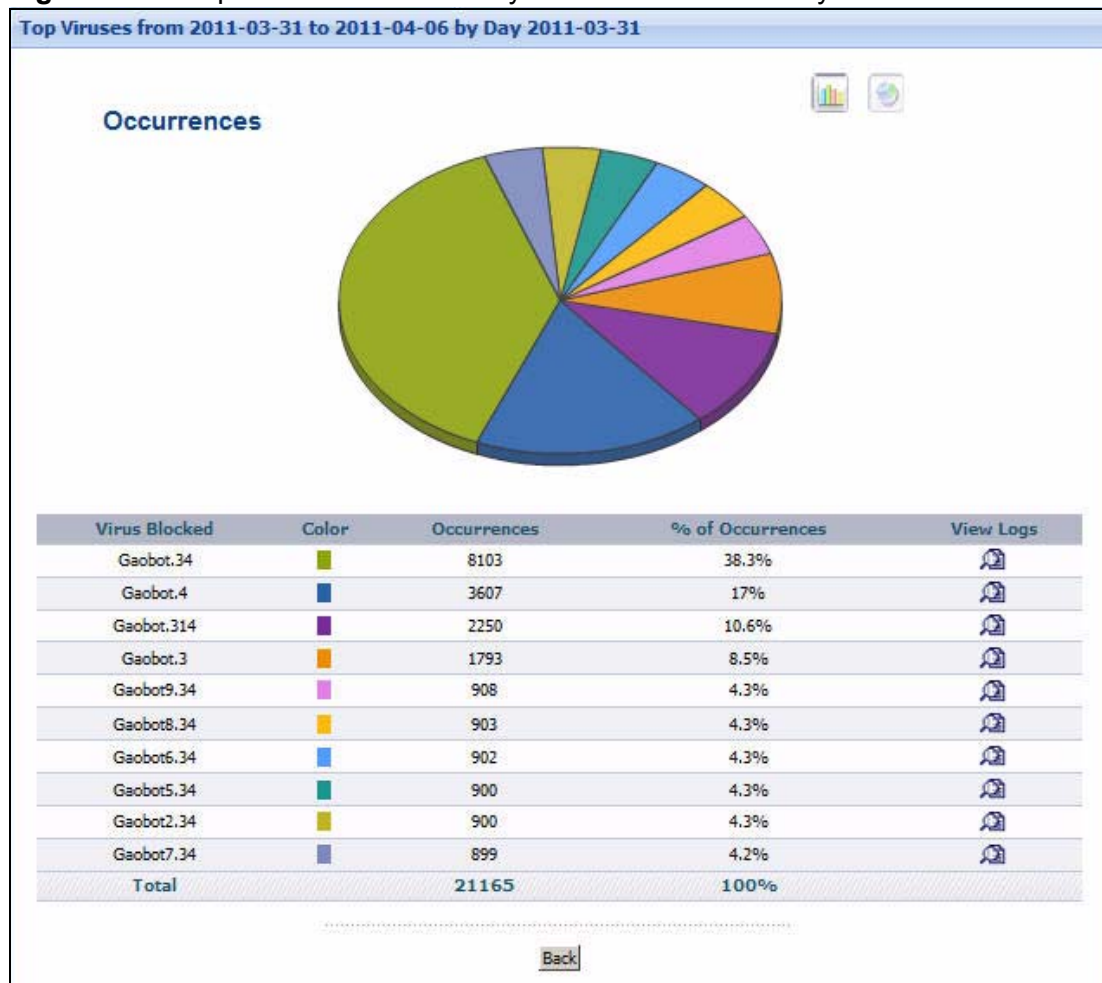
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.4.2 Virus Summary Drill-Down

Use this report to look at the viruses in a specific time interval.

Click on a specific time interval in **Report > Network Security > AntiVirus > Summary** to open this screen.

Figure 146 Report > Network Security > AntiVirus > Summary > Drill-Down



Each field is described in the following table.

Table 132 Report > Network Security > AntiVirus > Summary > Drill-Down

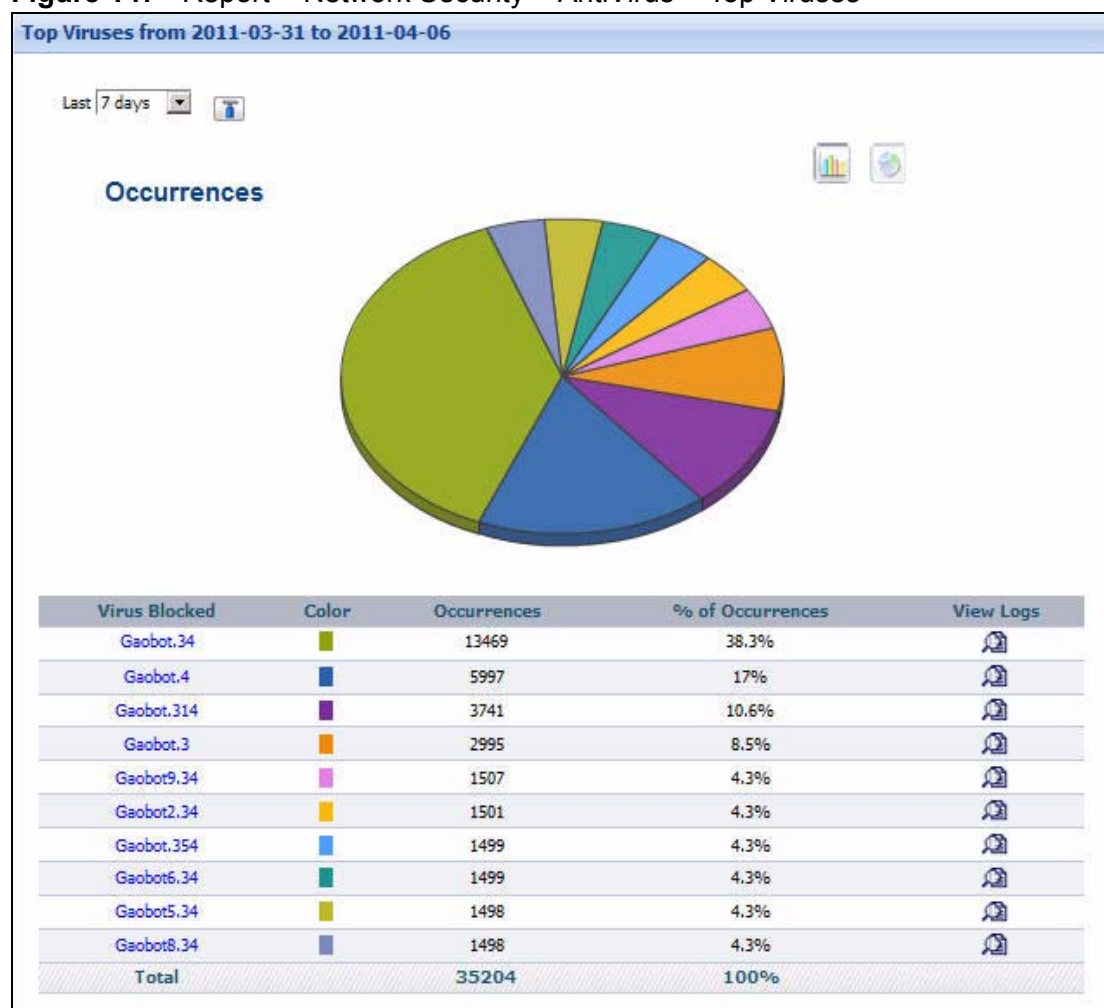
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the viruses stopped in the selected time interval, sorted by the number of occurrences of each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences in the selected time interval was made by each virus.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.4.3 Top Viruses

Use this report to look at the top viruses by number of occurrences.

Click **Report > Network Security > AntiVirus > Top Viruses** to open this screen.

Figure 147 Report > Network Security > AntiVirus > Top Viruses



Each field is described in the following table.

Table 133 Report > Network Security > AntiVirus > Top Viruses

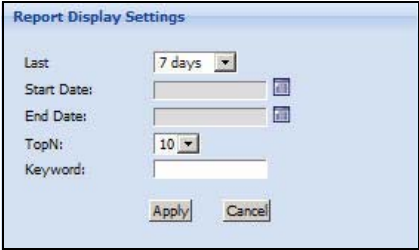
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Virus Blocked field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.

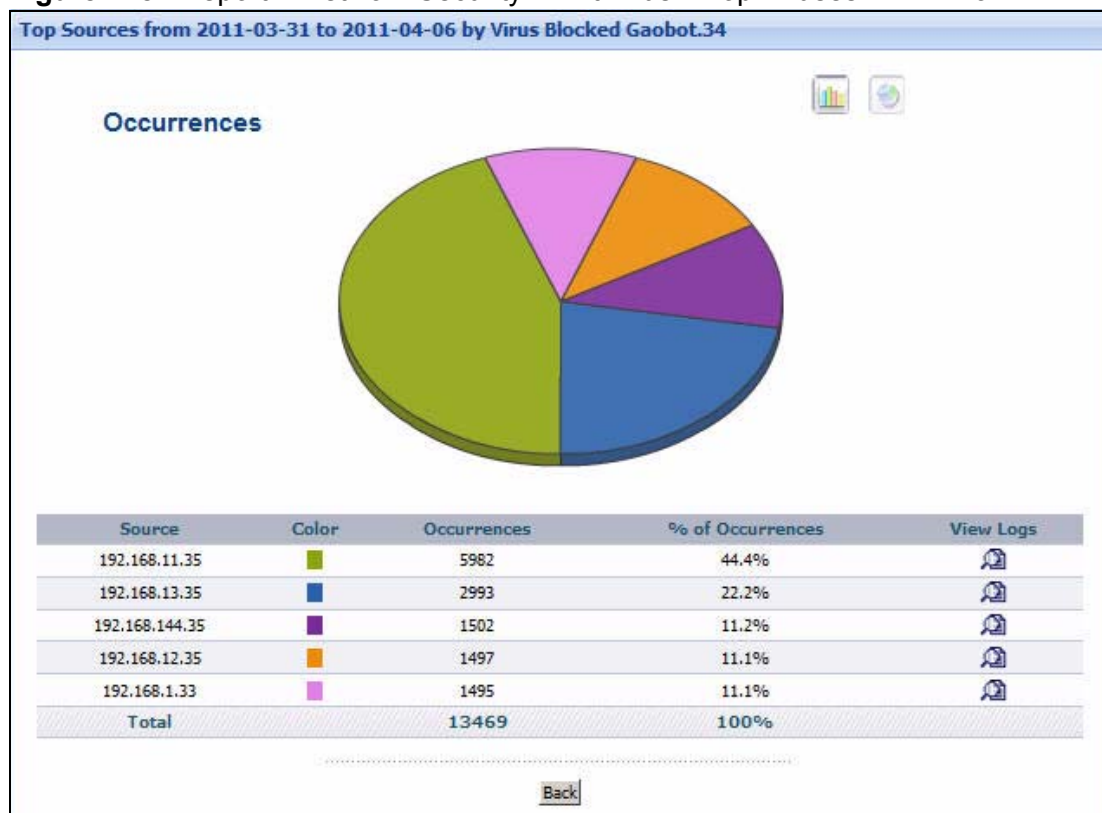
Table 133 Report > Network Security > AntiVirus > Top Viruses

LABEL	DESCRIPTION
% of Occurrences	This field displays what percentage each virus's occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

7.4.4 Top Viruses Drill-Down

Use this report to look at the top sources of any top virus.

Click on a specific virus in **Report > Network Security > AntiVirus > Top Viruses** to open this screen.

Figure 148 Report > Network Security > AntiVirus > Top Viruses > Drill-Down

Each field is described in the following table.

Table 134 Report > Network Security > AntiVirus > Top Viruses > Drill-Down

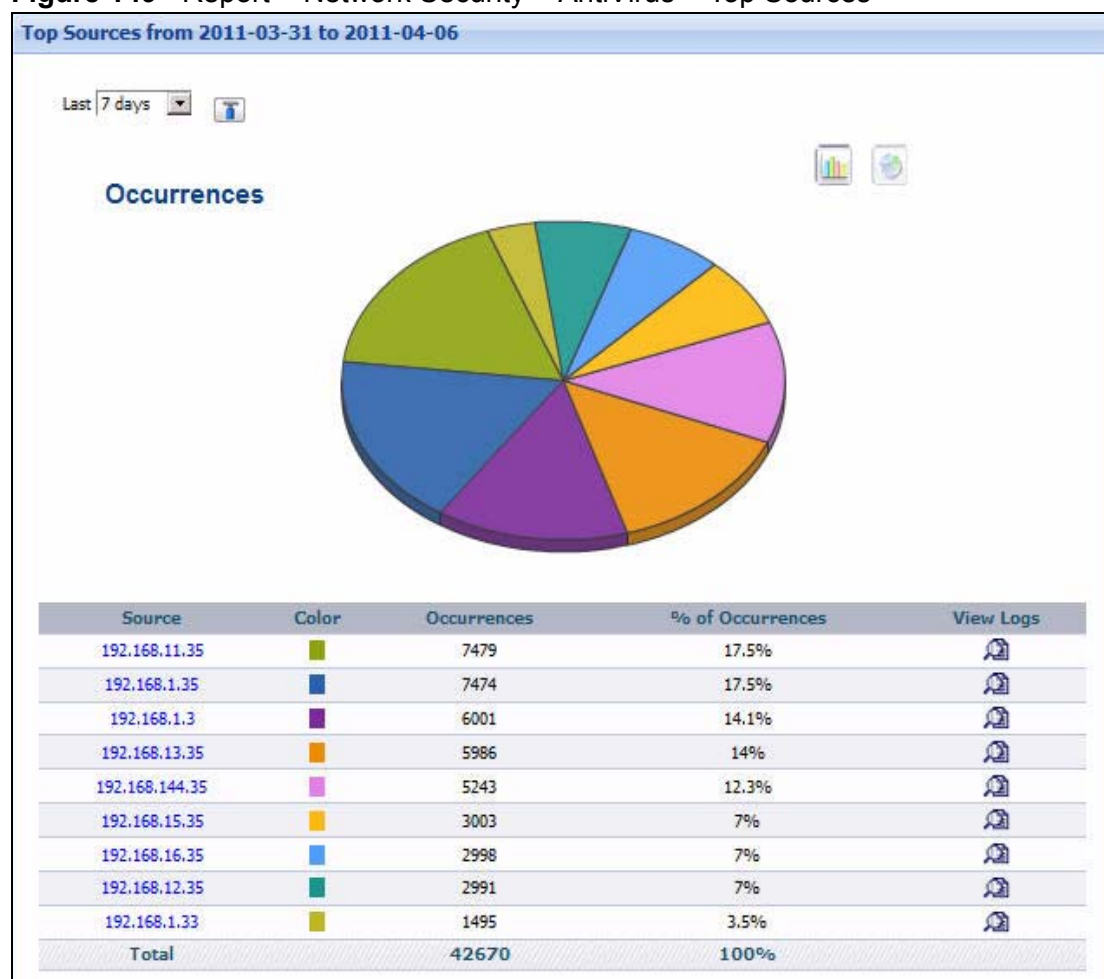
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected virus, sorted by the number of occurrences by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences of the selected virus from each source.
% of Occurrences	This field displays what percentage of all occurrences of the selected virus comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected virus of the selected virus is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.4.5 Top Virus Sources

Use this report to look at the top sources of virus occurrences by number of occurrences.

Click **Report > Network Security > AntiVirus > Top Sources** to open this screen.

Figure 149 Report > Network Security > AntiVirus > Top Sources



Each field is described in the following table.

Table 135 Report > Network Security > AntiVirus > Top Sources

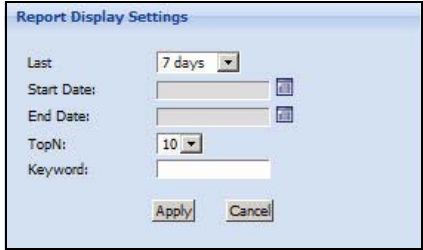
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 135 Report > Network Security > AntiVirus > Top Sources

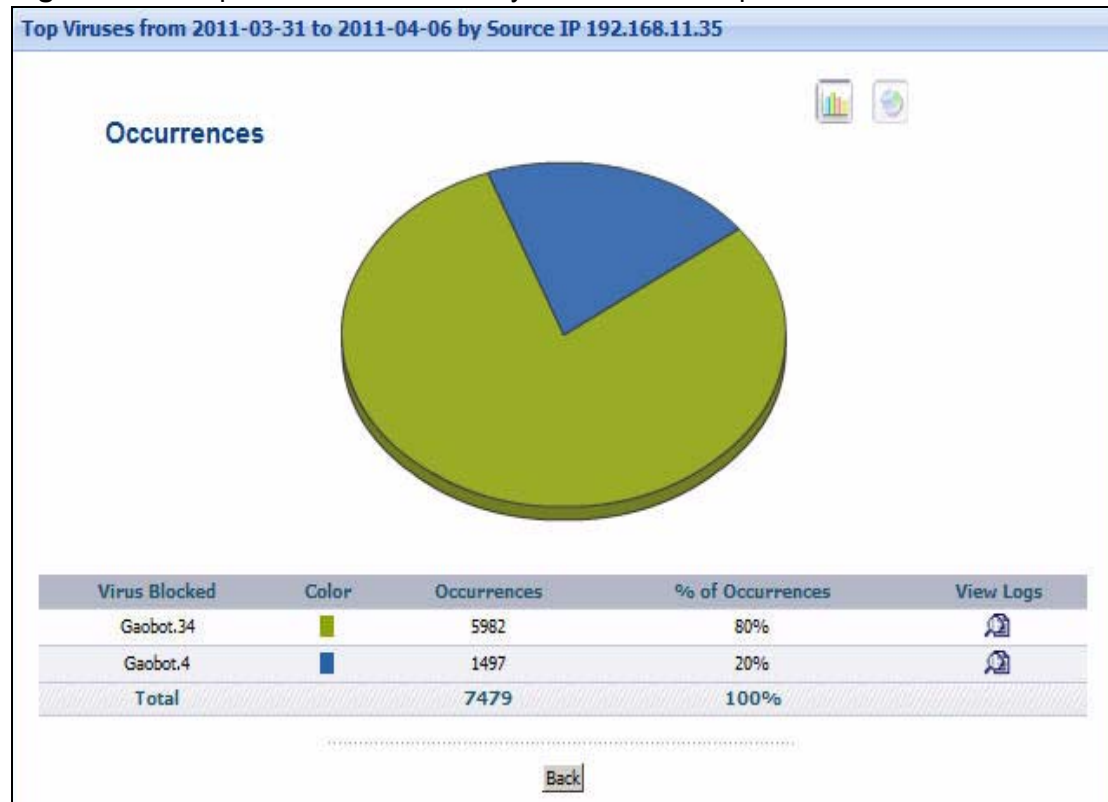
LABEL	DESCRIPTION
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top viruses for the selected source.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.4.6 Top Virus Sources Drill-Down

Use this report to look at the top viruses for any top source.

Click on a specific source in **Report > Network Security > AntiVirus > Top Sources** to open this screen.

Figure 150 Report > Network Security > AntiVirus > Top Sources > Drill-Down



Each field is described in the following table.

Table 136 Report > Network Security > AntiVirus > Top Sources > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from the selected source, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences from the selected source by each virus.
% of Occurrences	This field displays what percentage of all occurrences from the selected source was made by each virus.
View Logs	Click this icon to see the logs that go with the record.

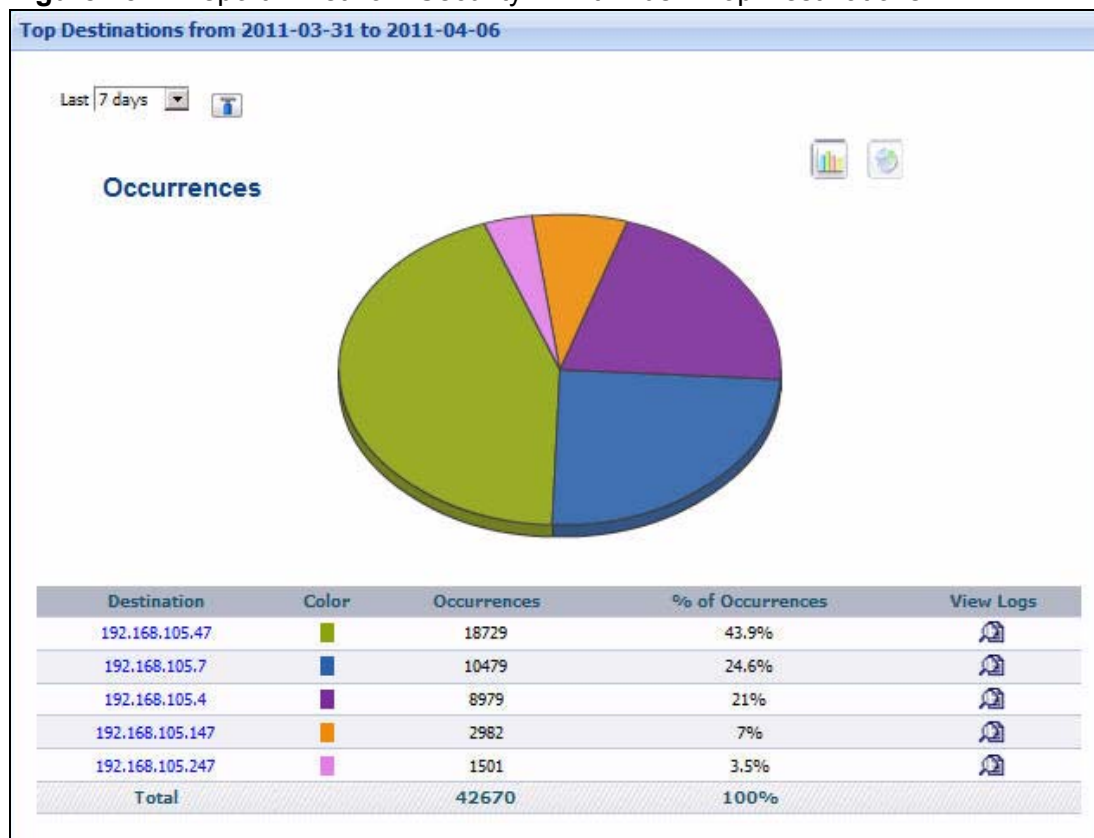
Table 136 Report > Network Security > AntiVirus > Top Sources > Drill-Down

LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.4.7 Top Virus Destinations

Use this report to look at the top destinations of virus occurrences by number of occurrences.

Click **Report > Network Security > AntiVirus > Top Destinations** to open this screen.

Figure 151 Report > Network Security > AntiVirus > Top Destinations

Each field is described in the following table.

Table 137 Report > Network Security > AntiVirus > Top Destinations

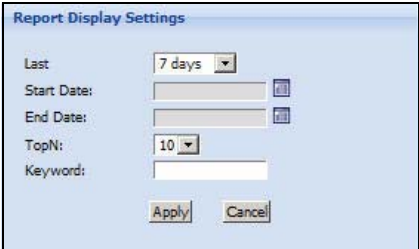
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.

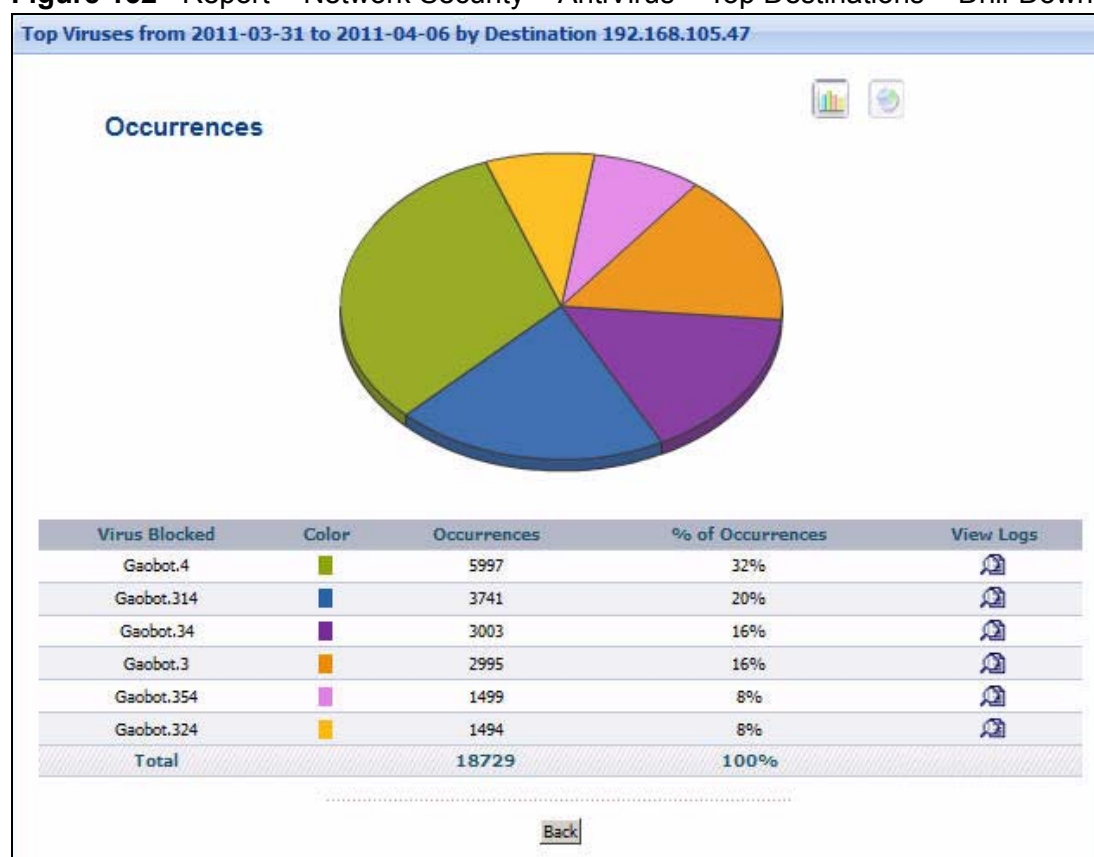
Table 137 Report > Network Security > AntiVirus > Top Destinations

LABEL	DESCRIPTION
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

7.4.8 Top Virus Destinations Drill-Down

Use this report to look at the top viruses for any top destination.

Click on a specific destination in **Report > Network Security > AntiVirus > Top Destinations** to open this screen.

Figure 152 Report > Network Security > AntiVirus > Top Destinations > Drill-Down

Each field is described in the following table.

Table 138 Report > Network Security > AntiVirus > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from going to the selected destination, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of times each virus was sent to the selected destination.
% of Occurrences	This field displays what percentage each virus made of the viruses sent to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

E-Mail Security

This chapter discusses how to use reports to look at E-Mail related security threats that were detected by the ZyXEL device's firewall.

8.1 Virus Found

These reports look at viruses that were detected by the ZyXEL device's anti-virus feature. The reports include viruses received through the following E-Mail related protocols: Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4 (IMAP4).

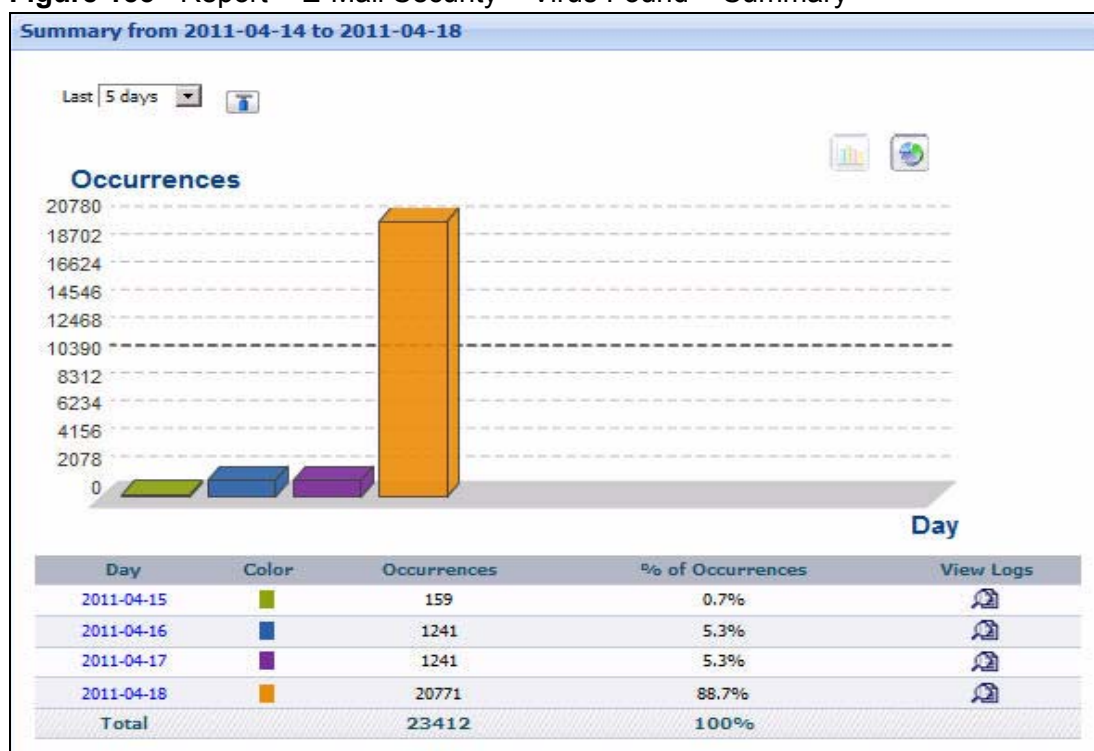
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus > General**. ZyXEL devices can log viruses based on the **Service** the virus was using. Make sure the ZyXEL device logs viruses you want to include in Vantage Report.

8.1.1 Virus Found Summary

Use this report to look at the number of virus occurrences by time interval.

Click **Report > E-Mail Security > Virus Found > Summary** to open this screen.

Figure 153 Report > E-Mail Security > Virus Found > Summary



Each field is described in the following table.

Table 139 Report > E-Mail Security > Virus Found > Summary

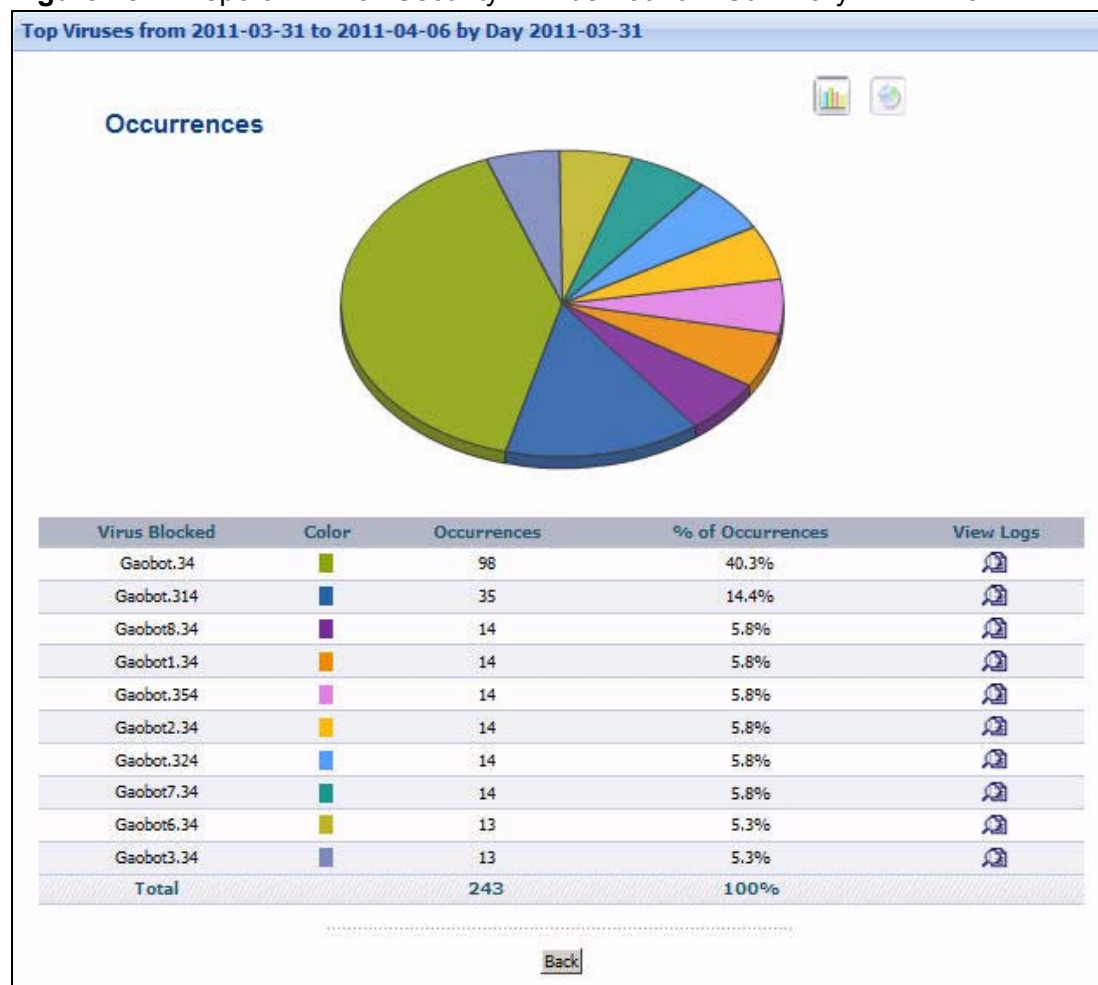
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.1.2 Virus Found Summary Drill-Down

Use this report to look at the viruses in a specific time interval.

Click on a specific time interval in **Report > E-Mail Security > Virus Found > Summary** to open this screen.

Figure 154 Report > E-Mail Security > Virus Found > Summary > Drill-Down



Each field is described in the following table.

Table 140 Report > E-Mail Security > Virus Found > Summary > Drill-Down

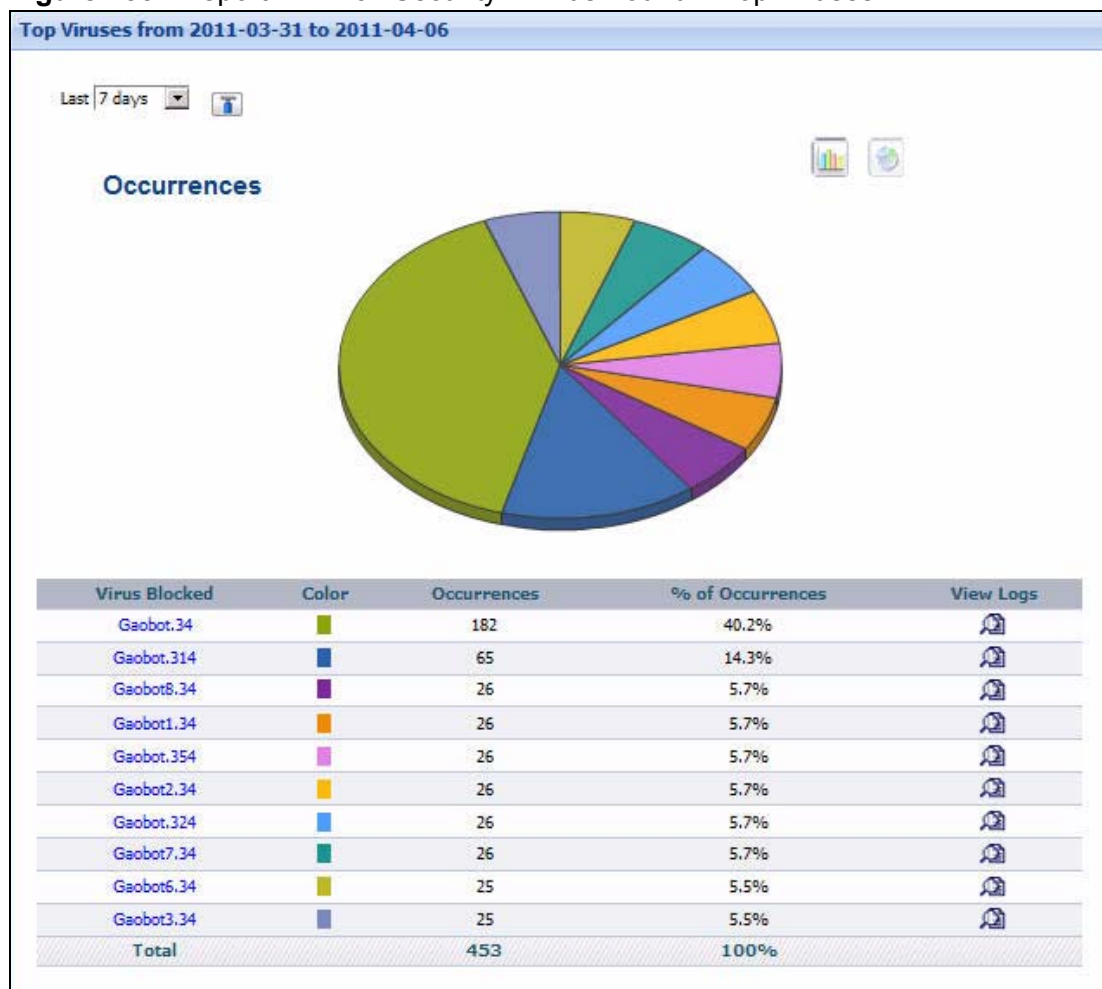
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the viruses stopped in the selected time interval, sorted by the number of occurrences of each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences in the selected time interval was made by each virus.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.1.3 Top Viruses

Use this report to look at the top viruses by number of occurrences.

Click **Report > E-Mail Security > Virus Found > Top Viruses** to open this screen.

Figure 155 Report > E-Mail Security > Virus Found > Top Viruses



Each field is described in the following table.

Table 141 Report > E-Mail Security > Virus Found > Top Viruses

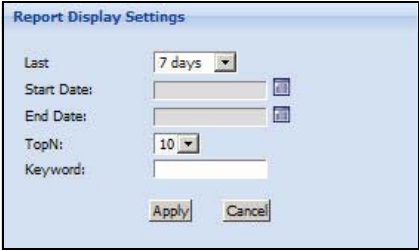
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Virus Blocked field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.

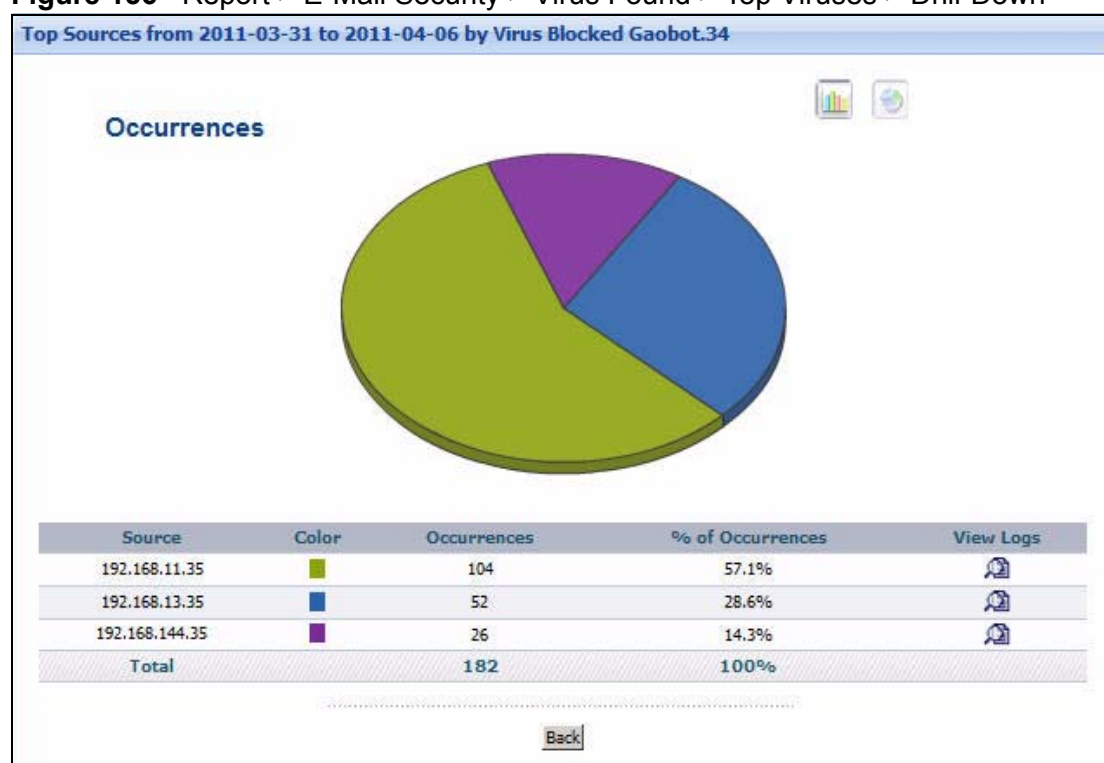
Table 141 Report > E-Mail Security > Virus Found > Top Viruses

LABEL	DESCRIPTION
% of Occurrences	This field displays what percentage each virus's occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

8.1.4 Top Viruses Drill-Down

Use this report to look at the top sources of any top virus.

Click on a specific virus in **Report > E-Mail Security > Virus Found > Top Viruses** to open this screen.

Figure 156 Report > E-Mail Security > Virus Found > Top Viruses > Drill-Down

Each field is described in the following table.

Table 142 Report > E-Mail Security > Virus Found > Top Viruses > Drill-Down

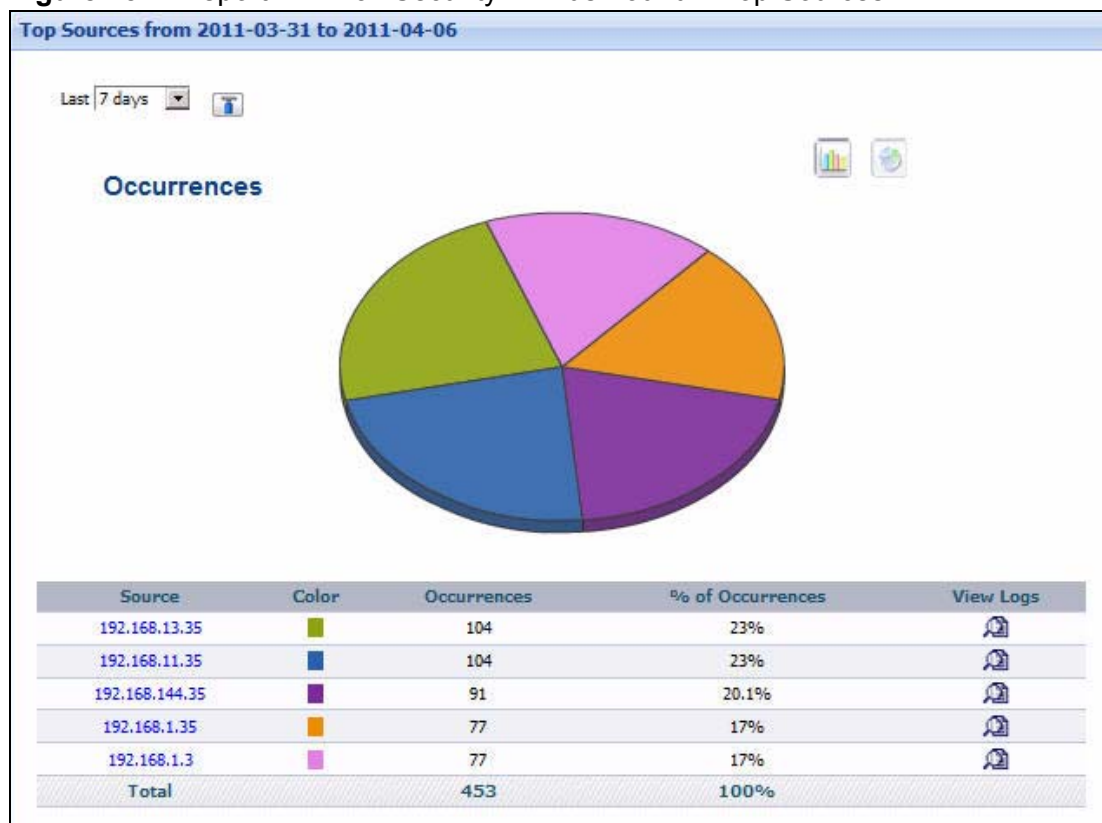
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected virus, sorted by the number of occurrences by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences of the selected virus from each source.
% of Occurrences	This field displays what percentage of all occurrences of the selected virus comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected virus of the selected virus is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.1.5 Top Virus Sources

Use this report to look at the top sources of virus occurrences by number of occurrences.

Click **Report > E-Mail Security > Virus Found > Top Sources** to open this screen.

Figure 157 Report > E-Mail Security > Virus Found > Top Sources



Each field is described in the following table.

Table 143 Report > E-Mail Security > Virus Found > Top Sources

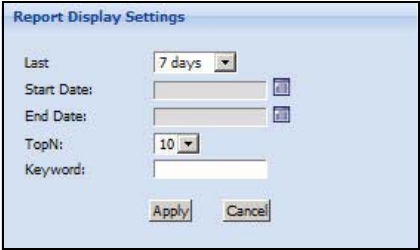
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 143 Report > E-Mail Security > Virus Found > Top Sources

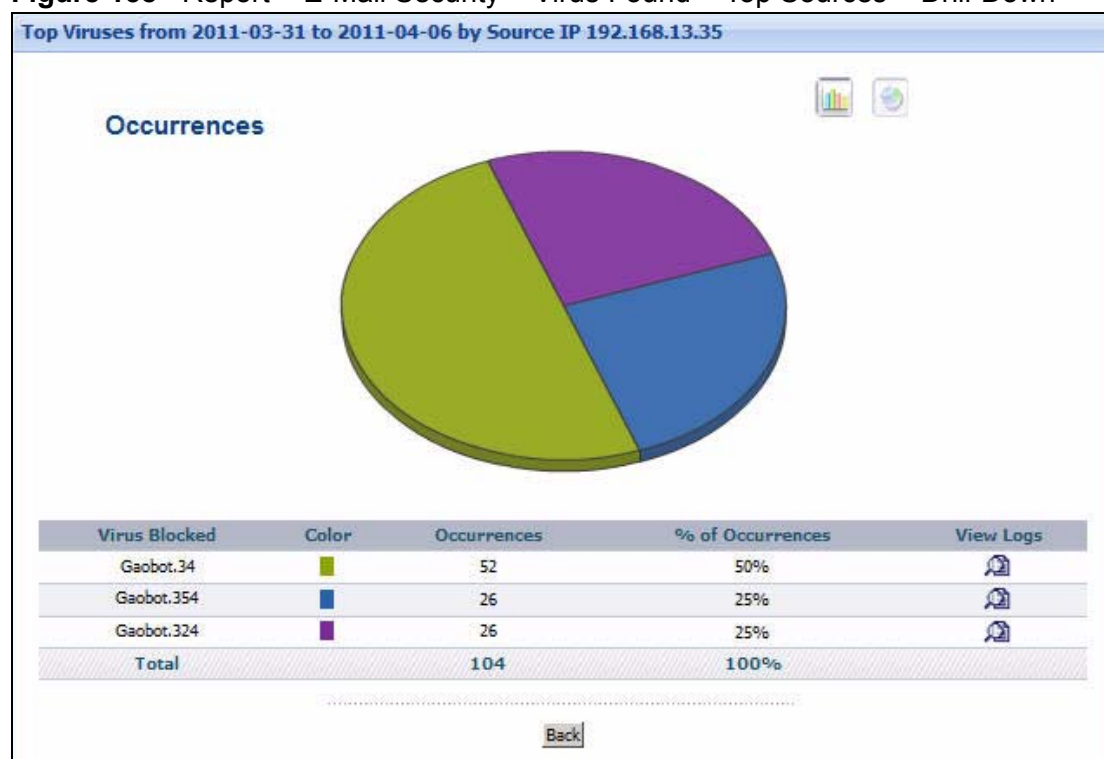
LABEL	DESCRIPTION
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top viruses for the selected source.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.1.6 Top Virus Sources Drill-Down

Use this report to look at the top viruses for any top source.

Click on a specific source in **Report > E-Mail Security > Virus Found > Top Sources** to open this screen.

Figure 158 Report > E-Mail Security > Virus Found > Top Sources > Drill-Down



Each field is described in the following table.

Table 144 Report > E-Mail Security > Virus Found > Top Sources > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from the selected source, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences from the selected source by each virus.
% of Occurrences	This field displays what percentage of all occurrences from the selected source was made by each virus.
View Logs	Click this icon to see the logs that go with the record.

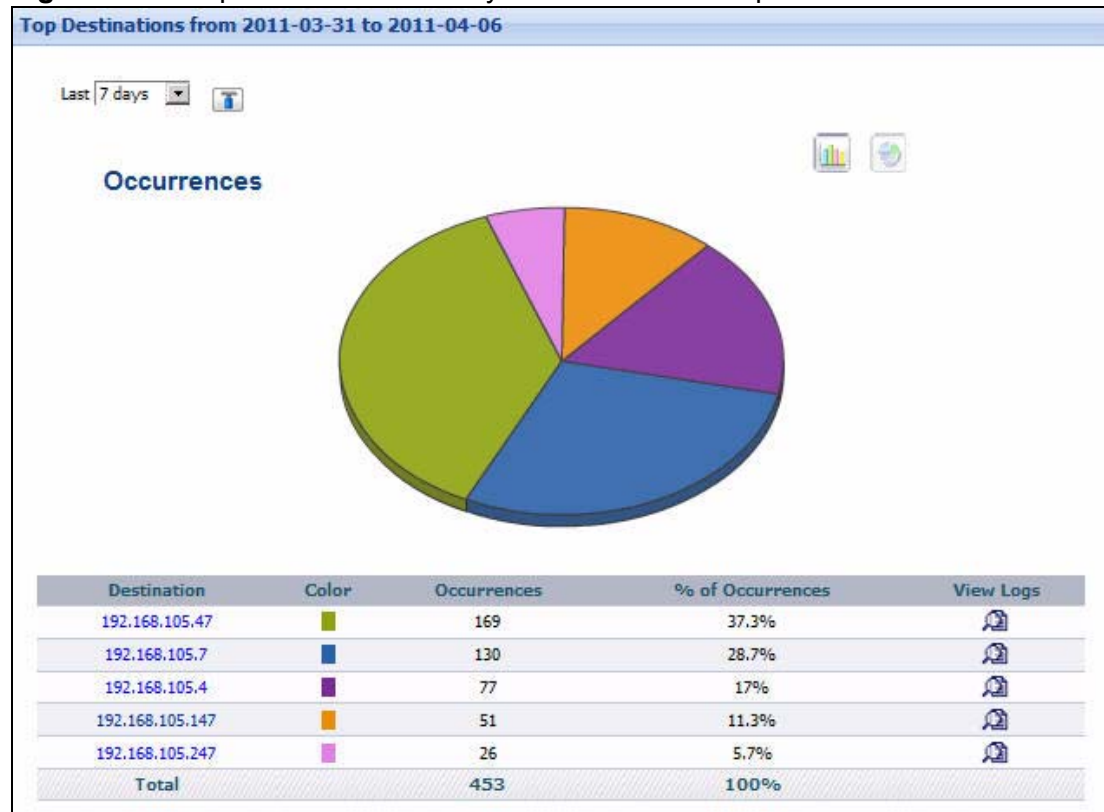
Table 144 Report > E-Mail Security > Virus Found > Top Sources > Drill-Down

LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.1.7 Top Virus Destinations

Use this report to look at the top destinations of virus occurrences by number of occurrences.

Click **Report > E-Mail Security > Virus Found > Top Destinations** to open this screen.

Figure 159 Report > E-Mail Security > Virus Found > Top Destinations

Each field is described in the following table.

Table 145 Report > E-Mail Security > Virus Found > Top Destinations

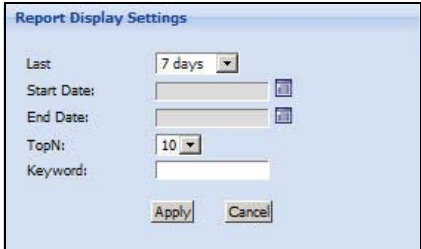
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.

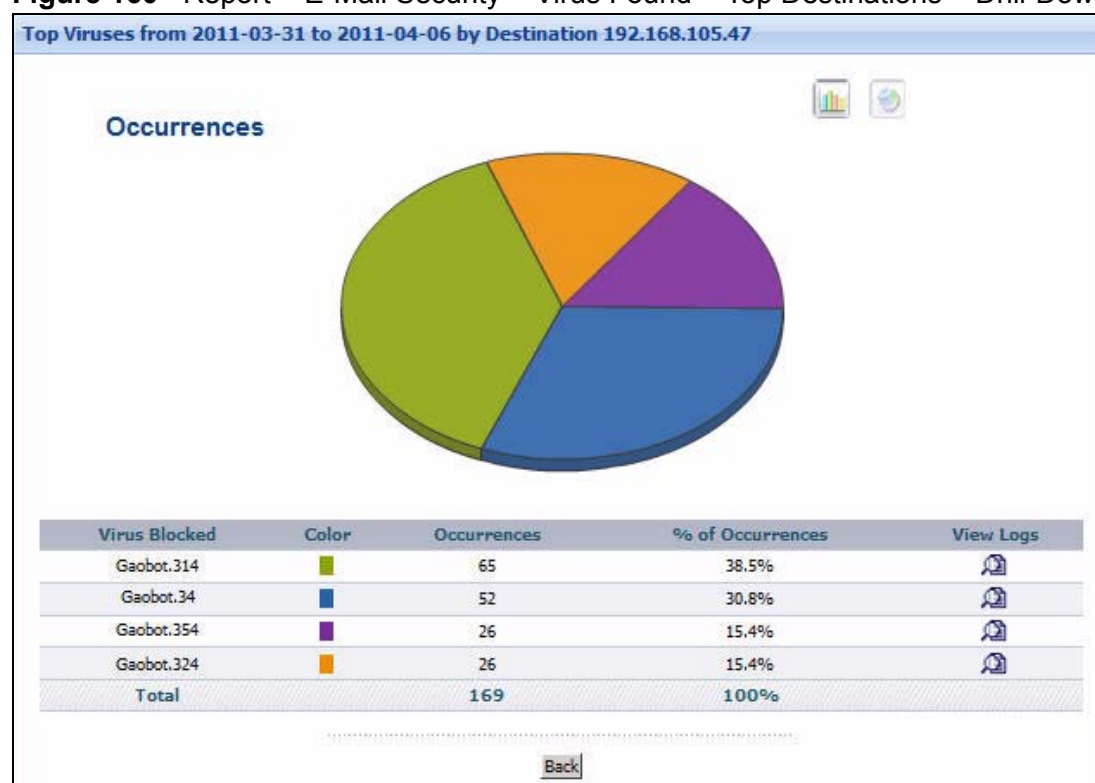
Table 145 Report > E-Mail Security > Virus Found > Top Destinations

LABEL	DESCRIPTION
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

8.1.8 Top Virus Destinations Drill-Down

Use this report to look at the top viruses for any top destination.

Click on a specific destination in **Report > E-Mail Security > Virus Found > Top Destinations** to open this screen.

Figure 160 Report > E-Mail Security > Virus Found > Top Destinations > Drill-Down

Each field is described in the following table.

Table 146 Report > E-Mail Security > Virus Found > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from going to the selected destination, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of times each virus was sent to the selected destination.
% of Occurrences	This field displays what percentage each virus made of the viruses sent to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.2 Spam

These reports look at spam messages that were detected by the ZyXEL device's anti-spam feature. You can also look at the top senders and sources of spam messages.

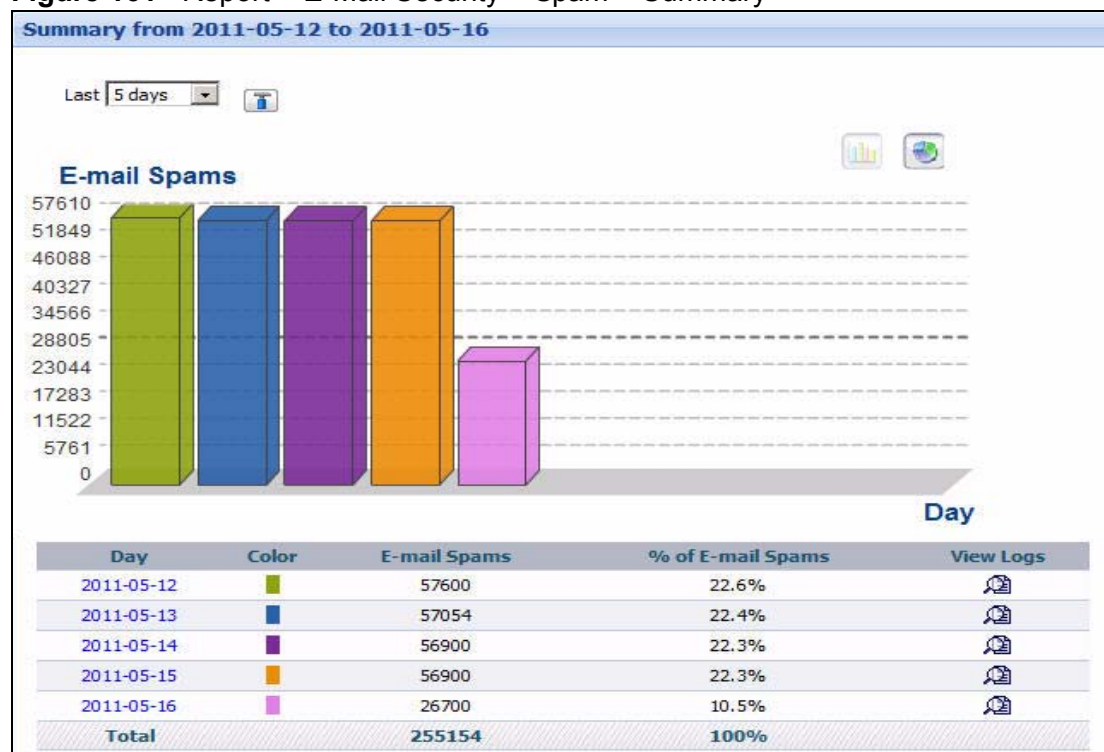
Note: To look at anti-spam reports, each ZyXEL device must record anti-spam messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Anti-Spam** is enabled.

8.2.1 Spam Summary

Use this report to look at the number of spam messages by time interval.

Click **Report > E-Mail Security > Spam > Summary** to open this screen.

Figure 161 Report > E-Mail Security > Spam > Summary



Each field is described in the following table.

Table 147 Report > E-Mail Security > Spam > Summary

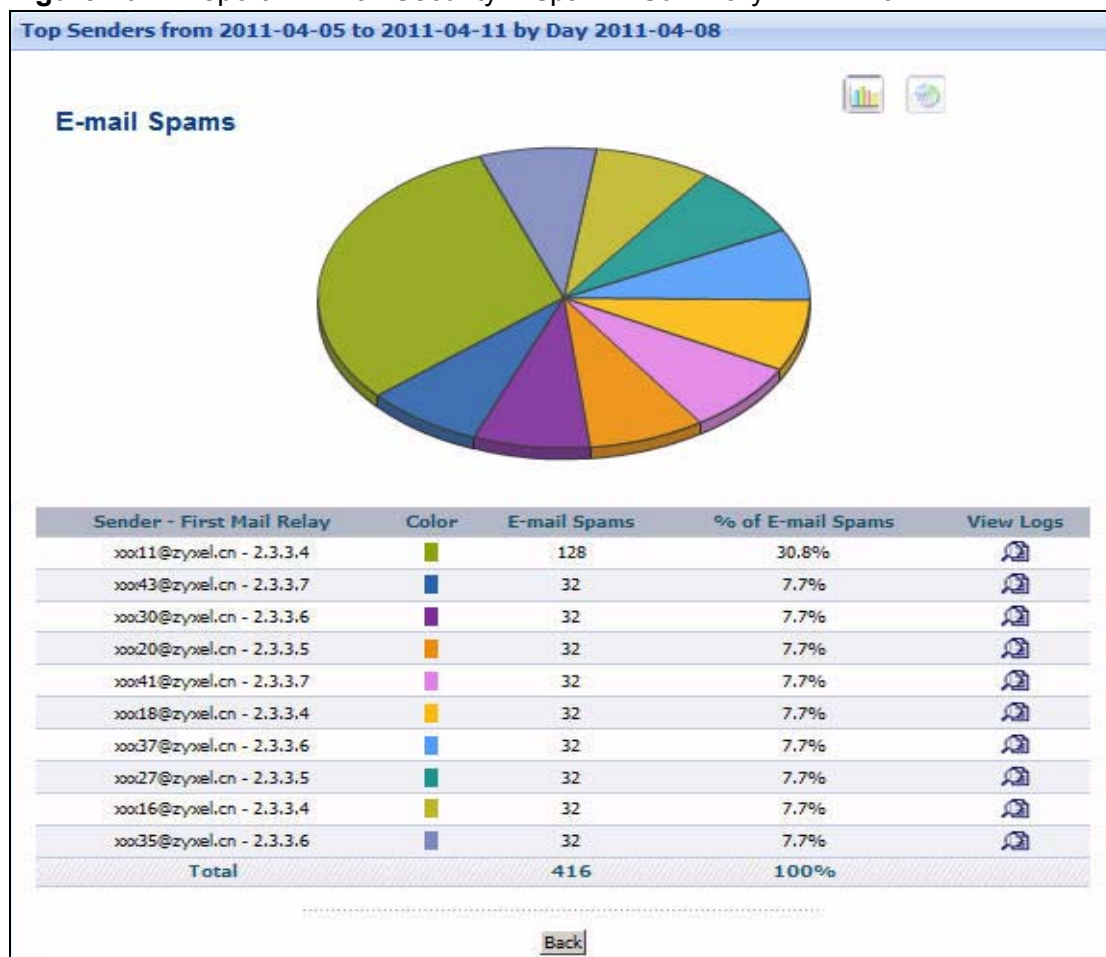
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top spam messages in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
E-mail Spams	This field displays the number of spam messages in the selected time interval.
% of E-mail Spams	This field displays what percentage of all spam messages was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.2.2 Spam Summary Drill-Down

Use this report to look at the top combinations of senders of spam messages and the first SMTP server to which the sender sends spam in a specific time interval. For example, if a sender sends spam through two SMTP servers, there are two entries for the sender, one with each SMTP server.

Click on a specific time interval in **Report > E-Mail Security > Spam > Summary** to open this screen.

Figure 162 Report > E-Mail Security > Spam > Summary > Drill-Down



Each field is described in the following table.

Table 148 Report > E-Mail Security > Spam > Summary > Drill-Down

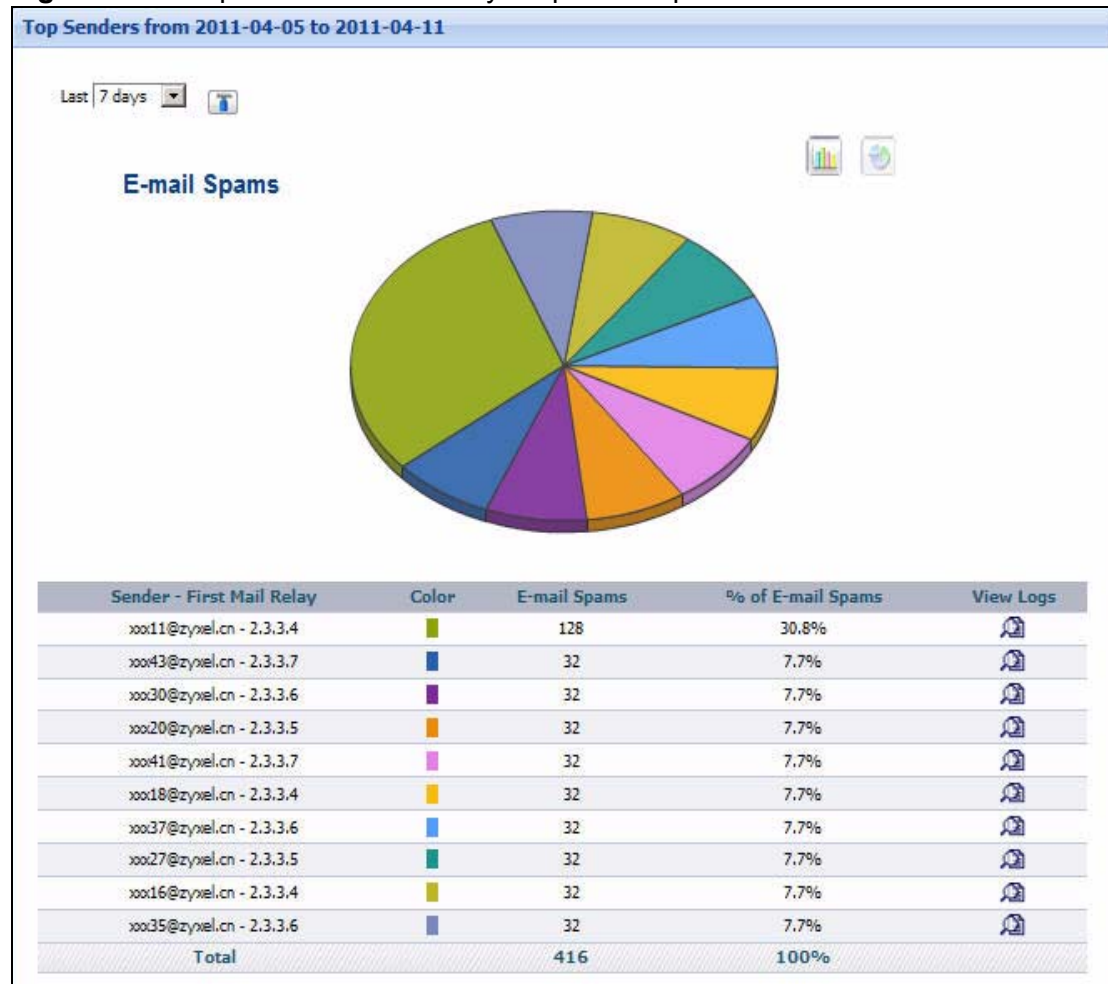
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Sender	This field displays the top combinations of senders of spam and the first SMTP server to which spam is sent in the selected time interval, sorted by the number of spam messages sent for each combination. Each sender is identified by its e-mail address. Each SMTP server is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each sender in the graph.
E-mail Spams	This field displays how many spam messages each sender sent.
% of E-mail Spams	This field displays what percentage of all spam messages in the selected time interval was sent by each sender.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the senders above. If the number of senders in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.2.3 Top Spam Senders

Use this report to look at the top combinations of senders of spam messages and the first SMTP server to which the sender sends spam. For example, if a sender sends spam through two SMTP servers, there are two entries for the sender, one with each SMTP server.

Click **Report > E-Mail Security > Spam > Top Senders** to open this screen.

Figure 163 Report > E-Mail Security > Spam > Top Senders



Each field is described in the following table.

Table 149 Report > E-Mail Security > Spam > Top Senders

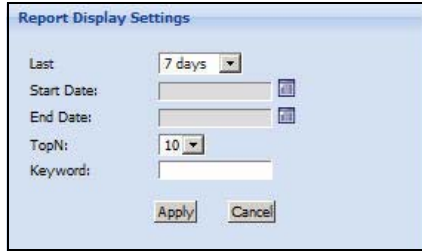
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Sender field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 149 Report > E-Mail Security > Spam > Top Senders

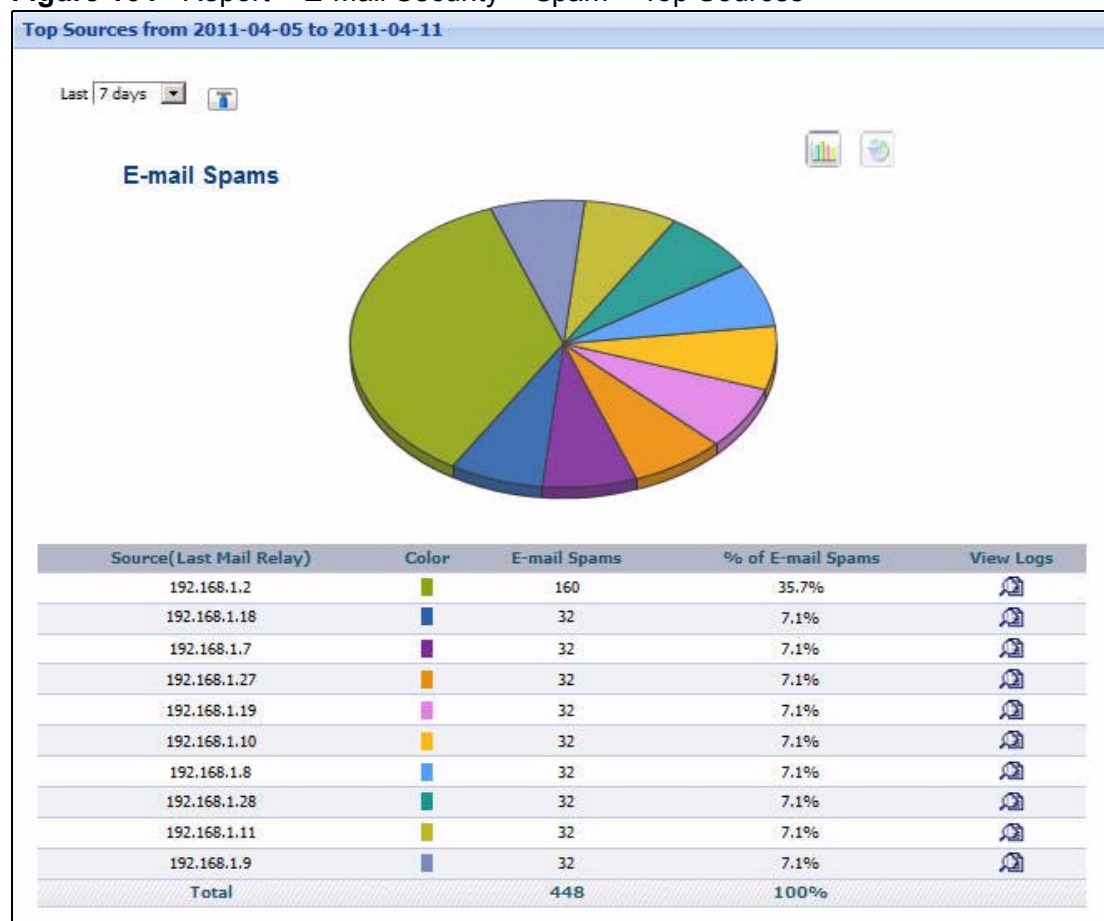
LABEL	DESCRIPTION
Sender	This field displays the top combinations of senders of spam and the first SMTP server to which the spam was sent, sorted by the number of spam messages sent for each combination. Each sender is identified by its e-mail address. Each SMTP server is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each sender in the graph.
E-mail Spams	This field displays how many spam messages each sender sent.
% of E-mail Spams	This field displays what percentage of all spam messages was sent by each sender.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the senders above.

8.2.4 Top Spam Sources

Use this report to look at the top sources of spam messages by number of messages.

Click **Report > E-Mail Security > Spam > Top Sources** to open this screen.

Figure 164 Report > E-Mail Security > Spam > Top Sources



Each field is described in the following table.

Table 150 Report > E-Mail Security > Spam > Top Sources

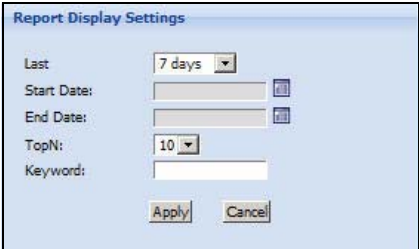
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top SMTP servers that sent spam to the selected device, sorted by the number of spam messages from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each SMTP server is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").

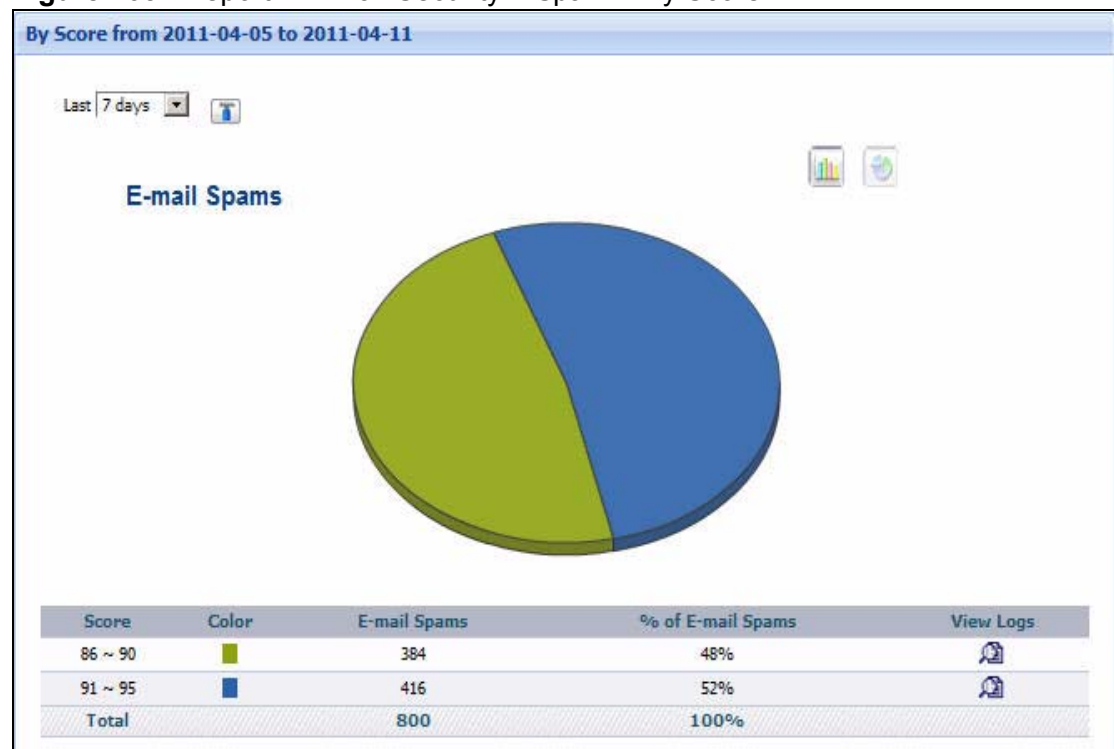
Table 150 Report > E-Mail Security > Spam > Top Sources

LABEL	DESCRIPTION
Color	This field displays what color represents each source in the graph.
E-mail Spams	This field displays the number of spam messages from each source.
% of E-mail Spams	This field displays what percentage of all spam messages came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.2.5 Spam Scores

Use this report to look at the scores calculated for spam messages by number of messages.

Click **Report > E-Mail Security > Spam > By Score** to open this screen.

Figure 165 Report > E-Mail Security > Spam > By Score

Each field is described in the following table.

Table 151 Report > E-Mail Security > Spam > By Score

LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Score	This field displays the scores calculated for spam messages by the selected device, sorted by the number of spam messages from each score. If the number of scores is less than the maximum number of records displayed in this table, every score is displayed.
Color	This field displays what color represents each score in the graph.
E-mail Spams	This field displays the number of spam messages with each score.
% of E-mail Spams	This field displays what percentage of all spam messages had each score.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the scores above.

8.3 Intrusion Hits

These reports look at intrusion signatures, types of intrusions, severity of intrusions, and the top sources and destinations of intrusions that are logged on the selected ZyXEL device. **Intrusions** are caused by malicious or suspicious packets sent with the intent of causing harm, illegally accessing resources or interrupting service. They are detected by the selected device's IDP feature. Specifically, these reports include intrusions in the SPAM IDP category on the ZyXEL device.

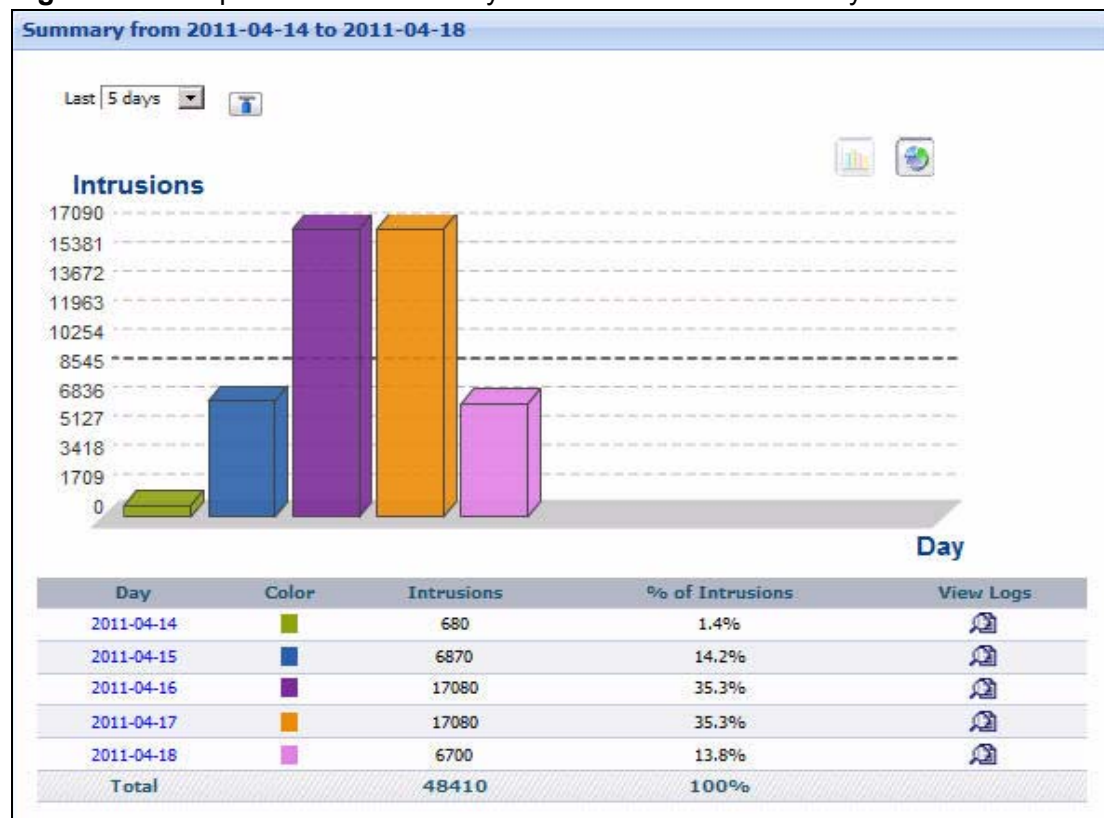
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP > Signature**, and make sure the ZyXEL device logs each **Attack Type** you want to see in Vantage Report.

8.3.1 Intrusion Hits Summary

Use this report to look at the number of intrusions by time interval.

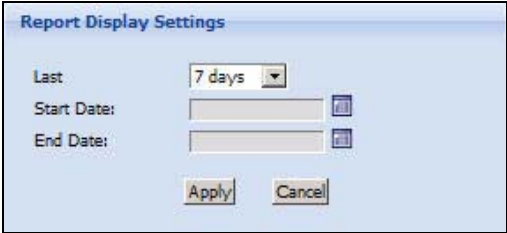
Click **Report > E-Mail Security > Intrusion Hits > Summary** to open this screen.

Figure 166 Report > E-Mail Security > Intrusion Hits > Summary



Each field is described in the following table.

Table 152 Report > E-Mail Security > Intrusion Hits > Summary

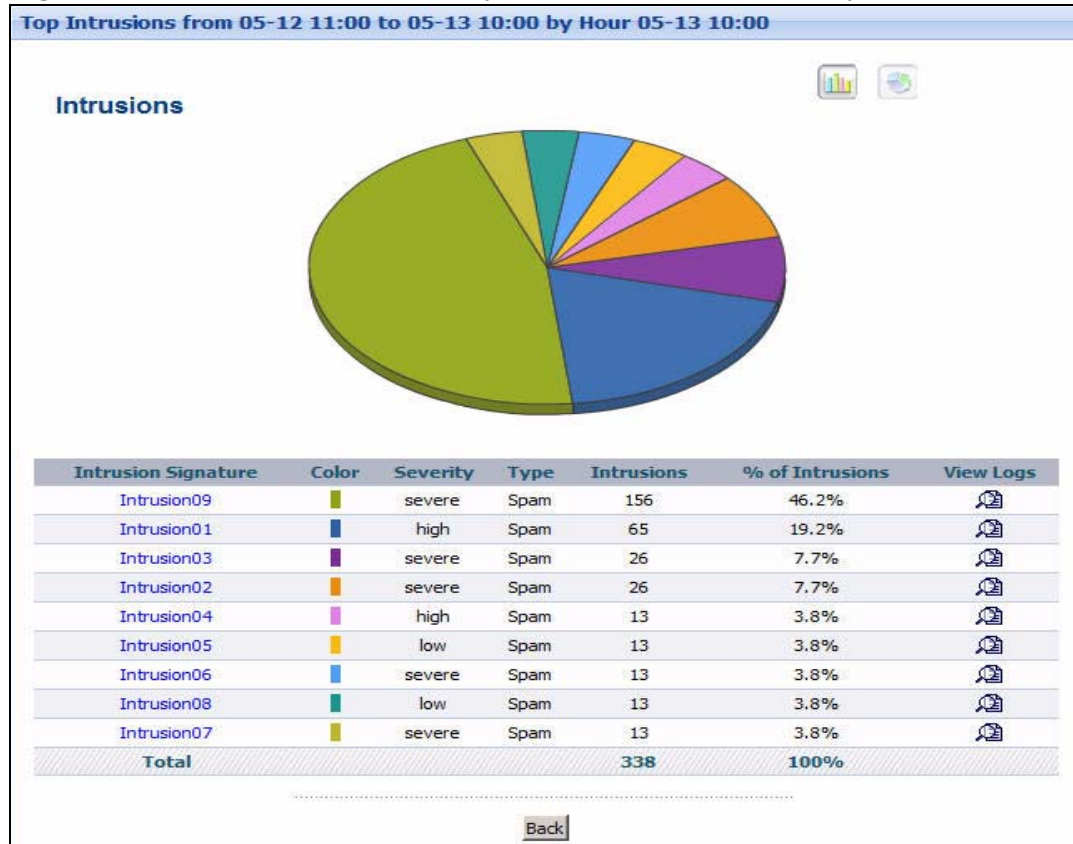
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the intrusion signatures in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Intrusions	This field displays the number of intrusions in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.3.2 Intrusion Hits Summary Drill-Down

Use this report to look at the intrusion signatures in a specific time interval.

Click on a specific time interval in **Report > E-Mail Security > Intrusion Hits > Summary** to open this screen.

Figure 167 Report > E-Mail Security > Intrusion Hits > Summary > Drill-Down



Each field is described in the following table.

Table 153 Report > E-Mail Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 168 on page 364).

Table 153 Report > E-Mail Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

Note: Clicking on some linked entries in the Intrusion screen will open a new window that provides details on the security issue encountered by the devices. The following screen is displayed.

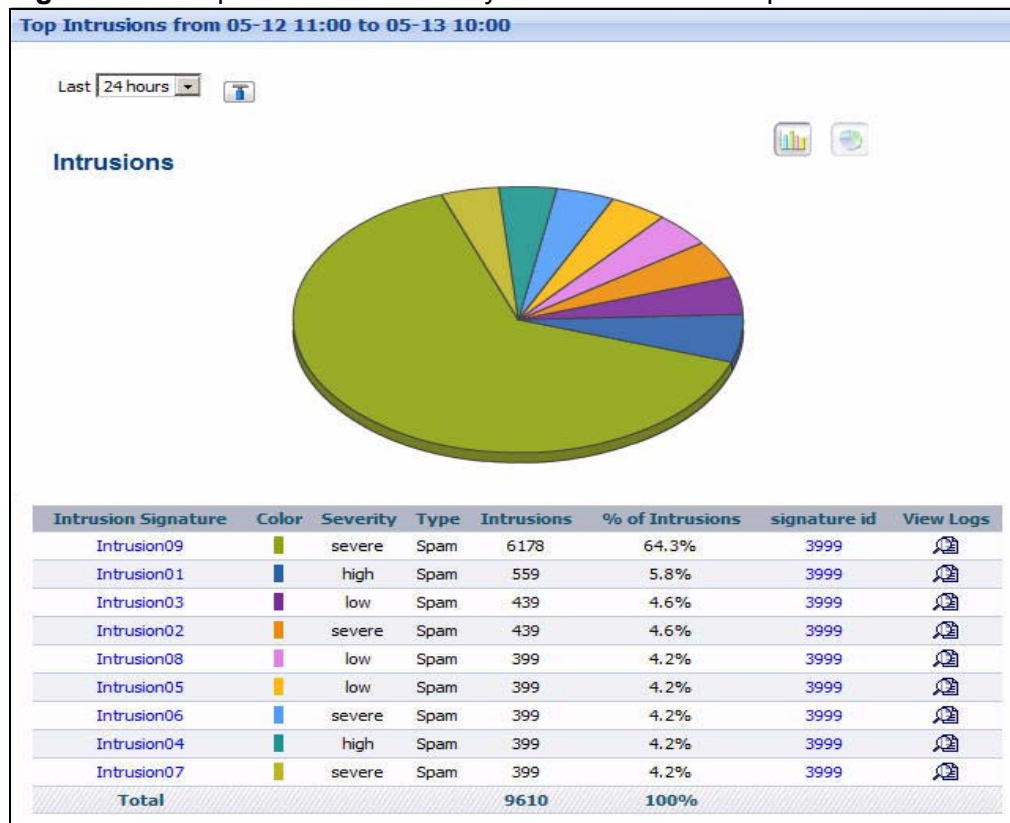
Figure 168 Security Issue Details

8.3.3 Top Intrusion Hits Signatures

Use this report to look at the top intrusion signatures by number of intrusions.

Click **Report > E-Mail Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 169 Report > E-Mail Security > Intrusion Hits > Top Intrusions



Each field is described in the following table.

Table 154 Report > E-Mail Security > Intrusion Hits > Top Intrusions

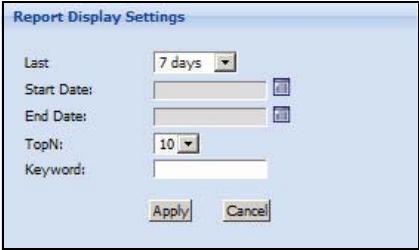
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Intrusion Signature field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature.
Color	This field displays what color represents each intrusion signature in the graph.

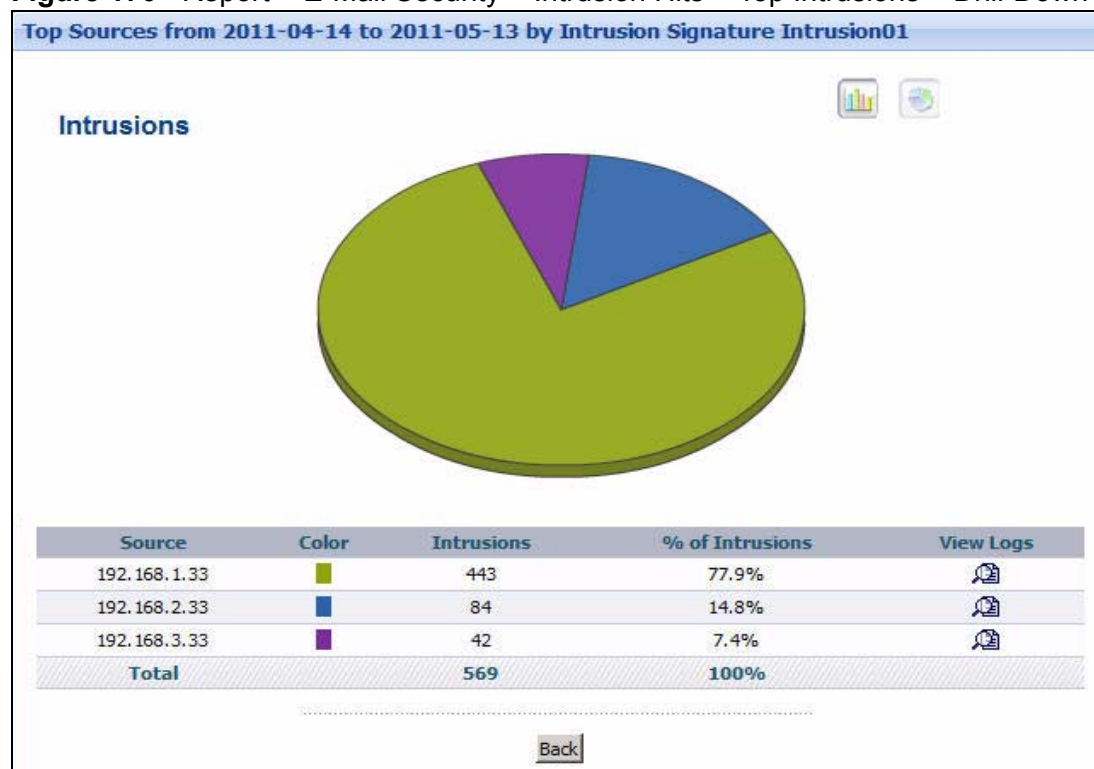
Table 154 Report > E-Mail Security > Intrusion Hits > Top Intrusions

LABEL	DESCRIPTION
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
signature id	This is the security issue identification number. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 168 on page 364).
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

8.3.4 Top Intrusion Hits Signatures Drill-Down

Use this report to look at the top sources of intrusions for any top signature.

Click on a specific intrusion signature in **Report > E-Mail Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 170 Report > E-Mail Security > Intrusion Hits > Top Intrusions > Drill-Down

Each field is described in the following table.

Table 155 Report > E-Mail Security > Intrusion Hits > Top Intrusions > Drill-Down

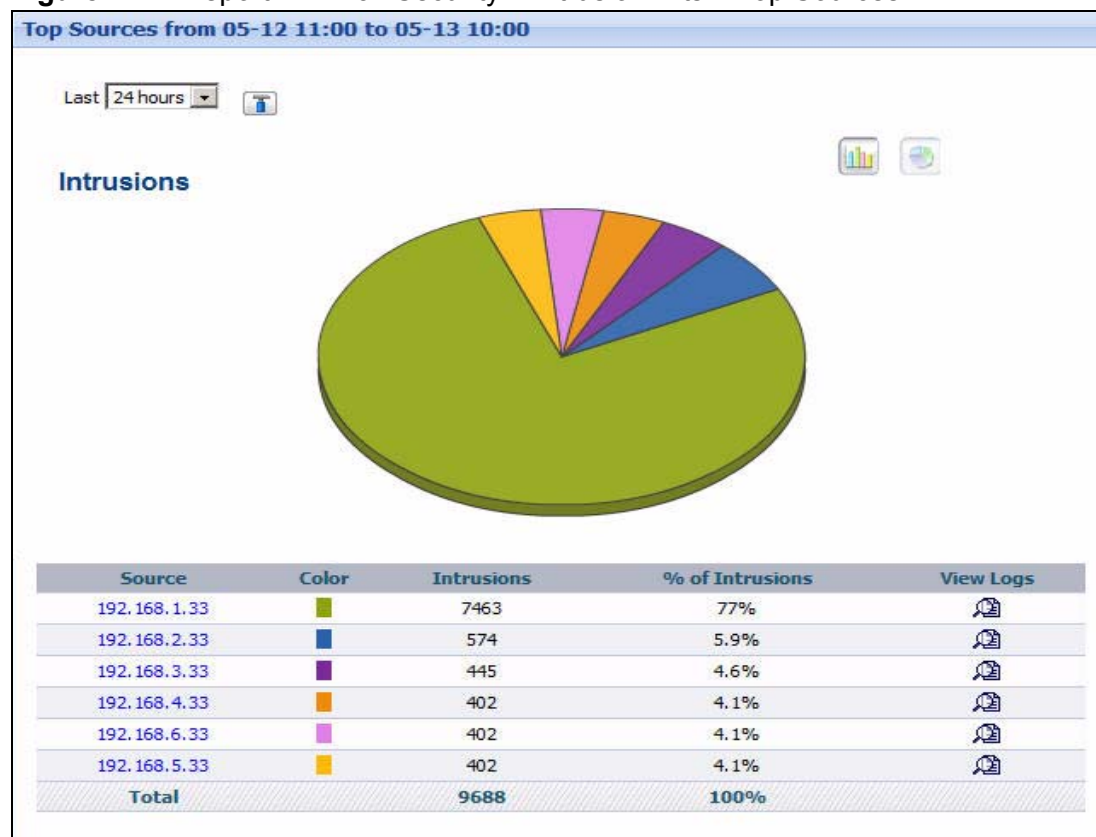
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected intrusion signature, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions using the selected intrusion signature was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected intrusion signature is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.3.5 Top Intrusion Hits Sources

Use this report to look at the top sources of intrusions by number of intrusions.

Click **Report > E-Mail Security > Intrusion Hits > Top Sources** to open this screen.

Figure 171 Report > E-Mail Security > Intrusion Hits > Top Sources



Each field is described in the following table.

Table 156 Report > E-Mail Security > Intrusion Hits > Top Sources

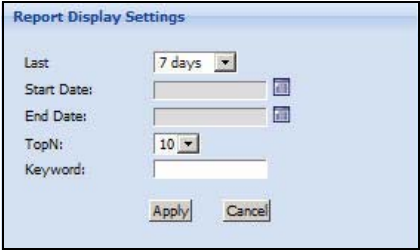
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 156 Report > E-Mail Security > Intrusion Hits > Top Sources

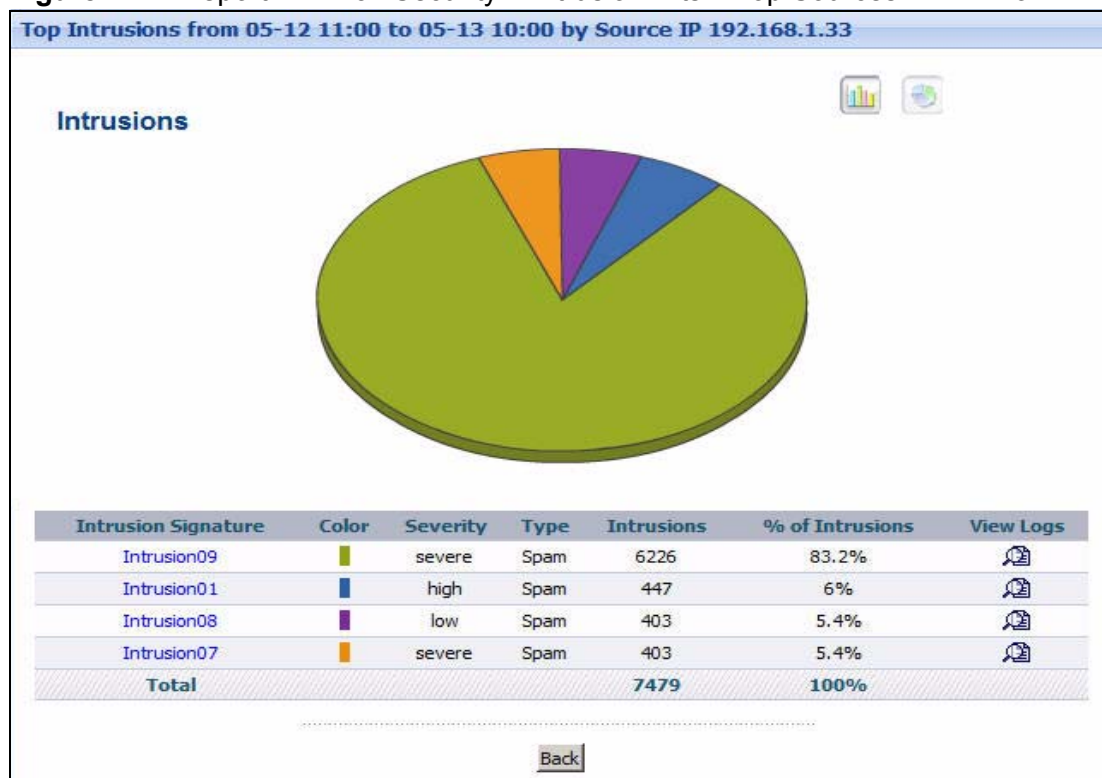
LABEL	DESCRIPTION
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top intrusion signatures for the selected source.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.3.6 Top Intrusion Hits Sources Drill-Down

Use this report to look at the top intrusion signatures for any top source.

Click on a specific source in **Report > E-Mail Security > Intrusion Hits > Top Sources** to open this screen.

Figure 172 Report > E-Mail Security > Intrusion Hits > Top Sources > Drill-Down



Each field is described in the following table.

Table 157 Report > E-Mail Security > Intrusion Hits > Top Sources > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures from the selected source, sorted by the number of intrusions by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by the selected source using each intrusion signature.

Table 157 Report > E-Mail Security > Intrusion Hits > Top Sources > Drill-Down

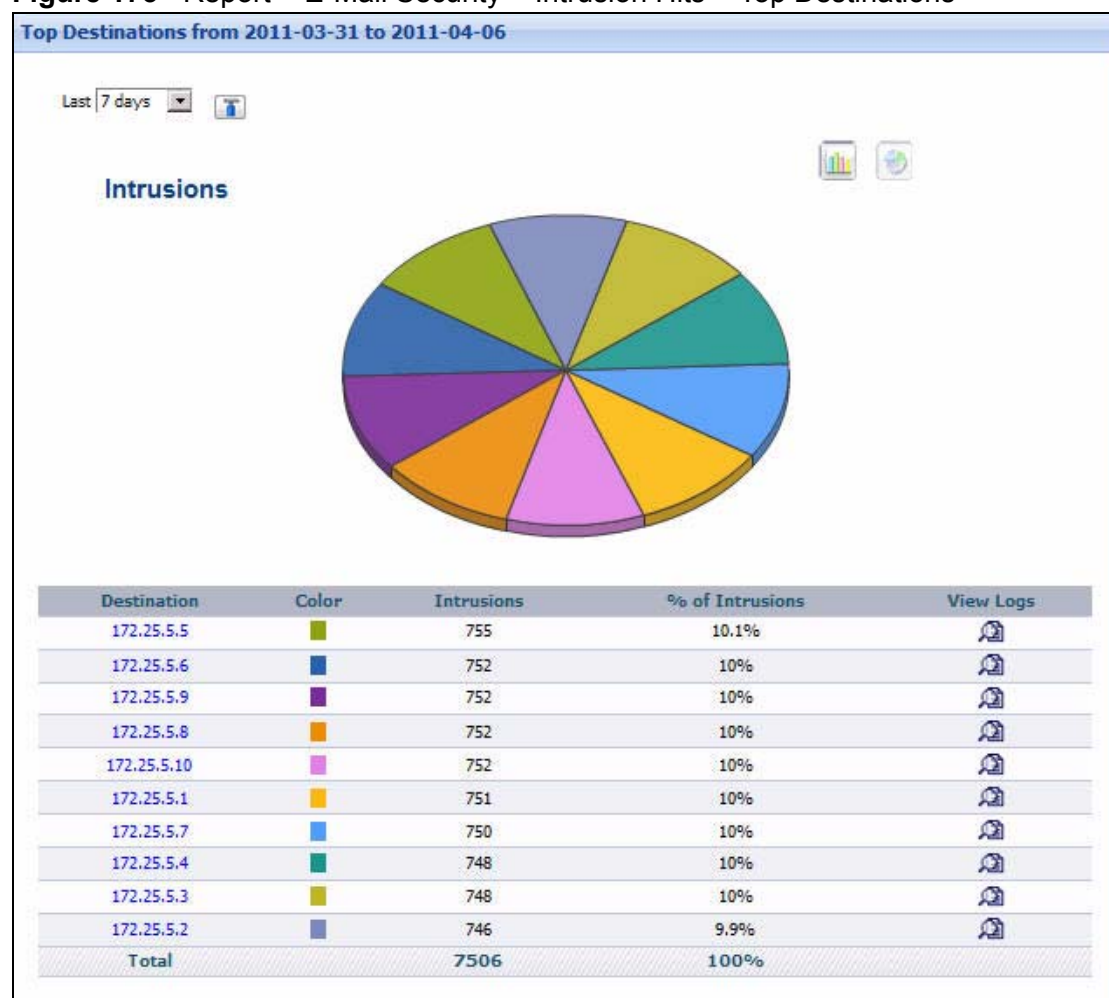
LABEL	DESCRIPTION
% of Intrusions	This field displays what percentage of all intrusions by the selected source was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.3.7 Top Intrusion Hits Destinations

Use this report to look at the top destinations of intrusions by number of intrusions.

Click **Report > E-Mail Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 173 Report > E-Mail Security > Intrusion Hits > Top Destinations



Each field is described in the following table.

Table 158 Report > E-Mail Security > Intrusion Hits > Top Destinations

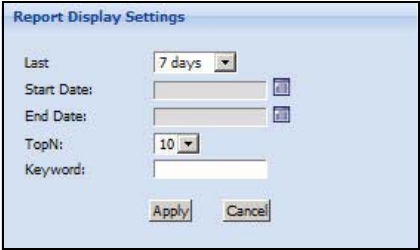
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 158 Report > E-Mail Security > Intrusion Hits > Top Destinations

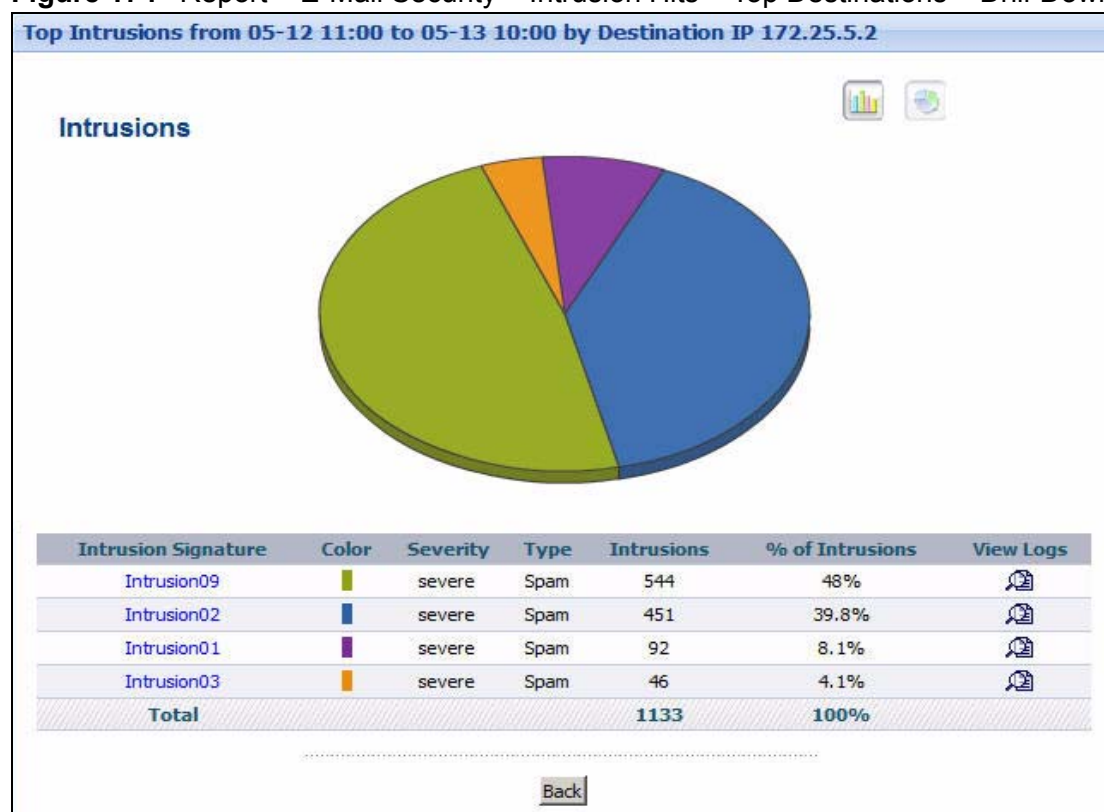
LABEL	DESCRIPTION
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top intrusion signatures for the selected destination.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

8.3.8 Top Intrusion Hits Destinations Drill-Down

Use this report to look at the top intrusion signatures for any top destination.

Click on a specific destination in **Report > E-Mail Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 174 Report > E-Mail Security > Intrusion Hits > Top Destinations > Drill-Down



Each field is described in the following table.

Table 159 Report > E-Mail Security > Intrusion Hits > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures sent to the selected destination, sorted by the number of intrusions at each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of each intrusion signature sent to the selected destination.

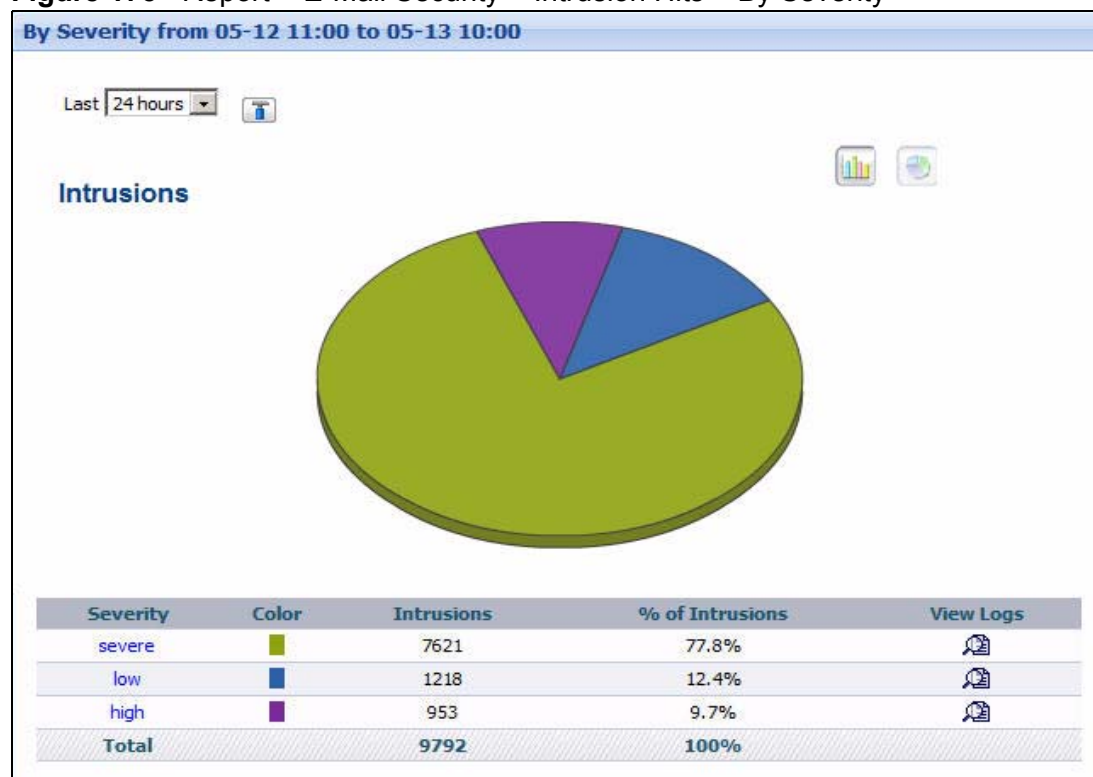
Table 159 Report > E-Mail Security > Intrusion Hits > Top Destinations > Drill-Down

LABEL	DESCRIPTION
% of Intrusions	This field displays what percentage of all intrusions sent to the selected destination belong to each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

8.3.9 Intrusion Hits Severities

Use this report to look at the severity (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug.

Click **Report > E-Mail Security > Intrusion Hits > By Severity** to open this screen.

Figure 175 Report > E-Mail Security > Intrusion Hits > By Severity

Each field is described in the following table.

Table 160 Report > E-Mail Security > Intrusion Hits > By Severity

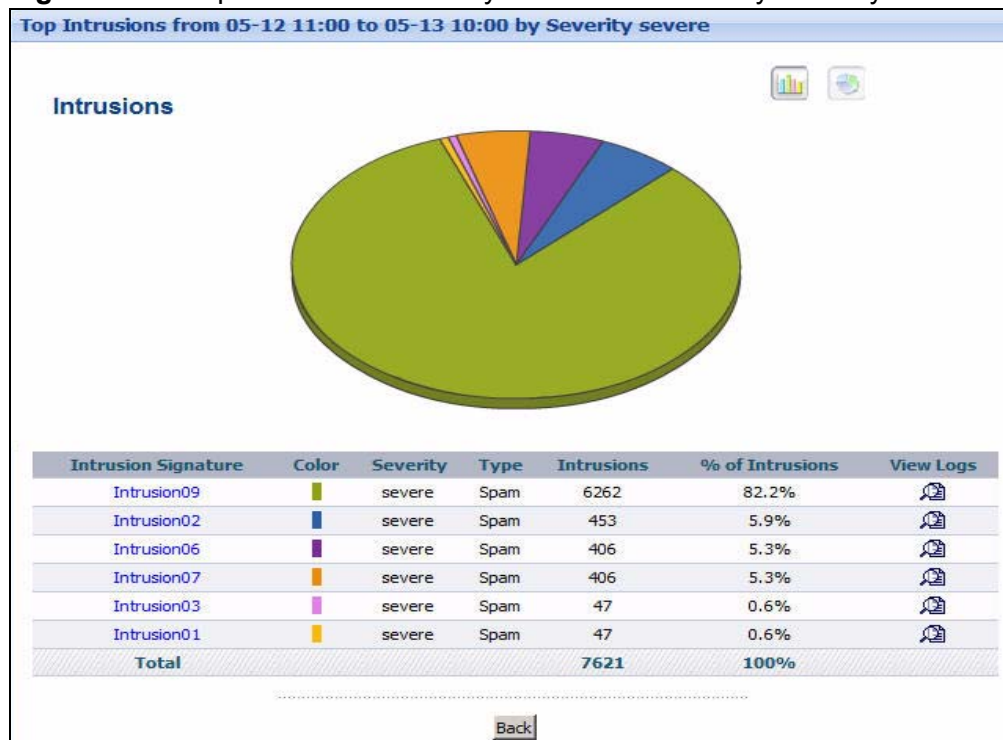
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

8.3.10 Intrusion Hits Severities Drill-Down

Use this report to look at the intrusion signatures for any severity.

Click on a specific severity in **Report > E-Mail Security > Intrusion Hits > By Severity** to open this screen.

Figure 176 Report > E-Mail Security > Intrusion Hits > By Severity > Drill-Down



Each field is described in the following table.

Table 161 Report > E-Mail Security > Intrusion Hits > By Severity > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the intrusion signatures of the selected severity, sorted by the number of intrusions by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.

Table 161 Report > E-Mail Security > Intrusion Hits > By Severity > Drill-Down

LABEL	DESCRIPTION
Intrusions	This field displays the number of intrusions of the selected severity using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions of the selected severity was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

Web Security

This chapter discusses how to use reports to look at Web related security threats that were detected by the ZyXEL device's firewall.

9.1 Security Threat

These reports look at the number of attempts to access Web security related blocked web sites by time interval as well as top blocked sites and hosts. Specifically, these reports include web sites detected by the ZYXEL device's content filter in the following categories: Phishing, Spyware/Malware Sources, Spyware Effects/Privacy Concerns and Proxy Avoidance.

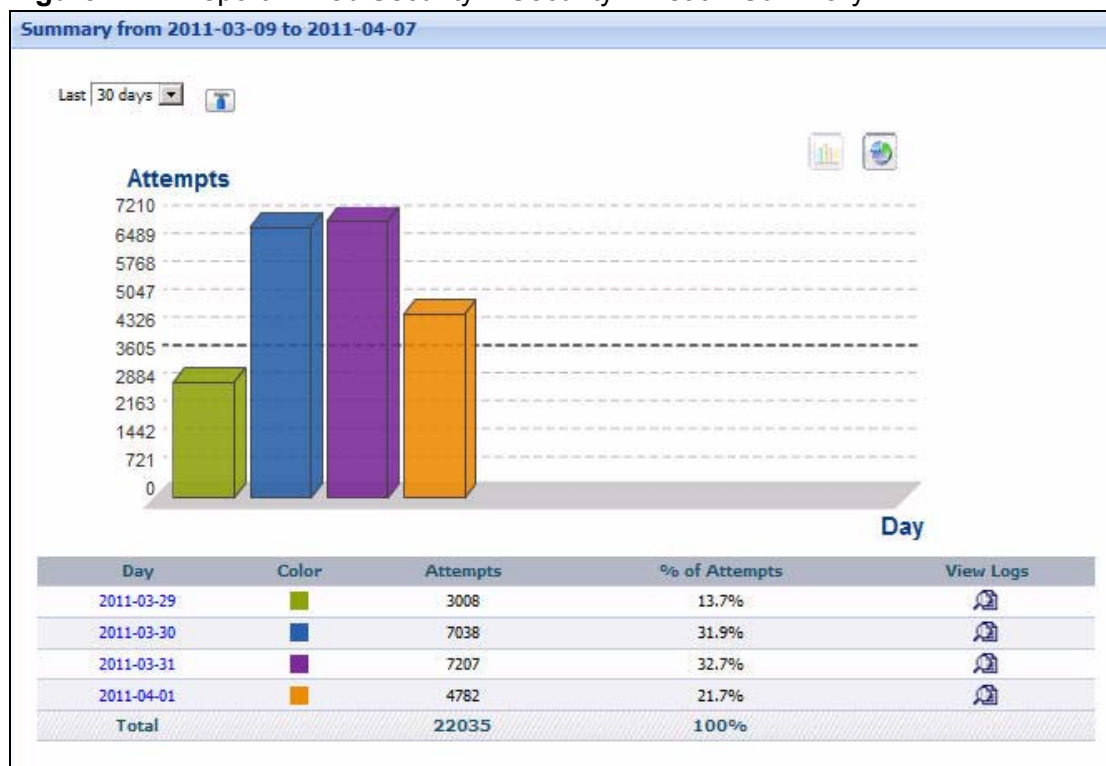
Note: To look at security policy reports, each ZyXEL device must record blocked web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

9.1.1 Security Threat Summary

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Web Security > Security Threat > Summary** to open this screen.

Figure 177 Report > Web Security > Security Threat > Summary

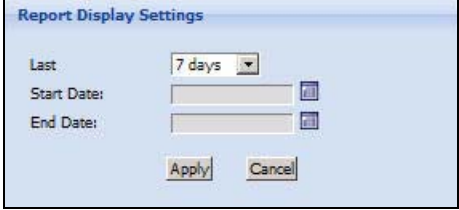


Each field is described in the following table.

Table 162 Report > Web Security > Security Threat > Summary

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 162 Report > Web Security > Security Threat > Summary

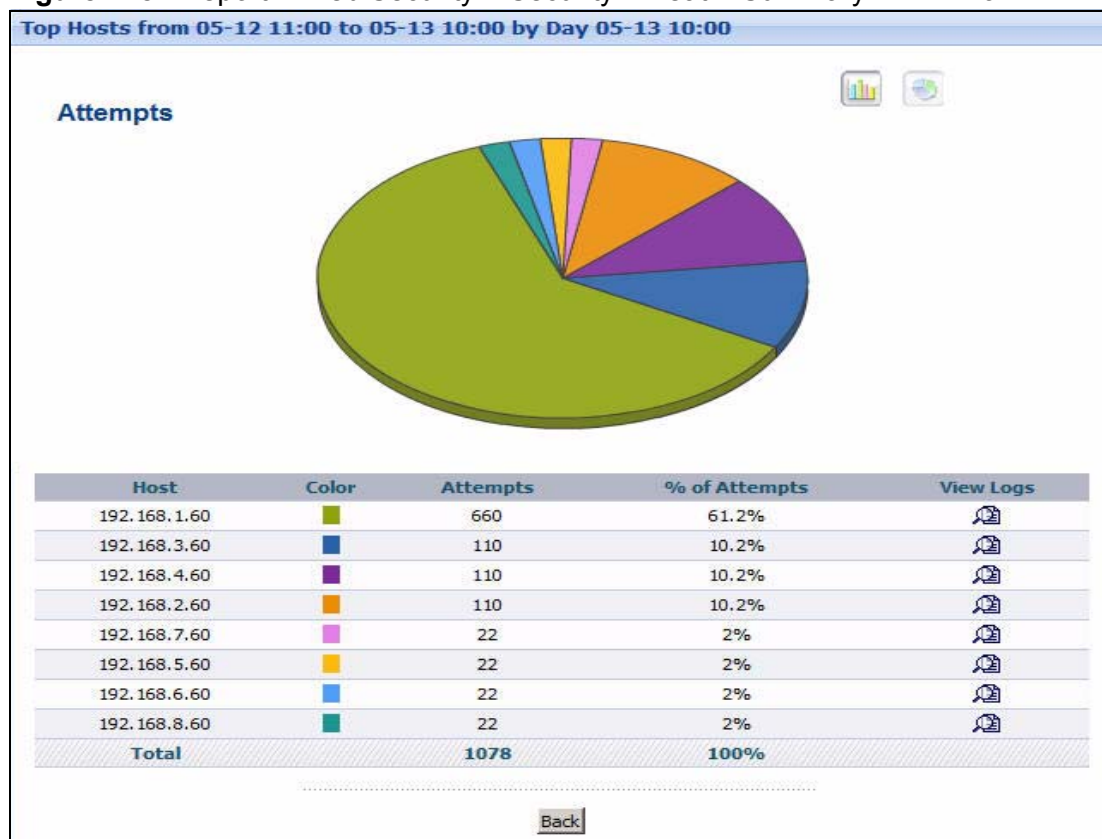
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts by each source to access blocked web sites in the selected time interval.
% of Attempts	This field displays what percentage of all blocked web access attempts was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

9.1.2 Security Threat Summary Drill-Down

Use this report to look at the top sources of attempts to access blocked web sites in a specific time interval.

Click on a specific time interval in **Report > Web Security > Security Threat > Summary** to open this screen.

Figure 178 Report > Web Security > Security Threat > Summary > Drill-Down



Each field is described in the following table.

Table 163 Report > Web Security > Security Threat > Summary > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of attempts to access blocked web sites in the selected time interval, sorted by the number of attempts by each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.

Table 163 Report > Web Security > Security Threat > Summary > Drill-Down

LABEL	DESCRIPTION
Attempts	This field displays the number of web access attempts the device blocked from each host.
% of Attempts	This field displays what percentage of all blocked web access attempts in the selected time interval was attributed to each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

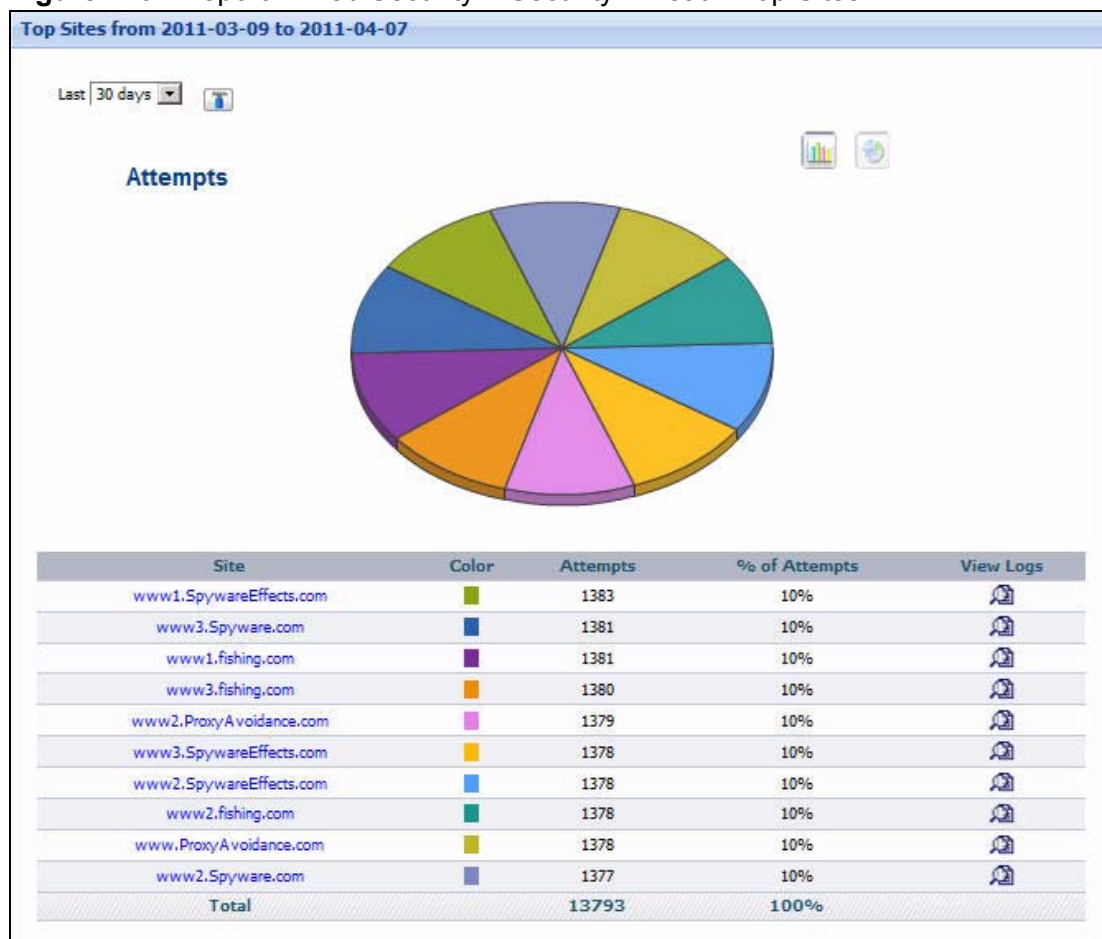
9.1.3 Security Threat Top Web Sites

Use this report to look at the top destinations of blocked web traffic.

Note: To look at security policy reports, each ZyXEL device must record blocked web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Web Security > Security Threat > Top Sites** to open this screen.

Figure 179 Report > Web Security > Security Threat > Top Sites

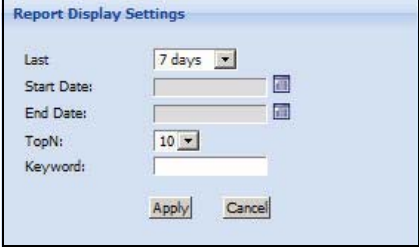


Each field is described in the following table.

Table 164 Report > Web Security > Security Threat > Top Sites

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 164 Report > Web Security > Security Threat > Top Sites

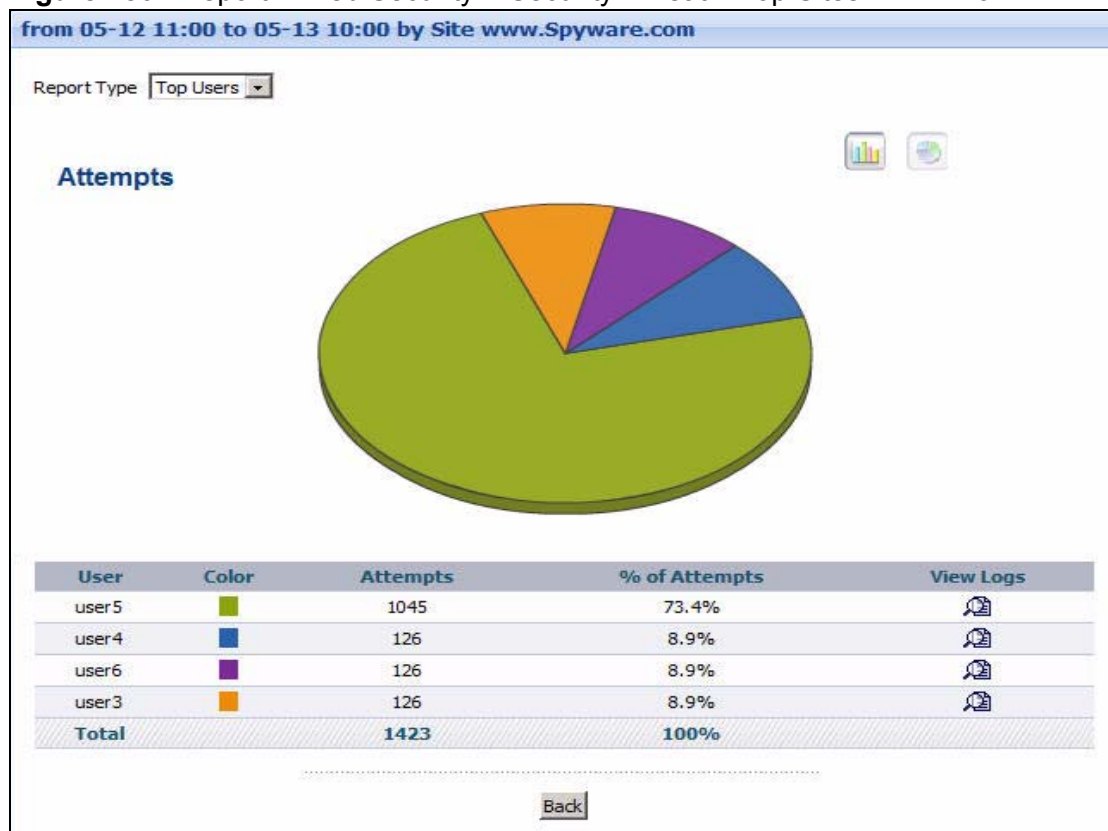
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of blocked web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays how much traffic (in megabytes) the device handled for each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

9.1.4 Security Threat Top Sites Drill-Down

Use this report to look at the top sources for any top destination of blocked web traffic.

Click on a specific destination in **Report > Web Security > Security Threat > Top Sites** to open this screen.

Figure 180 Report > Web Security > Security Threat > Top Sites > Drill-Down



Each field is described in the following table.

Table 165 Report > Web Security > Security Threat > Top Sites > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Users , Top Hosts or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 165 Report > Web Security > Security Threat > Top Sites > Drill-Down

LABEL	DESCRIPTION
Host	This field displays the top sources of blocked web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration , the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by each source to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

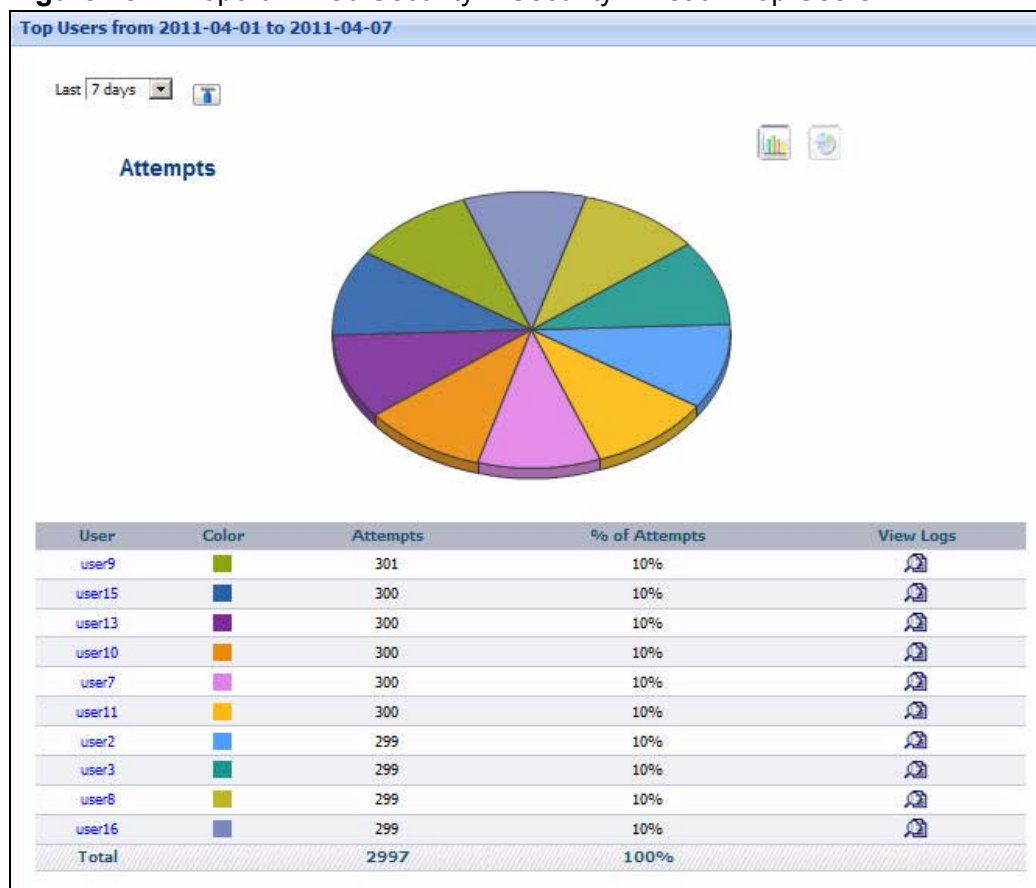
9.1.5 Security Threat Top Users

Use this report to look at the users for which the device blocked the most web site access attempts.

Note: To look at security policy Web blocked reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Web Security > Security Threat > Top Users** to open this screen.

Figure 181 Report > Web Security > Security Threat > Top Users

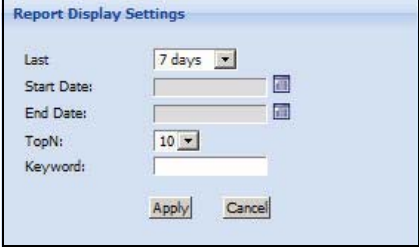


Each field is described in the following table.

Table 166 Report > Web Security > Security Threat > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 166 Report > Web Security > Security Threat > Top Users

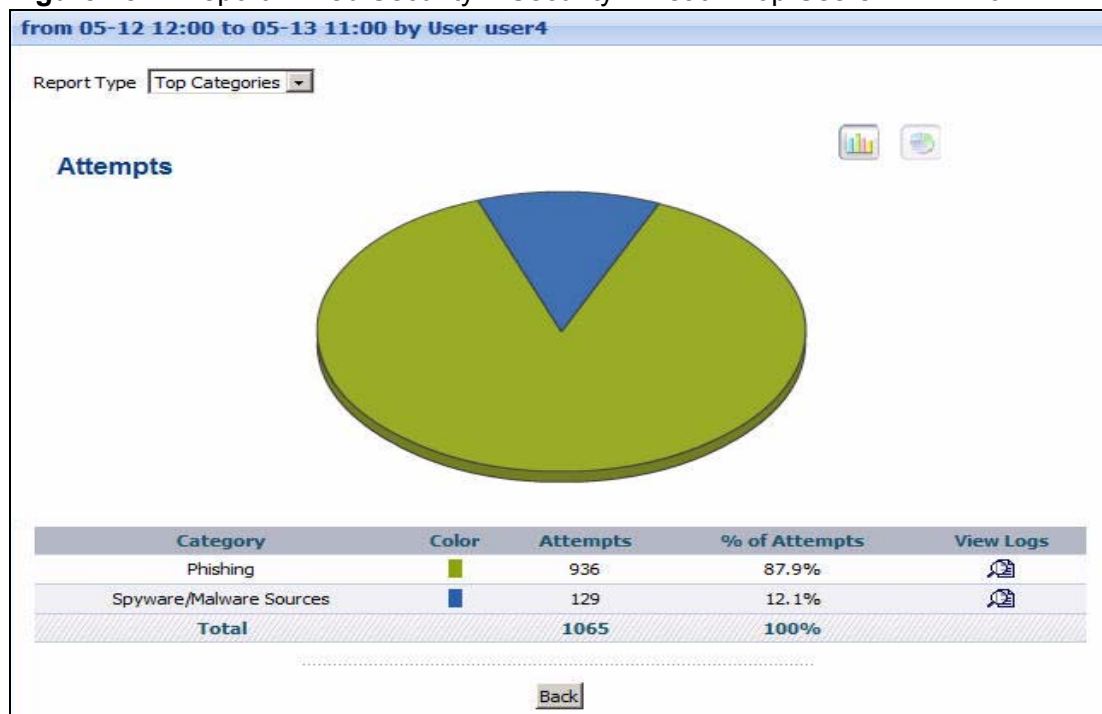
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users for which the device blocked the most web site access attempts, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each user.
% of Attempts	This field displays what percentage the user had of all blocked attempts to access web sites.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.1.6 Security Threat Top Users Drill-Down

Use this report to look at the top destinations for any user for which the device blocked the most web site access attempts.

Click on a specific source in **Report > Web Security > Security Threat > Top Users** to open this screen.

Figure 182 Report > Web Security > Security Threat > Top Users > Drill-Down



Each field is described in the following table.

Table 167 Report > Web Security > Security Threat > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Categories , Top Sites or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 167 Report > Web Security > Security Threat > Top Users > Drill-Down

LABEL	DESCRIPTION
Site	This field displays the top destinations of blocked web traffic from the selected user, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

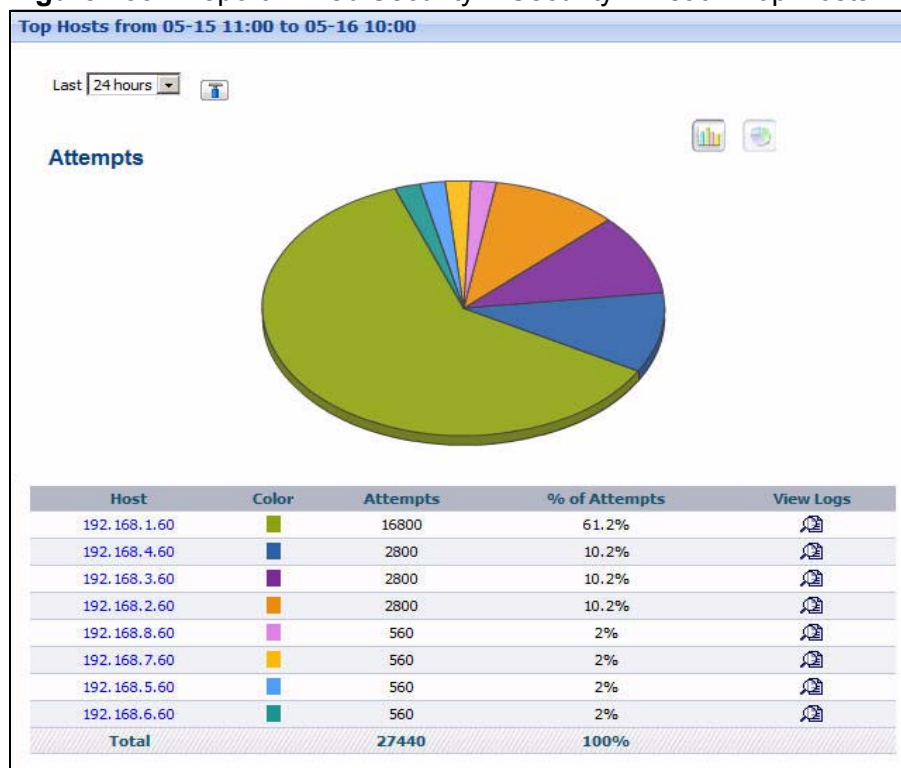
9.1.7 Security Threat Top Hosts

Use this report to look at the top sources of blocked web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Web Security > Security Threat > Top Hosts** to open this screen.

Figure 183 Report > Web Security > Security Threat > Top Hosts

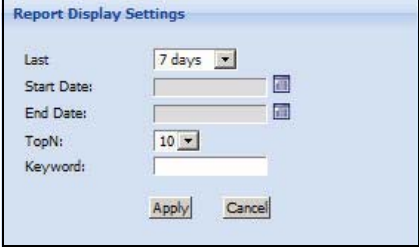


Each field is described in the following table.

Table 168 Report > Web Security > Security Threat > Top Hosts

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 168 Report > Web Security > Security Threat > Top Hosts

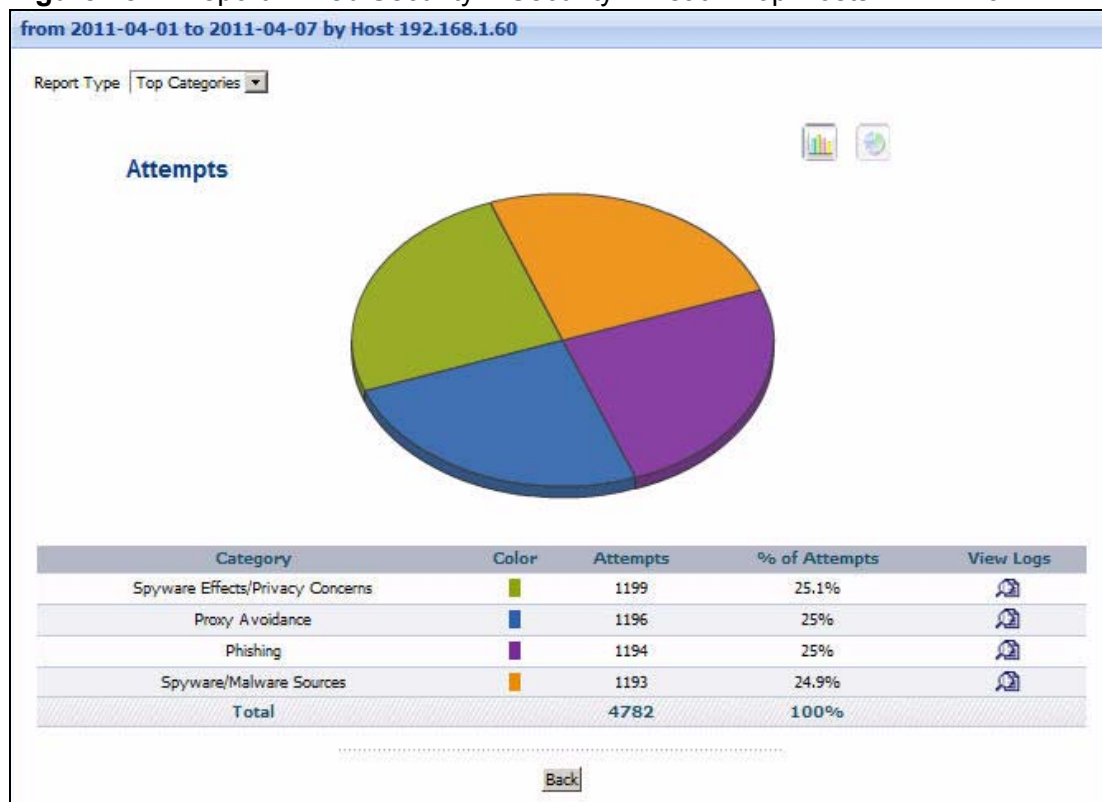
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of web site access attempts the device blocked from each source.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.1.8 Security Threat Top Hosts Drill-Down

Use this report to look at the top destinations for any top source of blocked web traffic.

Click on a specific source in **Report > Web Security > Security Threat > Top Hosts** to open this screen.

Figure 184 Report > Web Security > Security Threat > Top Hosts > Drill-Down



Each field is described in the following table.

Table 169 Report > Web Security > Security Threat > Top Hosts > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Categories , Top Sites or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 169 Report > Web Security > Security Threat > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Site	This field displays the top destinations of blocked web traffic from the selected source, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

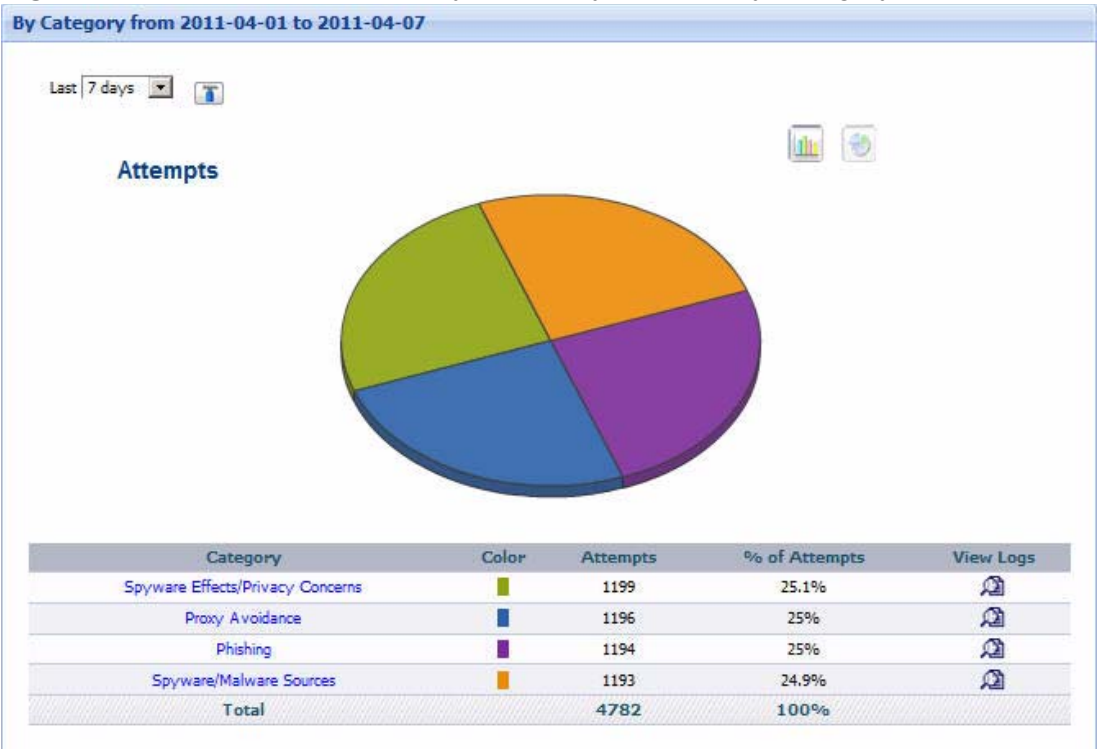
9.1.9 Security Threat Categories

Use this report to look at the categories of blocked web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Web Security > Security Threat > By Category** to open this screen.

Figure 185 Report > Web Security > Security Threat > By Category

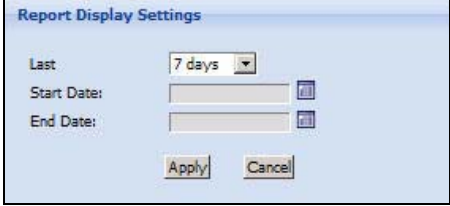


Each field is described in the following table.

Table 170 Report > Web Security > Security Threat > By Category

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 170 Report > Web Security > Security Threat > By Category

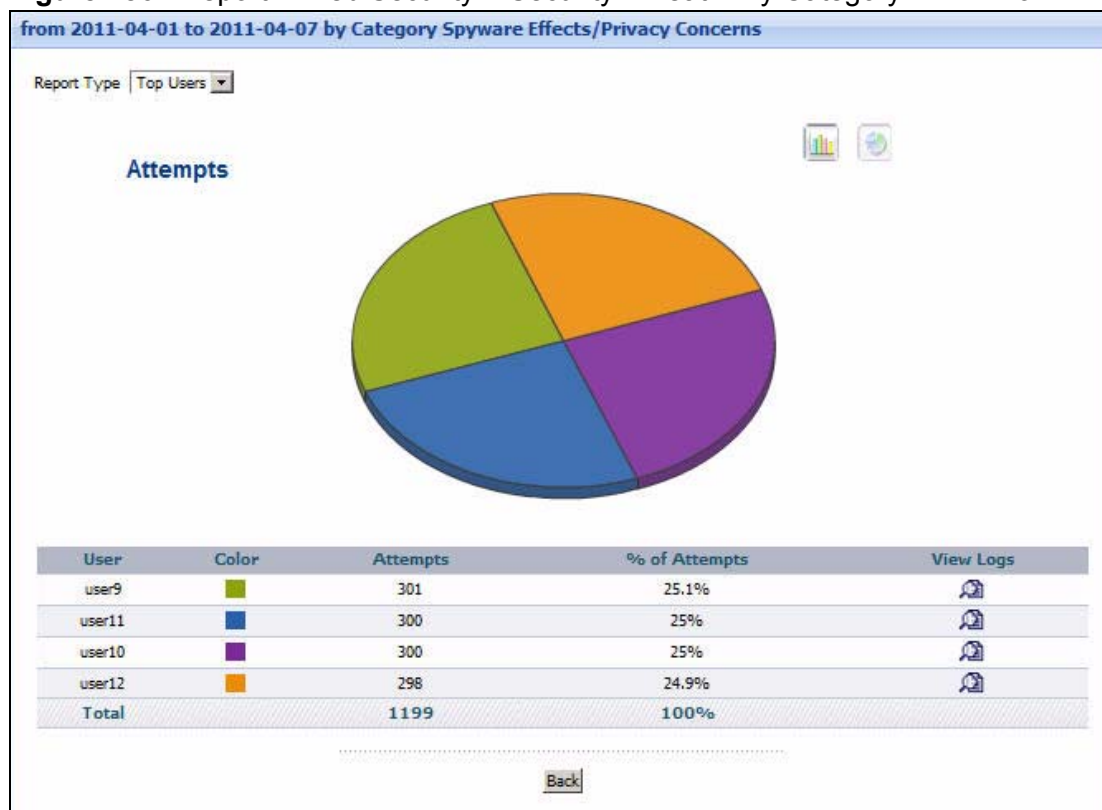
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access allowed web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

9.1.10 Security Threat Categories Drill-Down

Use this report to look at the destinations for any category of blocked web traffic.

Click on a specific category in **Report > Web Security > Security Threat > By Category** to open this screen.

Figure 186 Report > Web Security > Security Threat > By Category > Drill-Down



Each field is described in the following table.

Table 171 Report > Web Security > Security Threat > By Category > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Users , Top Sites , Top Hosts or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the destinations of blocked web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.

Table 171 Report > Web Security > Security Threat > By Category > Drill-Down

LABEL	DESCRIPTION
Attempts	This field displays the number of attempts to each destination in the selected category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites in the selected category went to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.
Back	Click this to return to the main report.

9.2 Virus Found

These reports look at Web security related viruses that were detected by the ZyXEL device's anti-virus feature. Specifically, these reports will include viruses received through the HTTP protocol.

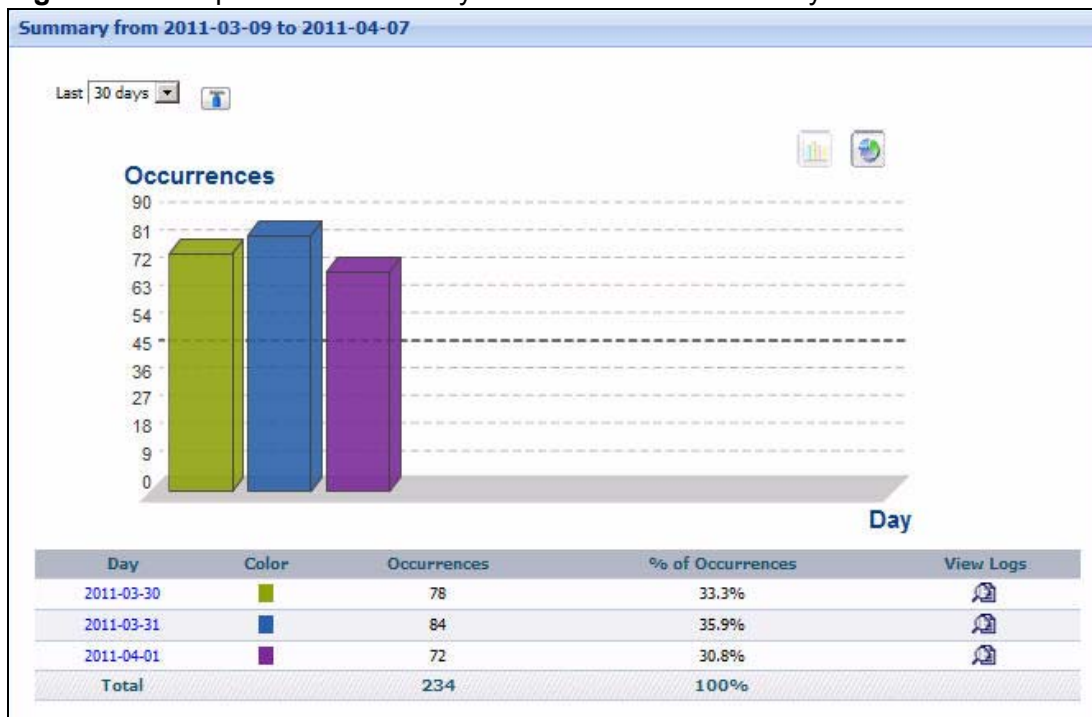
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus > General**. ZyXEL devices can log viruses based on the **Service** the virus was using. Make sure the ZyXEL device logs viruses you want to include in Vantage Report.

9.2.1 Virus Found Summary

Use this report to look at the number of virus occurrences by time interval.

Click **Report > Web Security > Virus Found > Summary** to open this screen.

Figure 187 Report > Web Security > Virus Found > Summary



Each field is described in the following table.

Table 172 Report > Web Security > Virus Found > Summary

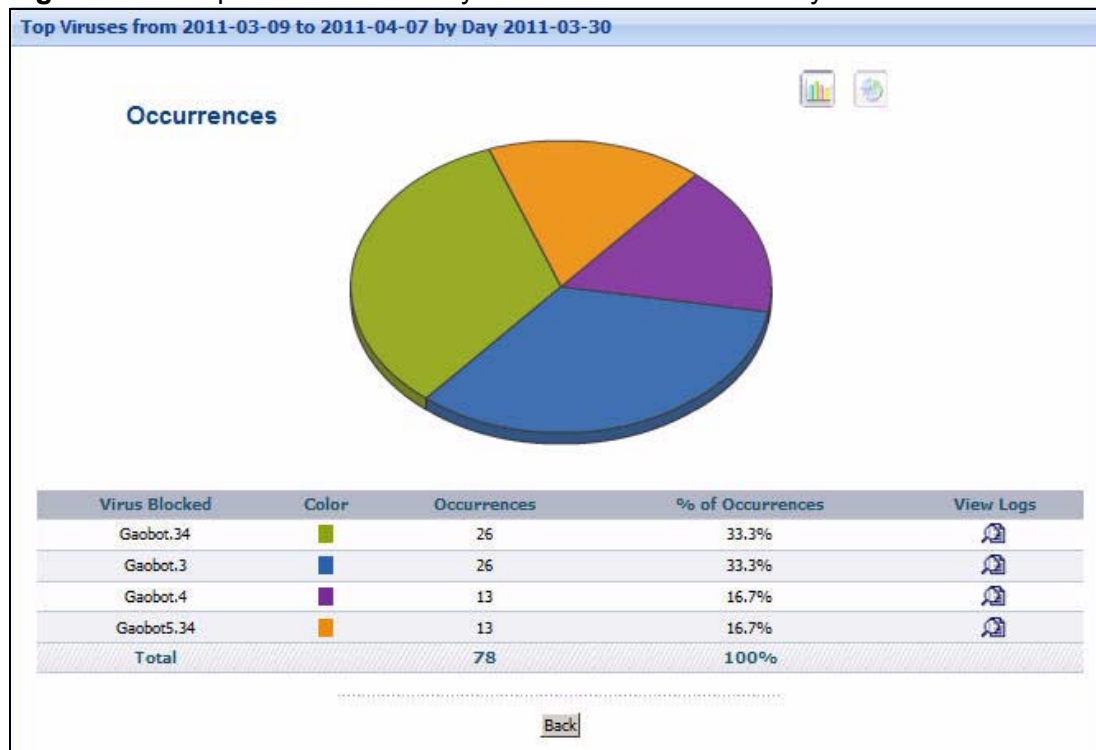
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

9.2.2 Virus Found Summary Drill-Down

Use this report to look at the viruses in a specific time interval.

Click on a specific time interval in **Report > Web Security > Virus Found > Summary** to open this screen.

Figure 188 Report > Web Security > Virus Found > Summary > Drill-Down



Each field is described in the following table.

Table 173 Report > Web Security > Virus Found > Summary > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the viruses stopped in the selected time interval, sorted by the number of occurrences of each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences in the selected time interval was made by each virus.

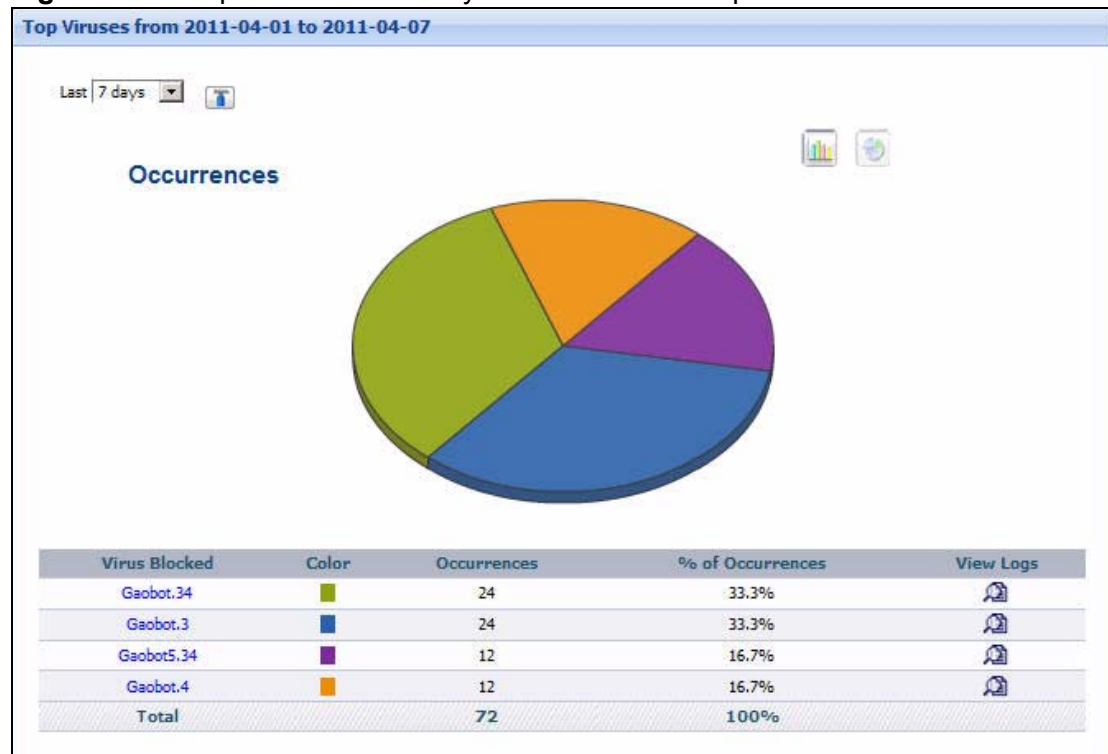
Table 173 Report > Web Security > Virus Found > Summary > Drill-Down

LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.2.3 Top Viruses

Use this report to look at the top viruses by number of occurrences.

Click **Report > Web Security > Virus Found > Top Viruses** to open this screen.

Figure 189 Report > Web Security > Virus Found > Top Viruses

Each field is described in the following table.

Table 174 Report > Web Security > Virus Found > Top Viruses

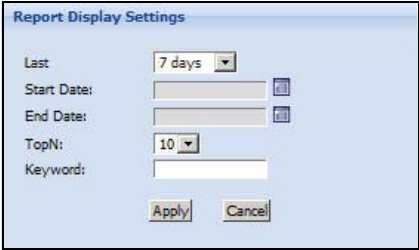
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Virus Blocked field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.

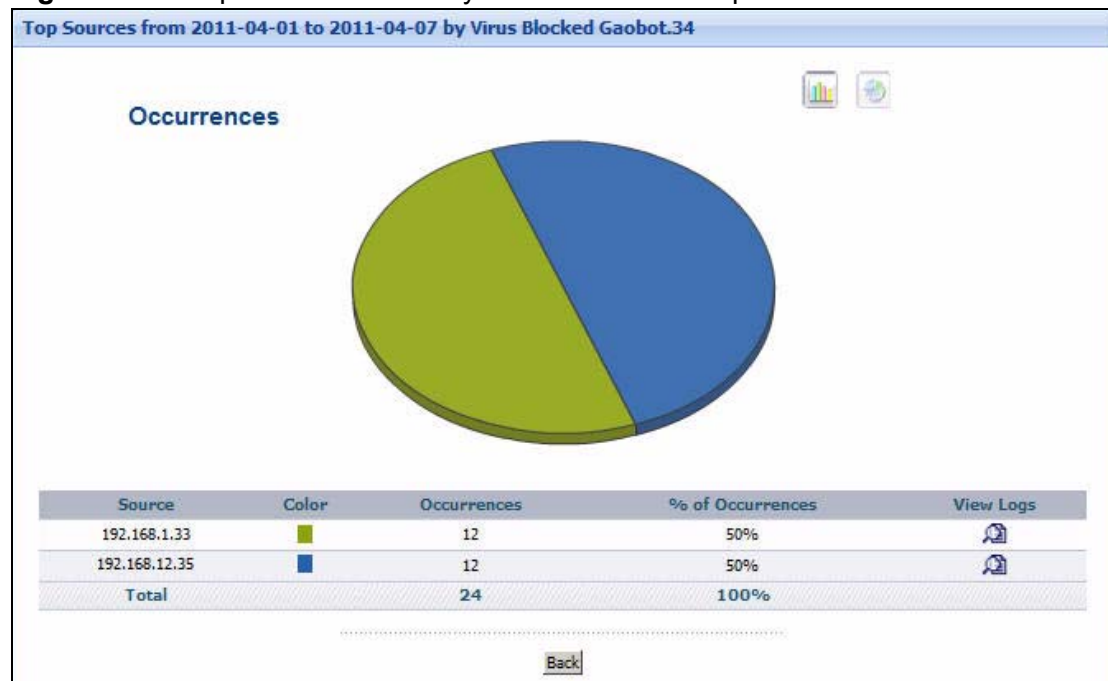
Table 174 Report > Web Security > Virus Found > Top Viruses

LABEL	DESCRIPTION
% of Occurrences	This field displays what percentage each virus's occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

9.2.4 Top Viruses Drill-Down

Use this report to look at the top sources of any top virus.

Click on a specific virus in **Report > Web Security > Virus Found > Top Viruses** to open this screen.

Figure 190 Report > Web Security > Virus Found > Top Viruses > Drill-Down

Each field is described in the following table.

Table 175 Report > Web Security > Virus Found > Top Viruses > Drill-Down

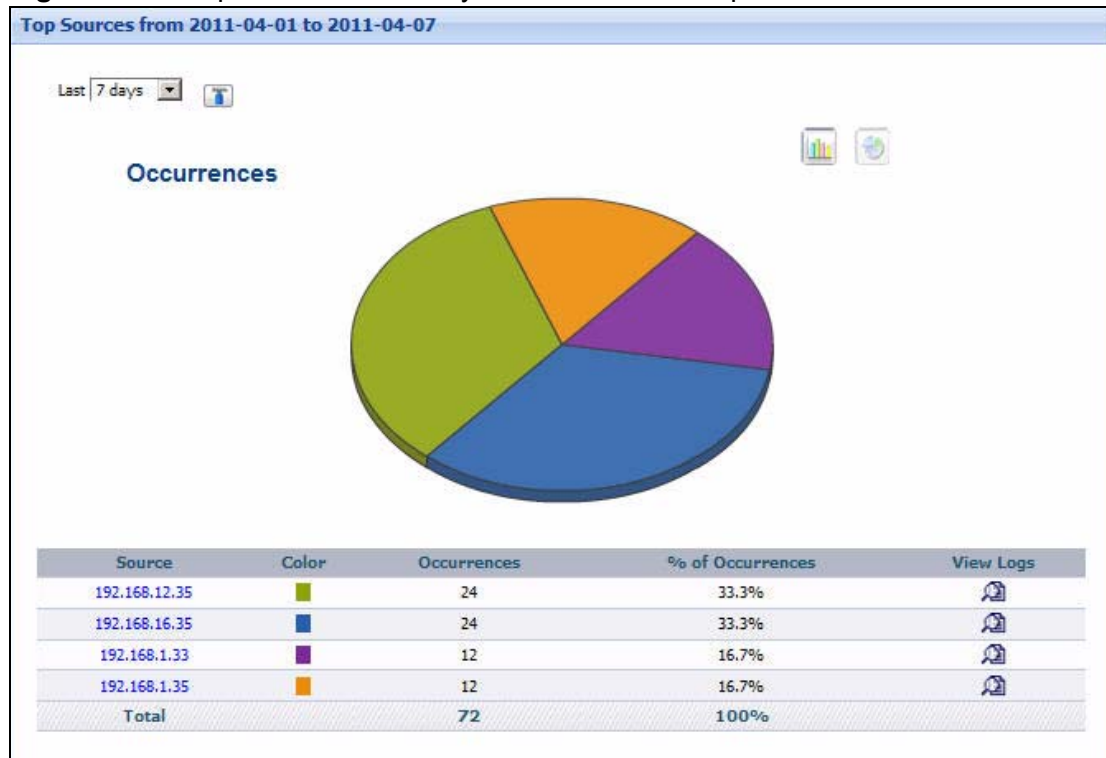
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected virus, sorted by the number of occurrences by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences of the selected virus from each source.
% of Occurrences	This field displays what percentage of all occurrences of the selected virus comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected virus of the selected virus is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.2.5 Top Virus Sources

Use this report to look at the top sources of virus occurrences by number of occurrences.

Click **Report > Web Security > Virus Found > Top Sources** to open this screen.

Figure 191 Report > Web Security > Virus Found > Top Sources



Each field is described in the following table.

Table 176 Report > Web Security > Virus Found > Top Sources

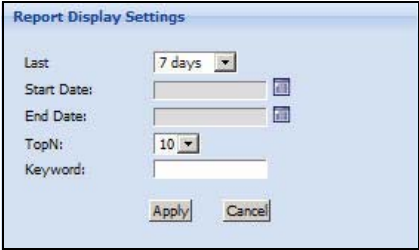
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

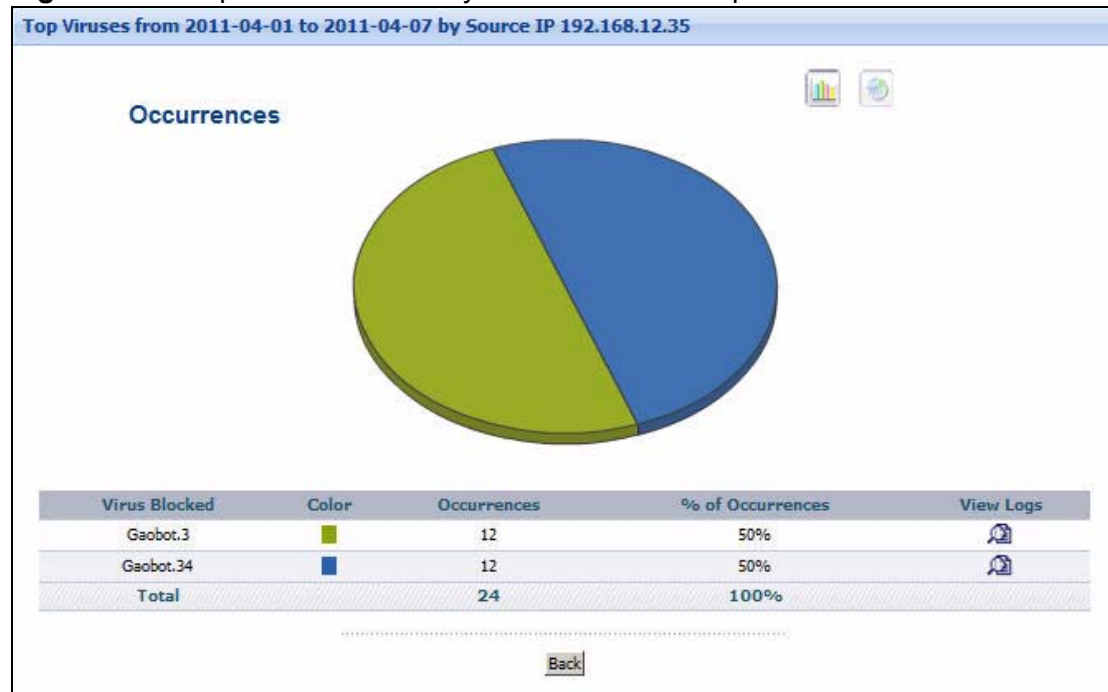
Table 176 Report > Web Security > Virus Found > Top Sources

LABEL	DESCRIPTION
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top viruses for the selected source.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.2.6 Top Virus Sources Drill-Down

Use this report to look at the top viruses for any top source.

Click on a specific source in **Report > Web Security > Virus Found > Top Sources** to open this screen.

Figure 192 Report > Web Security > Virus Found > Top Sources > Drill-Down

Each field is described in the following table.

Table 177 Report > Web Security > Virus Found > Top Sources > Drill-Down

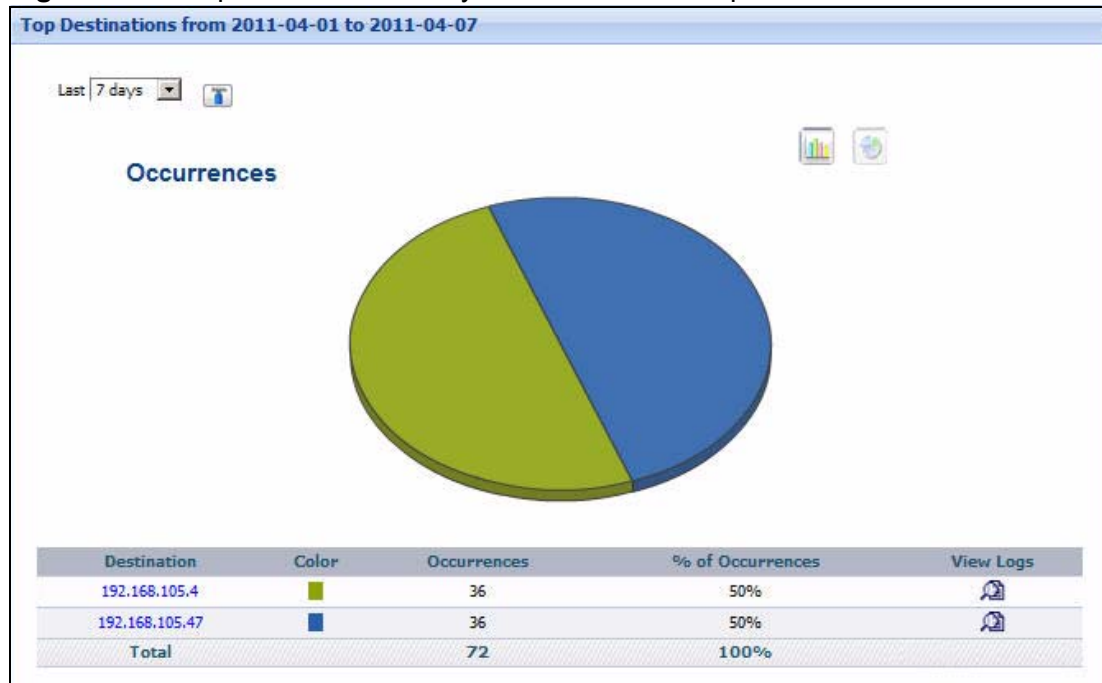
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from the selected source, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences from the selected source by each virus.
% of Occurrences	This field displays what percentage of all occurrences from the selected source was made by each virus.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.2.7 Top Virus Destinations

Use this report to look at the top destinations of virus occurrences by number of occurrences.

Click **Report > Web Security > Virus Found > Top Destinations** to open this screen.

Figure 193 Report > Web Security > Virus Found > Top Destinations



Each field is described in the following table.

Table 178 Report > Web Security > Virus Found > Top Destinations

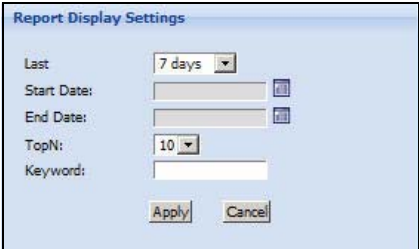
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.

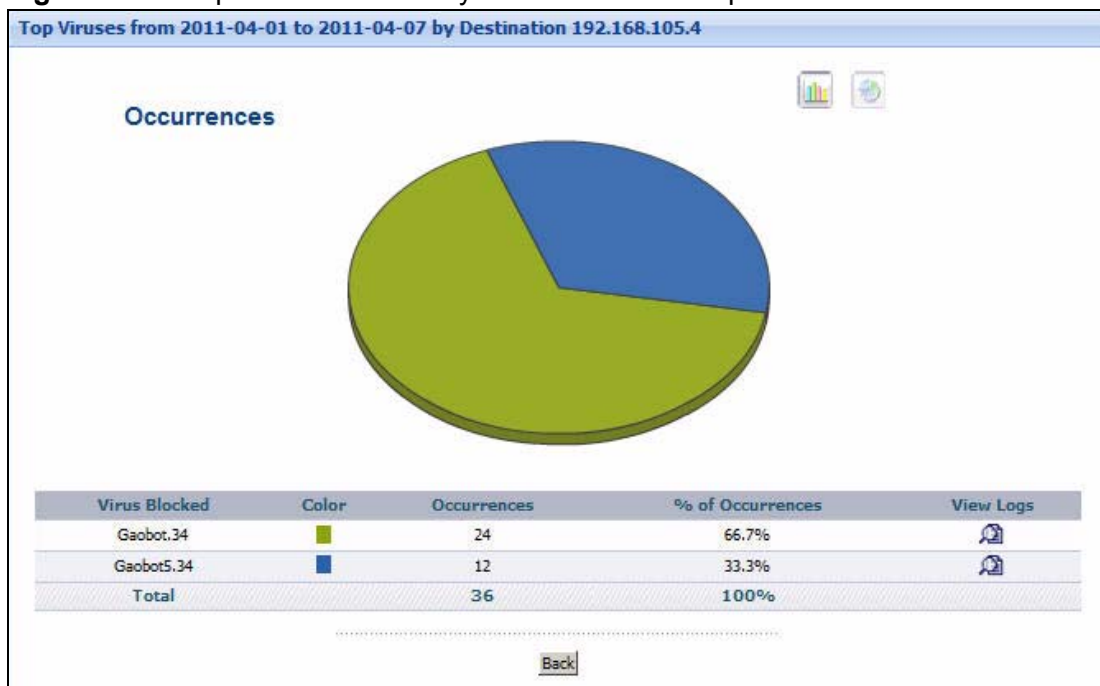
Table 178 Report > Web Security > Virus Found > Top Destinations

LABEL	DESCRIPTION
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

9.2.8 Top Virus Destinations Drill-Down

Use this report to look at the top viruses for any top destination.

Click on a specific destination in **Report > Web Security > Virus Found > Top Destinations** to open this screen.

Figure 194 Report > Web Security > Virus Found > Top Destinations > Drill-Down

Each field is described in the following table.

Table 179 Report > Web Security > Virus Found > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from going to the selected destination, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of times each virus was sent to the selected destination.
% of Occurrences	This field displays what percentage each virus made of the viruses sent to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.3 Intrusion Hits

These reports look at Web security related intrusion signatures, types of intrusions, severity of intrusions, and the top sources and destinations of intrusions that are logged on the selected ZyXEL device. **Intrusions** are caused by malicious or suspicious packets sent with the intent of causing harm, illegally accessing resources or interrupting service. They are detected by the selected device's IDP feature. Specifically, these reports include intrusions in the Web Attack IDP category on the ZyXEL device.

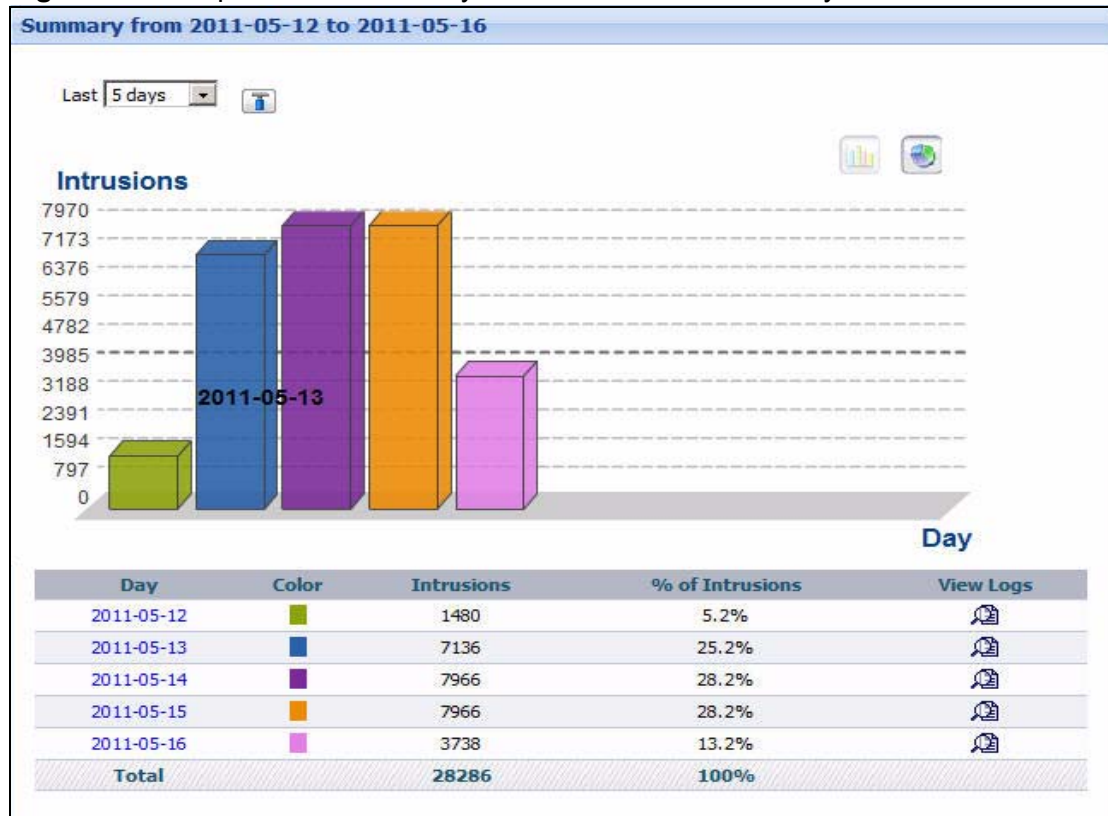
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP > Signature**, and make sure the ZyXEL device logs each **Attack Type** you want to see in Vantage Report.

9.3.1 Intrusion Hits Summary

Use this report to look at the number of intrusions by time interval.

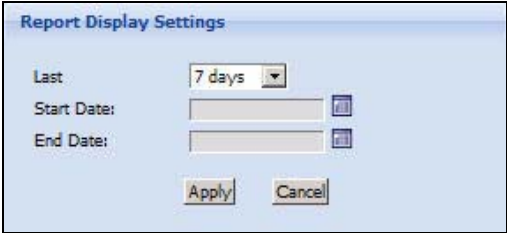
Click **Report > Web Security > Intrusion Hits > Summary** to open this screen.

Figure 195 Report > Web Security > Intrusion Hits > Summary



Each field is described in the following table.

Table 180 Report > Web Security > Intrusion Hits > Summary

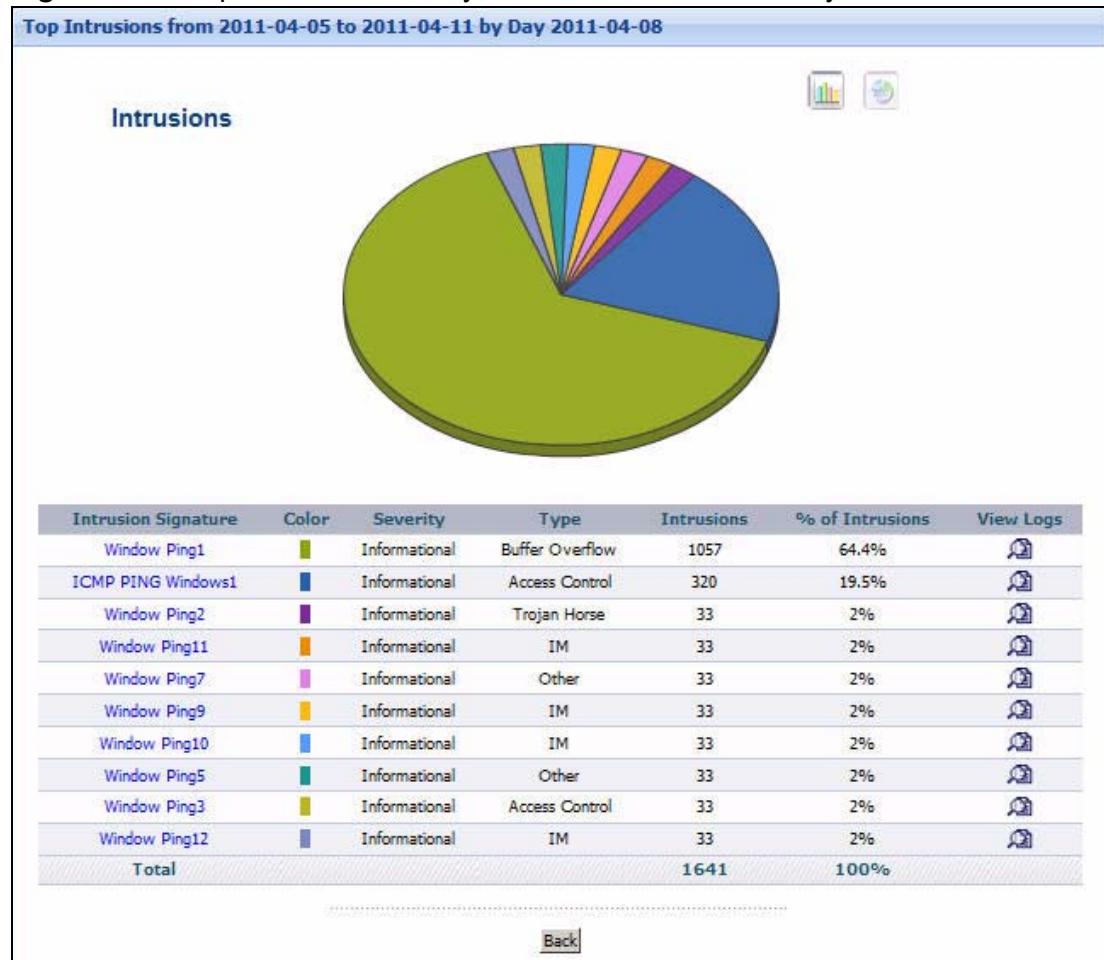
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the intrusion signatures in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Intrusions	This field displays the number of intrusions in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

9.3.2 Intrusion Hits Summary Drill-Down

Use this report to look at the intrusion signatures in a specific time interval.

Click on a specific time interval in **Report > Web Security > Intrusion Hits > Summary** to open this screen.

Figure 196 Report > Web Security > Intrusion Hits > Summary > Drill-Down



Each field is described in the following table.

Table 181 Report > Web Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 197 on page 423).
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

Note: Clicking on some linked entries in the Intrusion screen will open a new window that provides details on the security issue encountered by the devices. The following screen is displayed.

Figure 197 Security Issue Details

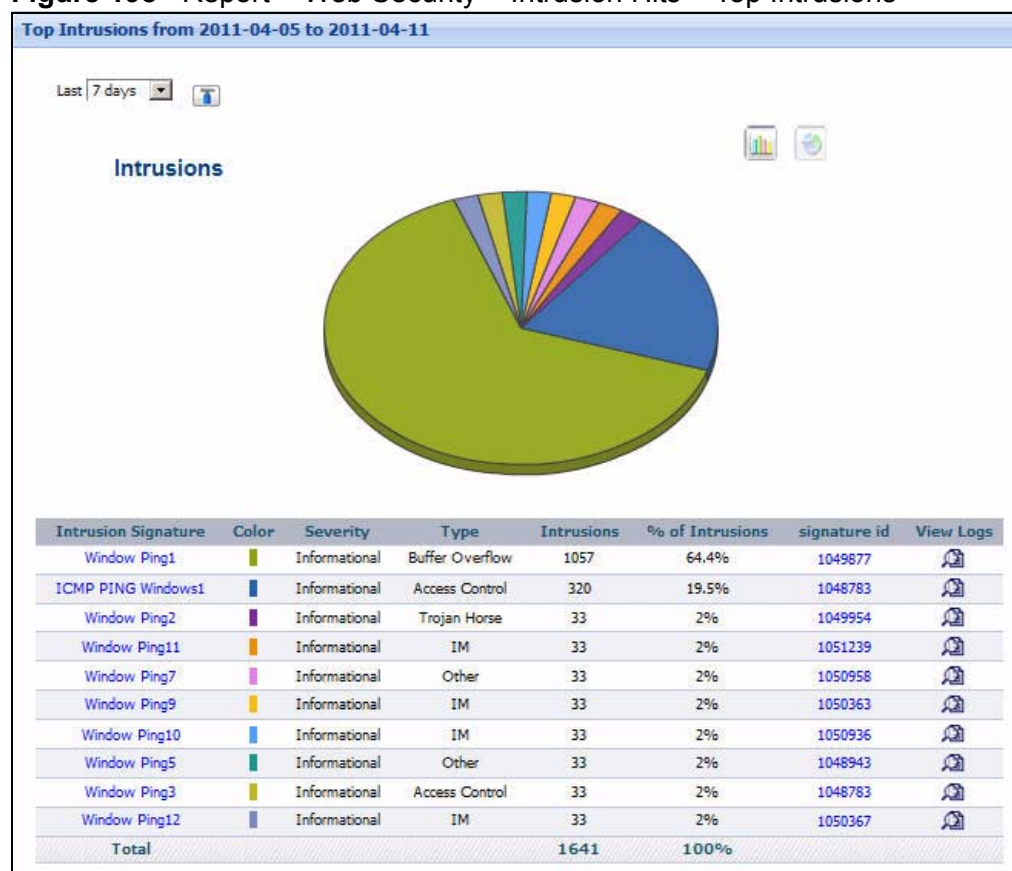


9.3.3 Top Intrusion Hits Signatures

Use this report to look at the top intrusion signatures by number of intrusions.

Click **Report > Web Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 198 Report > Web Security > Intrusion Hits > Top Intrusions



Each field is described in the following table.

Table 182 Report > Web Security > Intrusion Hits > Top Intrusions

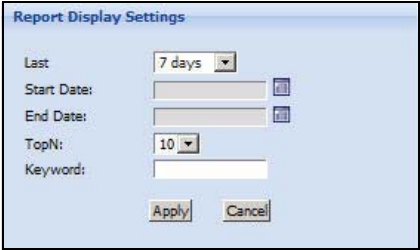
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Intrusion Signature field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature.
Color	This field displays what color represents each intrusion signature in the graph.

Table 182 Report > Web Security > Intrusion Hits > Top Intrusions

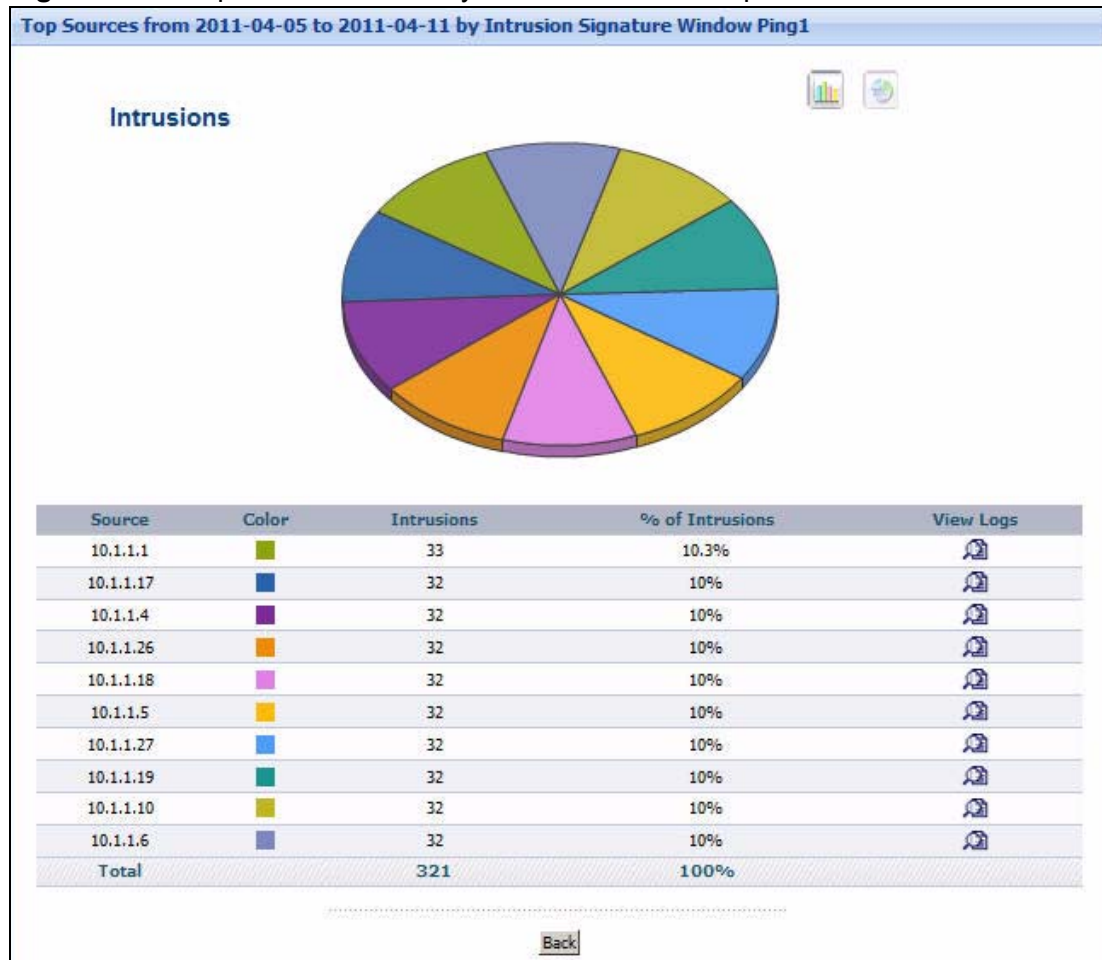
LABEL	DESCRIPTION
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
signature id	This is the security issue identification number. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 197 on page 423).
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

9.3.4 Top Intrusion Hits Signatures Drill-Down

Use this report to look at the top sources of intrusions for any top signature.

Click on a specific intrusion signature in **Report > Web Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 199 Report > Web Security > Intrusion Hits > Top Intrusions > Drill-Down



Each field is described in the following table.

Table 183 Report > Web Security > Intrusion Hits > Top Intrusions > Drill-Down

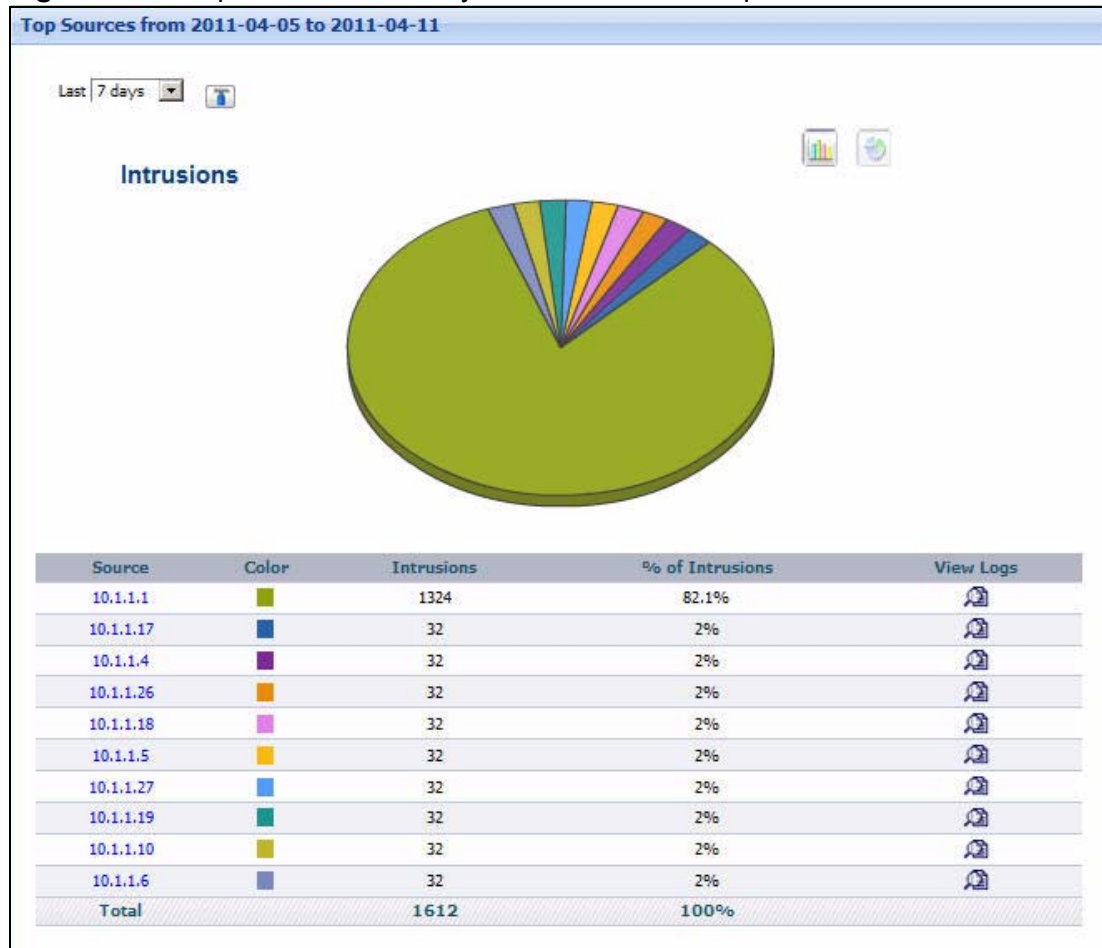
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected intrusion signature, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions using the selected intrusion signature was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected intrusion signature is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.3.5 Top Intrusion Hits Sources

Use this report to look at the top sources of intrusions by number of intrusions.

Click **Report > Web Security > Intrusion Hits > Top Sources** to open this screen.

Figure 200 Report > Web Security > Intrusion Hits > Top Sources



Each field is described in the following table.

Table 184 Report > Web Security > Intrusion Hits > Top Sources

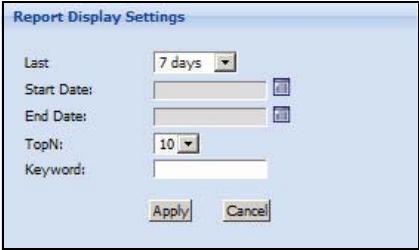
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Source field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 184 Report > Web Security > Intrusion Hits > Top Sources

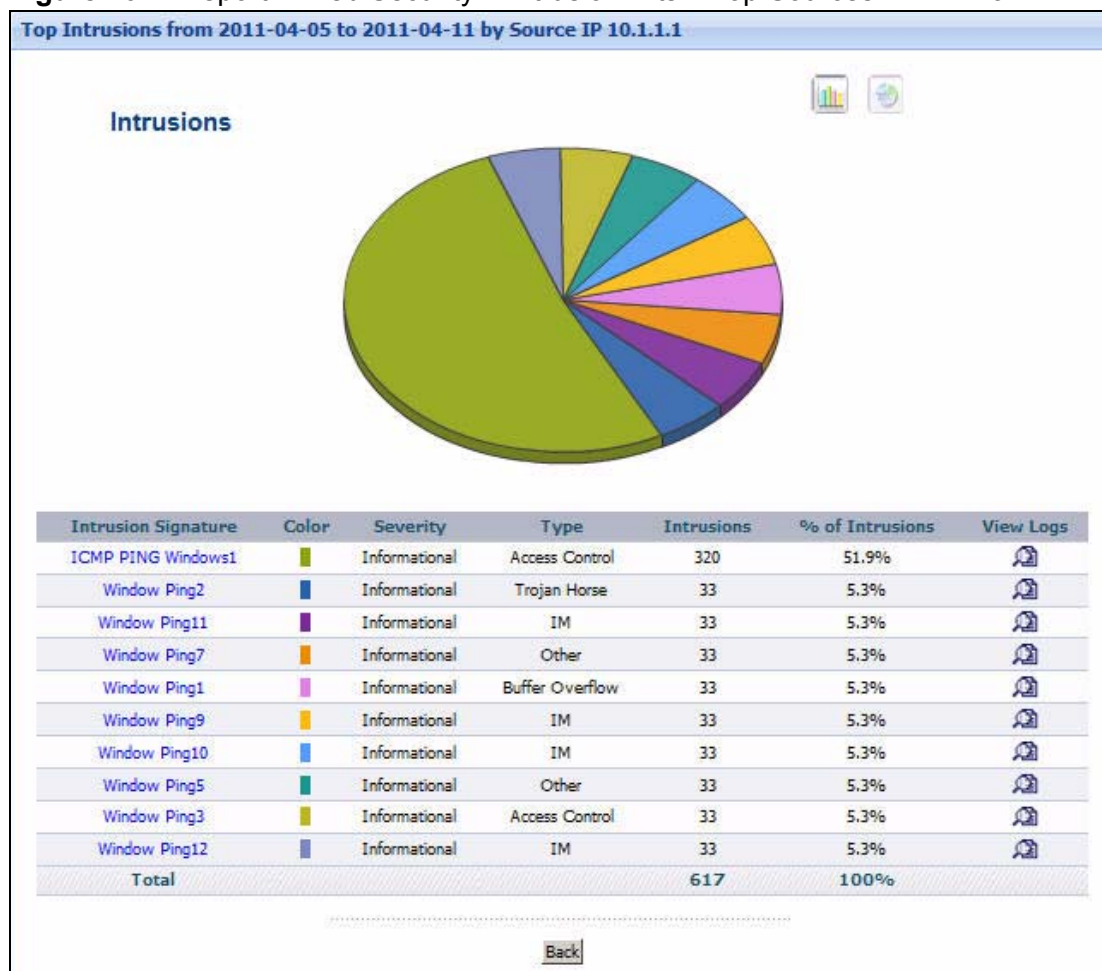
LABEL	DESCRIPTION
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top intrusion signatures for the selected source.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.3.6 Top Intrusion Hits Sources Drill-Down

Use this report to look at the top intrusion signatures for any top source.

Click on a specific source in **Report > Web Security > Intrusion Hits > Top Sources** to open this screen.

Figure 201 Report > Web Security > Intrusion Hits > Top Sources > Drill-Down



Each field is described in the following table.

Table 185 Report > Web Security > Intrusion Hits > Top Sources > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures from the selected source, sorted by the number of intrusions by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.

Table 185 Report > Web Security > Intrusion Hits > Top Sources > Drill-Down

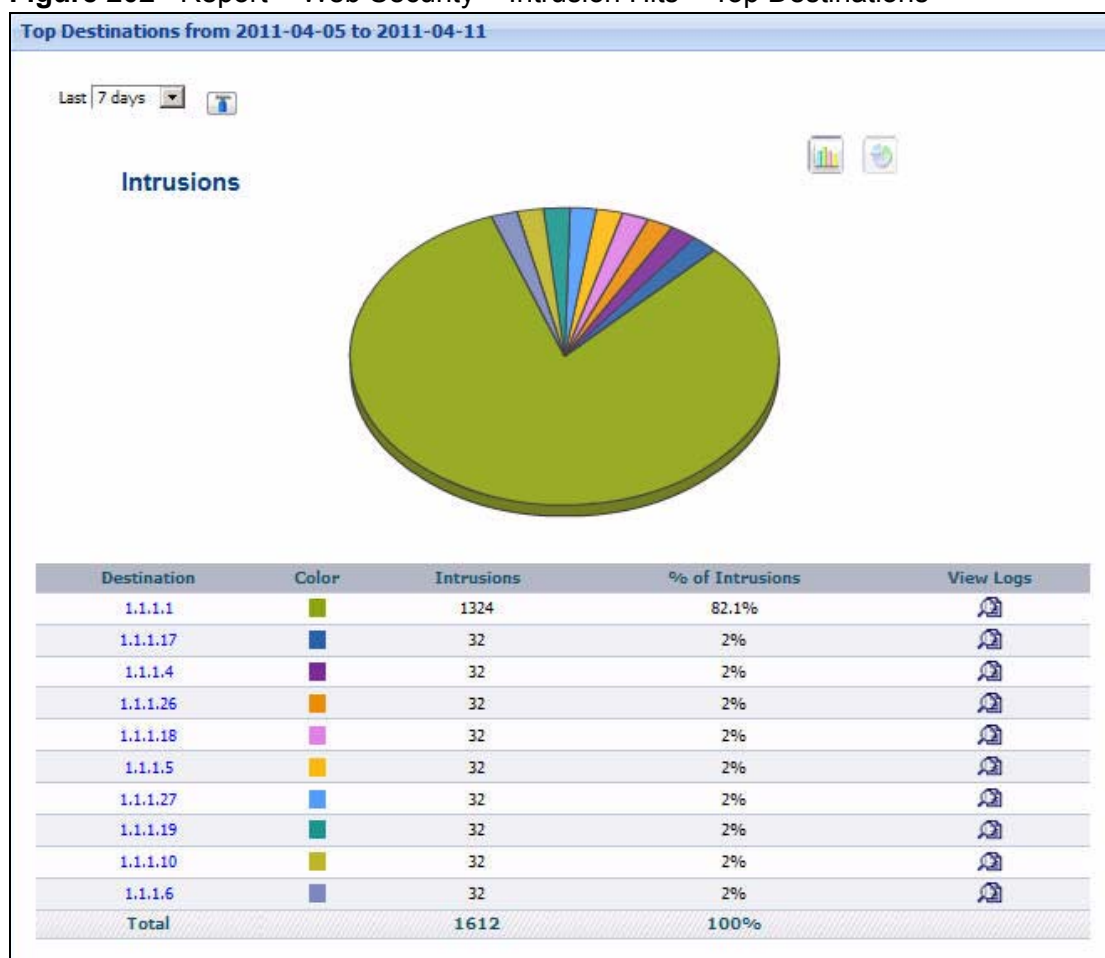
LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by the selected source using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions by the selected source was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.3.7 Top Intrusion Hits Destinations

Use this report to look at the top destinations of intrusions by number of intrusions.

Click **Report > Web Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 202 Report > Web Security > Intrusion Hits > Top Destinations



Each field is described in the following table.

Table 186 Report > Web Security > Intrusion Hits > Top Destinations

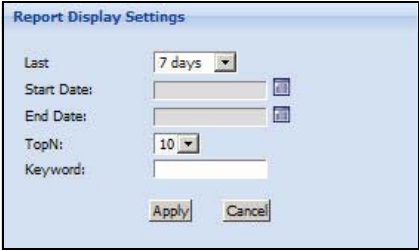
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Destination field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 186 Report > Web Security > Intrusion Hits > Top Destinations

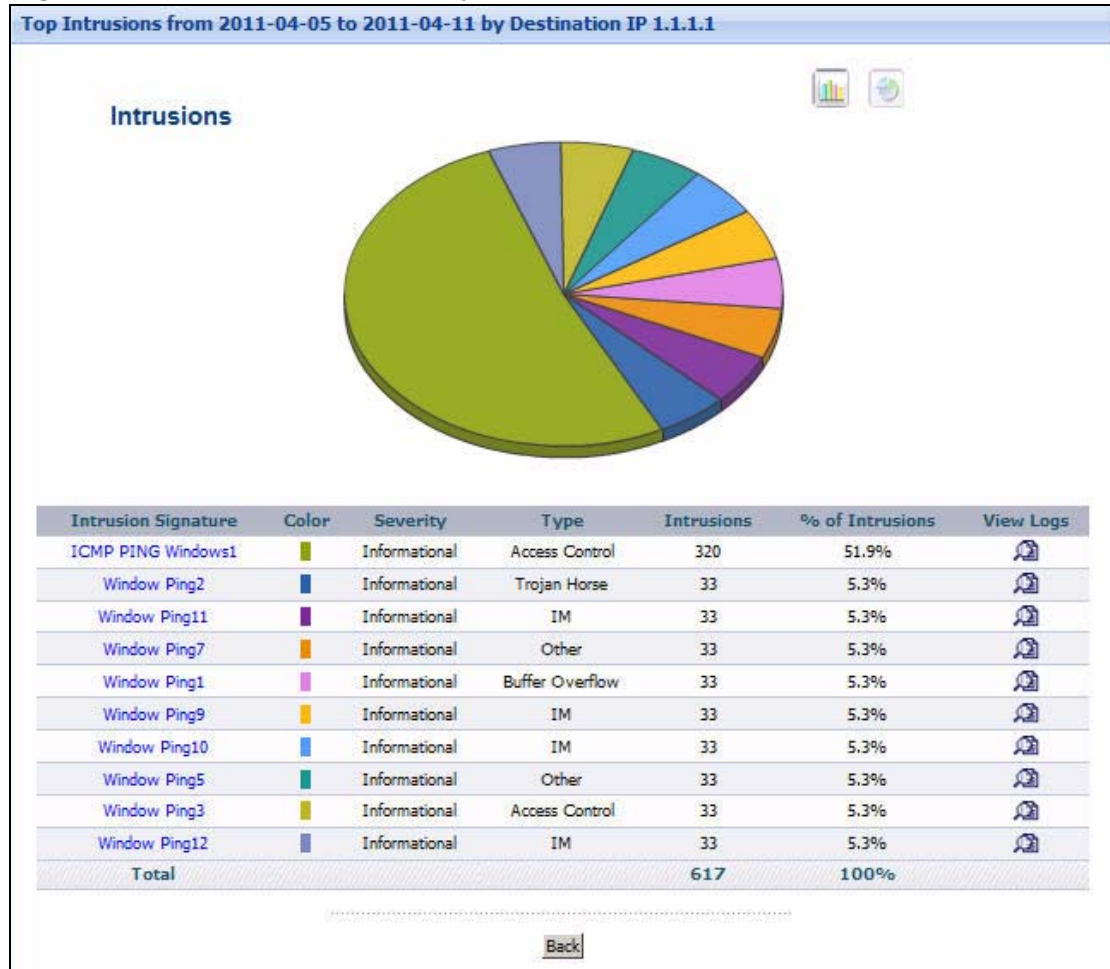
LABEL	DESCRIPTION
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If DNS Reverse is enabled in System > General Configuration, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top intrusion signatures for the selected destination.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

9.3.8 Top Intrusion Hits Destinations Drill-Down

Use this report to look at the top intrusion signatures for any top destination.

Click on a specific destination in **Report > Web Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 203 Report > Web Security > Intrusion Hits > Top Destinations > Drill-Down



Each field is described in the following table.

Table 187 Report > Web Security > Intrusion Hits > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures sent to the selected destination, sorted by the number of intrusions at each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.

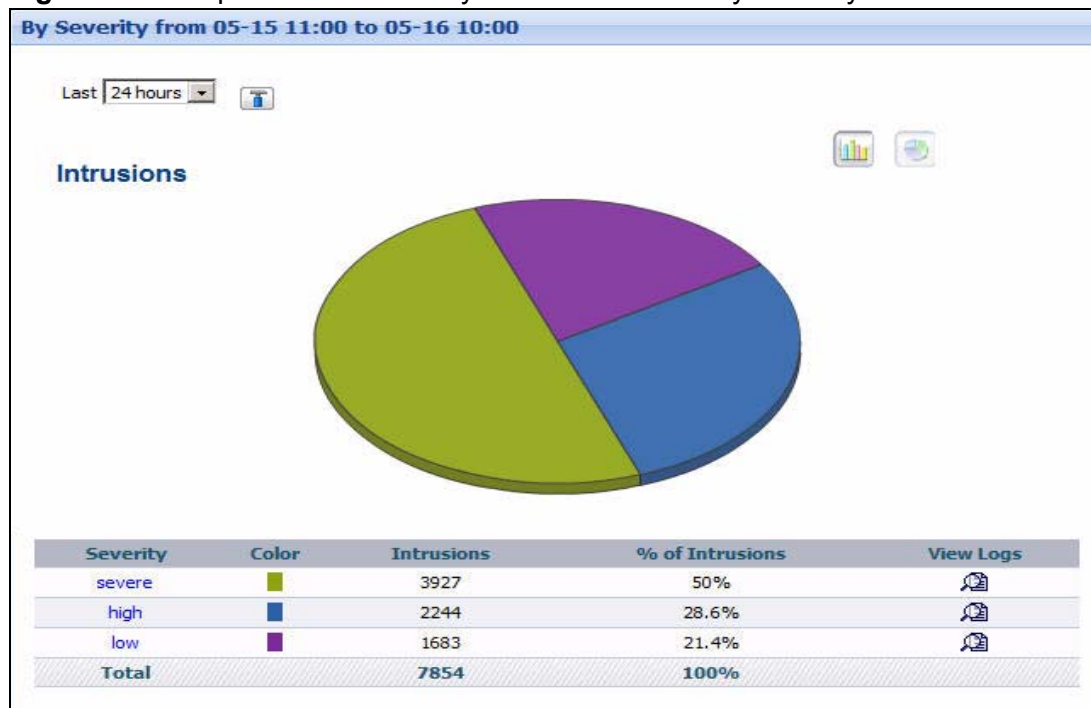
Table 187 Report > Web Security > Intrusion Hits > Top Destinations > Drill-Down

LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of each intrusion signature sent to the selected destination.
% of Intrusions	This field displays what percentage of all intrusions sent to the selected destination belong to each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.3.9 Intrusion Hits Severities

Use this report to look at the severity (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug.

Click **Report > Web Security > Intrusion Hits > By Severity** to open this screen.

Figure 204 Report > Web Security > Intrusion Hits > By Severity

Each field is described in the following table.

Table 188 Report > Web Security > Intrusion Hits > By Severity

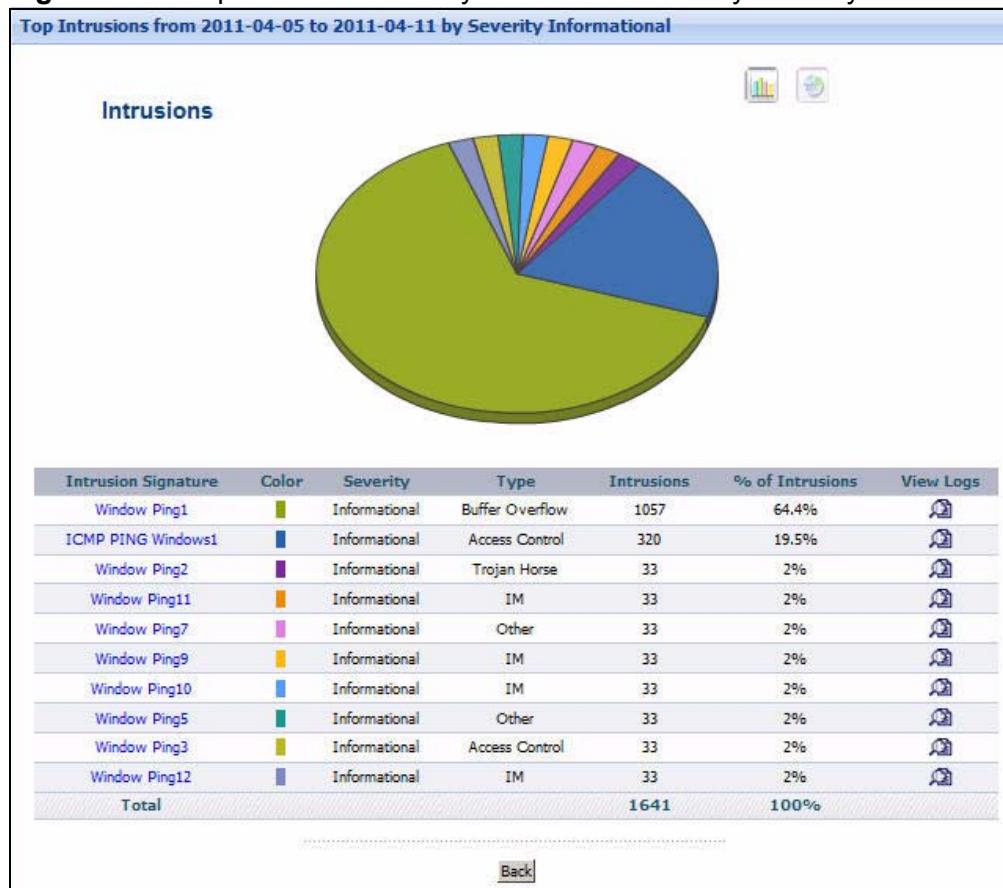
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

9.3.10 Intrusion Hits Severities Drill-Down

Use this report to look at the intrusion signatures for any severity.

Click on a specific severity in **Report > Web Security > Intrusion Hits > By Severity** to open this screen.

Figure 205 Report > Web Security > Intrusion Hits > By Severity > Drill-Down



Each field is described in the following table.

Table 189 Report > Web Security > Intrusion Hits > By Severity > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the intrusion signatures of the selected severity, sorted by the number of intrusions by each one.

Table 189 Report > Web Security > Intrusion Hits > By Severity > Drill-Down

LABEL	DESCRIPTION
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to IDP > Signature > Attack Type in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of the selected severity using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions of the selected severity was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

Security Policy Enforcement

This chapter discusses how you can check reports to look at what users and traffic were allowed or blocked by the application patrol and content filtering policies.

10.1 EPS

These screens display which computers passed or failed endpoint security (EPS) checking.

Endpoint Security (EPS), also known as endpoint control, is used to make sure users' computers comply with defined corporate policies before they can access the network or an SSL Secure Remote Access tunnel. After a successful user authentication, a user's computer must meet the endpoint security object's Operating System (OS) option and security requirements to gain access. You can configure the endpoint security object to require a user's computer to match just one of the endpoint security object's checking criteria or all of them. Configure endpoint security objects to use with the authentication policy and SSL Secure Remote Access features. See the User's Guide of your ZyWALL device for more information.

10.1.1 What Endpoint Security Can Check

The settings endpoint security can check vary depending on the OS of the user's computer. Depending on the OS, EPS can check user computers for the following:

- Operating System (Windows, Linux, Mac OSX, or others)
- Windows version and service pack version
- Windows Auto Update setting and installed security patches
- Personal firewall installation and activation
- Anti-virus installation and activation
- Windows registry settings
- Processes that the endpoint must execute
- Processes that the endpoint cannot execute

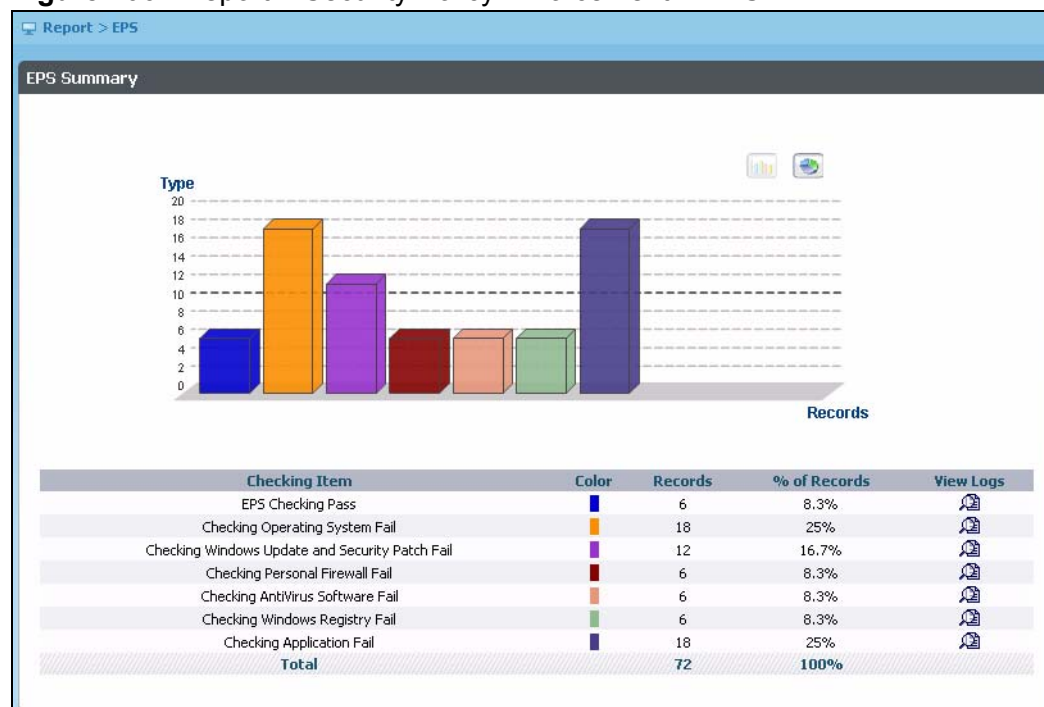
The size and version of specific files

10.1.2 EPS Summary

Use this screen to view statistics about the number of users' computers that passed or failed EPS checking with the reasons for failure displayed in a bar or pie graph.

Select a device in the device window on the left of the main screen and then click **Report > Security Policy Enforcement > EPS** to open the **EPS Summary** screen.

Figure 206 Report > Security Policy Enforcement > EPS



Each field is described in the following table.

Table 190 Report > Security Policy Enforcement > EPS

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to identify it. - Click on a slice in the pie chart to move it away from the pie chart a little.
Checking Item	This field displays the description about whether users' computers passed all the EPS checking items or failed a specific checking item on the selected device.

Table 190 Report > Security Policy Enforcement > EPS

LABEL	DESCRIPTION
Color	This field displays what color represents each EPS checking result in the graph.
Records	This field displays the number of users' computers that passed all the EPS checking items or failed a specific checking item.
% of Records	This field displays what percentage each EPS checking result's number of users' computers makes out of the total number of users' computers that attempted to access the corporate's network.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the EPS rules above.

10.1.3 View Logs

Use this screen to view detailed information about users who passed or failed the EPS checking items defined on the selected ZyWALL device.

Click **View Logs** next to an entry in the **Report > Security Policy Enforcement > EPS** screen to open the screen.

Figure 207 Report > Security Policy Enforcement > EPS > View Logs

User	IP	Message	Time
lizzy5	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy4	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy3	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy2	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy1	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27

Total Count:6 Total Page:1 First 1 Last Go

Each field is described in the following table.

Table 191 Report > Security Policy Enforcement > EPS > View Logs

LABEL	DESCRIPTION
User	This field displays who tried successfully or unsuccessfully to access the protected network.
IP	This field displays the IP address of the user's computer the user used to try to access the protected network.
Message	This field shows whether the user's session passed EPS checking or the reason it failed.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user tried to access the protected network.

Table 191 Report > Security Policy Enforcement > EPS > View Logs

LABEL	DESCRIPTION
Total Count	This field displays how many records there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the records.
First .. Last	Click First , Last , or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .
Back	Click this to close this screen.

10.2 Content Filter (All)

These reports look at the number of attempts to access web sites specified in the content filter (blocked, forward and warning) by time interval as well as top allowed sites and hosts.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Forward Web Sites**, **Warning Web Sites** and **Blocked Web Sites** are enabled.

10.2.1 Summary

Use this report to look at the number of attempts to access specified web sites by time interval.

Click **Report > Security Policy Enforcement > Content Filter (All) > Summary** to open this screen.

Figure 208 Report > Security Policy Enforcement > Content Filter (All) > Summary

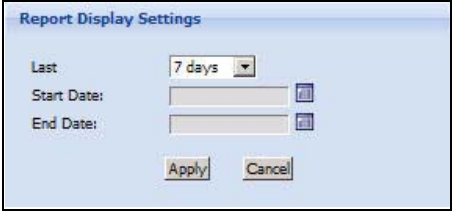


Each field is described in the following table.

Table 192 Report > Security Policy Enforcement > Content Filter (All) > Summary

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 192 Report > Security Policy Enforcement > Content Filter (All) > Summary

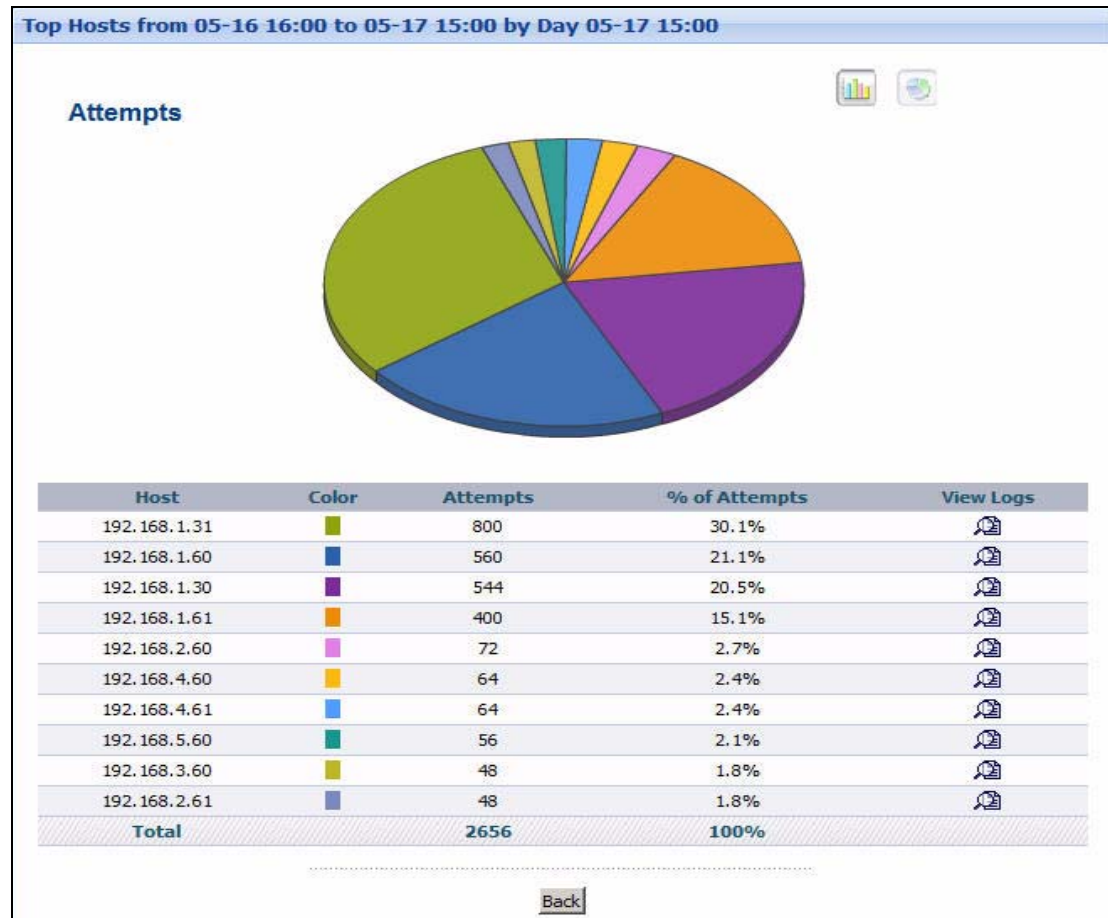
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access specified web sites in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts to access specified web sites in each time interval.
% of Attempts	This field displays the percentage of all attempts in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

10.2.2 Summary Drill-Down

Use this report to look at the top sources of attempts to access specified web sites in a specific time interval.

Click on a specific time interval in **Report > Security Policy Enforcement > Content Filter (All) > Summary** to open this screen.

Figure 209 Report > Security Policy Enforcement > Content Filter (All) > Summary > Drill-Down



Each field is described in the following table.

Table 193 Report > Security Policy Enforcement > Content Filter (All) > Summary > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 193 Report > Security Policy Enforcement > Content Filter (All) > Summary > Drill-Down

LABEL	DESCRIPTION
Host	This field displays the top sources of attempts to access specified web sites in the selected time interval, sorted by the number of attempts by each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration , the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts by each source to access specified web sites in the selected time interval.
% of Attempts	This field displays the percentage of all attempts in the selected time interval attributed to each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

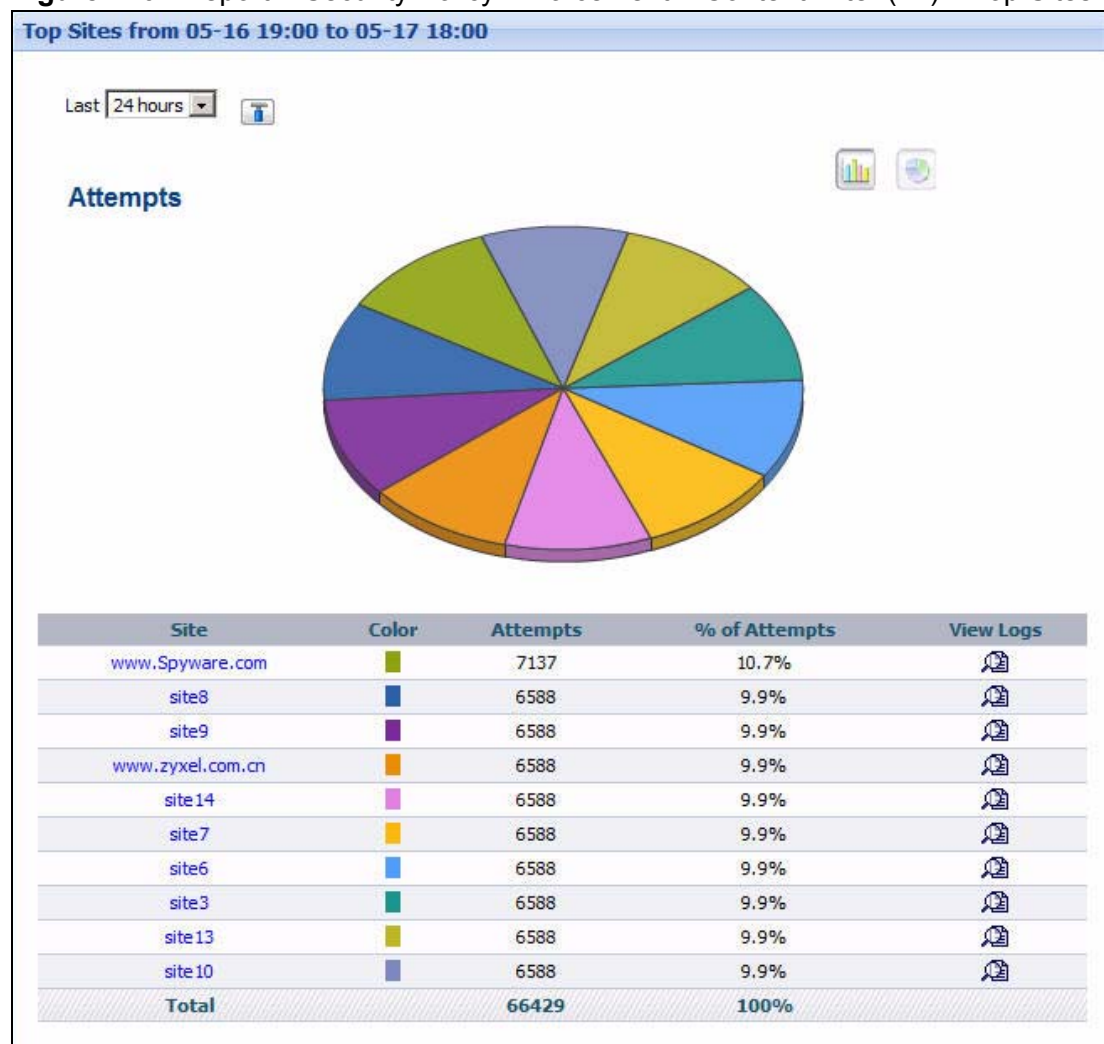
10.2.3 Top Sites

Use this report to look at the top destinations of web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Forward Web Sites**, **Warning Web Sites** and **Blocked Web Sites** are enabled.

Click **Report > Security Policy Enforcement > Content Filter (All) > Top Sites** to open this screen.

Figure 210 Report > Security Policy Enforcement > Content Filter (All) > Top Sites



Each field is described in the following table.

Table 194 Report > Security Policy Enforcement > Content Filter (All) > Top Sites

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 194 Report > Security Policy Enforcement > Content Filter (All) > Top Sites

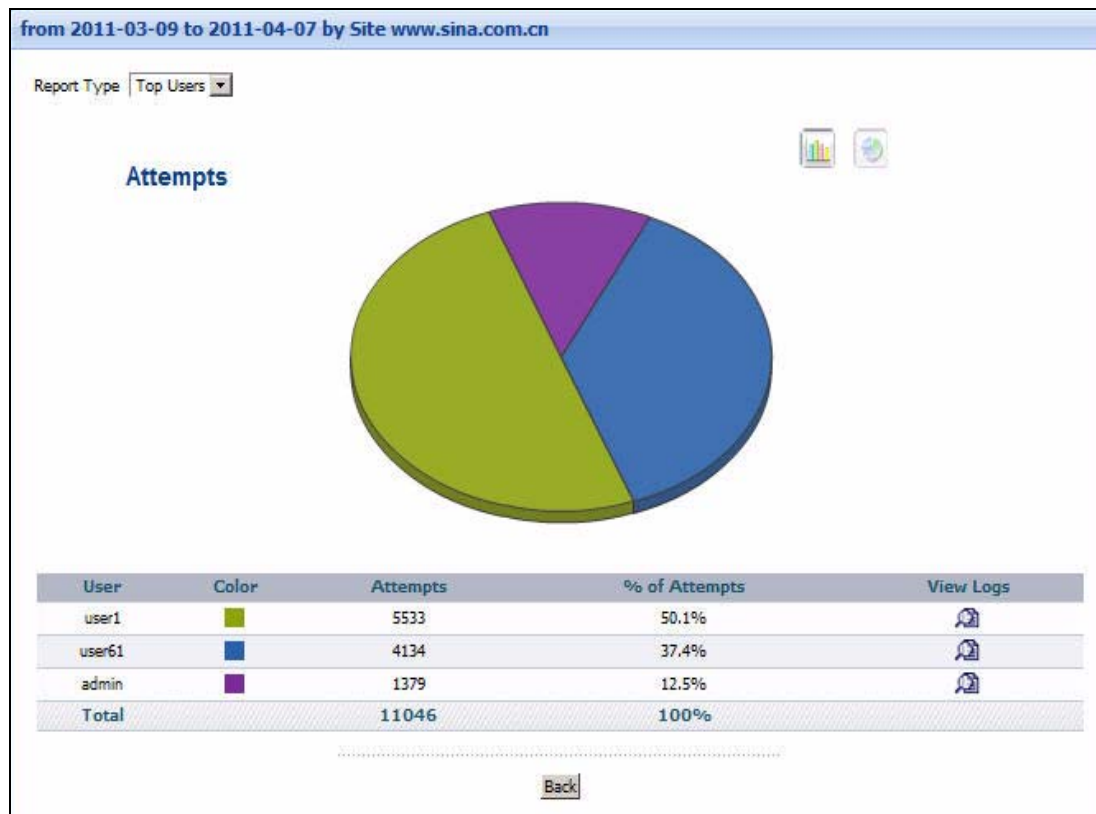
LABEL	DESCRIPTION
Site	This field displays the top destinations of web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts for each destination.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

10.2.4 Top Sites Drill-Down

Use this report to look at the top sources for any top destination of web traffic.

Click on a specific destination in **Report > Security Policy Enforcement > Content Filter (All) > Top Sites** to open this screen.

Figure 211 Report > Security Policy Enforcement > Content Filter (All) > Top Sites > Drill-Down



Each field is described in the following table.

Table 195 Report > Security Policy Enforcement > Content Filter (All) > Top Sites > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Users , Top Hosts or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 195 Report > Security Policy Enforcement > Content Filter (All) > Top Sites > Drill-Down

LABEL	DESCRIPTION
Host	This field displays the top sources of web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration , the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made by each source to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

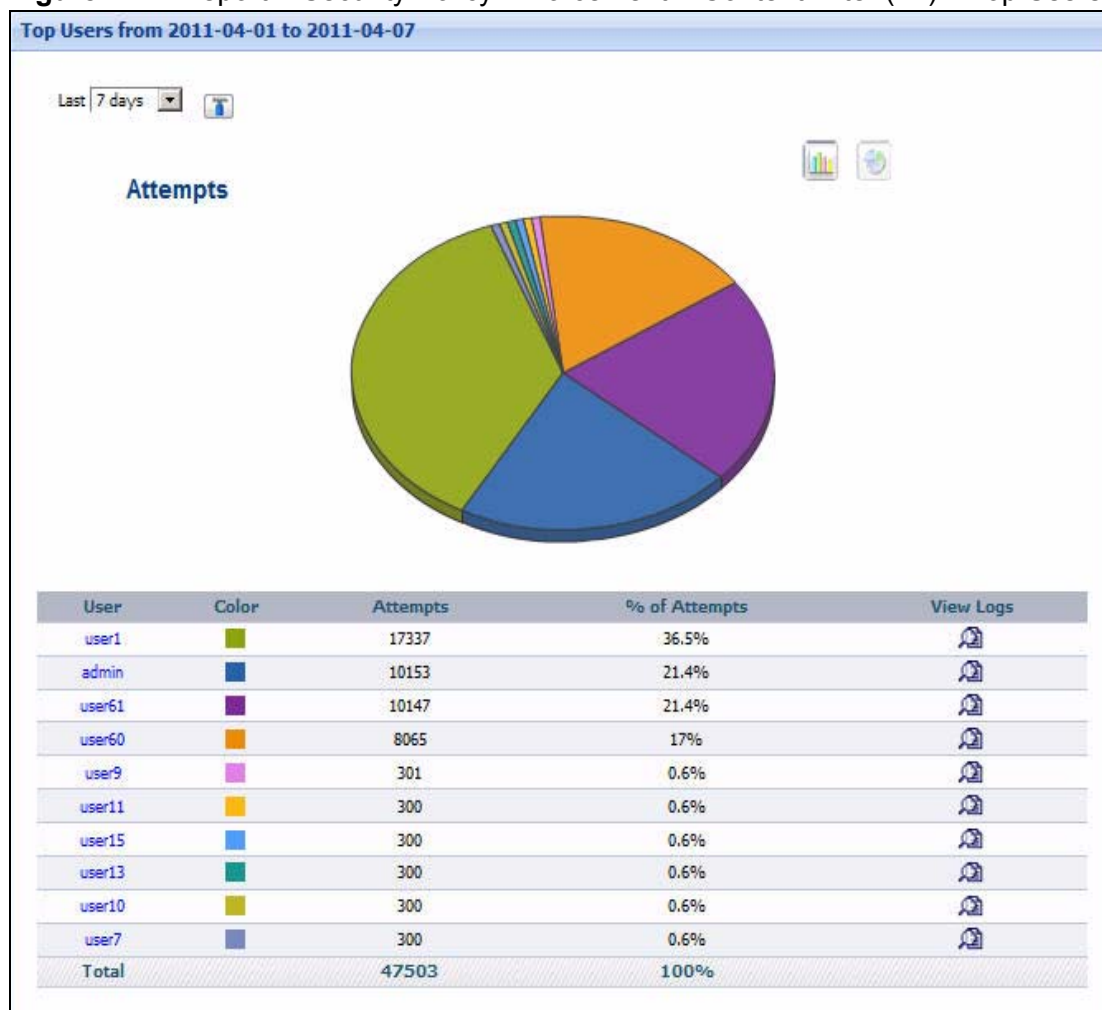
10.2.5 Top Users

Use this report to look at the top users of web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Forward Web Sites**, **Warning Web Sites** and **Blocked Web Sites** are enabled.

Click **Report > Security Policy Enforcement > Content Filter (All) > Top Users** to open this screen.

Figure 212 Report > Security Policy Enforcement > Content Filter (All) > Top Users

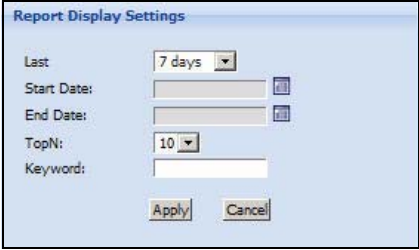


Each field is described in the following table.

Table 196 Report > Security Policy Enforcement > Content Filter (All) > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 196 Report > Security Policy Enforcement > Content Filter (All) > Top Users

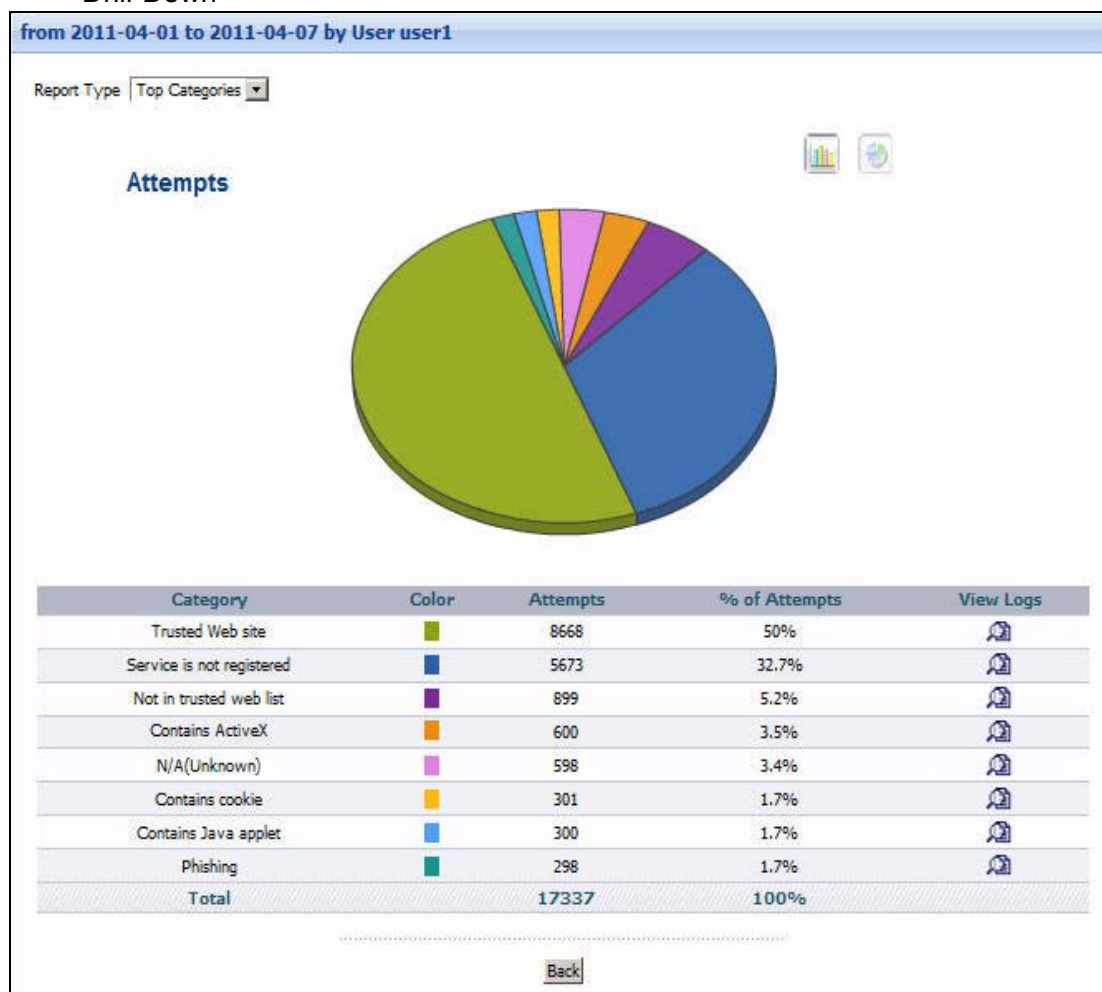
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users of web traffic, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected user.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how many times each user accessed the specified web sites.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made by each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.2.6 Top Users Drill-Down

Use this report to look at the top destinations for any top source of web traffic.

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (All) > Top Users** to open this screen.

Figure 213 Report > Security Policy Enforcement > Content Filter (All) > Top Users > Drill-Down



Each field is described in the following table.

Table 197 Report > Security Policy Enforcement > Content Filter (All) > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Categories , Top Sites or By Hour as the content to be displayed.

Table 197 Report > Security Policy Enforcement > Content Filter (All) > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic from the selected user, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected user to each destination.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made by the selected user to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected user is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

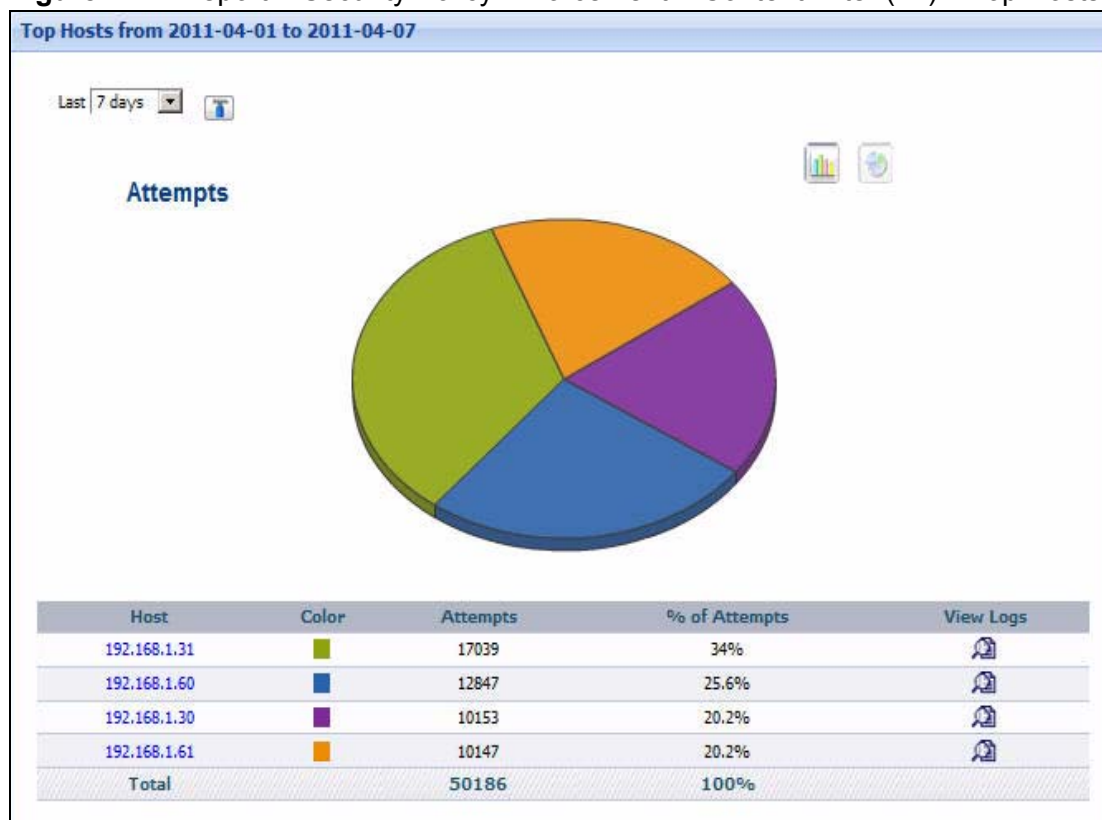
10.2.7 Top Hosts

Use this report to look at the top sources of web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Forward Web Sites**, **Warning Web Sites** and **Blocked Web Sites** are enabled.

Click **Report > Security Policy Enforcement > Content Filter (All) > Top Hosts** to open this screen.

Figure 214 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts

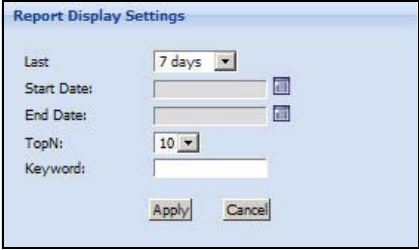


Each field is described in the following table.

Table 198 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 198 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts

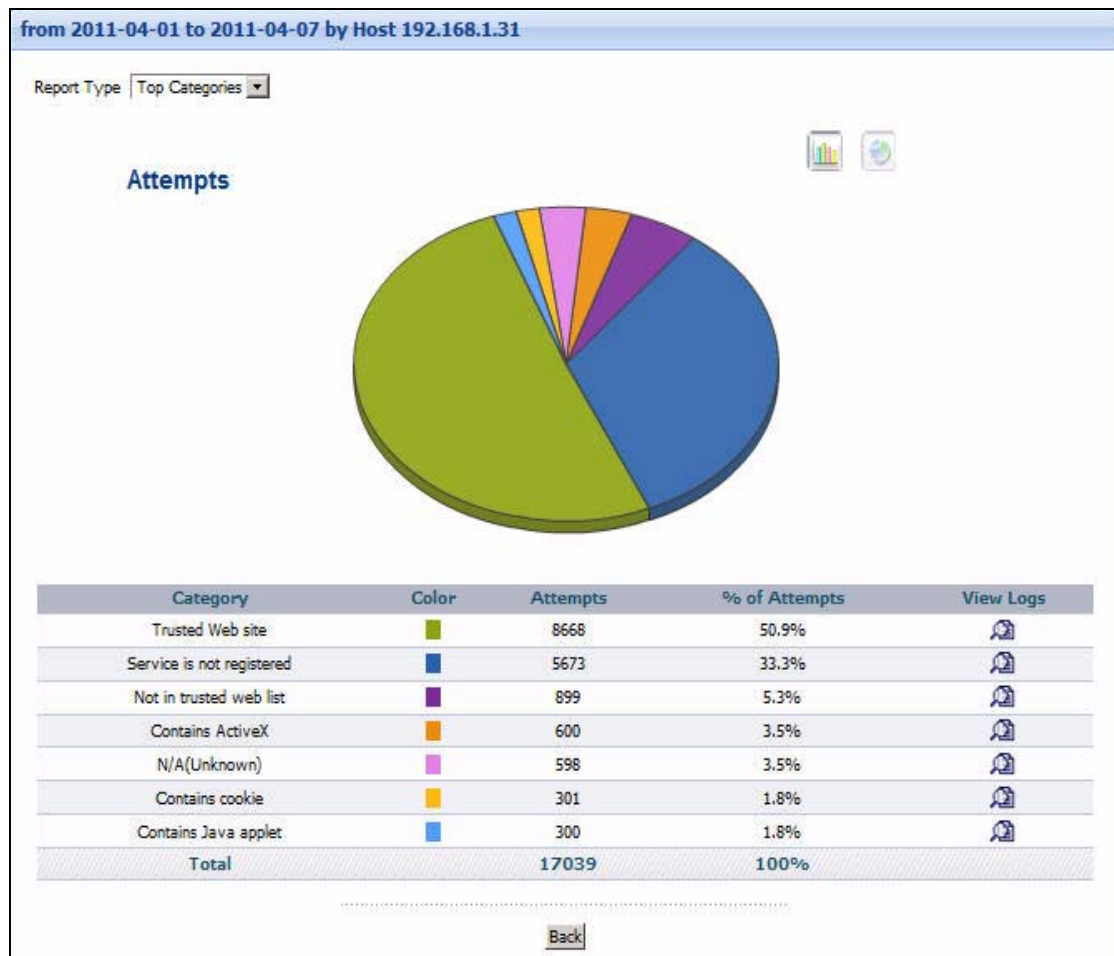
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how times each source accessed specified web sites.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made from each sources.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.2.8 Top Hosts Drill-Down

Use this report to look at the top destinations for any top source of web traffic.

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (All) > Top Hosts** to open this screen.

Figure 215 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts > Drill-Down



Each field is described in the following table.

Table 199 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Categories , Top Sites or By Hour as the content to be displayed.

Table 199 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic from the selected source, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

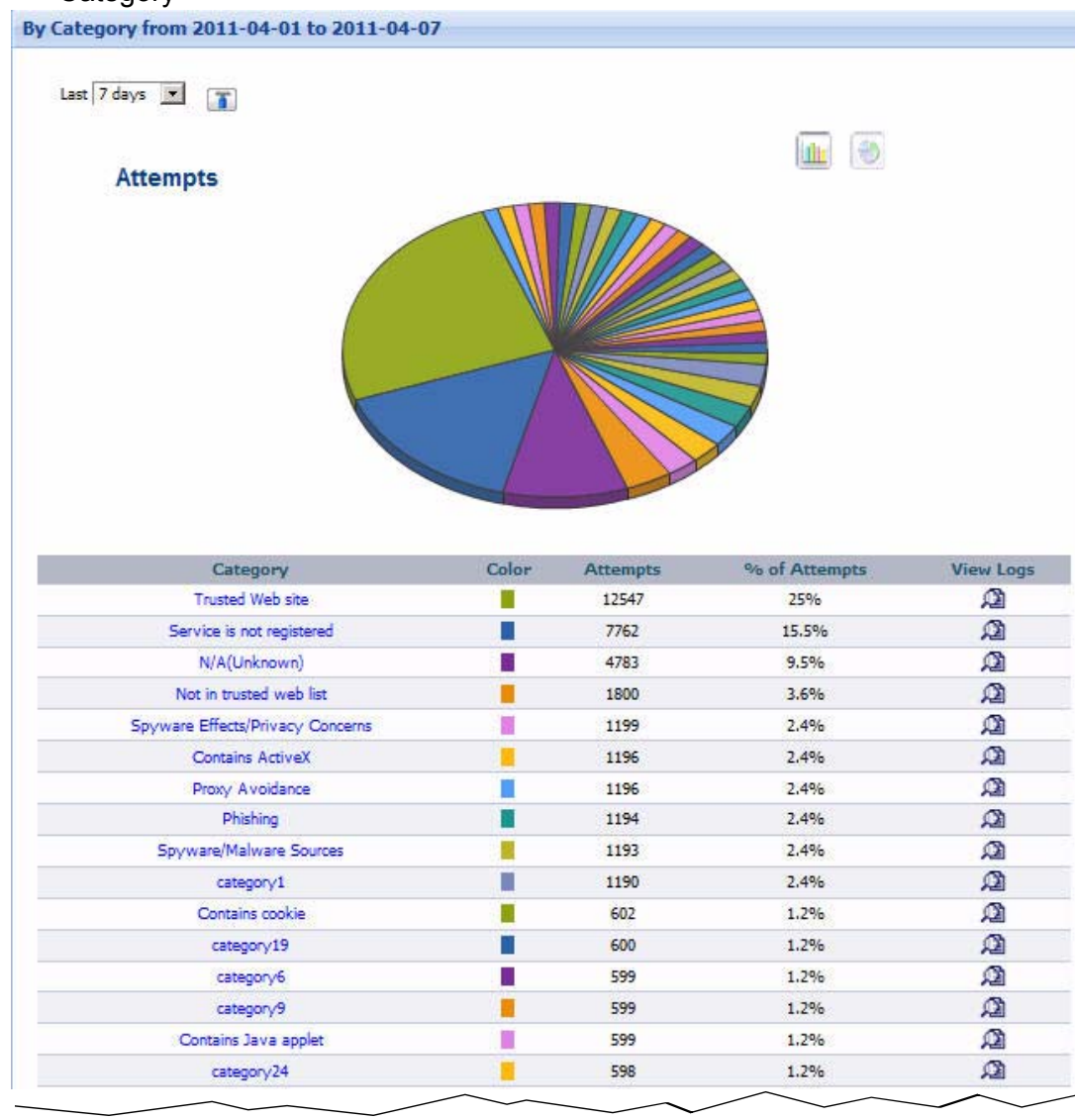
10.2.9 By Category

Use this report to look at the categories of web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Forward Web Sites**, **Warning Web Sites** and **Blocked Web Sites** are enabled.

Click **Report > Security Policy Enforcement > Content Filter (All) > By Category** to open this screen.

Figure 216 Report > Security Policy Enforcement > Content Filter (All) > By Category



Each field is described in the following table.

Table 200 Report > Security Policy Enforcement > Content Filter (All) > By Category

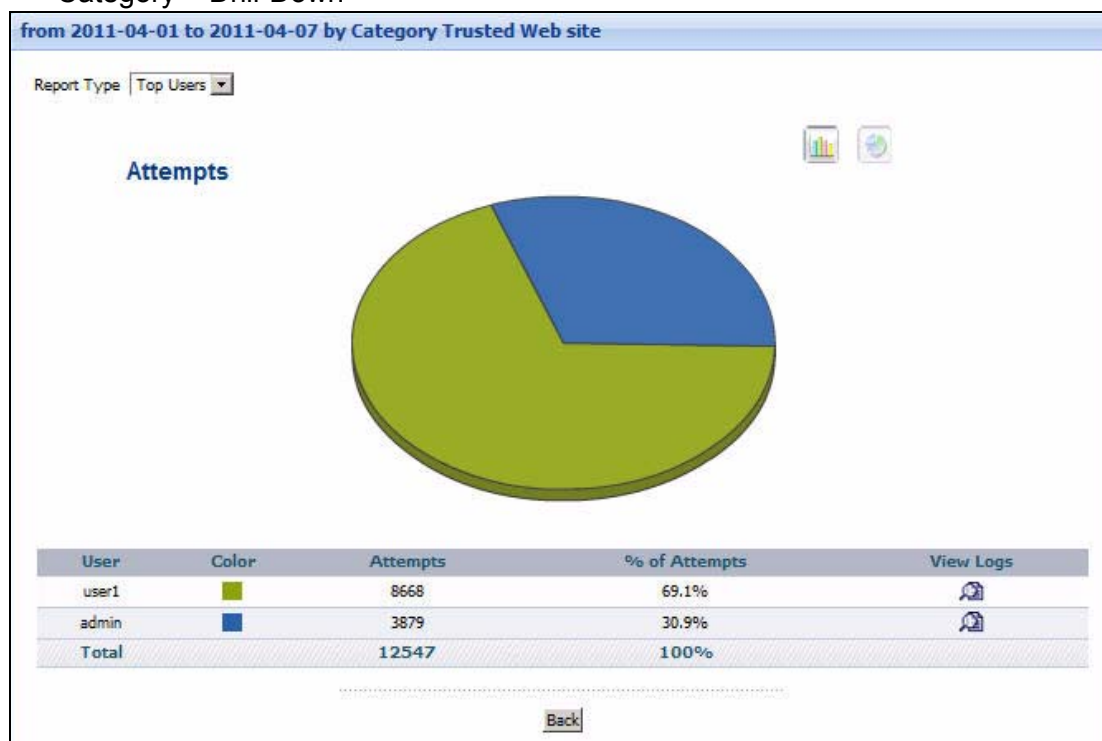
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access specified web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

10.2.10 By Category Drill-Down

Use this report to look at the destinations for any category of web traffic.

Click on a specific category in **Report > Security Policy Enforcement > Content Filter (All) > By Category** to open this screen.

Figure 217 Report > Security Policy Enforcement > Content Filter (All) > By Category > Drill-Down



Each field is described in the following table.

Table 201 Report > Security Policy Enforcement > By Category > Content Filter (All) > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Users , Top Sites , Top Hosts or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 201 Report > Security Policy Enforcement > By Category > Content Filter (All) > Drill-Down

LABEL	DESCRIPTION
Site	This field displays the destinations of web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts to each destination in the selected category.
% of Attempts	This field displays what percentage of all attempts to access specified web sites in the selected category went to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.
Back	Click this to return to the main report.

10.3 Content Filter (Blocked)

These reports look at the number of attempts to access blocked web sites by time interval as well as top blocked sites and hosts.

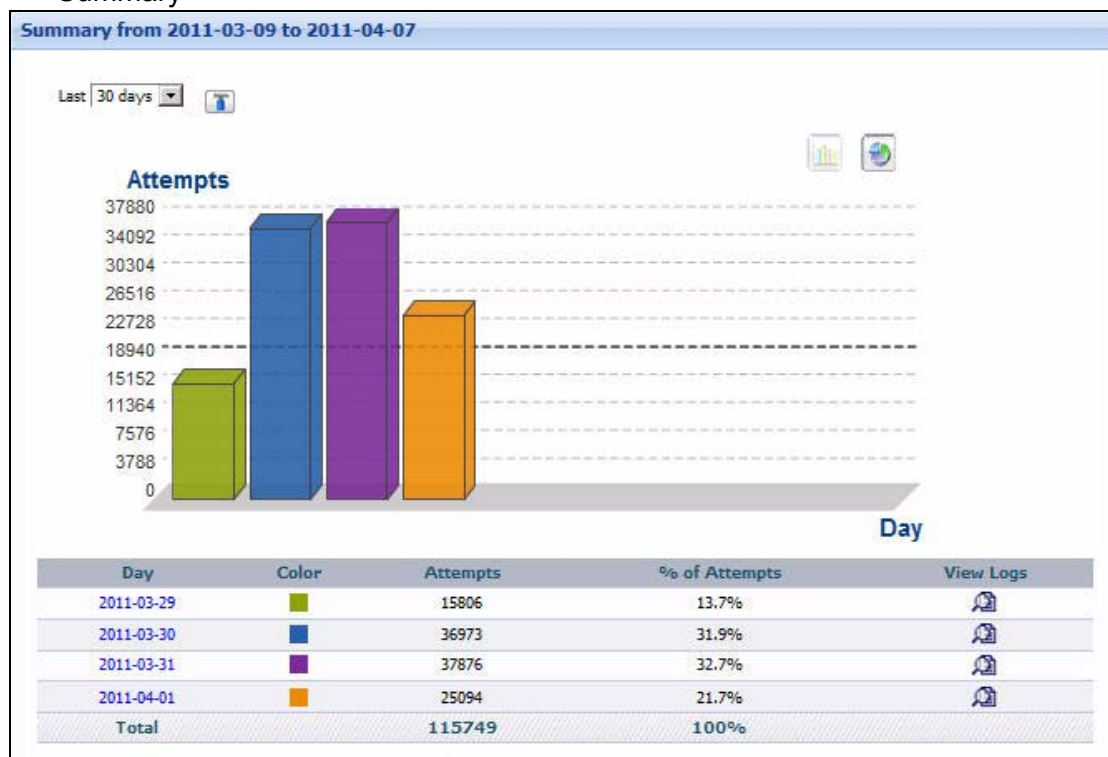
Note: To look at security policy reports, each ZyXEL device must record blocked web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

10.3.1 Summary

Note: To look at security policy reports, each ZyXEL device must record blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** are enabled.

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Summary** to open this screen.

Figure 218 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary

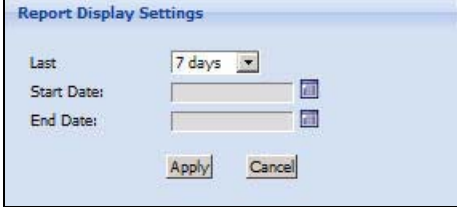


Each field is described in the following table.

Table 202 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 202 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary

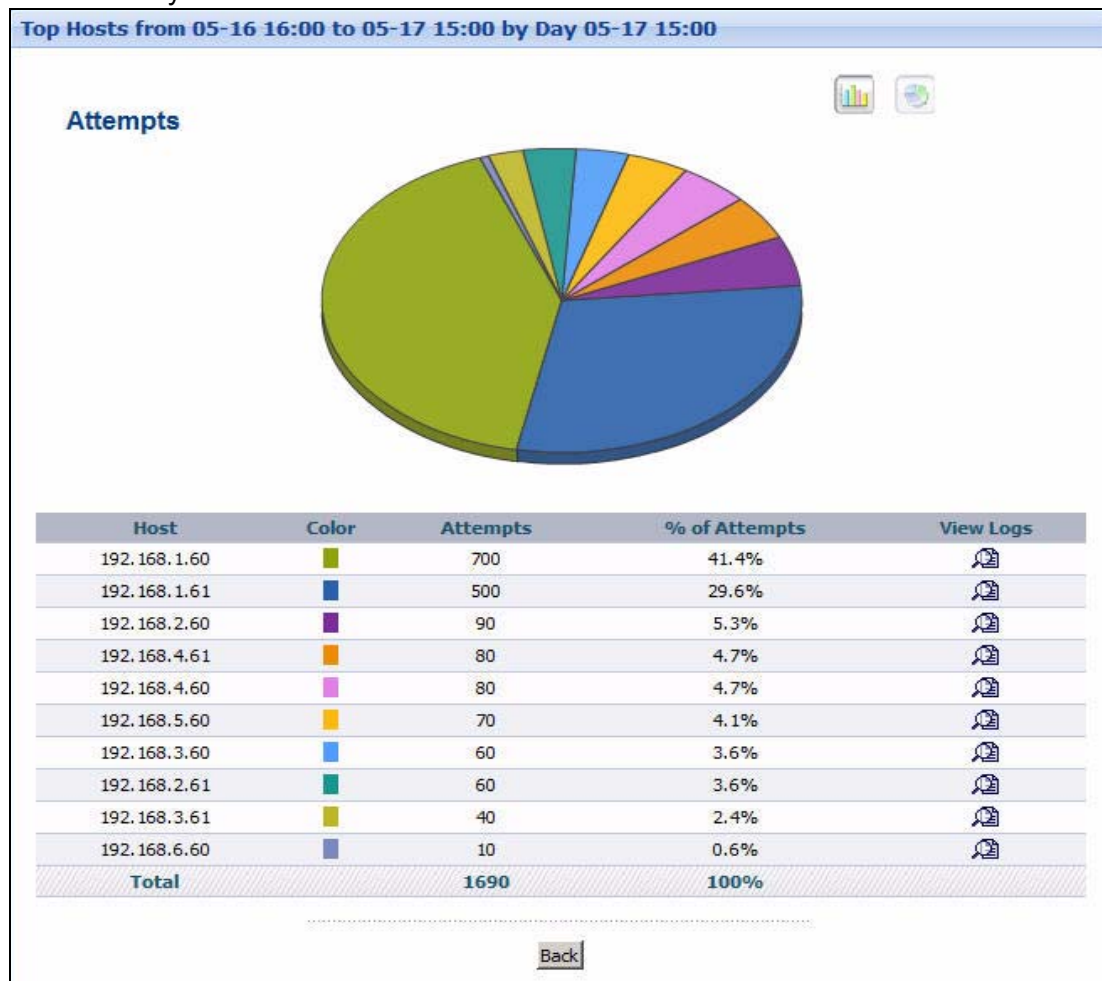
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the Last ... Days or Settings field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts by each source to access blocked web sites in the selected time interval.
% of Attempts	This field displays what percentage of all blocked web access attempts was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

10.3.2 Summary Drill-Down

Use this report to look at the top sources of attempts to access blocked web sites in a specific time interval.

Click on a specific time interval in **Report > Security Policy Enforcement > Content Filter (Blocked) > Summary** to open this screen.

Figure 219 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary > Drill-Down



Each field is described in the following table.

Table 203 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 203 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary > Drill-Down

LABEL	DESCRIPTION
Host	This field displays the top sources of attempts to access blocked web sites in the selected time interval, sorted by the number of attempts by each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration , the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each host.
% of Attempts	This field displays what percentage of all blocked web access attempts in the selected time interval was attributed to each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

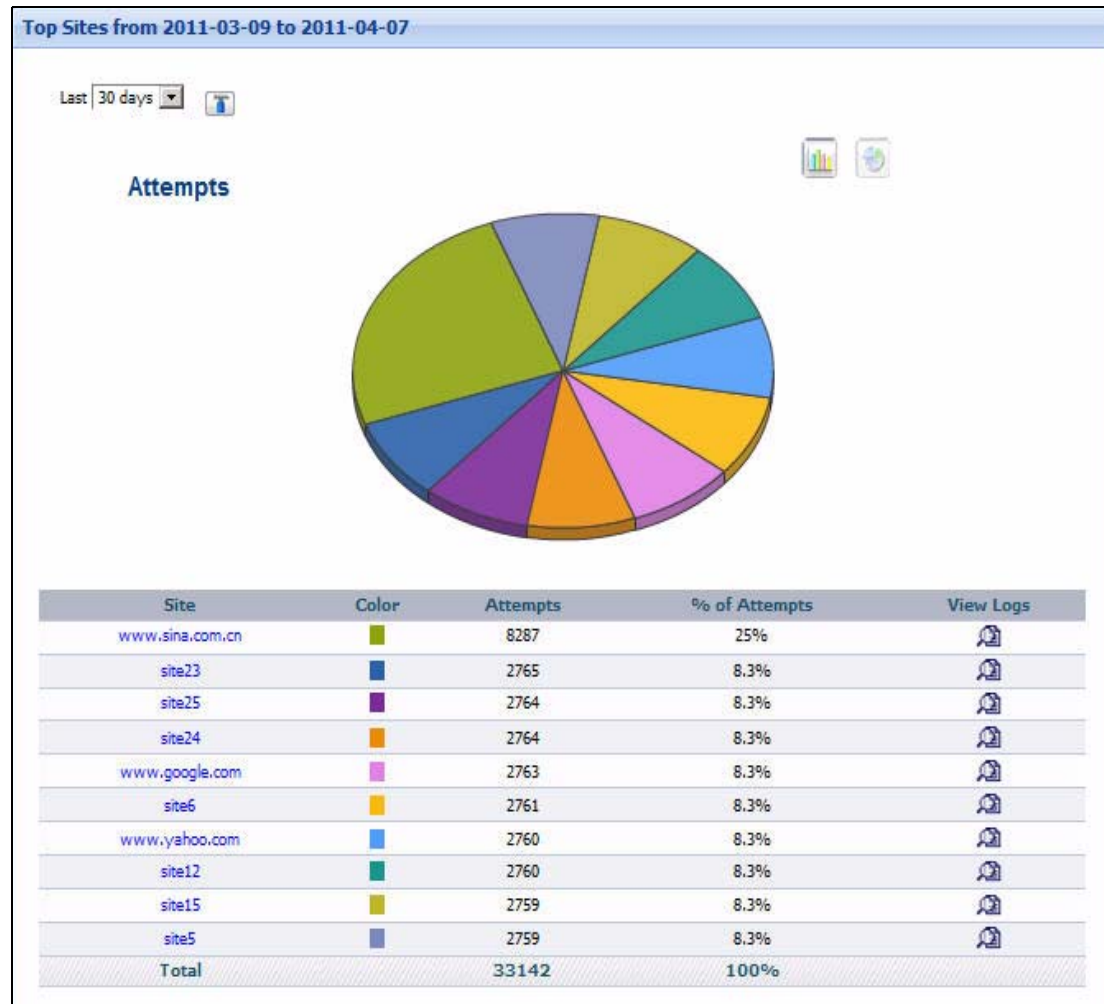
10.3.3 Top Blocked Sites

Use this report to look at the top destinations of blocked web traffic.

Note: To look at security policy reports, each ZyXEL device must record blocked web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites** to open this screen.

Figure 220 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites



Each field is described in the following table.

Table 204 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Site field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 204 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites

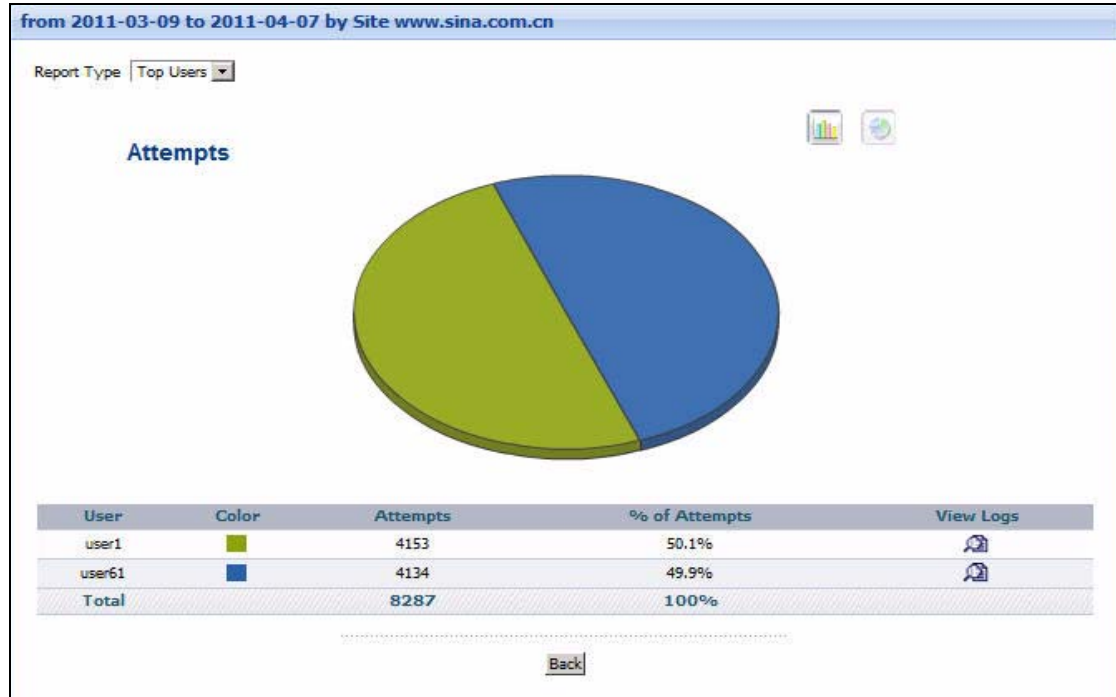
LABEL	DESCRIPTION
Site	This field displays the top destinations of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of blocked web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays how much traffic (in megabytes) the device handled for each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

10.3.4 Top Blocked Sites Drill-Down

Use this report to look at the top sources for any top destination of blocked web traffic.

Click on a specific destination in **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites** to open this screen.

Figure 221 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites > Drill-Down



Each field is described in the following table.

Table 205 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Users , Top Hosts or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.

Table 205 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites > Drill-Down

LABEL	DESCRIPTION
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by each source to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

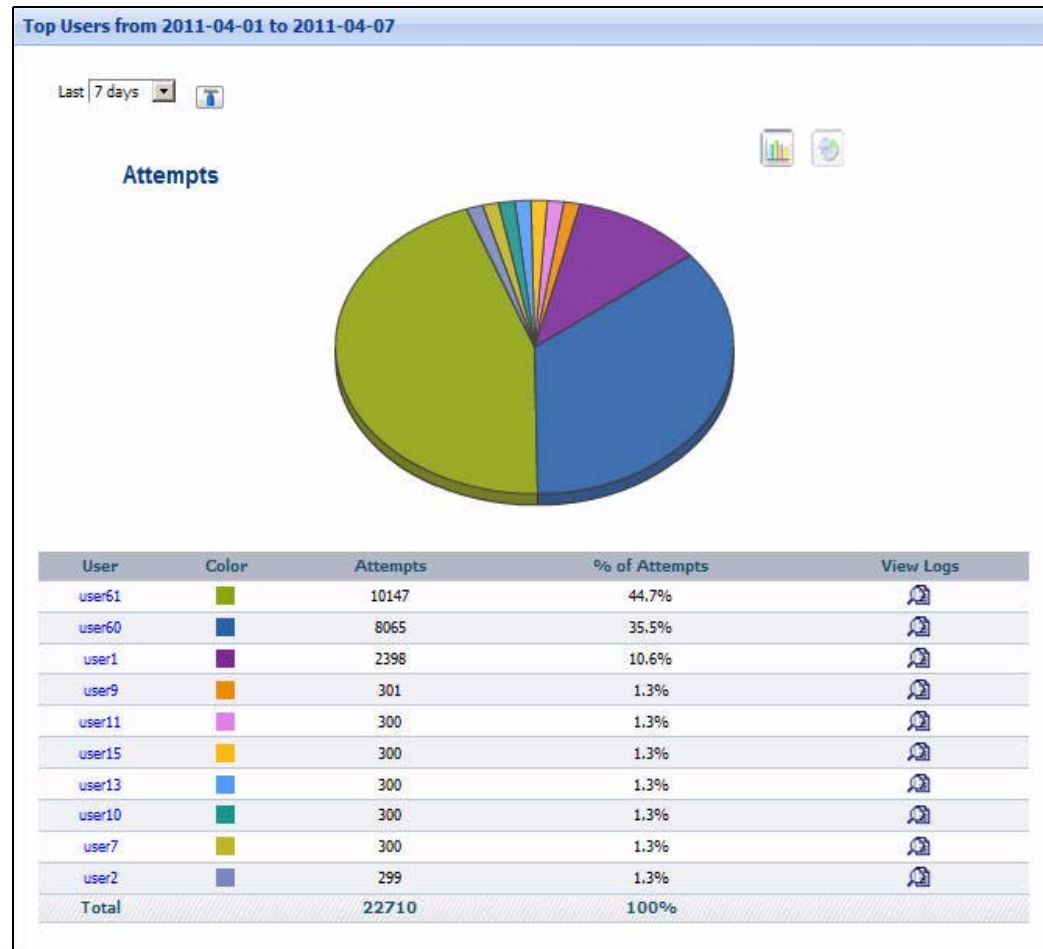
10.3.5 Top Blocked Users

Use this report to look at the users for which the device blocked the most web site access attempts.

Note: To look at security policy Web blocked reports, each ZyXEL device must record blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users** to open this screen.

Figure 222 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users

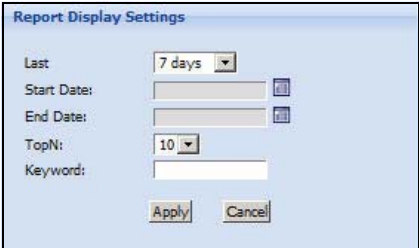


Each field is described in the following table.

Table 206 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 206 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users

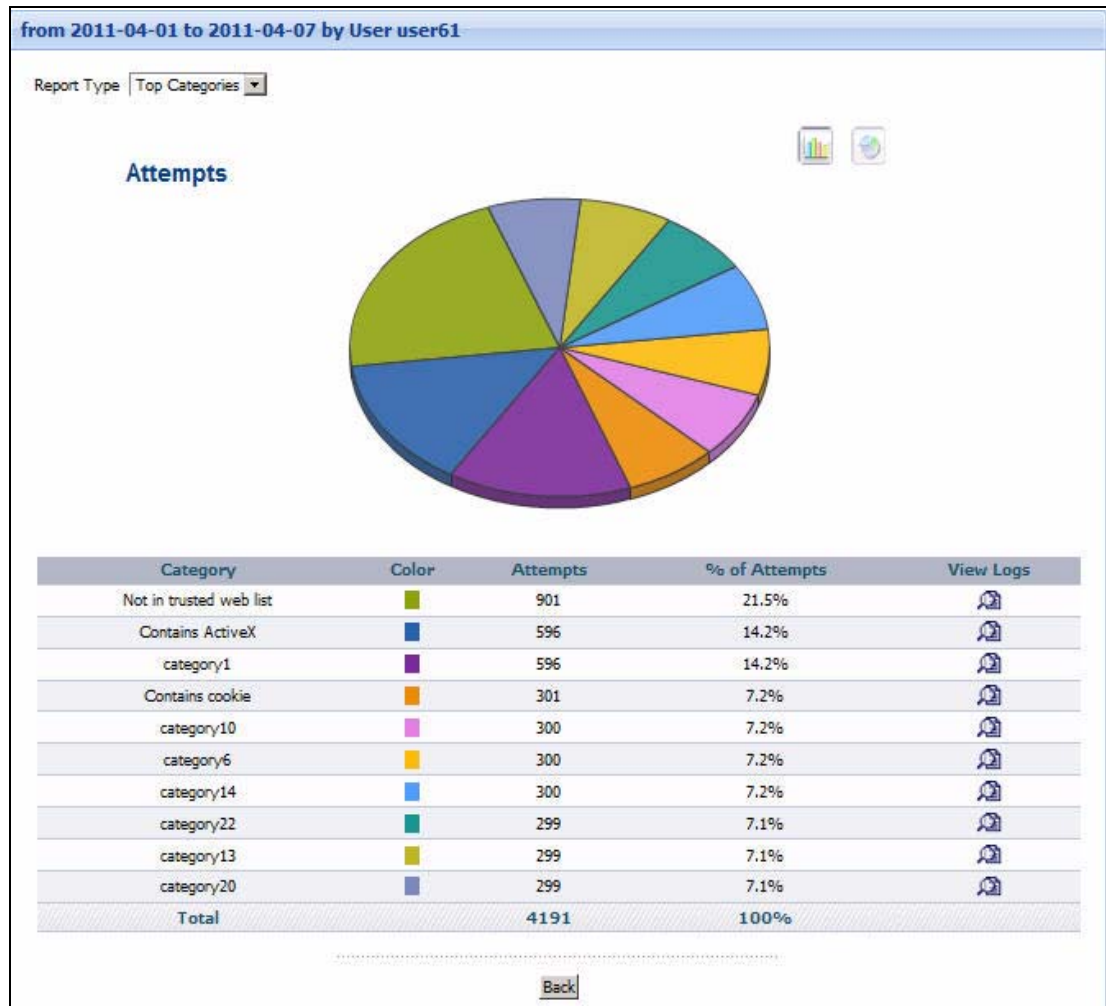
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users for which the device blocked the most web site access attempts, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each user.
% of Attempts	This field displays what percentage the user had of all blocked attempts to access web sites.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.3.6 Top Blocked Users Drill-Down

Use this report to look at the top destinations for any user for which the device blocked the most web site access attempts.

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users** to open this screen.

Figure 223 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users > Drill-Down



Each field is described in the following table.

Table 207 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Categories , Top Sites or By Hour as the content to be displayed.

Table 207 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic from the selected user, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

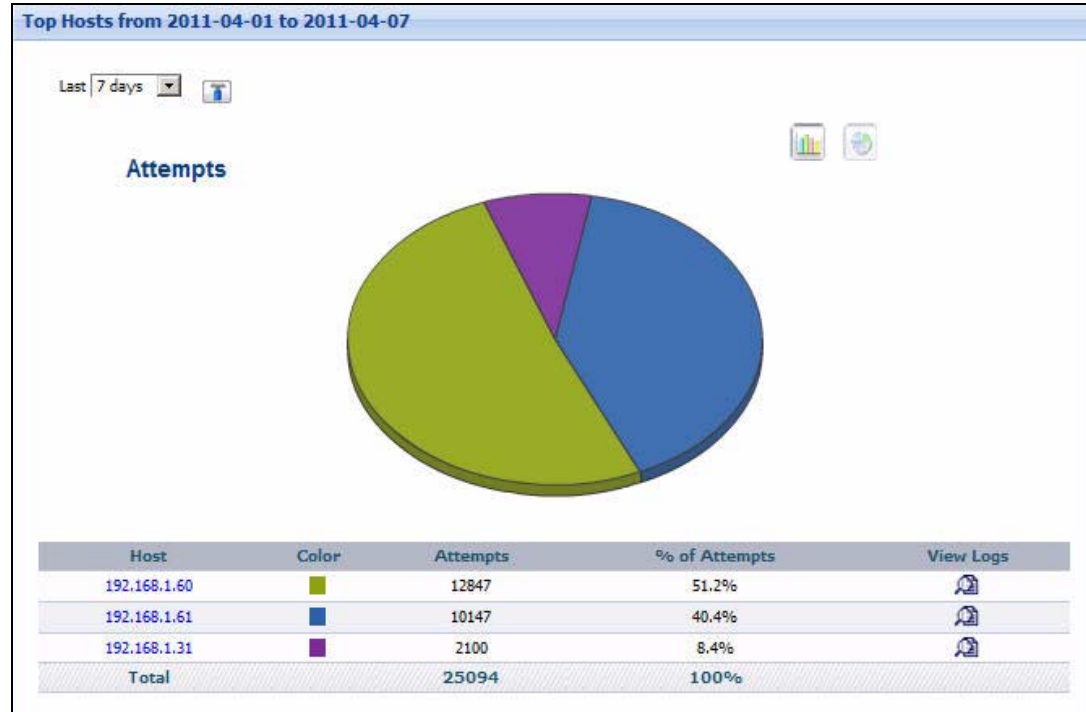
10.3.7 Top Blocked Hosts

Use this report to look at the top sources of blocked web traffic.

Note: To look at security policy reports, each ZyXEL device must record blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts** to open this screen.

Figure 224 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts



Each field is described in the following table.

Table 208 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 208 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts

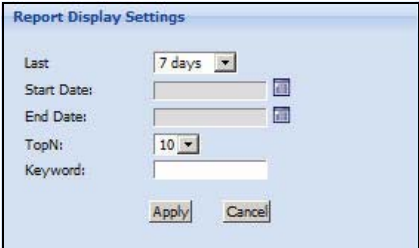
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of web site access attempts the device blocked from each source.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made from each source.

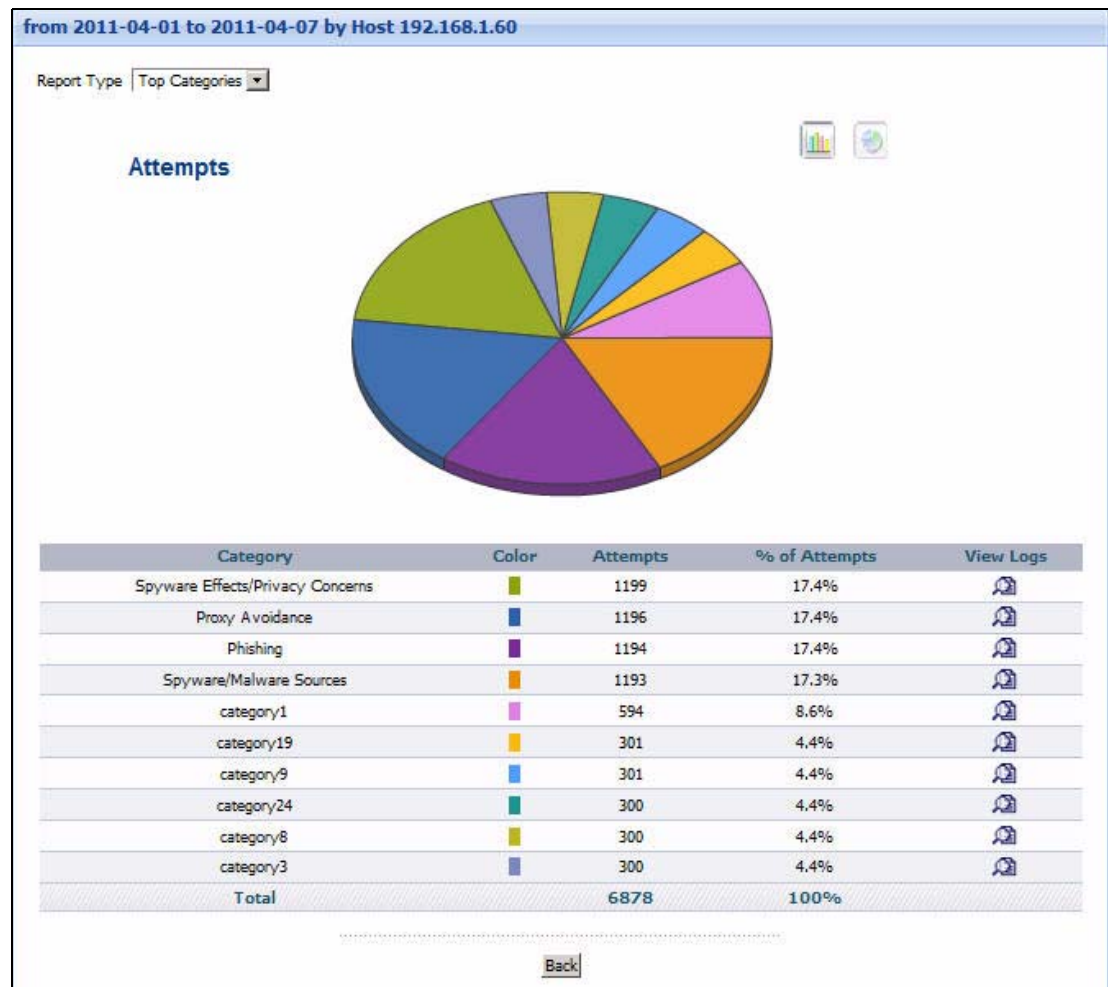
Table 208 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts

LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.3.8 Top Blocked Hosts Drill-Down

Use this report to look at the top destinations for any top source of blocked web traffic.

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts** to open this screen.

Figure 225 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts > Drill-Down

Each field is described in the following table.

Table 209 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Categories , Top Sites or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic from the selected source, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

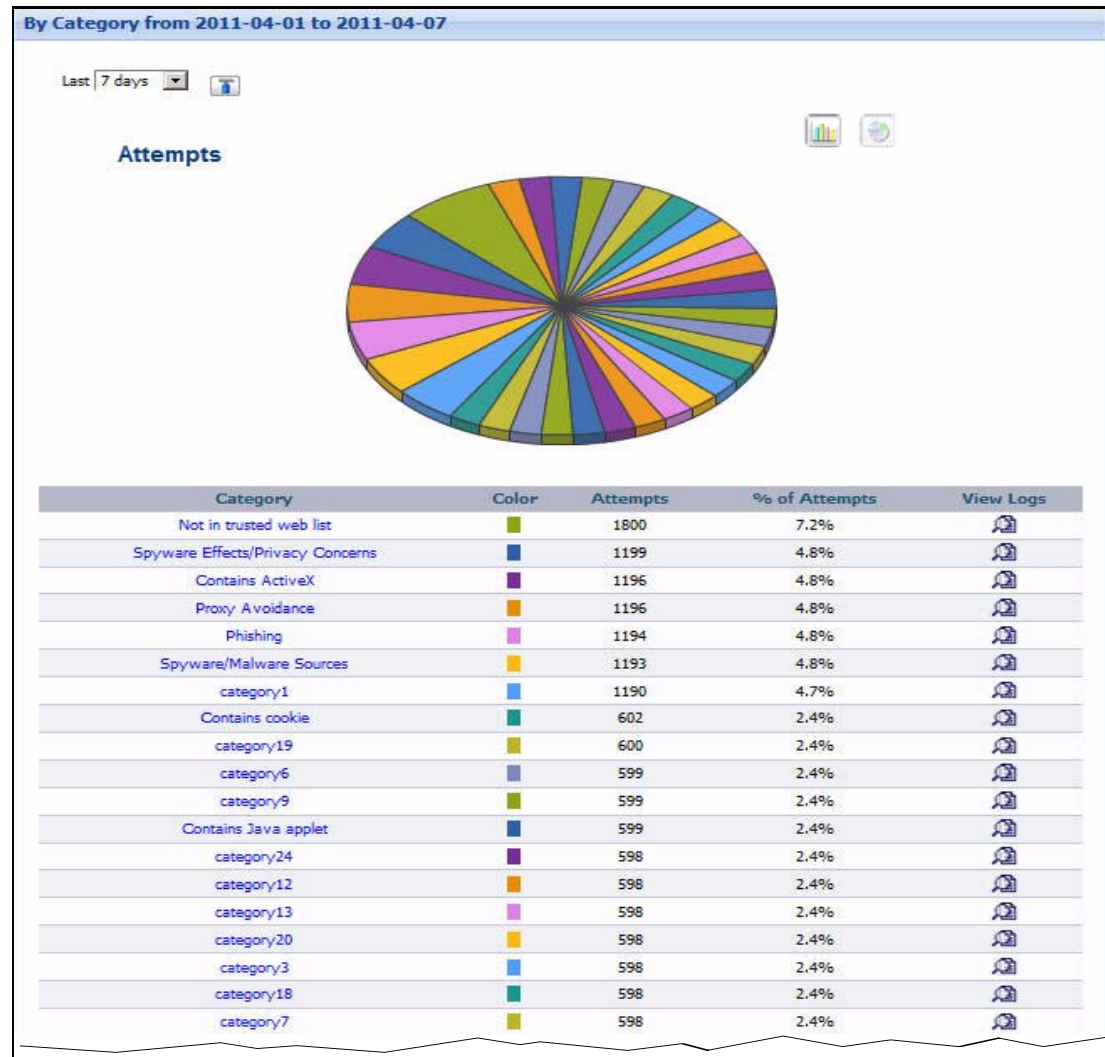
10.3.9 Blocked Web Categories

Use this report to look at the categories of blocked web traffic.

Note: To look at security policy reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Blocked Web Sites** is enabled.

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > By Category** to open this screen.

Figure 226 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category



Each field is described in the following table.

Table 210 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category

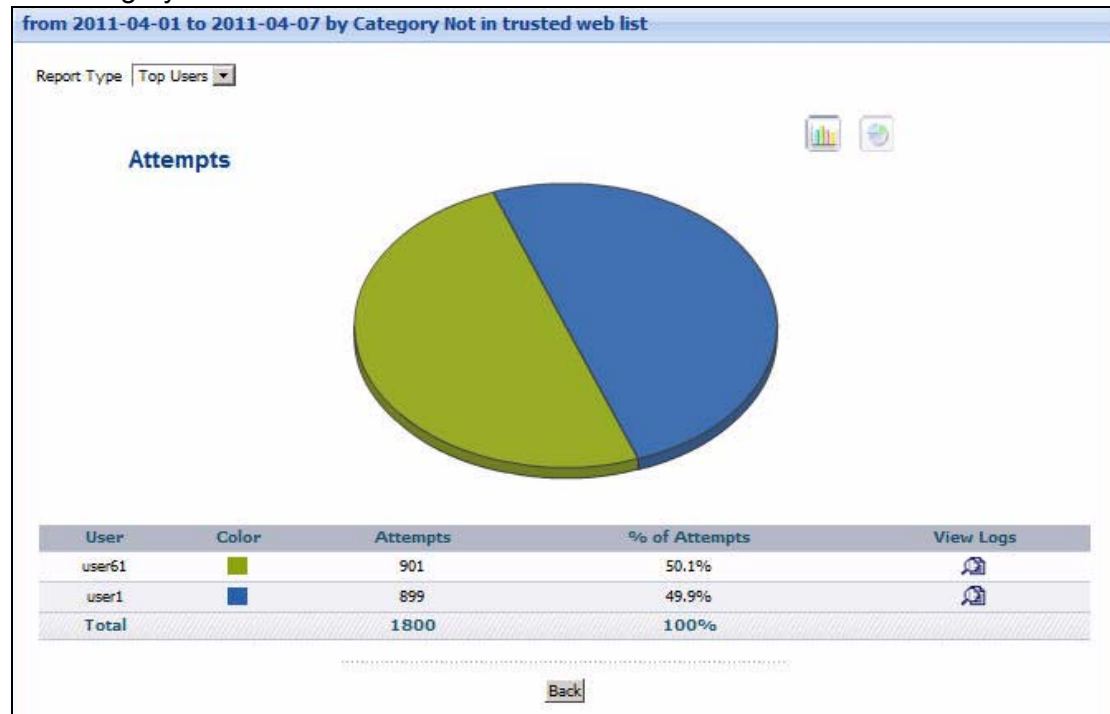
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access allowed web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

10.3.10 Blocked Web Categories Drill-Down

Use this report to look at the destinations for any category of blocked web traffic.

Click on a specific category in **Report > Security Policy Enforcement > Content Filter (Blocked) > By Category** to open this screen.

Figure 227 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category > Drill-Down



Each field is described in the following table.

Table 211 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the Last Days or Settings fields.
Report Type	Specify Top Users , Top Sites , Top Hosts or By Hour as the content to be displayed.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 211 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category > Drill-Down

LABEL	DESCRIPTION
Site	This field displays the destinations of blocked web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts to each destination in the selected category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites in the selected category went to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.
Back	Click this to return to the main report.

10.4 Application Access Control

These screens display the most-often blocked applications.

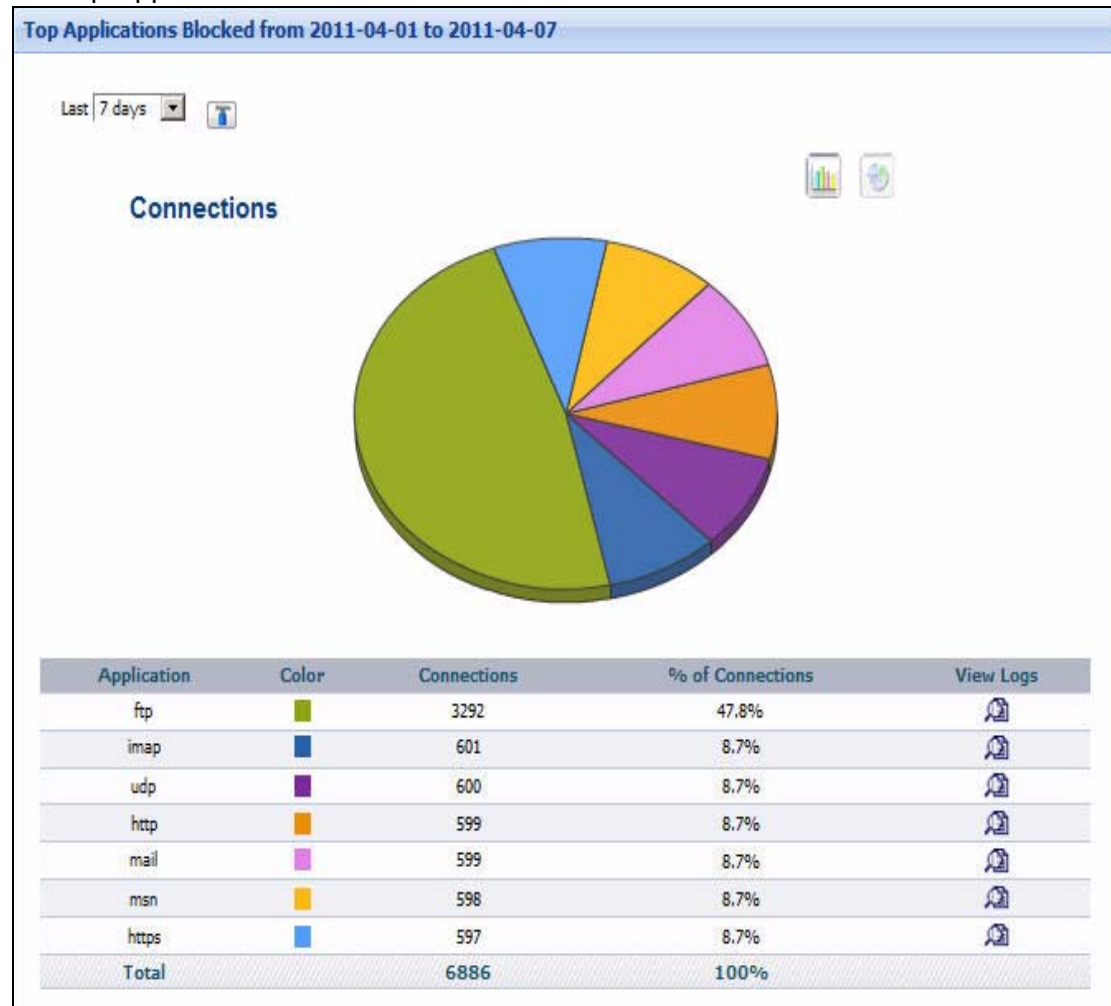
Note: To look at application access control reports, each ZyXEL device must record allowed applications and blocked applications and users in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Application Patrol** is enabled.

10.4.1 Top Applications Blocked

Use this report to look at the applications for which the device blocked the most connections.

Click **Report > Security Policy Enforcement > Application Access Control > Top Applications Blocked** to open this screen.

Figure 228 Report > Security Policy Enforcement > Application Access Control > Top Applications Blocked



Each field is described in the following table.

Table 212 Report > Security Policy Enforcement > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields. It does not include the Direction you select.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Application field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 212 Report > Security Policy Enforcement > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
Application	This field displays the name of the application for which the selected device blocked the most traffic, sorted by the amount of traffic for each one. If the number of applications is less than the maximum number of records displayed in this table, every application is displayed.
Color	This field displays what color represents each application in the graph.
Connections	This field displays the number of traffic events the device blocked for each application.
% of Connections	This field displays what percentage each application's number of blocked connections makes out of the total number of blocked connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the applications above.

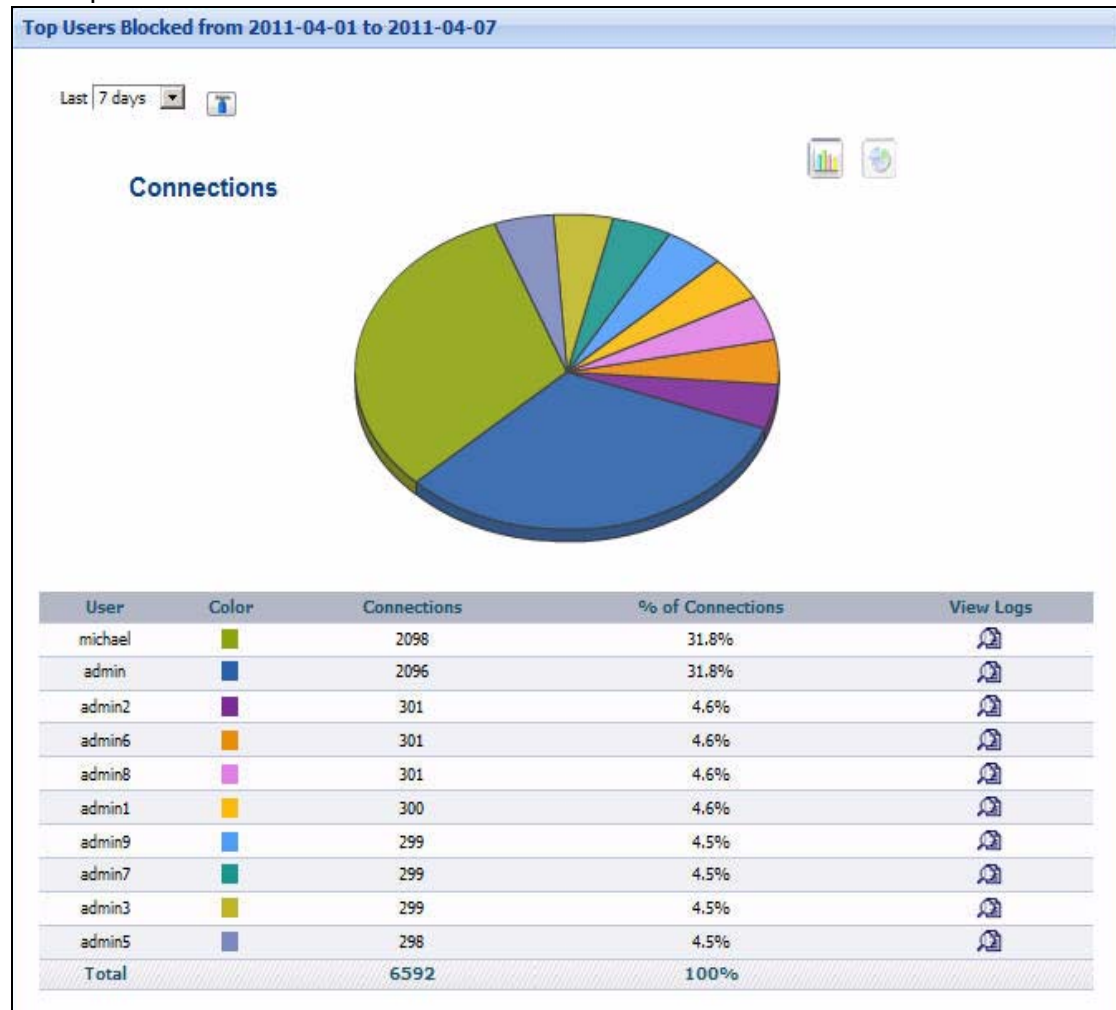
10.4.2 Top Users Blocked

Use this report to look at the users for which the device blocked the most connections.

Note: To look at security policy reports, each ZyXEL device must record users blocked by the application patrol in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Application Patrol** is enabled.

Click **Report > Security Policy Enforcement > Application Access Control > Top Users Blocked** to open this screen.

Figure 229 Report > Security Policy Enforcement > Application Access Control > Top Users Blocked



Each field is described in the following table.

Table 213 Report > Security Policy Enforcement > Application Access Control > Top Users Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields. It does not include the Direction you select.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 213 Report > Security Policy Enforcement > Application Access Control > Top Users Blocked

LABEL	DESCRIPTION
User	This field displays the users from which the selected device's application patrol blocked the most traffic, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Connections	This field displays the number of traffic events the device blocked for each user.
% of Connections	This field displays what percentage each user's number of blocked connections makes out of the total number of blocked connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

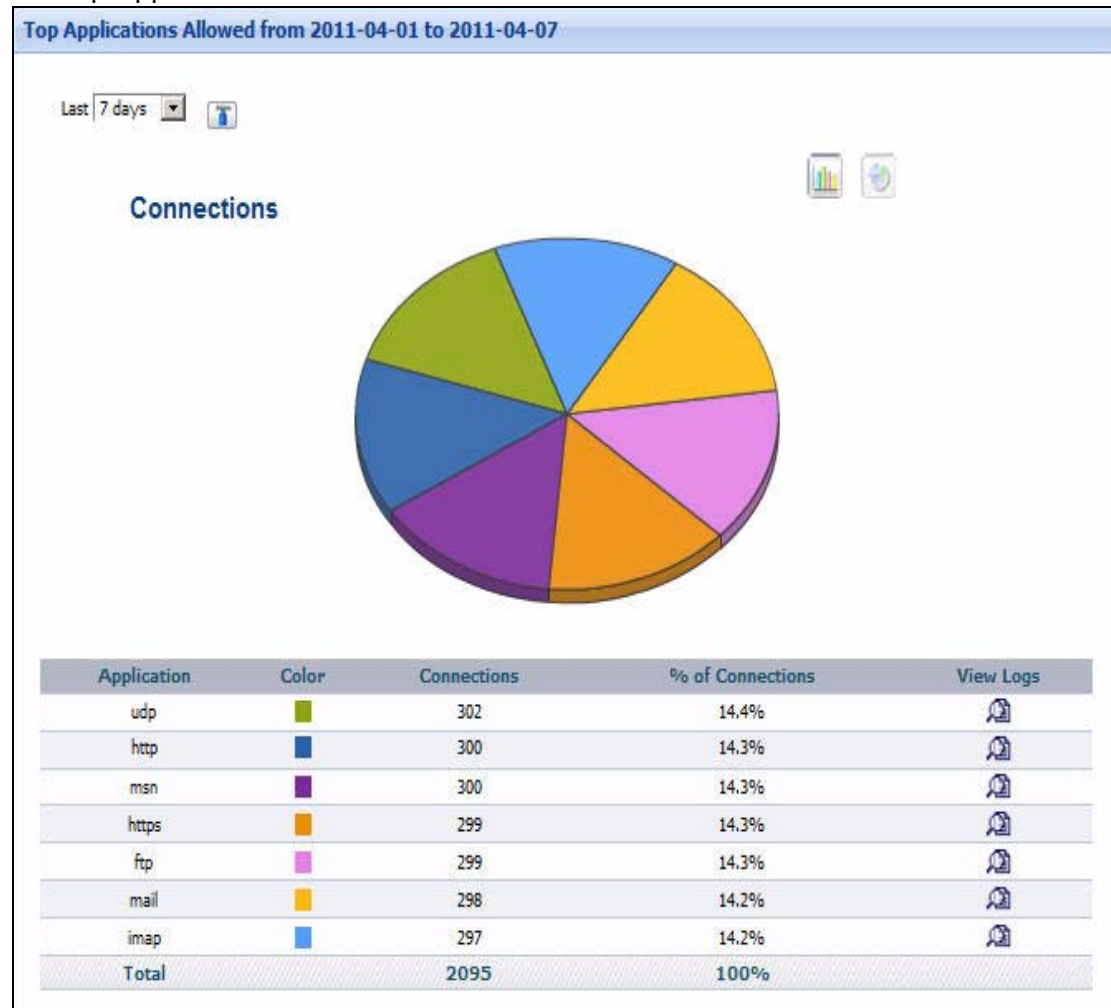
10.4.3 Top Applications Allowed

Use this report to look at the applications for which the device allowed the most connections.

Note: To look at security policy reports, each ZyXEL device must record forwarded applications in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Application Patrol** is enabled.

Click **Report > Security Policy Enforcement > Application Access Control > Top Applications Allowed** to open this screen.

Figure 230 Report > Security Policy Enforcement > Application Access Control > Top Applications Allowed



Each field is described in the following table.

Table 214 Report > Security Policy Enforcement > Application Access Control > Top Applications Allowed

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields. It does not include the Direction you select.
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Application field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the name of the application for which the selected device permitted connections, sorted by the number of connections for each one.

Table 214 Report > Security Policy Enforcement > Application Access Control > Top Applications Allowed

LABEL	DESCRIPTION
Color	This field displays what color represents each application in the graph.
Connections	This field displays the number of connections the application patrol allowed for each application.
% of Connections	This field displays what percentage each application's number of allowed connections makes out of the total number of allowed connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the application rules above.

This chapter discusses how you can check who successfully logged into the ZyXEL device or who tried to log in but failed.

11.1 Successful Logins

Use this screen to look at who successfully logged into the ZyXEL device. See [Section 2.6 on page 27](#) for more information about the source data used by the report.

Note: To use the authentication screens, each ZyXEL device must record authentication successes and failures in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **System Maintenance** is enabled.

Click **Report > Event > Login > Successful Login** to open the **Successful Login** screen.

Figure 231 Report > Event > Login > Successful Login

Successful Login from 2011-04-01 to 2011-04-07					
Login Type: Device Login Logs per Page: 10 Last 7 days					
Time	Login User	Login Type	Source IP	Action	Usage Time(Minute)
2011-04-01 18:46:21	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:21	Admin	console	10.1.1.5	login	
2011-04-01 18:46:20	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:20	Admin	console	10.1.1.5	login	
2011-04-01 18:46:19	Admin	console	10.1.1.5	login	
2011-04-01 18:46:18	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:18	Admin	console	10.1.1.5	login	
2011-04-01 18:46:17	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:17	Admin	console	10.1.1.5	login	
2011-04-01 18:46:16	Admin	ssh	10.1.1.5	login	
Total Count:6574 Total Page:658 First 1 2 3 4 5 6 7 8 9 10 Last Go					

Each field is described in the following table.

Table 215 Report > Event > Login > Successful Login

LABEL	DESCRIPTION
Login Type	Select Device Login to display a list of successful management logins to the ZyXEL device. Select UserAware Login to display a list of successful user logins to the ZyXEL device (to use the ZyXEL device's features such as Internet access or Secure Remote Access tunnels). This field is not available with all models.
Last ... Days	Select how many more days of information, ending with current information today, you want to look at. Select 1 if you only want to look at today's information.
Settings	Click this if you want to specify the select any Start Date and End Date. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. The Login Type field is the same as in the main screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user logged into the device.
Login User	This field displays who logged into the selected device.
Login Type	This field displays what type of connection the user used to log into the device.
Source IP	This field displays the IP address of the computer the user used to log into the selected device.
Action	This field displays if it is a login or logout operation.
Usage Time (Minute)	This field displays the time that elapses between the login and logout operation.
Total Count	This field displays how many records there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the records.

Table 215 Report > Event > Login > Successful Login

LABEL	DESCRIPTION
First .. Last	Click First , Last , or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .

11.2 Failed Logins

Use this screen to look at who tried to log in into the ZyXEL device (for management or monitoring purposes) but failed. See [Section 2.6 on page 27](#) for more information about the source data used by the report.

Note: To use the authentication screens, each ZyXEL device must record authentication successes and failures in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **System Maintenance** is enabled.

Click **Report > Event > Login > Failed Login** to open the **Failed Login** screen.

Figure 232 Report > Event > Login > Failed Login

Figure 2-22 Report Event Login Failed Login

Failed Login from 2011-04-05 to 2011-04-11

Logs per Page: 10 Last 7 days

Time	Login User	Login Type	Source IP
2011-04-08 15:02:46	admin	TELNET	192.168.1.33
2011-04-08 15:02:46	admin	FTP	192.168.1.33
2011-04-08 15:02:46	admin	WEB	192.168.1.33
2011-04-08 15:02:46	admin	WEB	192.168.1.33
2011-04-08 15:02:46	admin	SMT	192.168.1.33
2011-04-08 15:02:46	admin	FTP	192.168.1.33
2011-04-08 15:02:46	admin	TELNET	192.168.1.33
2011-04-08 15:02:46	admin	SMT	192.168.1.33
2011-04-08 15:02:46	admin	WEB	192.168.1.33
2011-04-08 15:02:46	admin	TELNET	192.168.1.33

Total Count:528 Total Page:53 First 1 2 3 4 5 6 7 8 9 10 Last Go

Each field is described in the following table.

Table 216 Report > Event > Device Login > Failed Login

LABEL	DESCRIPTION
Last ... Days	Select how many more days of information, ending with current information today, you want to look at. Select 1 if you only want to look at today's information.
Settings	Click this if you want to specify the select any Start Date and End Date . The Report Display Settings screen appears.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user tried unsuccessfully to log into the device.
Login User	This field displays who tried unsuccessfully to log into the selected device.
Login Type	This field displays what type of connection the user unsuccessfully tried to use to log into the device.
Source IP	This field displays the IP address of the computer the user used to try to log into the selected device.
Total Count	This field displays how many records there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the records.
First .. Last	Click First , Last , or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .

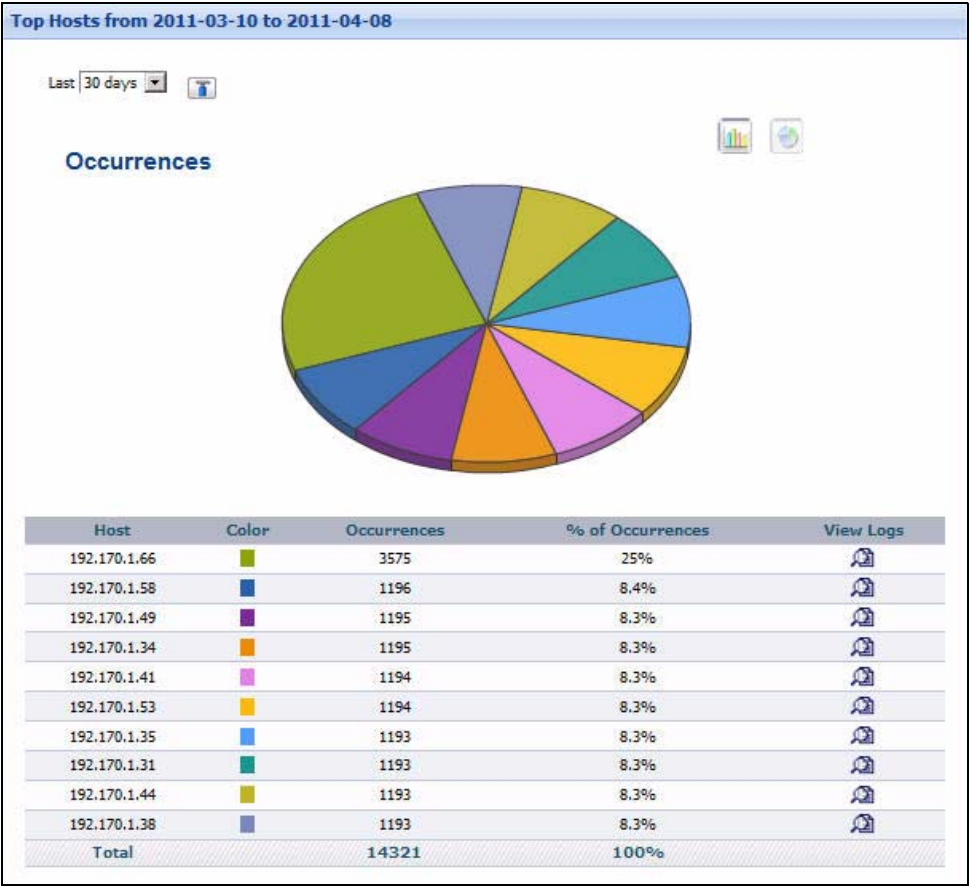
11.3 Top Sessions Per Host

Use this screen to see which hosts have most frequently gone over the maximum number of NAT sessions per host.

Note: To use this screen, the ZyXEL device must record instances of hosts exceeding the maximum number of NAT sessions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **System Maintenance** is enabled.

Click **Report > Event > Session Per Host > Top Hosts** to open this screen.

Figure 233 Report > Event > Session Per Host > Top Hosts



Each field is described in the following table.

Table 217 Report > Event > Session Per Host > Top Hosts

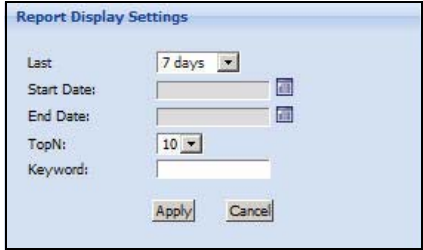
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the Host field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.

Table 217 Report > Event > Session Per Host > Top Hosts (continued)

LABEL	DESCRIPTION
Host	This field displays the top sources that have gone over the selected device's maximum number of NAT sessions per host, sorted by the number of occurrences for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If Hostname Reverse is enabled in System > General Configuration , the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of times each source has gone over the selected device's maximum number of NAT sessions per host.
% of Occurrences	This field displays what percentage each source's number of times it has exceeded the selected device's maximum number of NAT sessions per host makes out of the total number of times that it has occurred within the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

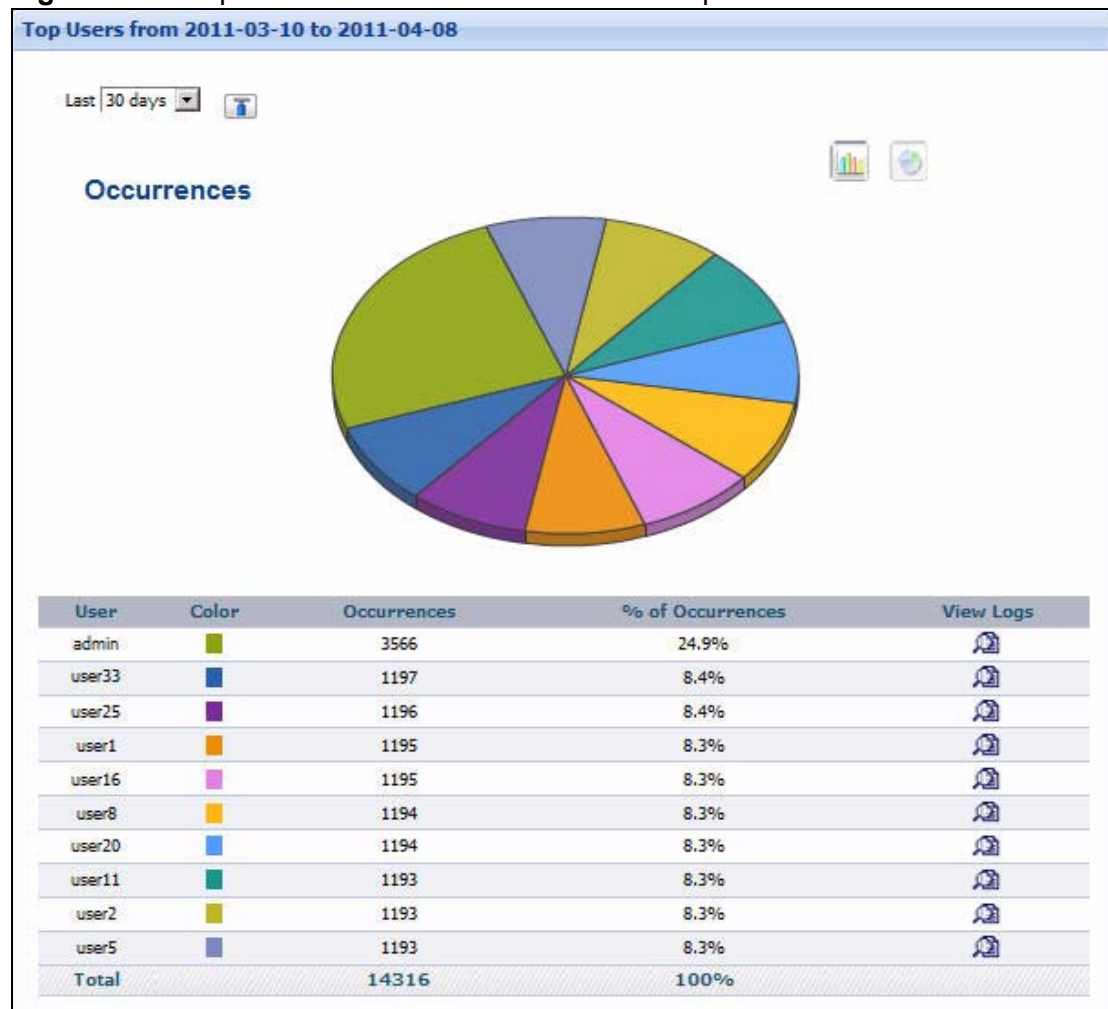
11.4 Top Sessions Per User

Use this screen to see which users have most frequently gone over the maximum number of NAT sessions per host.

Note: To use this screen, the ZyXEL device must record instances of users exceeding the maximum number of NAT sessions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **System Maintenance** is enabled.

Click **Report > Event > Session Per Host > Top Users** to open this screen.

Figure 234 Report > Event > Session Per Host > Top Users



Each field is described in the following table.

Table 218 Report > Event > Session Per Host > Top Users

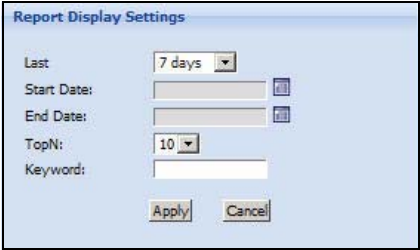
LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears.  Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes. TopN: select the number of records that you want to display. For example, select 10 to display the first 10 records. Keyword: enter part or all of any value you want to look for in the User field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. - Click the Pie View or the Bar View icon. You can specify the Default Chart Type in System > General Configuration. - Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. - Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users that have gone over the selected device's maximum number of NAT sessions per host, sorted by the number of occurrences for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.

Table 218 Report > Event > Session Per Host > Top Users (continued)

LABEL	DESCRIPTION
Color	This field displays what color represents each user in the graph.
Occurrences	This field displays the number of times each user has gone over the selected device's maximum number of NAT sessions per host.
% of Occurrences	This field displays what percentage each user's number of times it has exceeded the selected device's maximum number of NAT sessions per host makes out of the total number of times that it has occurred within the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

Schedule Report

This chapter discusses how you can use the **Report > Schedule Report** screen to set up and maintain daily, weekly, and one-time reports that Vantage Report sends by e-mail. See [Section 2.2 on page 24](#) for more information about e-mail in Vantage Report. Use the template screens to add and edit report templates.

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See [Section 14.2 on page 554](#) for more information.

Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves three days of information, weekly reports only consist of information from these three days, not seven days. See [Section 14.1 on page 549](#) for more information.

This feature can send e-mail messages with very large attachments (2+ MB). Some SMTP mail servers might not accept such large messages. In this case, there is a way to send e-mail messages without the attachments. See the **E-mail Attached Files** option in any of the **Customize ... Report** screens for more information. If you do not have Vantage Report send the attachments you can still view the reports. The Vantage Report server backs up all scheduled reports in the <vrpt_home>\vrpt\data\scheduler folder.

12.1 Scheduled Report Summary Screen

Use this screen to see the list of existing scheduled reports. Use the **Add** button to create new reports.

Click **Report > Schedule Report > Summary**. The following screen appears.

Figure 235 Report > Schedule Report > Summary

#	Index	To E-mail Address	E-mail Subject	Task Type
Total Count:0 Total Page:0 First Last Go				

Each field is described in the following table.

Table 219 Report > Schedule Report > Summary

LABEL	DESCRIPTION
#	Select this check box, and click Delete to delete the scheduled report.
Index	Click it to edit the scheduled report next to it. The Customize Scheduled Report screen appears. Otherwise, this field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
To E-mail Address	This field displays the first e-mail address to which the scheduled report is sent. If there are more, this field displays a couple of punctuation marks at the end.
E-mail Subject	This field displays the subject line in the e-mail message Vantage Report sends.
Task Type	This field displays what type of scheduled report this is.
Total Count	This field displays how many scheduled reports there are.
Total Page	This field displays how many screens it takes to display all the scheduled reports.
First .. Last	Click First , Last , or a specific page number to look at the scheduled reports on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .
Add	Click this to generate and send one or more statistical reports daily, weekly or in a time interval. The Customize Scheduled Report screen appears.
Delete	Click this to delete the selected scheduled report.

12.2 Customize Daily Report Screen

Use this screen to configure the Vantage Report to maintain and send daily reports.

Click **Report > Schedule Report > Summary**. Either click on the index number of the entry you want to edit or click **Add**. Choose **Daily Report** in the **Report Type**. The following screen appears.

Figure 236 Report > Schedule Report > Summary > Add (Daily Report)

Customize Daily Report

Report Type: Daily Report Add

* Destination E-mail Address: Remove

* E-mail Subject:

* E-mail Body:

☒ E-mail Attached Files ☐ Apply Template ZyXEL

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler
(Please find the attached file under this folder if the mail is too large to be delivered)

Format Report ☐ HTML ☐ PDF ☐ CSV(CSV does not support monitor feature)

☐ Include All Data in a Single Report (for PDF and CSV)

Report Time: 00:00

Report List

Load From Template Save To Template

Monitor > Hardware Status > CPU & Memory

☐ CPU Usage ☐ Memory Usage

Monitor > Network Traffic > Session Usage

☐ Session Usage

Monitor > Network Traffic > Bandwidth > Port Usage

☐ Port Usage

Port: Port1 Direction: Tx+Rx Add Delete

Monitor > Network Traffic > Bandwidth > Interface Usage

☐ Interface Usage

Interface Type: Ethernet Interface Name: wan1 Direction: Tx+Rx Add Delete

Monitor > Network Traffic > Web & FTP & Mail

☐ WEB ☐ FTP ☐ MAIL

Monitor > Secure Remote Access

☐ IPSec VPN ☐ SSL VPN

Monitor > Network Security > Attack & IDP & AntiVirus

☐ Attack ☐ Intrusion ☐ AntiVirus

Monitor > E-Mail Security > AntiVirus & AntiSpam & IDP

☐ AntiVirus ☐ AntiSpam ☐ Intrusion

Monitor > Web Security > Content Filter & AntiVirus & IDP

☐ Content Filter ☐ AntiVirus ☐ Intrusion

Monitor > Security Policy Enforcement > Firewall Access Control & App Patrol

☐ Firewall Access Control ☐ App Patrol

Network Traffic > Bandwidth

☐ Summary Interface:

☐ Top Protocols Direction:

☐ Top Hosts Sorting By:

☐ Top Users TopN:

☐ Top Destinations

Network Traffic > Web

☐ Top Sites Sorting By:

☐ Top Hosts TopN:

☐ Top Users

Network Traffic > FTP

☐ Top Sites Sorting By:

☐ Top Hosts TopN:

☐ Top Users

Network Traffic > Mail

☐ Top Sites

Sorting By: MBytes Transferred

☐ Top Hosts

TopN: 10

☐ Top Users

Add

Delete

Network Traffic > Customization

☐ Top Destinations

Customized Service: rtmp(udp:1)

☐ Top Sources

Sorting By: MBytes Transferred

☐ Top Users

TopN: 10

Add

Delete

Secure Remote Access > Site-to-Site(IPSec)

☐ Top Sites

Site: ALL

☐ Top Tunnels

Tunnel: ALL

☐ Top Protocols

Direction: Both

☐ Top Hosts

Sorting By: MBytes Transferred

☐ Top Users

TopN: 10

☐ Top Destinations

Add

Delete

Secure Remote Access > Client-to-Site(IPSec)

☐ Top Protocols

User: ALL

☐ Top Destinations

Direction: Both

☐ Top Users

Sorting By: MBytes Transferred

TopN: 10

Add

Delete

Secure Remote Access > Client-to-Site(SSL)

☐ Top Protocols

User: ALL

☐ Top Destinations

Direction: Both

☐ Top Applications

Sorting By: MBytes Transferred

☐ Top Users

TopN: 10

Add

Delete

Network Security > Attack

☐ Summary

☐ Top Attacks

TopN: 10

☐ Top Sources

☐ By Type

Network Security > IDP

- ☐ Summary
- ☐ Top Intrusions
- ☐ Top Sources TopN: 10
- ☐ Top Destinations
- ☐ By Severity

Network Security > AntiVirus

- ☐ Summary
- ☐ Top Viruses TopN: 10
- ☐ Top Sources
- ☐ Top Destinations

E-Mail Security > AntiVirus

- ☐ Summary
- ☐ Top Viruses TopN: 10
- ☐ Top Sources
- ☐ Top Destinations

E-Mail Security > AntiSpam

- ☐ Summary
- ☐ Top Senders TopN: 10
- ☐ Top Sources

E-Mail Security > IDP

- ☐ Summary
- ☐ Top Intrusions
- ☐ Top Sources TopN: 10
- ☐ Top Destinations
- ☐ By Severity

Web Security > Content Filter

- ☐ Summary
- ☐ Top Sites
- ☐ Top Hosts TopN: 10
- ☐ Top Users
- ☐ By Category

Web Security > AntiVirus

☐ Summary

☐ Top Viruses TopN: 10

☐ Top Sources

☐ Top Destinations

Web Security > IDP

☐ Summary

☐ Top Intrusions

☐ Top Sources TopN: 10

☐ Top Destinations

☐ By Severity

Security Policy Enforcement > Firewall Access Control

☐ Top Users Blocked TopN: 10

☐ Top Packets Blocked

Security Policy Enforcement > Content Filter(All)

☐ Summary

☐ Top Sites

☐ Top Hosts TopN: 10

☐ Top Users

☐ By Category

Security Policy Enforcement > Content Filter(Blocked)

☐ Summary

☐ Top Sites

☐ Top Hosts TopN: 10

☐ Top Users

☐ By Category

Security Policy Enforcement > Application Access Control

☐ Top Applications Blocked

☐ Top Users Blocked TopN: 10

☐ Top Applications Allowed

Event > Session Per Host

☐ Top Hosts TopN: 10

☐ Top Users

☐ Select All

Apply Reset Cancel

Each field is described in the following table.

Table 220 Report > Schedule Report > Summary > Add

LABEL	DESCRIPTION
Report Type	Choose Daily Report in this field.
Add	Enter the e-mail address(es) to which Vantage Report sends the selected report(s). Use a comma to separate each e-mail address and click Add. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Destination E-mail Address	The list of e-mail addresses you enter appears here. Select one and click Remove to delete that e-mail address from the list.
E-mail Subject	Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
E-mail Body	Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long.
E-mail Attached Files	Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. These report(s) are stored in <code>data\scheduler</code> in the Vantage Report installation directory.
Apply Template	Select the check box and a template if you want to use a customized report format.
Save Directory	This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is.
Format Report	Select the format(s) of the selected report(s). HTML format looks like the statistical reports you can see online.
Include All Data in a Single Report	This field is enabled if you selected PDF format. Select this if you want to combine all the selected report(s) into one file.
Report Time	Select the hour to start generating the report. Vantage Report sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having Vantage Report generate too many reports at the same time can affect performance. It is recommended that you vary the times for your reports.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the Select All check box at the bottom to select every report.

Table 220 Report > Schedule Report > Summary > Add

LABEL	DESCRIPTION
Load From Template	Click this to select a preconfigured template for a scheduled report.
Save To Template	Click this to save the daily report configuration as a template for future use.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.3 Customize Weekly Report Screen

Use this screen to configure the Vantage Report to maintain and send weekly reports.

Click **Report > Schedule Report > Summary**. Either click on the index number of the entry you want to edit or click **Add**. Choose **Weekly Report** in the **Report Type**. The following screen appears.

Figure 237 Report > Schedule Report > Summary > Add (Weekly Report)

Customize Weekly Report

Report Type: Weekly Report

* Destination E-mail Address:

* E-mail Subject:

* E-mail Body:

☒ E-mail Attached Files ☐ Apply Template ZyXEL

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler
(Please find the attached file under this folder if the mail is too large to be delivered)

Format Report ☐ HTML ☐ PDF ☐ CSV(CSV does not support monitor feature)

☐ Include All Data in a Single Report (for PDF and CSV)

Day to Submit: Sunday

Report List

Load From Template

Each field is described in the following table.

Table 221 Report > Schedule Report > Summary > Add (Weekly Report)

LABEL	DESCRIPTION
Report Type	Choose Weekly Report in this field.
Add	Enter the e-mail address(es) to which Vantage Report sends the selected report(s) and click Add. Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Destination E-mail Address	The list of e-mail addresses you enter appear here. Select one and click Remove to delete that e-mail address from the list.
E-mail Subject	Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
E-mail Body	Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long.
E-mail Attached Files	Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. These report(s) are stored in <code>data\scheduler</code> in the Vantage Report installation directory.
Apply Template	Select the check box and a template if you want to use a customized report format.
Save Directory	This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is.
Day to Submit	Select the day of the week to generate and send the selected report(s).
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the Select All check box at the bottom to select every report. Refer to Figure 236 on page 512 for the full view of Report List.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.4 Customize Overtime Report Screen

Use this screen to configure the Vantage Report to maintain and send reports during a specified period of time.

Click **Report > Schedule Report > Summary**. Either click on the index number of the entry you want to edit or click **Add**. Choose **Overtime Report** in the **Report Type**. The following screen appears.

Figure 238 Report > Schedule Report > Summary > Add (Overtime Report)

Each field is described in the following table.

Table 222 Report > Schedule Report > Summary > Add (Overtime Report)

LABEL	DESCRIPTION
Report Type	Choose Overtime Report in this field.
Add	Enter the e-mail address(es) to which Vantage Report sends the selected report(s) and click Add. Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Destination E-mail Address	The list of e-mail addresses you enter appear here. Select one and click Remove to delete that e-mail address from the list.

Table 222 Report > Schedule Report > Summary > Add (Overtime Report)

LABEL	DESCRIPTION
E-mail Subject	Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
E-mail Body	Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long.
E-mail Attached Files	Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. These report(s) are stored in <code>data\scheduler</code> in the Vantage Report installation directory.
Apply Template	Select the check box and a template if you want to use a customized report format.
Save Directory	This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is.
Start Date	Select the day to start collecting information for the selected report(s).
End Date	Select the day to stop collecting information for the selected report(s).
Start Time	Select the hour to start collecting information for the selected report(s). Vantage Report starts collecting information at the beginning of this hour.
End Time	Select the hour to stop collecting information for the selected report(s). Vantage Report stops collecting information at the end of this hour and generates the report. Vantage Report sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having Vantage Report generate too many reports at the same time can affect performance.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the Select All check box at the bottom to select every report. Refer to Figure 236 on page 512 for the full view of Report List.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.5 Configure Template List

Use this screen to see a list of report templates that provides what kind of details are available in reports.

Click **Report > Schedule Report > Configure Template** to open the **Configure Template List** screen.

Figure 239 Report > Schedule Report > Configure Template

#	Index	Name	Device Type	Note
Total Count:0 Total Page:0 First Last Go				
Add Delete				

Each field is described in the following table.

Table 223 Report > Schedule Report > Configure Template

LABEL	DESCRIPTION
#	Select this check box, and click Delete to delete the report template.
Index	This is the number of this template in the list. This field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
Name	This is the name that identifies the template inside Vantage Report. Click it to edit the template.
Device Type	This field displays which device this template can be generated for.
Note	This is a short description of the template.
Total Count	This field displays how many report templates there are.
Total Page	This field displays how many screens it takes to display all the scheduled reports.
First .. Last	Click First , Last , or a specific page number to look at the scheduled reports on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click Go .
Add	Click this to go to another screen to create a new report template.
Delete	Select the check box next to a template and click delete to remove the report template.

12.6 Template Add/Edit

Use this screen to customize a scheduled report template for a particular ZyXEL Device.

To access this screen, click **Add** in the **Report > Schedule Report > Configure Template** screen.

Figure 240 Report > Schedule Report > Configure Template > Add

Each field is described in the following table.

Table 224 Report > Schedule Report > Configure Template > Add

LABEL	DESCRIPTION
Name	Enter a name to identify the template inside Vantage Report. Numbers (0-9), letters (a-zA-Z), periods (.) and the underscore (_) are allowed. Spaces are not allowed. The name must start with a number or letter. Use up to 28 characters.
Device Type	Select the ZyXEL Device you would like to associate with the scheduled report template.
Note	Write a short description to identify the scheduled report template.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the Select All check box at the bottom to select every report. Refer to Figure 236 on page 512 for the full view of Report List.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.7 Logo Template

Use this screen to see the list of existing logo templates.

Click **Report > Schedule Report > Logo Template** to open the **Schedule Report Template List** screen.

Figure 241 Report > Schedule Report > Logo Template

The screenshot shows a web interface titled "Template List". It contains a table with the following columns: #, Index, Template Name, Template Title, and Sample Report. There is one row of data with the following values: a checkbox, the index "1", the name "ZyXEL", the title "ZyXEL Communications Corp.", and a "Download" button. Below the table, there is a summary line: "Total Count:1 Total Page:1 First 1 Last" followed by a "Go" button. At the bottom of the interface are two buttons: "Add" and "Delete".

#	Index	Template Name	Template Title	Sample Report
☐	1	ZyXEL	ZyXEL Communications Corp.	Download

Total Count:1 Total Page:1 First 1 Last [Go](#)

[Add](#) [Delete](#)

Each field is described in the following table.

Table 225 Report > Schedule Report > Logo Template

LABEL	DESCRIPTION
#	Select this check box, and click Delete to delete the report template.
Index	This is the number of this template in the list. This field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
Template Name	This is the name that identifies the template inside Vantage Report. Click it to edit the template.
Template Title	This field displays the title that appears at the top of the reports generated using this template.
Sample Report	Click the Download button to save a sample file using the report template to your computer.
Total Count	This field displays how many report templates there are.
Total Page	This field displays how many screens it takes to display all the scheduled reports.
First .. Last	Click First , Last , or a specific page number to look at the scheduled reports on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click Go .
Add	Click this to go to another screen to create a new report template.
Delete	Select the check box next to a template and click delete to remove the report template.

12.8 Logo Template Add/Edit

Use this screen to add or edit logo templates.

To access this screen, click **Add** in the **Report > Schedule Report > Logo Template** screen.

Figure 242 Report > Schedule Report > Logo Template > Add

Template View

PDF Template

Sample Logo

2006-07-19 16:00:00 to 2006-07-21 16:00:00

Sample Report Title

Network Attack > Attack > Top Attacks

Top Attacks from 2006-07-19 16 to 2006-07-21 16

Device Name : example device
MAC: 00A0C5000000

Attacks

Graphical Report

Attack	Color	Attacks	% of Attacks
land TCP	Blue	50	50%
land ICMP	Orange	30	30%
syn_flood TCP	Purple	20	20%
Total		100	100%

Report Data

2006-07-21 16:29:05

Template Configuration

Template Name:

Template Title:

Template Logo:

(The logo that is size of 110 x 30 and has white background is recommended.)

Each field is described in the following table.

Table 226 Report > Schedule Report > Logo Template > Add

LABEL	DESCRIPTION
Template View	This section of the screen displays a sample of the report layout.
PDF Template	Click this button to view a sample of a report in PDF format.
Template Configuration	Use this section of the screen to configure the template's name and the report title and upload a logo to display on the reports.

Table 226 Report > Schedule Report > Logo Template > Add

LABEL	DESCRIPTION
Template Name	Enter a name to identify the template inside Vantage Report. Numbers (0-9), letters (a-z, A-Z), periods (.) and the underscore (_) are allowed. Spaces are not allowed. The name must start with a number or letter. Use up to 28 characters.
Template Title	Enter the title that you want to appear at the top of the reports generated using this template. Use up to 50 ASCII characters. Spaces are allowed.
Template Logo	Type the location of the file that you want to display as the logo in the report or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. The template logo file must be .gif or .jpg.
Apply	Click this to save your settings and close the screen.
Cancel	Click this to close the screen without saving any changes.

Logs

These screens provide information for all log entries for devices being monitored by Vantage Report.

Note: The logs screens, fields and menus can vary according to which device the logs are collected for.

Vantage Report consolidates log entries. See [Appendix A on page 589](#) for Vantage Report's internal log consolidation frequency. See [Appendix C on page 645](#) and [Appendix B on page 599](#) for information on the logs.

13.1 Log Viewer

Use this screen to view logs that devices send to Vantage Report.

Click **Logs > Log Viewer > All Logs** to look at all log entries. The screen is shown next.

See [Section 2.3 on page 25](#) for more information about update frequencies for log entries. See [Section 2.6 on page 27](#) for more information about the source data used by the report.

Figure 243 Logs > Log Viewer > All Logs

The screenshot shows the Log Viewer interface with the following sections:

- Search Filters:**
 - Day: 2011-04-08
 - Start Time: 00:00, End Time: 24:00
 - Start Date: 2011-04-01, End Date: 2011-04-08
 - Category: All Categories
 - Severity: All
 - Logs per Page: 10
 - Reverse DNS: ☐
- Advanced Search:**
 - ☒ Advanced Search
 - Source IP: [text box]
 - Destination IP: [text box]
 - Keyword: [text box]
 - User: [text box]
 - Services: [Custom Service]
 - Protocol: All
 - Port: [text box]
- Buttons:** Search, Reset, Export
- Log Entries Table:**

Time	Source:Port	Destination:Port	User	Severity	Category	Message	Note
2011-04-01 18:48:54	192.168.1.20:1505	192.170.1.34:110	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:54	192.168.1.20:1505	192.170.1.33:25	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.20:1505	192.170.1.32:80	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.20:1505	192.170.1.31:53	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.60:443	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.59:443	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.58:443	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.57:443	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.56:443	lam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.55:443	lam	Info	Traffic Log	Traffic Log	Traffic Log
- Footer:** Total Count:774,739 Total Page:77,474 First 1 2 3 4 5 6 7 8 9 10 Last Go

The fields in the first three rows (and **Search** and **Reset**) appear when you open the report. The fields in the next two rows (above **Search**, **Reset** and **Export**) appear if you do not select **All Categories** in the **Category** field and select **Advanced Search**. The table of log entries appears after you click **Search**, even if there are no log entries for your search criteria. Each field is described in the following table.

Table 227 Logs > Log Viewer > All Logs

LABEL	DESCRIPTION
Day	Select this if you want to look at log entries from one day or part of one day. You cannot select a date earlier than the number of previous days that you configured in the System Setting > General Configuration screen. You can also click the Calendar icon to specify the date.
Start Time	Enter the time of the earliest log entries you want to see, if you select Day .

Table 227 Logs > Log Viewer > All Logs

LABEL	DESCRIPTION
End Time	Enter the time of the latest log entries you want to see, if you select Day .
Days	Select this if you want to look at log entries for a specific range of days.
Start Date	This field is enabled and required if you select Days . Enter the date of the earliest log entries you want to see. You cannot enter a date earlier than the number of previous days that you configured in the System Setting > General Configuration screen. You can also click the Calendar icon to specify the date.
End Date	This field is enabled and required if you select Days . Enter the date of the latest log entries you want to see. You cannot enter a date earlier than Start Date or later than today. You can also click the Calendar icon to specify the date.
Category	This field can vary according to which device the logs are collected for. Vantage Report. Select what type of log entries you want to see. You can also select All Categories .
Severity	This field depends on the logs received by Vantage Report from the selected ZyXEL device. Select what type of log entries you want to see. You can also select All . Severity ranking follows RFC 3164 of the SYSLOG protocol and is defined as follows. • Emergent - System is unusable • Alert - Action must be taken immediately • Critical - Critical conditions • Error - Error conditions • Warning - Warning conditions • Notice - Normal but significant condition • Info - Informational messages • Debug - Debug-level messages
Reverse DNS	Select this to display logs with the domain name of hosts instead of their IP addresses. If you select this and Vantage Report does not find the domain name of a host, it will display the IP address. This feature might increase the amount of time it takes to display log entries, however.
Advanced Search	This field is disabled if Category is All Categories . Select this if you want to use other search criteria to look at log entries.
Source IP	Enter the source IP address in the event that generated the log entry.
Services	Select the service whose log entries you want to see. If you select [Custom Service] , you have to specify the Protocol and Port too.
Destination IP	Enter the destination IP address in the event that generated the log entry.
Protocol	This field is enabled if Services is [Custom Service] . Select the protocol whose log entries you want to see.

Table 227 Logs > Log Viewer > All Logs

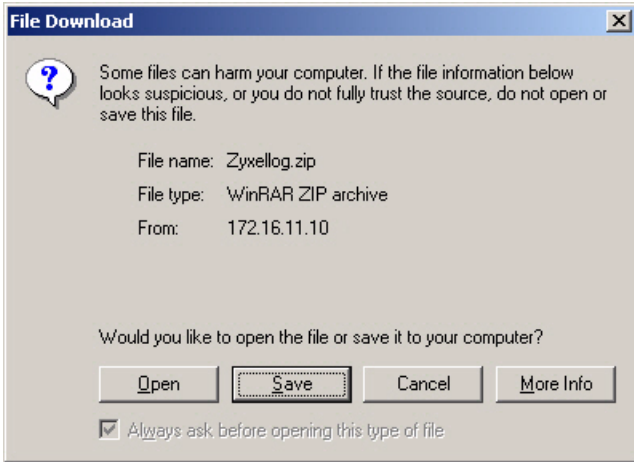
LABEL	DESCRIPTION
Keyword	Enter part or all of any value you want to look for in the Message field. You can use any printable ASCII character. The search is not case-sensitive.
Port	This field is enabled if Services is [Custom Service] . Select the destination port number whose log entries you want to see.
User	Enter a user's name (or part of the name) who is associated with the log entries that you want to see. This field is case insensitive.
Search	Click this to display the log entries based on the current search criteria.
Reset	Click this to set the search criteria to the values they had the last time you clicked Search . If you have not clicked Search yet, the search criteria return to their default values.
Export	This button is available when there are logs that matched your search criteria. Click this to export the results to a zip file. The screen pops up as shown next. Figure 244 Export Logs  • Click Open to open the zip file directly. • Click Save to save the zip file to the computer that you are currently using to access the Vantage Report server, then exit this screen. • Click Cancel to exit this screen without saving any changes. • Click More Info to view an on-line help page about downloading files.
Time	This field displays the time the Vantage Report server received the log entry, not the time the log entry was generated.
Source:Port	This field displays the source IP address and port (if any) of the event that generated the entry.
Destination:Port	This field displays the destination IP address and port (if any) of the event that generated the entry.
Category	This field displays the type of log entry.
Message	This field displays the reason the log entry was generated.
Note	This field displays additional information about the log entry.

Table 227 Logs > Log Viewer > All Logs

LABEL	DESCRIPTION
Total Count	This field displays how many log entries there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the log entries.
First .. Last	Click First , Last , or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .

Note: The following screens are available only to the `root` account or accounts in the 'super' group. Otherwise, these menus are not shown.

13.2 Log Receiver

These screens show the total number of logs that Vantage Report received from all registered devices by day and how many logs Vantage Report processed per second. It also shows the number of logs that Vantage Report received from each device over a selected range of days.

13.2.1 By Day (Summary)

Use this screen to look at the total number of logs that Vantage Report received by day. It also displays how many logs Vantage Report processed per second (on average).

Click **Logs > Log Receiver > By Day (Summary)**. The following screen displays.

Figure 245 Logs > Log Receiver > By Day (Summary)

By Day(Summary)		
Date	Log Number	Average Processing Speed(Logs/sec)
2011-03-30	1800382	20.8
2011-03-31	1842293	21.3
2011-04-01	1562517	18.1
2011-04-02	403770	4.7
2011-04-03	164667	1.9
2011-04-04	163884	1.9
2011-04-05	162597	1.9
2011-04-06	236871	2.7
2011-04-07	236665	2.7
2011-04-08	87658	1.0

Each field is described in the following table.

Table 228 Logs > Log Receiver > By Day (Summary)

LABEL	DESCRIPTION
Date	This field displays the day for which the logs were collected. Click the date to go to a screen that lists how many logs were received from each device on that day.
Log Number	This field displays how many logs were received on each day.
Average Processing Speed(Logs/sec)	This field displays the average number of logs the Vantage Report server processed per second on each day.

13.2.1.1 Log Receiver > By Day (Summary) > By Device Screen

Use this screen to look at the total number of logs that Vantage Report received from each registered device on a particular day.

Click on the link in an entry in **Logs > Log Receiver > By Day (Summary)** to access this screen.

Figure 246 Logs > Log Receiver > By Day (Summary) > By Device

By Device for 2011-04-08		
Device	Log Number	% of Log Number
0000AA791511	90646	99.6%
0019CB76F2DF	357	0.4%
Total	91003	100%

Back

All the fields are described in the following table.

Table 229 Logs > Log Receiver > By Day (Summary) > By Device

LABEL	DESCRIPTION
Device	This field displays the MAC addresses of the registered devices that sent logs on the day you clicked. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected day.
Log Number	This field displays how many logs were received from each device on the day you clicked.
% of Log Number	This field displays what percent of the day's total logs came from each device.

13.2.1.1.1 Log Receiver By Day (Summary) > By Device > By Category Screen

Use this screen to look at the number of logs that Vantage Report received according to the category of log (i.e., log type such as Login, Traffic log, etc.) from an individual device on a particular day.

Note that log categories vary according to the type of device selected.

Click on the link in an entry in **Logs > Log Receiver > By Day (Summary) > By Device** to access this screen.

Figure 247 Logs > Log Receiver > By Day (Summary) > By Device > By Category

By Category for device 0000AA791511 by Day 2011-04-08		
Category	Log Number	% of Log Number
Firewall	30458	33.6%
INTERFACE STATISTICS	26050	28.7%
Zysh	13854	15.3%
Default	7273	8.0%
Traffic Log	6338	7.0%
Policy Route	3997	4.4%
System Monitoring	2616	2.9%
System	27	<0.1%
DHCP	15	<0.1%
IPMAC Binding	14	<0.1%
FORCE AUTH	3	<0.1%
User	1	<0.1%
Total	90646	100%

[Back](#)

All the fields are described in the following table.

Table 230 Logs > Log Receiver > By Day (Summary) > By Device > By Category

LABEL	DESCRIPTION
Category	This field displays the types of logs that the device sent to Vantage Report during the day selected from the previous screen.
Log Number	This field displays how many of the device's logs belonged to each category.
% of Log Number	This field displays what percent of the day's total logs came from each category.

13.3 By Device

Use this screen to look at the number of logs that Vantage Report received from each device over a selected range of days.

Click **Logs > Log Receiver > By Device**. The following screen displays. Logs > Log Receiver > By Device. The following screen displays.

Figure 248 Logs > Log Receiver > By Device

Device	Log Number	% of Log Number
0000AA791511	91653	99.3%
0019CB76F2DF	667	0.7%
Total	92320	100%

Each field is described in the following table.

Table 231 Logs > Log Receiver > By Device

LABEL	DESCRIPTION
Last ... Days	Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The Report Display Settings screen appears. Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include days that are older than Store Log Days in System > General Configuration. Click Apply to update the report immediately, or click Cancel to close this screen without any changes.
Device	This field displays the MAC addresses of the devices that sent logs on the days you selected. They are sorted according to the number of logs received by each, in descending order. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected days.

Table 231 Logs > Log Receiver > By Device

LABEL	DESCRIPTION
Log Number	This field displays how many logs Vantage Report received from each device.
% of Log Number	This field displays what percent of the selected time period's total logs came from each category.

13.3.1 Log Receiver > By Device > By Category Screen

Use this screen to look at the number of logs that Vantage Report received according to the category of log (i.e., log type such as Login, Traffic log, etc.) from an individual device over a selected range of days.

Note that the categories vary according to the type of device selected.

To access this screen, click the link in an entry in the **Logs > Log Receiver > By Device** screen.

Figure 249 Logs > Log Receiver > By Device > By Category

Category	Log Number	% of Log Number
Firewall	31624	34.2%
INTERFACE STATISTICS	26320	28.4%
Zysh	13995	15.1%
Default	7356	7.9%
Traffic Log	6514	7.0%
Policy Route	4039	4.4%
System Monitoring	2643	2.9%
System	27	<0.1%
DHCP	16	<0.1%
IPMAC Binding	14	<0.1%
FORCE AUTH	3	<0.1%
User	1	<0.1%
Total	92552	100%

Back

All the fields are described in the following table.

Table 232 System > Log Receiver > By Device > By Category

LABEL	DESCRIPTION
Category	This field displays the types of logs that the device sent to Vantage Report during the selected day.
Log Number	This field displays how many logs Vantage Report received from the device during the selected time period.
% of Log Number	This field displays what percent of the device's logs came from each category.

13.4 VRPT System Logs

Use this screen to view system, device and user information, events, scheduled reports and data maintenance records related to Vantage Report.

Click **Logs > Log Viewer > VRPT System Logs**. The following screen displays.

Figure 250 Logs > VRPT System Logs

VRPT System Logs

Notification:[none]

Severity: ALL

Category: All Categories

Logs per Page: 10

Start Date: 2011-03-30

End Date: 2011-04-08

Search

Reset

#	Time	Severity	Category	Message
1	2011-04-08 10:41:30	INFO	User	User root has logged in from 172.23.26.4
2	2011-04-08 10:14:00	INFO	User	User root has logged in from 172.23.26.4
3	2011-04-08 08:42:06	INFO	User	User root has logged in from 172.23.26.4
4	2011-04-08 01:17:33	INFO	DataMaintenance	Start to merge logs
5	2011-04-08 01:17:33	INFO	DataMaintenance	Start to remove overdue logs
6	2011-04-08 01:17:33	INFO	DataMaintenance	Start to purge & archive logs
7	2011-04-07 17:59:18	INFO	User	User root has logged in from 172.23.26.4
8	2011-04-07 17:25:39	INFO	User	User root has logged in from 172.23.26.4
9	2011-04-07 16:51:45	INFO	User	User root has logged in from 172.23.26.4
10	2011-04-07 16:48:38	INFO	User	User root has logged in from 172.23.26.4

Total Count:93 Total Page:10 First 1 2 3 4 5 6 7 8 9 10 Last

Go

Each field is described in the following table.

Table 233 Logs > VRPT System Logs

LABEL	DESCRIPTION
Severity	Select what type of log entries in terms of severity you want to see. You can also select All. Severity ranking is as follows. • Fatal - System is unusable. • Error - Error conditions • Warn - Warning conditions • Info - Informational messages
Category	Select what category type of log entries you want to see. You can also select All Categories. The categories are as follows: • System - See information about Vantage Report's disk space. • Device - Check which devices were added, edited or removed in the Vantage Report. • Alert - Select this to see logs pertaining to rule-based alerts. See Chapter 14 on page 561 for more details. • User - See a list of users who logged in or logged out. • Schedule Report - Select this to see logs pertaining to scheduled reports. See Chapter 12 on page 509 for more details. • Data Maintenance - Check if logs have been purged, removed, archived or merged.
Logs per Page	Specify how many log entries you want to view per page.
Start Date	Enter the time of the earliest log entry you want to see.
End Date	Enter the time of the latest log entry you want to see.
Search	Click this to display the log entries based on the current search criteria.
Reset	Click this to set the search criteria to the values they had the last time you clicked Search . If you have not clicked Search yet, the search criteria return to their default values.
#	This is the number identifying the entry, with the number 1 entry being the latest event to be logged.
Time	This is the time when the event was logged by the Vantage Report.
Severity	This is the severity of the system log entry.
Category	This is the category where the event belongs to.
Message	This is the log message for the specific entry. See Appendix A on page 589 for Vantage Report's internal log consolidation frequency. See Appendix C on page 645 and Appendix B on page 599 for information on the logs.
Total Count	This field displays how many log entries there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the log entries.

Table 233 Logs > VRPT System Logs

LABEL	DESCRIPTION
First .. Last	Click First , Last , or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .

13.5 Log Archiving

These screens allow you to archive past logs to a preferred location (local directory, FTP or network server) as a ZIP file. You can set the day(s) or time interval when Vantage Report performs this task.

You can view, import/export, or delete log archives for a particular device.

Note: If the storage space is not enough for the size of the log archive, Vantage Report sends out an alert e-mail and generates a system log.

13.5.1 File Archiving Settings

Use this screen to archive past logs to a preferred location (local directory or FTP/storage server) as a ZIP file.

Click **Logs > Log Archiving > File Archiving Settings**. The screen display varies according to your storage location preference.

Figure 251 Logs > Log Archiving > File Archiving Settings

Each field is described in the following table.

Table 234 Logs > Log Archiving > File Archiving Settings

LABEL	DESCRIPTION
Enable Archiving	Click this to enable Vantage Report to archive log files.
Zip Creation Interval: every... Days (1-7)	Set every which day or the time interval the Vantage Report archives the generated log files for record keeping.
Enable Encryption	Select this if you want to encrypt archive files.
Password	This field is available when you select Enable Encryption . Enter up to 20 alphanumeric characters for the key used for file encryption. You have to use the same password to decrypt the file when you want to view the archived logs.
Hash Option	Select which hash algorithm to use for verifying the integrity of log data in archives. SHA1 (Secure Hash Algorithm) is generally considered stronger than MD5 (Message Digest 5), but it is also slower.
Local Host	Select this to store the archive to a local folder in the computer where the Vantage Report is installed. This is the default storage setting for the Vantage Report.
FTP Site	Select this to store the archive to an FTP site. Additional fields appear when you choose this option. See Section 13.5.1.1 on page 539 for more details.
Storage Server	Select this to store the archive to a storage server. Additional fields appear when you choose this option. See Section 13.5.1.2 on page 540 for more details.
Archive Location	Specify where you want Vantage Report to store log archives. The fields vary according to your preferred storage location. - Select Local Host to store archives in the local directory of the Vantage Report. - Select FTP Site to store the archives in an FTP server. Make sure you know the FTP Host/IP address, User Name and Password. - Select Storage Server to store the archives on a storage server, such as a Network Attached Storage (NAS) server. Make sure you know the Network Folder server location, User Name and Password.
Save	Click this to save your settings.
Reset	Click this to change the settings in this screen to the last-saved values.

13.5.1.1 File Transfer Protocol

Use this screen to store archive files on a File Transfer Protocol (FTP) server.

Click **Logs > Log Archiving > File Archiving Settings**. Choose **Ftp Site** to display the following fields.

Figure 252 Logs > Log Archiving > File Archiving Settings > Ftp Site

Each field is described in the following table..

Table 235 Logs > Log Archiving > File Archiving Settings > FTP Site

LABEL	DESCRIPTION
Ftp Host/IP	Enter the location of the File Transfer Protocol (FTP) server you want to use in the Ftp Host/IP field.
Ftp Port	Enter the port number the FTP server uses for the service.
User Name	Enter the User Name for your FTP account.
Password	Enter the Password for your FTP account.
File path	You can specify in which FTP folder you want to store the archive in the File Path field (optional).

See [Figure 253 on page 541](#) for descriptions of other table fields found in this screen.

13.5.1.2 Storage Server

Use this screen to store archive files on a storage server, such as a Network Attached Storage (NAS) server.

Click **Logs > Log Archiving > File Archiving Settings**. Choose **Storage Server** to display the following fields.

Figure 253 Logs > Log Archiving > File Archiving Settings > Storage Server

Each field is described in the following table..

Table 236 Logs > Log Archiving > File Archiving Settings > Storage

LABEL	DESCRIPTION
Network Folder	Enter the server location where you want to store the archive in the Network Folder field.
Authentication	Click Authentication if your server prompts for identification before allowing access.
User Name	Enter the User Name for server login if authentication is required.
Password	Enter the corresponding Password for server login if authentication is required.

See [Figure 254 on page 542](#) for descriptions of other table fields found in this screen.

13.5.2 View Archived Files

Use this screen to view archived logs for a particular day or range of days. Vantage Report imports the archived logs from the location where they are stored and enables you to view them in the web browser.

Click **Logs > Log Viewer > View Archived Files**. The following screen displays.

Figure 254 Logs > Log Archiving > View Archived Files

Search Archived Files

Device : Start Date : End Date :

Files per Page :

Device	File Name	Start Date	End Date	File Size (MBytes)	Status	Action
ZLD_200	0000AA785206_20110401_20110401.zip	2011-04-01	2011-04-01	6.3	Not imported	

Total Count: 1 Total Page: 1 First 1 Last Go

Each field is described in the following table.

Table 237 Logs > Log Archiving > View Archived Files

LABEL	DESCRIPTION
Device	This field displays the name of the devices that have archived logs on Vantage Report. You can also select All .
Start Date	Enter the date of the earliest log entries you want to see. You can also click the Calendar icon to specify the date.
End Date	Enter the date of the latest log entries you want to see. You cannot enter a date earlier than Start Date . You can also click the Calendar icon to specify the date.
Files per page	Select the number of archived files to view on each page.
Search	Click this to see the archives in the date range you specified.
Refresh Archive Files	Click this to update the screen and see the latest log files immediately.
Device	This refers to the ZyXEL Device the logs are generated for.
File Name	This is the file name of the log archive.
Start Date	This is the date of the earliest log entry in the archive.
End Date	This is the date of the latest log entry in the archive.
File Size (MBytes)	This is the size of the log archive.
Hash	Click MD5 or SHA1 to view the corresponding hash value produced using the MD5 or SHA1 algorithm while the archive file is generated. You can make sure the data integrity if this value is the same as the one produced from the same archive file you downloaded using the same hash generation tool.
Status	This column shows whether the archive is Imported or Not Imported . If it is imported, you can view the logs in the web browser. You can click on the icons in the Action column to set the status for each log archive.

Table 237 Logs > Log Archiving > View Archived Files

LABEL	DESCRIPTION
Action	Select whether to Export , Import , Delete or Transfer an archive. Click on the corresponding icon of the action you want to apply.
Total Count	This field displays how many log entries there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the log entries.
First .. Last	Click First , Last , or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .

13.5.3 Log Transfer

Use this screen to send an archived file to one or multiple people using e-mail. You can also configure the mail subject and content in this screen.

Click a **Transfer** icon next to an archive entry in the **Logs > Log Archiving > View Archived Files** screen. The following screen displays.

Figure 255 Logs > Log Archiving > View Archived Files

Send Archived File

Receiver: *separate with ";" for multiple receivers

Subject:

Attachment: 0000AA785206_20110401_20110401.zip

Content:

Each field is described in the following table.

Table 238 Logs > Log Archiving > View Archived Files

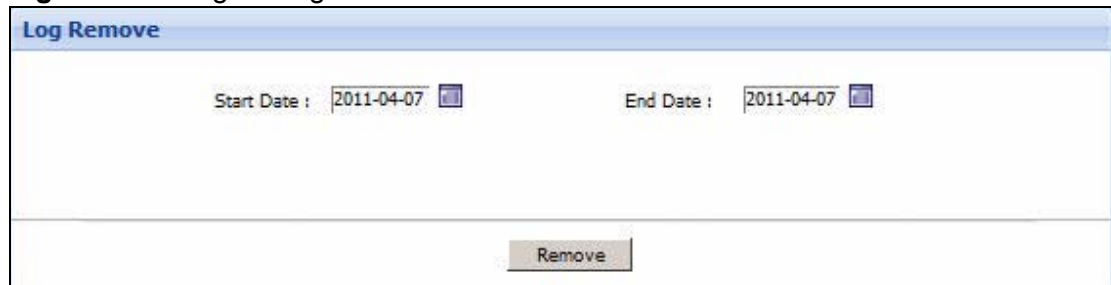
LABEL	DESCRIPTION
Receiver	Type the e-mail address(es) of people to whom you want to forward the archive file. Use a semicolon (;) to separate multiple e-mail addresses. You can type up to 100 characters in this field.
Subject	Type a short description for this mail.
Attachment	This field displays the name of the selected archive file.
Content	Type the descriptive information for this mail.
Send	Click this to send this mail to the specified e-mail addresses.

13.6 Log Remove

Use this screen to purge logs collected over a specified period of time. This helps clear up space in Vantage Report.

Click **Logs > Log Remove**. The following screen displays.

Figure 256 Logs > Log Remove



Each field is described in the following table.

Table 239 Logs > Log Remove

LABEL	DESCRIPTION
Start Date	Enter the date of the earliest log entries you want to remove. You can also click the Calendar icon to specify the date.
End Date	Enter the date of the latest log entries you want to remove. You cannot enter a date earlier than Start Date . You can also click the Calendar icon to specify the date.
Remove	Click this to remove the said log records.

PART III

System Setting, User Management and Troubleshooting

System Setting (549)

User Management (577)

Troubleshooting (583)

System Setting

The `root` account or the accounts in the 'super' group can use the system screens to:

- Maintain global reporting settings, such as how many days of logs to keep and default chart type
- Maintain mail server settings
- Add, remove, or edit groups and users who can access Vantage Report
- Backup the current configuration and restore a different configuration
- Export the current device panel to XML and import devices from XML
- Upgrade to a new software release of Vantage Report
- Register Vantage Report (You have to register Vantage Report if you want to get the trial version, upgrade to the full version, or increase the number of devices Vantage Report supports.)
- Monitor the number of logs received by time or by device
- Get basic information about Vantage Report

Other users can use the system screens to

- Edit their user account settings, including the password
- Get basic information about Vantage Report

14.1 General Configuration Screen

Note: Only the `root` account or accounts in the 'super' group can open this screen.

Use this screen to maintain global reporting settings, such as how many days of logs to keep and default chart type.

Click **System Setting > General Configuration** to open the **General Configuration** screen.

Figure 257 System Setting > General Configuration

Each field is described in the following table.

Table 240 System Setting > General Configuration

LABEL	DESCRIPTION
Default Chart Type	Select the default chart type in statistical report screens.
Default Page Style	Select the default page style in statistical report screens.
DNS Reverse	Select Enable if you want Vantage Report to do reverse DNS lookups in statistical reports. It has no effect in Log Viewer . In reverse DNS lookups, Vantage Report looks for the domain name associated with IP addresses that it displays. If Vantage Report finds the domain name, it displays the domain name and the IP address in the field. If it does not find the domain name, it only displays the IP address. This feature might increase the amount of time it takes to display statistical reports, however.
Hostname Reverse	Select Enable if you want Vantage Report to display the host names for local computers instead of IP addresses. It has no effect in Log Viewer . In hostname reverse lookups, Vantage Report looks for the host name associated with local IP addresses that it displays. If Vantage Report finds the host name, it displays the host name and the IP address in the field. If it does not find the host name, it only displays the IP address. This feature might increase the amount of time it takes to display statistical reports, however. You also need to configure the host computers and ZyXEL device (see Section 14.1.1 on page 551).
Low Free Disk Mark	When the amount of available disk space falls below this number of gigabytes, Vantage Report sends a notification to the e-mail address (if any) for the root user account.
Stored Log Days	Enter the number of days you want to store logs in Vantage Report before removing them.
Language Choose	Choose the language for the Vantage Report.
Apply	Click this to save your settings.
Reset	Click this to change the settings in this screen to the last-saved values.

14.1.1 Configuring for Hostname Reverse

Besides enabling hostname, do the following to allow the hostname reverse function to work.

- 1 Turn on hostname reverse in Vantage Report.
- 2 Enable the default NetBIOS setting in the host computers.
- 3 Configure any software firewalls installed on the host computers to allow NetBIOS packets from the Vantage server.
- 4 Set the ZyXEL device to allow NetBIOS traffic between interfaces. You need to configure both the individual interface screens (like LAN, WAN, DMZ) and the firewall to allow NetBIOS packets from the Vantage server.

14.1.1.1 Enabling the Default NetBIOS Setting in Host Computers

The following procedure gives an example of how to enable the default NetBIOS settings in host computers using Windows 2000, XP, Vista or 7.

- 1 For Windows XP, click **Start > Control Panel**.

For Windows 2000, click **Start > Settings > Control Panel**.

For Windows Vista/7, click **Start > Control Panel**.

Figure 258 Windows XP: Start Menu

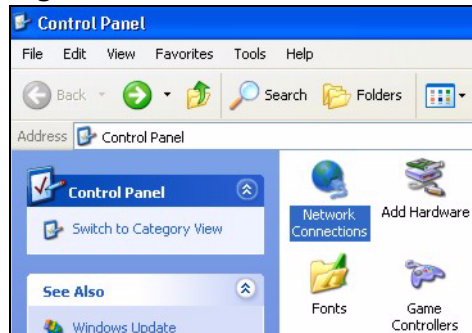


- 2 For Windows XP, click **Network Connections**.

For Windows 2000, click **Network and Dial-up Connections** and then **Local Area Connection**.

For Windows Vista/7, double click **Network and Sharing Center**.

Figure 259 Windows XP: Control Panel



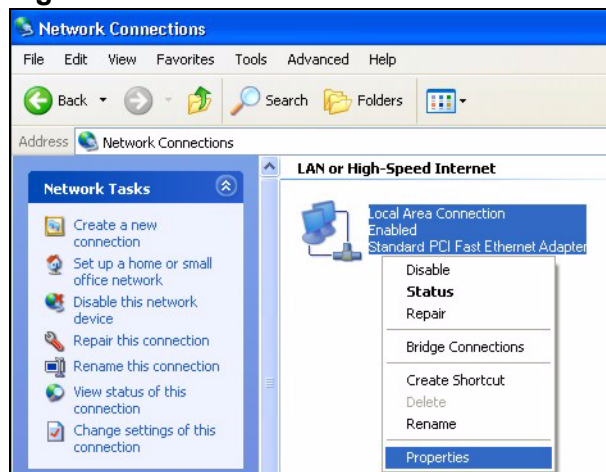
- 3 For Windows XP, right-click **Local Area Connection** and then click **Properties**.

For Windows 2000, the **Local Area Connection Status** window appears. click **Properties**.

For Windows Vista, click **View status** next to the **Connection** field. A screen appears and then click **Properties**.

For Windows 7, click **Local Area Connection** and then click **Properties**.

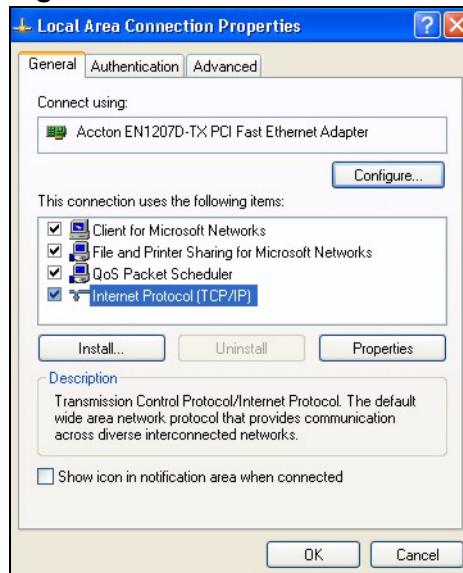
Figure 260 Windows XP: Control Panel: Network Connections: Properties



- 4 For Windows XP/2000, select **Internet Protocol (TCP/IP)** (under the **General** tab) and click **Properties**.

For Windows Vista/7, select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.

Figure 261 Windows XP: Local Area Connection Properties

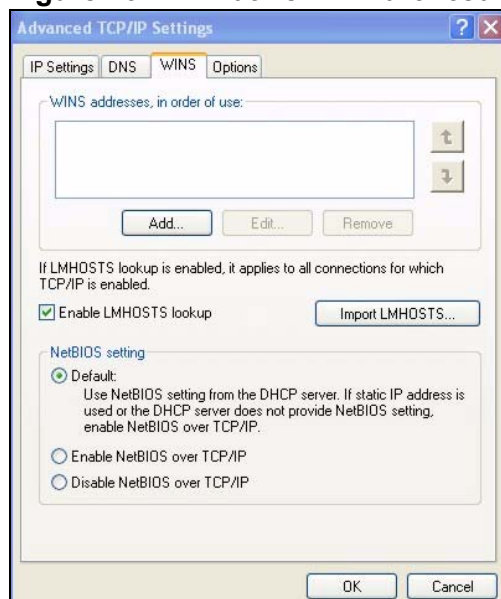


- 5 For Windows XP, the **Internet Protocol TCP/IP Properties** window opens. Click the **WINS** tab.

For Windows 2000, the **Internet Protocol TCP/IP Properties** window opens. Click **Advanced** and then the **WINS** tab.

In Windows Vista/7, The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens, click **Advanced** and then the **WINS** tab.

Figure 262 Windows XP: Advanced TCP/IP Settings: WINS



- 6 For Windows XP/Vista/7, select the **Default** NetBIOS setting and click **OK**.
For Windows 2000, select **Use NetBIOS setting from the DHCP server** and click **OK**.
- 7 Click **OK** (and **Close**) to close the previously opened windows.
- 8 Turn on your ZyXEL device and restart your computer (if prompted).

14.2 Server Configuration Screen

Note: Only the `root` account or accounts in the 'super' group can open this screen.

Use the **Server Configuration** screen to set up mail server and web server configuration for Vantage Report. See [Section 2.2 on page 24](#) for more information. Click **System Setting > Server Configuration** to open the **Server Configuration** screen.

Figure 263 System Setting > Server Configuration

The screenshot shows the 'Server Configuration' window. It has two main sections: 'Mail Server Configuration' and 'Web Server Configuration'.
Mail Server Configuration: Includes fields for 'SMTP IP Address or Domain Name', 'Sender E-mails', and 'Receiver E-mails(separated by commas)'. There is a checkbox for 'Authentication'. Below it are 'User Name' and 'Password' fields. A 'Test' button is next to the text 'Send Test E-mail to Administrator and the addresses in Receiver E-mails:'.
Web Server Configuration: Includes a 'Web Server Port' field with the value '8080' and a red asterisk indicating it is required.
At the bottom are 'Apply' and 'Reset' buttons.

Each field is described in the following table.

Table 241 System Setting > Server Configuration

LABEL	DESCRIPTION
Mail Server Configuration	Use this part of the screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports.
SMTP IP Address or Domain Name	Enter the IP address or domain name of the SMTP mail server on which Vantage Report has an account to send e-mail messages.
Sender E-mails	Enter the complete e-mail address for the Vantage Report account.

Table 241 System Setting > Server Configuration

LABEL	DESCRIPTION
Receiver E-mails (seperated by commas)	Enter the e-mail address you want to be the receiver when Vantage Report sends e-mail. This is the e-mail address to which Vantage Report e-mail appears to be sent.
Authentication	Check this to supply your credentials to the SMTP server you want to use.
User Name	Enter the user name for the email account. If the user name is not required, leave this field blank.
Password	Enter the password for the email account. If the password is not required, leave this field blank.
Send Test E-mail to Administrator	Note: You should click Apply before you click Test. Click this to send a test message from the Vantage Report account to the e-mail address, if any, for the <code>root</code> user account.
Web Server Configuration	Use this part of the screen to configure the port number Vantage Report uses for web services.
Web Server Port	Enter the port number you want Vantage Report to use for web services. Make sure this port number does not conflict with other services in your network.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.

14.3 Data Maintenance Screens

Note: Only the `root` account or accounts in the 'super' group can open these screens.

Use the data maintenance screens to backup the current configuration, restore a different configuration, export the device panel, or import a different device panel.

14.3.1 Data Backup and Data Restore Screen

Note: Only the `root` account or accounts in the 'super' group can open this screen.

You can use this screen to backup or restore the settings in the **General Configuration**, **Server Configuration**, **User Management**, and **Device List** screens. The backup format is XML. You cannot backup or restore the logs, traffic

information, or other settings. To access this screen, click **System Setting > Data Maintenance > Configuration**.

Figure 264 System Setting > Data Maintenance > Configuration

Each field is described in the following table.

Table 242 System Setting > Data Maintenance > Configuration

LABEL	DESCRIPTION
Backup	Click this to look at or save the current settings in the General Configuration, Server Configuration, User Management, and Device List screens. Vantage Report saves the current settings in XML format.
File Name / Browse	Enter the XML file name that contains the settings you want to restore. You can also click Browse .
Restore	Click this to load the settings in the specified file name.
Reset	Click this to clear the fields in this screen.

14.3.2 Device List Screen

Note: Only the `root` account or accounts in the 'super' group can open this screen.

You can use this screen to export the current device panel to an XML file, or you can add devices stored in XML format to Vantage Report. To access this screen, click **System Setting > Data Maintenance > Device List**.

Figure 265 System Setting > Data Maintenance > Device List

Each field is described in the following table.

Table 243 System Setting > Data Maintenance > Device List

LABEL	DESCRIPTION
Export	Click this to look at or save the current device panel in XML format.
File Name / Browse	Enter the XML file name that contains the devices you want to add. You can also click Browse .
Import	Click this to add the devices in the specified file name. You cannot add any of the devices in the XML file if the total number of devices (current device panel + devices in XML file) is more than your license allows.
Reset	Click this to clear the fields in this screen.

14.4 Upgrade Screen

Note: Only the `root` account or accounts in the 'super' group can open this screen.

Note: Before you use this screen, read the documentation for the new release to make sure you understand the upgrade process.

Use this screen to install new releases of Vantage Report. Do not use this screen to upgrade to the full version. To access this screen, click **System Setting > Upgrade**.

Figure 266 System Setting > Upgrade

Each field is described in the following table.

Table 244 System Setting > Upgrade

LABEL	DESCRIPTION
Package Path / Browse	Enter the path to the release of Vantage Report that you want to install. You can also click Browse .
Apply	Click this to install the selected release. Follow the prompts.
Reset	Click this to clear the fields in this screen.

14.5 Registration Screens

Note: Only the `root` account or accounts in the 'super' group can open these screens.

Use these screens to

- Upgrade to the full version of Vantage Report; or
- Increase the number of devices you can manage with the full version.

Note: Vantage Report uses myZyXEL.com for registration and activation. You have to use the registration screens to log into myZyXEL.com. You cannot log in to myZyXEL.com separately to register or activate Vantage Report.

The following information may be required for registration.

Table 245 Information for Using an Existing MyZyXEL.com Account

If you want to use an existing myZyXEL.com account, you need your ...
• myZyXEL.com user name • myZyXEL.com password

Table 246 Information for Upgrading the Version or Number of Devices

To add more devices for the full version, you need your ...
• license key (E-Vantage Report)

14.5.1 Registration Summary Screen

To access this screen, click **System Setting > Registration**.

Figure 267 System Setting > Registration

Registration	
VRPT Full Version	
Account on myZyXEL.com:	fmzmd4tolq
Authentication Code(AC):	0528A1BE5E9BA7617F1B89E2CA6EDB046506
Max Supported Devices:	100
License Allowed Devices:	80
Managed Devices:	44
Refresh Upgrade	

The fields in this screen depend on what version (basic or full) of Vantage Report you have and whether or not you have used the registration screens to log into myZyXEL.com. All the fields are described in the following table.

Table 247 System Setting > Registration

LABEL	DESCRIPTION
Account on myZyXEL.com	This field appears if you have used the registration screens to log into myZyXEL.com before. It displays the user name of your myZyXEL.com account.
Authentication Code (AC)	This field displays the authentication code for Vantage Report. You have to enter this number in myZyXEL.com if you log in to myZyXEL.com directly.
Max Supported Devices	This field appears if you have the full version. It displays the maximum number of devices Vantage Report can currently support, regardless of the number of licenses you purchase. You can never increase the number of devices in Vantage Report higher than this value, regardless of how many licenses you have. In other words, this is the maximum value of License Allowed Devices .
License Allowed Devices	This field appears if you have the full version. It displays the number of devices you can add in Vantage Report based on your current license(s).
Managed Devices	This field appears if you have the full version. It displays the number of devices you currently have added in Vantage Report.
Refresh	Click this to update the information in this screen.

Table 247 System Setting > Registration

LABEL	DESCRIPTION
Trial	This appears if you have the basic version and if you have not installed the trial version yet. Click this to get the trial version of Vantage Report. The Registration screen appears.
Upgrade	Click this to upgrade to the full version of Vantage Report or to increase the number of devices in Vantage Report. If you cannot upgrade Vantage Report further (in other words, if you can already add the maximum number of devices in Vantage Report), an error message is displayed. Otherwise, the Registration screen appears.

14.5.2 Registration > Upgrade Screen

Note: The Vantage Report server must be connected to the Internet to use this screen.

To access this screen, click **Trial** or **Upgrade** in **System Setting > Registration**.

Figure 268 System Setting > Registration > Upgrade Screen

Some fields do not appear if you have already used this screen to log into myZyXEL.com, if you have a myZyXEL.com account, or if you are getting the trial version. The fields are described in the following table.

Table 248 System Setting > Registration > Upgrade Screen

LABEL	DESCRIPTION
License Key	Enter the E-Vantage Report license key if you are adding more devices for the full version.
New myZyXEL.com account	Select this if you want Vantage Report to create a new myZyXEL.com account for you.
Existing myZyXEL.com account	Select this if you want to use an existing myZyXEL.com account.
User Name	If you are creating a new myZyXEL.com account, enter the user name that you would like to use. Your user name must be 6 - 20 alphanumeric characters and/or underscores(_) long. If you are using an existing myZyXEL.com account, enter the user name for that account.

Table 248 System Setting > Registration > Upgrade Screen

LABEL	DESCRIPTION
Password	If you are creating a new myZyXEL.com account, enter the password that you would like to use. Your password must be 6 - 20 alphanumeric characters and/or underscores(_) long. If you are using an existing myZyXEL.com account, enter the password for that account.
Confirm Password	This field appears if you are creating a new myZyXEL.com account. Retype your password.
E-mail Address	This field appears if you are creating a new myZyXEL.com account. Enter the e-mail address where you would like to be notified about your new myZyXEL.com account.
Country	This field appears if you are creating a new myZyXEL.com account. Select the country where you work.
Upgrade	Click this to get the trial version, upgrade to the full version, or increase the number of devices in Vantage Report.
Cancel	Click this to return to the Registration summary screen without registering.

14.6 Notification

Use this screen to manage your Vantage Report notifications. Based on the monitoring data collected and the notifications you set, Vantage Report can send e-mail, E-mail SMS, and/or Web SMS notifications to you when events happen in monitored devices.

Click **System Setting > Notification** to display the following screen.

Figure 269 System Setting > Notification

#	Notification Name	Level	Description
Total Count:0 Total Page:0 First Last Go			
Add Delete			

The fields are described in the following table.

Table 249 System Setting > Notification

LABEL	DESCRIPTION
#	This is the index number of a notification.
Notification Name	This is the name identifying the notification. You can edit the settings of this notification by clicking this link. See Section 14.6.1 on page 563 to see the Add/Edit screen for notifications.
Level	This specifies the severity of the notification, which may be the following: • FATAL - System is unusable • WARN - Warning conditions • INFO - Informational messages Severity labels are user-defined. You can determine how the severity labels apply to each type of event when you are setting the parameters for the notification file. You can set this in the Add/Edit screen (see Section 14.6.1 on page 563).
Description	This shows the basic information for the notification.
Total Count	This field displays how many rules are recorded.
Total Page	This field displays how many screens it takes to display all the rules.
First .. Last	Click First , Last , or a specific page number to look at the rules on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .
Add	Click this to add the rule to the Vantage Report.
Delete	Select the check box(es) of the rule(s) you want to delete and then click this button. Click OK in the confirmation dialog box.

14.6.1 Add/Edit a Notification

Use this screen to create or edit a notification. Click **Add** or click a notification's name in the **System Setting > Notification** screen to open the following screen.

Figure 270 System Setting > Notification > Add/Edit

Notification Setting

Basic Information

Notification Name: *

Severity Notification:

Discription:

Email

E-mail Status :

Destination E-mail Address:

SMS-SMTP

SMS-SMTP Status :

To Address:

Message Subject:

Message Body:

SMS-HTTP

SMS-HTTP Status :

URL:

Postdata:

The fields are described in the following table.

Table 250 System Setting > Notification > Add/Edit

LABEL	DESCRIPTION
Notification Name	Type up to 30 alphanumeric characters for the name of the notification. Underscores (_) are allowed.
Severity Notification	Select the severity of the notification. The available options are: • FATAL - System is unusable • WARN - Warning conditions • INFO - Informational messages
Description	This shows the basic information for the notification.
Email	
Email Status	Select Active to enable the Vantage Report to send this type of notification to the configured e-mail address(es) in the Destination E-mail Address field. Alternatively, select Paused to disable it.
add	Type a valid e-mail address and click this to add it to the Destination E-mail Address list. Repeat to add more than one e-mail addresses.
Destination E-mail Address	This is a list of receiver e-mail addresses. You can select an e-mail address and then click remove to delete it from the list.
SMS-SMTP	
SMS-SMTP Status	Select Active to enable the Vantage Report to send this type of notification to the configured address(es) below using E-mail Short Message Service (SMS). Alternatively, select Paused to disable it.
To Address	Type one or more valid SMS addresses. Use a comma (,) to separate multiple addresses. An SMS address is usually your cell phone number plus an '@' and your SMS service provider's domain name. For example, 1234567890@abcdefg.com. Check your service provider if you are not sure about this.
Message Subject	Type up to 50 printable characters for the mail subject. Spaces are allowed. Mouse over the information icon to see what variables you can use for the mail subject. The available variables are: %msg: Use this to show the content of the notification. %level: Use this to show the severity level of the notification. %server: Use this to show the IP address of the mail server used to send the notification. %title: Use this to show the title of the notification. %category: Use this to show the category of the notification.

Table 250 System Setting > Notification > Add/Edit

LABEL	DESCRIPTION
Message Body	Type up to 160 printable characters for the mail content. Spaces are allowed. Mouse over the information icon to see what variables you can use for the mail content. The available variables are: %msg : Use this to show the content of the notification. %level : Use this to show the severity level of the notification. %server : Use this to show the IP address of the mail server used to send the notification. %title : Use this to show the title of the notification. %category : Use this to show the category of the notification.
SMS-HTTP	
SMS-HTTP Status	Select Active to enable the Vantage Report to send this type of notification to the configured URL(s) below using Web SMS. Alternatively, select Paused to disable it.
URL	Type up to 539 characters for the address of a web site that provides the Web SMS service.
Postdata	Enter any POST parameters for the HTTP request. A POST request sends additional data after the URL to the web server. Leave this empty for a GET request or you are not sure about it.
Apply	Click this to save the changes to the Vantage Report.
Reset	Click this to reset all field values back to the previous settings in this screen.
Cancel	Click this to exit this screen without saving any changes.

14.7 Rule-Based Alert

Use this screen to manage your Vantage Report alert system. Based on the monitoring data collected and the rules you set, Vantage Report can send e-mail notifications and keep you in the loop on events happening in monitored devices.

Click **System Setting > Rule-based Alert** to display the following screen.

Figure 271 System Setting > Rule-based Alert

Summary of Rule Files

#	Rule Name	Platform Type	Devices	Notification
Total Count: 0 Total Pages: 0 First Last Go				

Add Delete

The fields are described in the following table.

Table 251 System Setting > Rule-based Alert

LABEL	DESCRIPTION
#	This is the index number of a rule.
Rule Name	This is the name identifying the rule. You can edit the parameters of this rule by clicking on this link. See Section 14.7.1 on page 566 to see the Add/Edit screen for rules.
Level	This specifies the severity of the alert, which may be the following. • FATAL - System is unusable • WARN - Warning conditions • INFO - Informational messages Note that severity labels are user-defined. You can determine how the severity labels apply to each type of event when you are setting the parameters for the rule file. You can set this in the Add/Edit screen (see Section 14.7.1 on page 566).
Platform Type	This specifies what firmware platform the rule applies to. Firmware platform can either be ZLD or ZYNOS .
Devices	This field specifies in which monitored devices the rule applies.
To E-mail Address	This shows the e-mail address where you would like to be notified of alerts.
Total Count	This field displays how many rules are recorded.
Total Page	This field displays how many screens it takes to display all the rules.
First .. Last	Click First , Last , or a specific page number to look at the rules on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .
Add	Click this to add the rule to the Vantage Report.
Delete	Select the check box(es) of the rule(s) you want to delete and then click this button. Click OK in the confirmation dialog box.

14.7.1 Add/Edit a Rule-based Alert

These screens allow you to add a new rule file or edit an existing one.

Click **System Setting > Rule-based Alert**. To edit an existing rule click the link of the existing **Rule Name**. To add a new rule, click **Add**.

The following screen displays.

Figure 272 System Setting > Rule-based Alert > Add/Edit > CPU/Memory/Session Usage

The screenshot shows the 'Rule File' configuration window. At the top, there is a 'Rule Name' field and a 'Choose Platform Type' dropdown set to 'ZLD'. Below this is the 'Filters' section, which includes a 'Condition' dropdown set to 'CPU Usage'. Under 'CPU Usage', there is a 'CPU Usage' field with a dropdown set to '>=' and a value of '0', followed by a '%' symbol. To the right is a 'Period' field with a value of '1' and a 'minutes' label. Below these fields are 'Add Criteria' and 'Remove Criteria' buttons. A radio button group allows selecting 'Match all of the following' (unselected) or 'Match any of the following' (selected). Below this is a large empty box for additional criteria. The 'Alert Setting' section includes a note 'First alert will send immediately!', and fields for 'Second alert after:' (1 minutes) and 'Third alert after:' (1 minutes). A note below states: '* If you want to disable second or third alert, you should fill '0' in relevant box.' The 'Select Devices' section has checkboxes for 'root', 'HQ', 'usg1000', 'aaron', and 'zld', along with a 'Select All' checkbox. The 'Notification' section has a 'Notification Choose:' dropdown set to '[none]' and a small icon button. At the bottom are 'Apply', 'Reset', and 'Cancel' buttons.

The fields in this screen are described in [Table 252 on page 568](#).

The following sections describe the **System Setting > Rule-based Alert > Add/Edit** screens according to the **Condition** filter selected.

The **Condition** filter differs for each platform type (either **ZLD** or **ZYNOS** as of the time of this writing). Furthermore, the fields under **Filters** varies according to the **Condition** filter you want to set the rule for.

14.7.1.1 CPU, Memory and Session Usage

Note: These condition filters only apply to the ZLD platform type.

In case you want to know how much of the system resources are being used by the monitored devices, use this screen to configure a rule for CPU, memory and session usage conditions.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **CPU Usage, Memory Usage** or **Session Usage** in the **Condition** field.

The fields are described in the following table.

Table 252 System Setting > Rule-based Alert > Add/Edit > CPU/Memory/Session Usage

LABEL	DESCRIPTION
Rule Name	This is the name identifying the rule. If you are adding a new rule, you can enter up to 28 alphanumeric characters for the rule name. If you are editing a rule, this field cannot be changed.
Choose Platform Type	This specifies what firmware platform the rule applies to. Select between ZLD or ZYNOS .
Information icon	Click this for a quick look of which devices belong to which platform type.
Filters	Set the criteria for the alert-based rule in this section.
Condition	Select CPU Usage, Memory Usage or Session Usage in this field.
(CPU/Memory/Session) Usage.. %	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • >= - Select this if you want to be alerted when a device uses resources greater than or equal to the percentage value you set. • <= - Select this if you want to be alerted when a device uses resources less than or equal to the percentage value you set. • < - Select this if you want to be alerted when a device uses resources greater than the percentage value you set. • > - Select this if you want to be alerted when a device uses resources less than the percentage value you set. For example, choose CPU Usage , select >= and set the percentage value to 75. This means Vantage Report sends an alert once a monitored device uses or exceeds usage of 75% of CPU resource allocation for a set time (see Period.. minutes field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device uses or exceeds usage of 75% of CPU resource allocation for 5 minutes, Vantage Report sends out an alert.
Add Criteria	Click this to add the set criteria to the list box.
Remove Criteria	Select a criteria from the list box and click Remove to delete this criteria.
Match all of the following	Click this if you want all criteria to apply before Vantage Report sends out a notification.
Match any of the following	Click this if you want Vantage Report to send out a notification even if only one criteria has been met.
Alert Setting	Vantage Report sends out a notification immediately as soon as conditions set in the rule are detected. Set when you want Vantage Report to send out the second and third notifications in this section.

Table 252 System Setting > Rule-based Alert > Add/Edit > CPU/Memory/Session Usage

LABEL	DESCRIPTION
Second Alert after.. minutes	Specify when you want Vantage Report to send a second e-mail notification. Enter the number of minutes between 1 to 60. Enter 0 to disable this.
Third alert after.. minutes	Specify when you want Vantage Report to send a third e-mail notification. Enter the number of minutes between 1 to 60. Enter 0 to disable this.
Select Devices	Check which devices the rule applies to. Click Select All if you want the conditions you set to be monitored for all devices.
Notification	
Notification Choose	Select a notification profile that applies to this rule. Click the Setting icon to take you to the System Setting > Notification screen (see Section 14.6 on page 561) for managing notification profiles.
Apply	Click this to add the rule or apply the edits to an existing rule.
Reset	Click this to leave all the fields blank or back to the original values if you are editing a previous configuration.
Cancel	Click this to go back to the Rule-Based Alert screen.

14.7.1.2 Port Usage

Use this screen to configure an alert rule for port usage.

Note: This condition filter only applies to the ZLD platform type.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Port Usage** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 273 System Setting > Rule-based Alert > Add/Edit > Port Usage

Condition: Port Usage

Port: port1

Direction: Tx+Rx

Traffic: >= 0 KBytes/s

Period: 1 minutes

Add Criteria Remove Criteria

The fields above are described in the following table.

Table 253 System Setting > Rule-based Alert > Add/Edit > Port Usage

LABEL	DESCRIPTION
Condition	Select Port Usage in this field.
Port	Select which port in the device you want to monitor.
Direction	Select if you want to check outgoing (Tx) or incoming (Rx) traffic. You can also choose both (Tx+Rx).

Table 253 System Setting > Rule-based Alert > Add/Edit > Port Usage

LABEL	DESCRIPTION
Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • >= - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • <= - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • < - Select this if you want to be alerted when a device uses resources greater than the value you set. • > - Select this if you want to be alerted when a device uses resources less than the value you set. For example, choose Port1 port and Tx direction, select >= and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes/s outgoing traffic on port 1 for a set time (see Period.. minutes field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of outgoing port traffic for 5 minutes, Vantage Report sends out an alert.

See [Section Table 252 on page 568](#) for descriptions of other table fields found in this screen.

14.7.1.3 Interface Usage

Use this screen to configure an alert rule for interface type (such as **Ethernet**, **VLAN** or **Bridge**) used by the selected device(s).

Note: This condition filter only applies to the ZLD platform type.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Interface Usage** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 274 System Setting > Rule-based Alert > Add/Edit > Interface Usage

The screenshot shows a configuration form for 'Interface Usage'. It includes dropdown menus for 'Condition' (set to 'Interface Usage'), 'Interface Type' (set to 'Ethernet'), 'Direction' (set to 'Tx+Rx'), 'Interface Name' (set to 'ge1'), and 'Traffic' (set to '>= 0 KBytes/s'). A text input field for 'Period' is set to '1 minutes'. At the bottom, there are two buttons: 'Add Criteria' and 'Remove Criteria'.

The fields above are described in the following table.

Table 254 System Setting > Rule-based Alert > Add/Edit > Interface Usage

LABEL	DESCRIPTION
Condition	Select Interface Usage in this field.
Interface Type	Select which interface mode you want to monitor. Interface refers to the connectivity implementation of the device to the network or other devices. Choose one of the following. • Ethernet • VLAN • PPP (stands for Point-to-Point Protocol) • Bridge • Dial-backup • 3G (stands for 3rd Generation) • wireless
Interface Name	Select the specific name for devices that can have multiple interface profiles.
Direction	Select if you want to check outgoing (Tx) or incoming (Rx) traffic. You can also choose both (Tx+Rx).
Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • >= - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • <= - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • < - Select this if you want to be alerted when a device uses resources greater than the value you set. • > - Select this if you want to be alerted when a device uses resources less than the value you set. For example, choose Ethernet, specifying lan1 interface and Tx direction, select >= and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes/s outgoing traffic on lan1 of the Ethernet interface for a set time (see Period.. minutes field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of interface traffic for 5 minutes, Vantage Report sends out an alert.

See [Section Table 252 on page 568](#) for descriptions of other table fields found in this screen.

14.7.1.4 Service

Use this screen to configure an alert rule based on a service (such as **Web**, **Mail** or **FTP**) used by the selected device(s).

Note: This condition filter only applies to both the ZLD and ZYNOS platform types.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Service** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 275 System Setting > Rule-based Alert > Add/Edit > Service

Condition: Service

Service Type: WEB

Service Traffic: >= 0 KBytes

Period: 1 minutes

Add Criteria Remove Criteria

The fields above are described in the following table.

Table 255 System Setting > Rule-based Alert > Add/Edit > Service

LABEL	DESCRIPTION
Condition	Select Service in this field.
Interface Type	Select which service type you want to monitor. Choose one of the following. • WEB • FTP • MAIL • IPSec VPN • SSL VPN

Table 255 System Setting > Rule-based Alert > Add/Edit > Service

LABEL	DESCRIPTION
Service Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • >= - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • <= - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • < - Select this if you want to be alerted when a device uses resources greater than the value you set. • > - Select this if you want to be alerted when a device uses resources less than the value you set. For example, choose MAIL, select >= and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes for mail for a set time (see Period.. minutes field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of mail traffic for 5 minutes, Vantage Report sends out an alert.

See [Section Table 252 on page 568](#) for descriptions of other table fields found in this screen.

14.7.1.5 Attack/Intrusion/Antivirus/Antispam

Use this screen to configure an alert rule for the number of attacks, intrusions, virus and spam detected on the selected device(s).

Note: These condition filters apply to both ZLD and ZYNOS platform types.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select either **Attack**, **Intrusion**, **Antivirus** or **Antispam** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 276 System Setting > Rule-based Alert > Add/Edit > Attack/Intrusion/Antivirus/Antispam

Condition: Attack

Attacks: >= 0

Period: 1 minutes

Add Criteria Remove Criteria

The fields above are described in the following table.

Table 256 System Setting > Rule-based Alert > Add/Edit > Attack/Intrusion/Antivirus/Antispam

LABEL	DESCRIPTION
Condition	Select either Attack , Intrusion , Antivirus or Antispam in this field.
Attacks	Set your filters according to how many attacks, intrusions, virus and spam are detected on a device. The following parameters can be used. • >= - Select this if you want to be alerted when number of encounters is greater than or equal to the value you set. • <= - Select this if you want to be alerted when number of encounters is less than or equal to the value you set. • < - Select this if you want to be alerted when number of encounters is greater than the value you set. • > - Select this if you want to be alerted when number of encounters is less than the value you set. For example, choose Attack, select >= and set the percentage value to 5. This means Vantage Report sends an alert once a monitored device receives 5 attacks for a set time (see Period.. minutes field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device received 5 attacks within 5 minutes, Vantage Report sends out an alert.

See [Section Table 252 on page 568](#) for descriptions of other table fields found in this screen.

14.7.1.6 Bandwidth

Use this screen to configure an alert rule for bandwidth traffic used by the selected device(s).

Note: This condition only applies to the ZYNOS platform type.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Bandwidth** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 277 System Setting > Rule-based Alert > Add/Edit > Service

The screenshot shows a web interface for configuring a rule-based alert. The 'Condition' dropdown is set to 'Bandwidth'. Below it, the 'Traffic' field contains a dropdown set to '>=' followed by a text input '0' and the unit 'KBytes/s'. To the right, the 'Period' field contains a text input '1' followed by the unit 'minutes'. At the bottom of the configuration area are two buttons: 'Add Criteria' and 'Remove Criteria'.

The fields above are described in the following table.

Table 257 System Setting > Rule-based Alert > Add/Edit > Service

LABEL	DESCRIPTION
Condition	Select Bandwidth in this field.
Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • >= - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • <= - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • < - Select this if you want to be alerted when a device uses resources greater than the value you set. • > - Select this if you want to be alerted when a device uses resources less than the value you set. For example, select >= and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes/s bandwidth for a set time (see Period.. minutes field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of bandwidth for 5 minutes, Vantage Report sends out an alert.

See [Section Table 252 on page 568](#) for descriptions of other table fields found in this screen.

User Management

The `root` account or accounts in the 'super' group can use these screens to view, add, edit, or remove Vantage Report groups and users. Other users can only use these screens to look at and edit their user settings, including their password. The screens are the same except where noted below.

15.1 Group Screen

Use the **Group** screen to set up user group for Vantage Report.

Click **User Management > Group** to open the **Group** screen.

Note: Only the `root` account or accounts in the 'super' group can open this screen.

Figure 278 User Management > Group

#	Group Name	Type	Description
☐	yvonne	Normal	

Total Count:11 Total Page:2 First 1 2 Last Go

Add Delete

Each field is described in the following table.

Table 258 User Management > Group

LABEL	DESCRIPTION
#	Select the check box next to a user group, and click Delete to remove the group. This does not apply to the super group since you cannot delete it.
Group Name	This field displays the name of the user group. You can also click this to edit the group settings. The Add/Edit Group screen appears.

Table 258 User Management > Group

LABEL	DESCRIPTION
Type	This field displays the type of the user group. Super displays if the group has read/write/execute permissions for all Vantage Report screens. Normal displays if the group has read/write permissions for the Monitor, Report and Logs > Log Reviewer screens. Read-Only displays if the group has read permissions only for the Monitor, Report and Logs > Log Reviewer screens.
Description	This field displays the description for the group.
Total Count	This field displays how many groups there are.
Total Page	This field displays how many screens it takes to display all the groups.
First .. Last	Click First , Last , or a specific page number to look at the groups on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .
Add	Click this to create a new group. The Add/Edit Group screen appears.
Delete	Click this to delete the groups that are selected in Index field. You cannot to delete a group if it still contains any users.

15.1.1 Group > Add/Edit Group Screen

Use this screen to add or edit a user group.

Click the link in an entry in **User Management > Group** to access this screen.

Figure 279 User Management > Group > Add/Edit Group

All the fields are described in the following table.

Table 259 User Management > Group > Add/Edit Group

LABEL	DESCRIPTION
Basic Information	Use this part of the screen to view the group name you selected and to modify the description.
Group Name	If you are editing an existing group, this field is read-only. It displays the name of the user. If you are creating a new group, enter the user name for the new account. The user name must be 1-28 alphanumeric characters and/or underscores(_) long, and it must begin with a letter or underscore.
Type	Select the user group type. If you select Normal, the members of this group can access the Monitor, Report and Logs screens with read/write permissions. If you select Read-Only, the members of this group can access the Monitor, Report and Logs screens with read permissions only.
Description	Enter the description for the user group.
Supported Devices	Use this part of the screen to select the devices the user group can view. The available folders and devices are listed, select individual devices or a folder to select all devices under it. Select the Select All to select all folders and devices.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to return to the previous screen without saving any changes.

15.2 Account Screen

Use the **Account** screen to manage user accounts for Vantage Report.

Click **User Management > Account** to open the **Account** screen.

Figure 280 User Management > Account

Index	User Name	E-mail	Description	Group	Status
☐	joshua			super	offline
☐	jacky8			super	offline
☐	readonly			ReadOnlyGroup	offline

Total Count:23 Total Page:3 First 1 2 3 Last Go

Add Delete

Other (non-**root**) users can only see their account in this screen. Each field is described in the following table.

Table 260 User Management > Account

LABEL	DESCRIPTION
Index	Select the check box next to a user account, and click Delete to remove the account. This does not apply to the root account since you cannot delete it.
User Name	This field displays the user name used to log in. You can also click this to edit the account settings. The Add/Edit User Account screen appears.
E-mail	This field displays the e-mail address associated with the user account. This address is used for notifications (root only) and forgotten passwords.
Description	This field displays the description for the user account.
Group	This field displays the group the user account belongs to.
Status	This field displays whether or not the user is logged in to Vantage Report. off line - this user is not currently logged in on line - this user is currently logged in
Total Count	This field displays how many accounts there are.
Total Page	This field displays how many screens it takes to display all the accounts.
First .. Last	Click First , Last , or a specific page number to look at the accounts on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click Go .
Add	Click this to create a new user account. The Add/Edit User Account screen appears.
Delete	Click this to delete the user accounts that are selected in Index field. If a user is currently logged in, the user is kicked out of the system the next time the session accesses the Vantage Report server.

15.2.1 Account > Add/Edit User Account Screen

Use this screen to add or edit a user account.

To access this screen, click **User Management > Account**, and click a user name to edit it or click the **Add** button to create a new account.

Figure 281 User Management > Account > Add/Edit User Account

The screenshot shows a web form titled 'Add User'. It contains the following fields: 'User Name:', 'Password:', 'Confirm:', 'E-mail:', 'Group:', and 'Description:'. The 'Group' field is a dropdown menu with 'super' selected. Each of the first five fields has a red asterisk to its right. The 'Description' field is a text area. At the bottom of the form are three buttons: 'Apply', 'Reset', and 'Cancel'.

Each field is described in the following table.

Table 261 User Management > Account > Add/Edit User Account

LABEL	DESCRIPTION
User Name	If you are editing an existing account, this field is read-only. It displays the user name used to log in. If you are creating a new account, enter the user name for the new account. The user name must be 1-28 alphanumeric characters and/or underscores(_) long, and it must begin with a letter or underscore.
Password	If you are editing an existing account, this field displays the same number of asterisks, regardless of the current password. You can change the password. If you are creating a new account or changing the password of an existing account, enter the password for the new account. The password must be 4-30 alphanumeric characters and/or underscores(_) long.
Confirm	Type the password again to verify it, if you are creating a new account or changing the password of an existing account.
E-mail	Enter the e-mail address associated with the user account. This address is used for notifications (root only) and forgotten passwords.
Group	Select the group for the user account. The 'super' group can view all devices, just like the root account.
Description	Enter the description for the user account.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

I cannot start the Vantage Report sever.

- 1 Make sure the following system variables are defined.

`PATH=%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem`

Do the following to check these variables in different operating systems.

- In Windows 2000, click **Start > Settings > Control Panel > System > Advanced > Environment Variables**.
- In Windows XP, click **Start > Control Panel > System > Advanced > Environment Variables**.
- In Windows Vista/7, click **Start > Control Panel > System > Advanced system settings > Advanced > Environment Variables**.

Make sure the variables are in the **System Variables** box.

- 2 If the problem continues, follow these steps to collect logs.

- Edit the file `<Installed directory>\vrpt\conf\log4j.properties`.

Change the following:

`log4j.logger.com.zyxel.vantage.vrpt = INFO`

`log4j.logger.com.zyxel.vantage.web = INFO`

To:

`log4j.logger.com.zyxel.vantage.vrpt = DEBUG`

`log4j.logger.com.zyxel.vantage.web = DEBUG`

- Restart the Vantage Report server.
- Get the log files from the `<Installed directory>\vrpt\log` folder and send them to your local vendor.

There is no information in any report for my device.

- 1 If you just added the device, wait. See [Table 2 on page 25](#) for the amount of time it takes for information to appear in each report.
- 2 Look for the device's MAC address in `<Installed directory>\vrpt\log\LogRecord.log` in the Vantage Report installation directory. This file keeps track of all the log entries received by the syslog server in Vantage Report, including log entries for devices that are not set up in Vantage Report.
 - If the MAC address is in the file, Vantage Report is receiving information from the device. Wait. If the **Attribute** is **Unregistered**, however, the MAC address is not set up correctly in Vantage Report. See section [3.4](#).
 - If the MAC address is not in the file, Vantage Report is not receiving information from the device. Make sure you have configured the ZyXEL devices correctly. See section [2.6](#).
- 3 Make sure packets on TCP port 3316, UDP port 514, and the port number you specified during installation are forwarded to the Vantage Report server, especially if the Vantage Report server runs behind a NAT or firewall.
- 4 Check the amount of available disk space on the Vantage Report server. If it is less than the value in [Appendix A on page 589](#), the Vantage Report server stops receiving log entries.
- 5 Make sure your ZyXEL devices support Vantage Report. Check the release notes for the current firmware version.
- 6 Check the connections between the ZyXEL devices and Vantage Report server.
- 7 Make sure the system times on the Vantage Report server and the managed devices are configured correctly.

If the problem continues, contact your local vendor.

[There is information in some reports, but there is no information in others.](#)

- 1 Make sure your ZyXEL devices support these reports. Check the release notes for the current firmware version.
- 2 Make sure you have configured the ZyXEL devices correctly. See section [2.6](#).
- 3 Make sure there are log entries or traffic statistics for the report dates you selected. For example, if there were no attacks yesterday, yesterday's attack report is empty.

If the problem continues, contact your local vendor.

My web configurator screens still show information from the previous version (like the old version number) after a successful upgrade.

- 1 Clear the browser's cache on your computer.
 - In Internet Explorer, click **Tools** > **Internet Option** > **Delete Cookies** > **Delete files**.
 - In Firefox, click **Tools** > **Options** > **Privacy** > **Cache** > **Clear Cache Now**.
 - In Mozilla, click **Edit** > **Preferences** > **Privacy** > **Cache** > **Clear**.
- 2 Close your browser and open a new web configurator session. The version number should be updated.

PART IV

Appendices and Index

Product Specifications (589)

ZyWALL USG Series and ZyWALL 1050
Log Descriptions (599)

ZyNOS Log Descriptions (645)

Open Software Announcements (671)

Legal Information (709)

Index (711)

Product Specifications

All values are accurate at the time of writing.

See [Table 2 on page 25](#) for specifications about the time it takes the Vantage Report server to process information from ZyXEL devices.

Table 262 Supported Operation System Specifications

OPERATION SYSTEM	TYPE
Windows XP Professional	32 bits
Windows 2000	32 bits
Windows 2003 Server	32 bits
Windows Vista	32 bits / 64 bits
Windows 2008 Server	32 bits / 64 bits
Windows 7	32 bits / 64 bits

Table 263 Web Configurator Specifications

FEATURE	SPECIFICATION
URL	http://{Vantage Report server IP}:8080/vrpt http://localhost:8080/vrpt (web configurator on same machine as server)
Default User Name	root
Default Password	root
MySQL port number	3316 (TCP)
Syslog port number	514 (UDP)

Table 264 System Notifications Specifications

FEATURE	SPECIFICATION
Maximum number of logs for each device	15,000,000
Warning: Maximum number of logs for each device	10,000,000
Minimum amount of free disk space required to run Vantage Report	800 MB
Warning: Minimum amount of free disk space required to run Vantage Report	Per Low free disk Mark.

Table 265 Feature Specifications

FEATURE	SPECIFICATION
Maximum Number of Entries in the Table at the Bottom of Each Statistical Report	30
Log Consolidation Frequency	4 minutes

Table 266 Key Features

FEATURE	DESCRIPTION
Executive Dashboard	Get a quick top level summary of activity across devices. You can also easily drill-down to get more details on any area of interest. Select which reports or monitors you want Vantage Report to display first when you login.
Customizable Reports	Display company logos, record information and edit report titles to match customer accounts.
Device Monitors and Logs	Monitor the status of all your ZyXEL devices in one application. You can also look at the logs for all your ZyXEL devices in Vantage Report. In normal operation, this information should be no older than five minutes, worst-case.
Real-time Syslog Viewer	As soon as events are shown in the monitors and reports, you can see the log details in the log viewer.
Statistical Reports	Generate reports for historical analysis. These reports include bandwidth usage, service usage, Secure Remote Access usage, web filter (blocked sites), attack, intrusion, anti-virus, anti-spam, authentication, and endpoint security (EPS) reports. (Some reports are not available for every ZyXEL device.)
Drill-Down Reports	In most statistical reports, look at more details for clearer understanding and better decisions. For example, when you look at the top web sites, you can look at which users are accessing each one.
Report Formats	Generate statistical reports in PDF or HTML format.
Reverse DNS Lookup	Where possible, see domain names, instead of IP addresses, in statistical reports.
Reverse Hostname Lookup	Where possible, see host names, instead of IP addresses, in statistical reports.
Scheduled Reports	Set up regular times to generate and e-mail statistical reports.
Registration, Activation, and Upgrades	Register and activate on myZyXEL.com through Vantage Report. This makes getting the trial version and upgrading simpler.
System Service	Run and manage Vantage Report as a system service.
Administration	Create separate accounts for network administrators and device administrators. These accounts do not give access to administration screens for Vantage Report.
File Management and Data Maintenance	Backup Vantage Report configurations, including various statistical "snapshots", and restore them later.

The following tables list which features Vantage Report supports with various firmware versions of various devices.

Table 267 VRPT 3.6 Feature Support for USG Series and ZyWALL 1050 Devices

MENU ITEM		ZYWALL 1050 / ZYWALL USG ^A
		1.01 / 2.00 / 2.01 / 2.20
Dashboard		Y
Monitor		
Device Dashboard		Y
Hardware Status		
	CPU Usage	Y
	Memory Usage	Y
Network Traffic		
	Session Usage	Y
	Bandwidth	
	Port Usage	Y
	Interface Usage	Y
	Web	Y
	FTP	Y
	Mail	Y
Secure Remote Access		
	Site-to-site (IPSec)	Y
	Client-to-site(SSL)	Y
Network Security		
	Firewall Access Control	Y
	Attack	Y
	Intrusion Hits	Y
	Antivirus	Y
E-Mail Security		
	Virus Found	Y
	Spam	Y
	Intrusion Hits	Y
Web Security		
	Security Threat	Y
	Virus Found	Y
	Intrusion Hits	Y
Security Policy Enforcement		
	Content Filter	Y
	App Patrol	Y
Report		
Network Traffic		
	Bandwidth	Y
	WEB	Y

Table 267 VRPT 3.6 Feature Support for USG Series and ZyWALL 1050 Devices

MENU ITEM		ZYWALL 1050 / ZYWALL USG ^A
		1.01 / 2.00 / 2.01 / 2.20
	FTP	Y
	MAIL	Y
	Customization	Y
Secure Remote Access		
	Site-to-Site IPSec	Y
	Client-to-Site IPSec	Y
	Client-to-Site (SSL)	Y
	Xauth	Y
Network Security		
	Firewall Access Control	Y
	Attack	Y
	Intrusion Hits	Y
	Antivirus	Y
E-Mail Security		
	Virus Found	Y
	Spam	Y
	Intrusion Hits	Y
Web Security		
	Security Threat	Y
	Virus Found	Y
	Intrusion Hits	Y
Security Policy Enforcement		
	EPS	Y
	Content Filter(All)	Y
	Content Filter(Blocked)	Y
	Application Access Control	Y
Event		
	Login	Y
	Session Per Host	Y
Schedule Report		
	Summary	Y
	Configure Template	Y
	Logo Template	Y
Log		
Log Viewer		Y
Log Receiver		Y
VRPT System Logs		Y
Log Archiving		Y
Log Remove		Y

A. ZyWALL USG series includes ZyWALL 100 / 200 / 300 / 1000 / 2000.

Table 268 VRPT 3.6 Feature Support for ZyNOS Devices

MENU ITEM			ZYWALL				P-	IDP
			ZYWALL 2	ZYWALL 2 PLUS / 2WG	ZYWALL P1 / 5 / 35 / 70	ZYWALL P1 / 5 / 35 / 70	P-662 P-652	IDP 10
			3.62	4.02	3.63 / 3.64 / 3.65	4.00 / 4.01 / 4.02	3.40	2.00
Monitor								
	Dashboard		Y	Y	Y	Y	Y	Y
	Bandwidth		N/A	Y	Y	Y	N/A	Y
	CPU Usage		N/A	N/A	N/A	N/A	N/A	N/A
	Memory Usage		N/A	N/A	N/A	N/A	N/A	N/A
	Session Usage		N/A	N/A	N/A	N/A	N/A	N/A
	Port Usage		N/A	N/A	N/A	N/A	N/A	N/A
	Interface Usage		N/A	N/A	N/A	N/A	N/A	N/A
	Service		N/A	Y	Y	Y	N/A	Y
	Attack		Y	Y	Y	Y	Y	N/A
	Intrusion		N/A	Y	N/A	Y	N/A	Y
	AntiVirus		N/A	Y	N/A	Y	N/A	N/A
	AntiSpam		N/A	Y	N/A	Y	N/A	N/A
Report > Traffic								
	Bandwidth							
		Summary	N/A	Y	Y	Y	N/A	Y
		Top Protocols	N/A	Y	Y	Y	N/A	Y
		Top Hosts	N/A	Y	Y	Y	N/A	Y
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
		Top Destinations	N/A	Y	Y	Y	N/A	Y
	WEB							
		Top Sites	N/A	Y	Y	Y	N/A	Y
		Top Hosts	N/A	Y	Y	Y	N/A	Y
		Top Users	N/A	N/A	N/A	N/A	N/A	Y
	FTP							
		Top Sites	N/A	Y	Y	Y	N/A	Y
		Top Hosts	N/A	Y	Y	Y	N/A	Y
		Top Users	N/A	N/A	N/A	N/A	N/A	Y
	MAIL							
		Top Sites	N/A	Y	Y	Y	N/A	Y
		Top Hosts	N/A	Y	Y	Y	N/A	Y
		Top Users	N/A	N/A	N/A	N/A	N/A	Y
	Customization							
		Customization	N/A	Y	Y	Y	N/A	Y

Table 268 VRPT 3.6 Feature Support for ZyNOS Devices

MENU ITEM			ZYWALL				P-	IDP
			ZYWALL 2	ZYWALL 2 PLUS / 2WG	ZYWALL P1 / 5 / 35 / 70	ZYWALL P1 / 5 / 35 / 70	P-662 P-652	IDP 10
			3.62	4.02	3.63 / 3.64 / 3.65	4.00 / 4.01 / 4.02	3.40	2.00
		Top Destinations	N/A	Y	Y	Y	N/A	Y
		Top Sources	N/A	Y	Y	Y	N/A	Y
		Top Users	N/A	N/A	N/A	N/A	N/A	Y
Report > VPN								
	Site-to-Site							
		Link Status	N/A	N/A	N/A	N/A	N/A	N/A
		Traffic Monitor	N/A	N/A	N/A	N/A	N/A	N/A
		Top Sites	N/A	N/A	N/A	N/A	N/A	N/A
		Top Tunnels	N/A	N/A	N/A	N/A	N/A	N/A
		Top Protocols	N/A	Y	Y	Y	N/A	N/A
		Top Hosts	N/A	Y	Y	Y	N/A	N/A
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
		Top Destinations	N/A	N/A	N/A	N/A	N/A	N/A
	Remote Access (IPSec)							
		User Status	N/A	N/A	N/A	N/A	N/A	N/A
		Top Protocols	N/A	N/A	N/A	N/A	N/A	N/A
		Top Destinations	N/A	N/A	N/A	N/A	N/A	N/A
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
	Remote Access (SSL)							
		User Status	N/A	N/A	N/A	N/A	N/A	N/A
		Top Protocols	N/A	N/A	N/A	N/A	N/A	N/A
		Top Destinations	N/A	N/A	N/A	N/A	N/A	N/A
		Top Applications	N/A	N/A	N/A	N/A	N/A	N/A
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
	Xauth							
		Successful Login	Y	Y	Y	Y	N/A	N/A
		Failed Login	Y	Y	Y	Y	N/A	N/A
Report > Network Attack								
	Attack							
		Summary	Y	Y	Y	Y	Y	N/A

Table 268 VRPT 3.6 Feature Support for ZyNOS Devices

MENU ITEM			ZYWALL				P-	IDP
			ZYWALL 2	ZYWALL 2 PLUS / 2WG	ZYWALL P1 / 5 / 35 / 70	ZYWALL P1 / 5 / 35 / 70	P-662 P-652	IDP 10
			3.62	4.02	3.63 / 3.64 / 3.65	4.00 / 4.01 / 4.02	3.40	2.00
		Top Attacks	Y	Y	Y	Y	Y	N/A
		Top Sources	Y	Y	Y	Y	Y	N/A
		By Type	N/A	N/A	N/A	N/A	N/A	N/A
	Intrusion							
		Summary	N/A	N/A	N/A	Y	N/A	Y
		Top Intrusions	N/A	N/A	N/A	Y	N/A	Y
		Top Sources	N/A	N/A	N/A	Y	N/A	Y
		Top Destinations	N/A	N/A	N/A	Y	N/A	Y
		By Severity	N/A	N/A	N/A	Y	N/A	Y
	AntiVirus							
		Summary	N/A	N/A	N/A	Y	N/A	N/A
		Top Viruses	N/A	N/A	N/A	Y	N/A	N/A
		Top Sources	N/A	N/A	N/A	Y	N/A	N/A
		Top Destinations	N/A	N/A	N/A	Y	N/A	N/A
	AntiSpam							
		Summary	N/A	N/A	N/A	Y (N/A for ZyWALL P1)	N/A	N/A
		Top Senders	N/A	N/A	N/A	Y (N/A for ZyWALL P1)	N/A	N/A
		Top Sources	N/A	N/A	N/A	Y (N/A for ZyWALL P1)	N/A	N/A
Report > Security Policy								
	Firewall Access Control							
		Top Users Blocked	N/A	N/A	N/A	N/A	N/A	N/A
		Top Packets Blocked	Y	Y	Y	Y	N/A	N/A
	Application Access Control							
		Top Applications Blocked	N/A	N/A	N/A	N/A	N/A	N/A
		Top Users Blocked	N/A	N/A	N/A	N/A	N/A	N/A

Table 268 VRPT 3.6 Feature Support for ZyNOS Devices

MENU ITEM			ZYWALL				P-	IDP
			ZYWALL 2	ZYWALL 2 PLUS / 2WG	ZYWALL P1 / 5 / 35 / 70	ZYWALL P1 / 5 / 35 / 70	P-662 P-652	IDP 10
			3.62	4.02	3.63 / 3.64 / 3.65	4.00 / 4.01 / 4.02	3.40	2.00
		Top Applications Allowed	N/A	N/A	N/A	N/A	N/A	N/A
	Web Blocked							
		Summary	Y	Y	Y	Y	N/A	N/A
		Top Sites	Y	Y	Y	Y	N/A	N/A
		Top Hosts	Y	Y	Y	Y	N/A	N/A
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
		By Category	Y	Y	Y	Y	N/A	N/A
	Web Allowed							
		Summary	Y	Y	Y	Y	N/A	N/A
		Top Sites	Y	Y	Y	Y	N/A	N/A
		Top Hosts	Y	Y	Y	Y	N/A	N/A
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
Report > Event								
	Login							
		Successful Login	Y	Y	Y	Y	N/A	N/A
		Failed Login	Y	Y	Y	Y	N/A	N/A
	Sessions Per Host							
		Top Hosts	Y	Y	Y	Y	N/A	N/A
		Top Users	N/A	N/A	N/A	N/A	N/A	N/A
Report > EPS			N/A	N/A	N/A	N/A	N/A	N/A
Report > Schedule Report								
	Summary		Y	Y	Y	Y	N/A	N/A
	Configure Template		Y	Y	Y	Y	N/A	N/A
	Logo Template		Y	Y	Y	Y	N/A	N/A
Logs								
	Log Viewer		Y	Y	Y	Y	Y	Y
	Log Receiver							
		By Day (Summary)	Y	Y	Y	Y	Y	Y
		By Device	Y	Y	Y	Y	Y	Y
	VRPT System Logs		Y	Y	Y	Y	Y	Y
	Log Archiving							

Table 268 VRPT 3.6 Feature Support for ZyNOS Devices

MENU ITEM			ZYWALL				P-	IDP
			ZYWALL 2	ZYWALL 2 PLUS / 2WG	ZYWALL P1 / 5 / 35 / 70	ZYWALL P1 / 5 / 35 / 70	P-662 P-652	IDP 10
			3.62	4.02	3.63 / 3.64 / 3.65	4.00 / 4.01 / 4.02	3.40	2.00
		File Archiving Settings	Y	Y	Y	Y	Y	Y
		View Archived Files	Y	Y	Y	Y	Y	Y
	Log Remove		Y	Y	Y	Y	Y	Y

ZyWALL USG Series and ZyWALL 1050 Log Descriptions

This appendix provides descriptions of example log messages for the ZyWALL 1050 and ZyWALL USG Series.

Table 269 Content Filter Logs

LOG MESSAGE	DESCRIPTION
Content filter has been enabled	An administrator turned the content filter on.
Content filter has been disabled	An administrator turned the content filter off.

Table 270 Forward Web Site Logs

LOG MESSAGE	DESCRIPTION
%s: Trusted Web site	The device allowed access to a web site in a trusted domain. %s: website host
%s	The device allowed access to a web site. The content filtering service is registered and activated or the service is not activated in a profile, this is a web site that is not blocked according to a profile and the default policy is not set to block. %s: website host
%s: Service is not registered	The device allowed access to a web site. The content filtering service is unregistered and the default policy is not set to block. %s: website host

Table 271 Blocked Web Site Logs

LOG MESSAGE	DESCRIPTION
%s : %s	The rating server responded that the web site is in a specified category and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
%s: Unrated	The rating server responded that the web site cannot be categorized and access was blocked according to a content filter profile. %s: website host
%s: Service is unavailable	Content filter rating service is temporarily unavailable and access to the web site was blocked due to: 1. Can't resolve rating server IP (No DNS) 2. Invalid service license 4. Rating service is restarting 5. Can't connect to rating server 6. Query failed 7. Query timeout 8. Too many queries 9. Unknown reason %s: website host
%s: %s(cache hit)	The web site's category exists in the device's local cache and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
%s: Not in trusted web list	The web site is not a trusted host/domain, and the device blocks all traffic except for trusted web sites. %s: website host
%s: Contains ActiveX	The web site contains ActiveX and access was blocked according to a profile. %s: website host
%s: Contains Java applet	The web site contains Java applet and access was blocked according to a profile. %s: website host
%s: Contains cookie	The web site contains a cookie and access was blocked according to a profile. %s: website host

Table 271 Blocked Web Site Logs (continued)

LOG MESSAGE	DESCRIPTION
%s: Proxy mode is detected	The system detected a proxy connection and blocked access according to a profile. %s: website host
%s: Forbidden Web site	The web site is in forbidden web site list. %s: website host
%s: Keyword blocking	The web content matched a user defined keyword. %s: website host
%s: Blocking by default policy	No content filter policy is applied and access was blocked since the default action is block. %s: website host

Table 272 User Logs

LOG MESSAGE	DESCRIPTION
%s %s has logged in from %s	The specified user signed in. 1st %s: Administrator Limited-Admin User Ext-User Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s has logged out from %s	The specified user signed out. 1st %s: Administrator Limited-Admin User Ext-User Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s from %s has been logged out (re-auth timeout)	The specified user was signed out by the device due to a re-authentication timeout. 1st %s: Administrator Limited-Admin User Ext-User Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.

Table 272 User Logs (continued)

LOG MESSAGE	DESCRIPTION
%s %s from %s has been logged out (lease timeout)	The specified user was signed out by the device due to a lease timeout. 1st %s: Administrator Limited-Admin User Ext-User Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s from %s has been logged out (idle timeout)	The specified user was signed out by the device due to an idle timeout. 1st %s: Administrator Limited-Admin User Ext-User Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
Console is put into lockout	Too many failed login attempts were made on the console port so the device is blocking login attempts on the console port.
Address %u.%u.%u.%u is put into lockout	Too many failed login attempts were made from an IP address so the device is blocking login attempts from that IP address. %u.%u.%u.%u: the source address of the user's login attempt
Login attempt is made on a lockout address from %s	A login attempt came from an IP address that the device has locked out. %u.%u.%u.%u: the source address of the user's login attempt
Failed %s login attempt (reach the maximum number of user)	The device blocked a login because the maximum login capacity has already been reached. %s: service name
Failed %s login attempt (reach the maximum number of simultaneous logon)	The device blocked a login because the maximum simultaneous login capacity for the administrator or access account has already been reached. %s: service name

Table 273 myZyXEL.com Logs

LOG MESSAGE	DESCRIPTION
Send registration message to MyZyXEL.com server has failed.	The device was not able to send a registration message to MyZyXEL.com.
Get server response has failed.	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
Timeout for get server response.	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
User has existed.	The user name already exists in MyZyXEL.com's database. So the user can't use it for device registration and needs to specify another one.
User does not exist.	The user name does not yet exist in MyZyXEL.com's database. So the user can use it for device registration.
Internal server error.	MyZyXEL.com's database had an error when checking the user name.
Device registration has failed:%s.	Device registration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by the myZyXEL.com server
Device registration has succeeded.	The device registered successfully with the myZyXEL.com server.
Registration has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
%s: Trial service activation has failed:%s.	Trail service activation failed for the specified service, an error message returned by the MyZyXEL.com server will be appended to this log. 1st %s: service name 2nd %s: error message returned by the myZyXEL.com server
%s: Trial service activation has succeeded.	Trail service was activated successfully for the specified service. %s: service name
Trial service activation has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
Standard service activation has failed:%s.	Standard service activation failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by the myZyXEL.com server
Standard service activation has succeeded.	Standard service activation has succeeded.

Table 273 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Standard service activation has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
Service expiration check has failed:%s.	The service expiration day check failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by myZyXEL.com server
Service expiration check has succeeded.	The service expiration day check was successful.
Service expiration check has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
Server setting error.	The device could not retrieve the myZyXEL.com server's IP address or FQDN from local.
Resolve server IP has failed.	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
Verify server's certificate has failed.	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate.
Connect to MyZyXEL.com server has failed.	The device could not connect to the MyZyXEL.com server.
Do account check.	The device started to check whether or not the user name in MyZyXEL.com's database.
Do device register.	The device started device registration.
Do trial service activation.	The device started trail service activation.
Do standard service activation.	The device started standard service activation.
Do expiration check.	The device started the service expiration day check.
Build query message has failed.	Some information was missing in the packets that the device sent to the MyZyXEL.com server.
Parse receive message has failed.	The device cannot parse the response returned by the MyZyXEL.com server. Maybe some required fields are missing.
Resolve server IP has failed. Update stop.	The update has stopped because the device couldn't resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
Verify server's certificate has failed. Update stop.	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate. The update has stopped.
Send download request to update server has failed.	The device's attempt to send a download message to the update server failed.
Get server response has failed.	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.

Table 273 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Timeout for get server response.	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
Send update request to update server has failed.	The device could not send an update message to the update server.
Update has failed. Because of lack must fields.	The device received an incomplete response from the update server and it caused a parsing error for the device.
Update server is busy now. File download after %d seconds.	The update server was busy so the device will wait for the specified number of seconds and send the download request to the update server again.
Device has latest file. No need to update.	The device already has the latest version of the file so no update is needed.
Device has latest signature file; no need to update	The device already has the latest version of the signature file so no update is needed.
Connect to update server has failed.	The device cannot connect to the update server.
Wrong format for packets received.	The device cannot parse the response returned by the server. Maybe some required fields are missing.
Server setting error. Update stop.	The device could not resolve the update server's FQDN to an IP address through gethostbyname(). The update process stopped.
Build query message failed.	Some information was missing in the packets that the device sent to the server.
Starting signature update.	The device started an IDP signature update.
Signature download has succeeded.	The device successfully downloaded a signature file.
Signature update has succeeded.	The device successfully downloaded and applied an IDP signature file.
Signature update has failed:%s.	The signature update signature failed, an error message returned by the update server will be appended to this log. %s: error message returned by update server
Signature download has failed.	The device still can't download the IDP signature after 3 retries.
Signature update has failed. Do %d retry.	The IDP signature update failed, so the device will process 3 retries. %d: retry times (1~3)
Resolve server IP has failed.	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
Connect to MyZyXEL.com server has failed.	The device could not connect to the MyZyXEL.com server.

Table 273 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Build query message has failed.	Some information was missing in the packets that the device sent to the server.
Verify server's certificate has failed.	The device could not process an HTTPS connection because it could not verify the server's certificate.
Get server response has failed.	The device sent packets to the server, but did not receive a response. The root cause may be that the connection is abnormal.
Expiration daily-check has failed:%s.	The daily check for service expiration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by myZyXEL.com server
Do expiration daily-check has failed. Because of lack must fields.	The device received an incomplete response to the daily service expiration check and the packets caused a parsing error for the device.
Server setting error.	The device could not retrieve the server's IP address or FQDN from local.
Do expiration daily-check has failed.	The daily check for service expiration failed.
Do expiration daily-check has succeeded.	The daily check for service expiration was successful.
Expiration daily-check will trigger PPP interface. Do self-check.	Before the device sends an expiration day check packet, it needs to check whether or not it will trigger a PPP connection.
System bootup. Do expiration daily-check.	The device processes a service expiration day check immediately after it starts up.
After register. Do expiration daily-check immediately.	The device processes a service expiration day check immediately after device registration.
Time is up. Do expiration daily-check.	The processes a service expiration day check every 24 hrs.
Read MyZyXEL.com storage has failed.	Read data from EEPROM has failed.
Open /proc/MRD has failed.	This error message is shown when getting MAC address.
IDP service has expired.	The IDP service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count.
Content-Filter service has expired.	The content filtering service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count.
Unknown TLS/SSL version: %d.	The device only supports SSLv3 protocol. %d: SSL version assigned by client.

Table 273 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Load trusted root certificates has failed.	The device needs to load the trusted root certificate before the device can verify a server's certificate. This log displays if the device failed to load it.
Certificate has expired.	Verification of a server's certificate failed because it has expired.
Self signed certificate.	Verification of a server's certificate failed because it is self-signed.
Self signed certificate in certificate chain.	Verification of a server's certificate failed because there is a self-signed certificate in the server's certificate chain.
Verify peer certificates has succeeded.	The device verified a server's certificate while processing an HTTPS connection.
Certification verification failed: Depth: %d, Error Number(%d):%s.	Verification of a server's certificate failed while processing an HTTPS connection. This log identifies the reason for the failure. 1st %d: certificate chain level 2nd %d: error number %s: error message
Certificate issuer name:%s.	Verification of the specified certificate failed because the device could not get the certificate's issuer name. %s is the certificate name.
The wrong format for HTTP header.	The header format of a packet returned by a server is wrong.
Timeout for get server response.	After the device sent packets to a server, the device did not receive any response from the server. The root cause may be a network delay issue.
Download file size is wrong.	The file size downloaded for AS is not identical with content-length
Parse HTTP header has failed.	Device can't parse the HTTP header in a response returned by a server. Maybe some HTTP headers are missing.

Table 274 IDP Logs

LOG MESSAGE	DESCRIPTION
System internal error. Detect IDP engine status failed.	System internal error. Get IDP engine activation flag failed.
System internal error. Enable IDP failed.	Enable IDP engine activation flag failed.
System internal error.Disable IDP failed.	Disable IDP engine activation flag failed.

Table 274 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
Enable IDP succeeded.	Enable IDP engine succeeded.
Disable IDP succeeded.	Disable IDP engine succeeded.
Enable IDP engine failed.	Insert IDP engine failed.
Disable IDP engine failed.	Remove IDP engine failed.
Enable IDP engine succeeded.	Insert IDP engine succeeded.
Disable IDP engine succeeded.	Remove IDP engine succeeded.
IDP service is not registered. Packet Inspection feature will not be activated.	IDP service is not registered. IDP service packet inspection feature and signature update will both be deactivated.
IDP service trial license is expired. Packet Inspection feature will not be activated.	IDP service trial license is expired. IDP service packet inspection feature and signature update will both be deactivated.
IDP service standard license is expired. Update signature failed.	IDP service standard license is expired. IDP signature cannot update.
IDP service standard license is not registered. Update signature failed.	IDP service standard license is not registered. IDP signature cannot update.
IDP service trial license is expired. Update signature failed.	IDP service trial license is expired. IDP signature cannot update.
IDP service trial license is not registered. Update signature failed.	IDP service trial license is expired. IDP signature cannot update.
Custom signature add error: sid <sid>, <error_message>.	Custom signature adding failed. Error sid and message will be shown.
Custom signature import error: line <line>, sid <sid>, <error_message>.	Custom signature importing failed. Error line number of file, sid and message will be shown
Custom signature replace error: line <line>, sid <sid>, <error_message>.	Custom signature replacing failed. Error line number of file, sid and message will be shown

Table 274 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
Custom signature edit error: sid <sid>, <error_message>.	Custom signature editing failed. Error sid and message will be shown.
Custom signature more than <num>. Replacement custom signature number is <num>.	Custom signature replacement failed. Display maximum rule number and replacement rule number.
Custom signature more than <num>. Remaining custom signature number is <num>. Adding custom signature number is <num>.	Custom signature adding failed. Display maximum rule number, remaining rule number and adding rule number.
Get custom signature number error.	Get custom rule number failed.
Add custom signature error: signature <sid> is over length.	Custom signature adding failed. Rule content length is too long.
Edit custom signature error: signature <sid> is over length.	Custom signature editing failed. Rule content length is too long.
IDP off-line update failed. File damaged.	IDP signature off-line update failed. Signature file maybe corrupt.
IDP signature update failed. File crashed.	IDP signature update failed. Decrypt signature file failed.
IDP signature update failed. File damaged.	IDP signature update failed. Decompress signature file failed.
IDP signature update failed. File update failed.	IDP signature update failed. Update signature file failed.
IDP signature update failed. Can not update last update time.	IDP signature update failed. Update last update time failed.
IDP signature update failed. Can not update synchronized file.	IDP signature update failed. Rebuild IDP DHA synchronized file failed.
IDP signature update successful. Signature version: <version>.	IDP signature update successful.
System internal error. Create IDP debug directory failed	System internal error. Create IDP debug directory failed.
System internal error. Create IDP statistics entry failed.	System internal error. Create IDP statistics entry failed.

Table 274 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
System internal error. Out of memory. IDP activation unchanged.	System internal error. System is out of memory. IDP activation unchanged.
System internal error. Create IDP proc failed. IDP activation failed.	System internal error. Create IDP process failed. IDP activation failed.
[type=<type>] <message>, Action: <action>, Severity: <severity>	IDP triggered event log. <type> = {sig(<id>) scan-detection(<attack>) flood-detection(<attack>) http-inspection(<attack>) tcp-decoder(<attack>) udp-decoder(<attack>) icmp-decoder(<attack>) }, <attack> = attack type. <severity> = {very low low medium high severe}
Program DFA failed.	IDP program DFA to hardware search engine failed.
IDP signature update failed. Fail to create temporary directory	IDP signature update failed. Create /tmp/sig directory failed
IDP signature update failed. Fail to extract temporary file.	IDP signature update failed. Extract signature package to /tmp/sig failed.
IDP signature update failed. Invalid IDP config file.	IDP signature update failed. Sig_check_update check failed.
IDP signature update failed. Invalid signature content.	IDP signature update failed. Sig_query check signature content failed.
System internal error. Create IDP traffic anomaly entry failed.	System internal error. Create IDP traffic anomaly entry failed.
Query signature version failed.	Unable to get signature version from new signature package download from update server
Can not get signature version.	Unable to get signature version from new signature package download from update server

Table 275 Application Patrol Logs

LOG MESSAGE	DESCRIPTION
System fatal error: 60005001.	Application patrol zysh initialization failed. Protocol file import error.
System fatal error: 60005002.	Application patrol zysh initialization failed. Shared memory failed.
System fatal error: 60005017.	Application patrol zyio failed. Fail to do zyio operation.

Table 275 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
System fatal error: 60005018.	Application patrol kernel error. Fail to communicate with kernel module.
System fatal error: 60005019.	Application patrol configuration group error. Fail to retrieve use group from use object.
System fatal error: 60006004.	Application patrol daemon (process) shared memory key generating fail.
System fatal error: 60006021.	Error generating application patrol semaphore key.
System fatal error: 60006031.	Warning application patrol resources ran out! New configuration of affected rule [%s:%d] is discarded.
System fatal error: 60018001.	Application patrol daemon (process) out of share memory address pool.
System fatal error: 60018002.	Application patrol daemon (process) ran out of pre-allocated share memory.
System fatal error: 60018003.	Application patrol daemon (process) failed to lock shared memory.
System fatal error: 60018004.	Application patrol daemon (process) failed to unlock shared memory.
System fatal error: 60018005.	Error generating application patrol semaphore key.
System fatal error: 60018006.	Application patrol daemon (process) fails to create share memory.
System fatal error: 60018007.	Error opening /dev/l7_action device.
System fatal error: 60018008.	Error when do ioctl L7_ACTION_IOCTL_ADDR_USAGE.
System fatal error: 60018009.	Error when do ioctl L7_ACTION_IOCTL_ADDR_USAGE.
System fatal error: 60018010.	Error when do ioctl L7_ACTION_IOCTL_PROTO_ADDR_NUMS.
System fatal error: 60018011.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018012.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018013.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018014.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018015.	Fail to retrieve user event from uamd.
System fatal error: 60018016.	Application patrol daemon (process) shared memory generate failed.
System fatal error: 60018017.	Fail to get share memory.

Table 275 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
System fatal error: 60018018.	Fail to get attach memory.
System fatal error: 60018019.	Application patrol daemon receive restart signal.
System fatal error: 60018020.	Application patrol daemon signal handler failed.
System fatal error: 60018021.	Application patrol daemon initialization failed.
System fatal error: 60018022.	Application patrol daemon startup failed.
System fatal error: 60018023.	Application patrol daemon stop.
Activate App. Patrol has succeeded.	Activate application patrol has succeeded.
No '%s' protocol.	The protocol %s does not exist. %s: Protocol Name
Service %s has been activated.	Protocol %s is active. %s: Protocol Name
Deactivate App Patrol has succeeded.	Deactivation of application patrol has succeeded.
Initialize App. Patrol has succeeded.	Initialization application patrol has succeeded.
App Patrol Name=%s Type=%s %s=%d Protocol=%s Action=%s	Packets logging. 1st %s: Protocol Name, 2nd %s: Category Name, 3rd %s: Default Rule or Exception Rule, 1st %d: Rule Index, 4th %s: TCP or UDP, 5th %s: Action.
App Patrol resources ran out. User %s is unrestricted by rule [%s:%d]. 1st %s: User Name, 2nd %s: Protocol Name, 1st %d: Rule Index	The application patrol daemon (process) resource pool is full, current login user %s is unrestricted by rule %d of protocol %s. 1st %s: User Name, 1st %d: Rule Index, 2nd %s: Protocol Name.

Table 276 IKE Logs

LOG MESSAGE	DESCRIPTION
%s:%s has not announced DPD capability	%s:%s is the peer IP:Port. Peer has not announced capability.
[COOKIE] Invalid cookie, no sa found	Cannot find SA according to the cookie.

Table 276 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
[DPD] No response from "%s:%s using existing Phase-1 SA in %u seconds. Trying with Phase-1 rekey.	%s:%s is the peer IP:Port. %u is the retry time. Dead Peer Detection (DPD) detected no response from peer.
[HASH] : Tunnel [%s] Phase 1 hash mismatch	%s is the tunnel name. When negotiating Phase-1, the exchange hash did not match.
[HASH] : Tunnel [%s] Phase 2 hash mismatch"	%s is the tunnel name. When negotiating Phase-2, the calculated quick mode authentication hash did not match.
[ID] : Invalid ID information	ID payload is not valid (in Phase-1 is local/peer ID, in Phase-2 is local/remote policy).
[ID] : Tunnel [%s] Local IP mismatch	%s is the tunnel name. When negotiating Phase-1, the local tunnel IP did not match the My IP in VPN gateway.
[ID] : Tunnel [%s] My IP mismatch	%s is the tunnel name. When negotiating Phase-1 and selecting matched proposal, My IP Address could not be resolved.
[ID] : Tunnel [%s] Phase 1 ID mismatch	%s is the tunnel name. When negotiating Phase-1, the peer ID did not match.
[ID] : Tunnel [%s] Phase 2 Local ID mismatch	%s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.
[ID] : Tunnel [%s] Phase 2 Remote ID mismatch	%s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.
[ID] : Tunnel [%s] Remote IP mismatch	%s is the tunnel name. When negotiating Phase-1, the peer tunnel IP did not match the secure gateway address in VPN gateway.
[SA] : Malformed IPsec SA proposal	When selecting a matched proposal, some protocol was given more than once.
[SA] : No proposal chosen	When selecting a matched proposal in phase-1 or phase-2, so proposal was selected.
[SA] : Tunnel [%s] Phase 1 authentication algorithm mismatch	%s is the tunnel name. When negotiating Phase-1, the authentication algorithm did not match.
[SA] : Tunnel [%s] Phase 1 authentication method mismatch	%s is the tunnel name. When negotiating Phase-1, the authentication method did not match.
[SA] : Tunnel [%s] Phase 1 encryption algorithm mismatch	%s is the tunnel name. When negotiating Phase-1, the encryption algorithm did not match.
[SA] : Tunnel [%s] Phase 1 invalid protocol	%s is the tunnel name. When negotiating Phase-1, the packet was not a ISKAMP packet in the protocol field.
[SA] : Tunnel [%s] Phase 1 invalid transform	%s is the tunnel name. When negotiating Phase-1, the transform ID was invalid.

Table 276 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
[SA] : Tunnel [%s] Phase 1 key group mismatch	%s is the tunnel name. When negotiating Phase-1, the DH group of the attribute list `attrs' did not match the security policy.
[SA] : Tunnel [%s] Phase 1 negotiation mode mismatch	%s is the tunnel name. When negotiating Phase-1, the negotiation mode did not match.
[SA] : Tunnel [%s] Phase 2 authentication algorithm mismatch	%s is the tunnel name. When negotiating Phase-2, the authentication algorithm did not match.
[SA] : Tunnel [%s] Phase 2 encapsulation mismatch	%s is the tunnel name. When negotiating Phase-2, the encapsulation did not match.
[SA] : Tunnel [%s] Phase 2 encryption algorithm mismatch	%s is the tunnel name. When negotiating Phase-2, the encryption algorithm did not match.
[SA] : Tunnel [%s] Phase 2 pfs mismatch	%s is the tunnel name. When negotiating Phase-2, the PFS specified did not match.
[SA] : Tunnel [%s] Phase 2 pfs unsupported: %d	%s is the tunnel name. When negotiating Phase-2, this device does not support the PFS specified.
[SA] : Tunnel [%s] Phase 2 SA encapsulation mismatch	%s is the tunnel name. When negotiating Phase-2, the SA encapsulation did not match.
[SA] : Tunnel [%s] Phase 2 SA protocol mismatch	%s is the tunnel name. When negotiating Phase-2, the SA protocol did not match.
[SA] : Tunnel [%s] SA sequence size mismatch	%s is the tunnel name. When negotiating Phase-2, the SA sequence size did not match.
[XCHG] exchange type is not IP, AGGR, or INFO	This device is the responder and this is the initiator's first packet, but exchange type is not IP, AGGR, or INFO and the packet is ignored.
Cannot resolve My IP Addr %s for Tunnel [%s]	1st %s is my ip address. 2nd %s is the tunnel name. When selecting a matched proposal in phase-1, the engine could not get My-IP address.
Cannot resolve Secure Gateway Addr %s for Tunnel [%s]	1st %s is my ip address. 2nd %s is the tunnel name; When selecting a matched proposal in phase-1, the engine could not get the correct secure gateway address.
Could not dial dynamic tunnel "%s"	%s is the tunnel name. The tunnel is a dynamic tunnel and the device cannot dial it.
Could not dial incomplete tunnel "%s"	%s is the tunnel name. The tunnel setting is not complete.
Could not dial manual key tunnel "%s"	%s is the tunnel name. The manual key tunnel cannot be dialed.
DPD response with invalid ID	When receiving a DPD response with invalid ID ignored.
DPD response with no active request	When receiving a DPD response with no active query.

Table 276 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
IKE Packet Retransmit	When retransmitting the IKE packets.
Phase 1 IKE SA process done	When Phase 1 negotiation is complete.
Recv Main Mode request from [%s]	%s is the remote name; When receiving a request to enter Main mode.
Recv Aggressive Mode request from [%s]	%s is the remote name; When receiving a request to enter Aggressive mode.
Recv DPD request from "%s:%s"	%s:%s is peer IP:Port. The device received a Dead Peer Detection request.
Recv DPD response from "%s:%s"	%s:%s is peer IP:Port. The device received a Dead Peer Detection response.
Recv: [SA]%s[KE]%s[ID] %s[CERT]%s[CR]%s[HASH] %s[SIG]%s[NONCE]%s[DEL] %s[VID]%s[ATTR]%s	This is a combined message for incoming IKE packets.
Send Main Mode request to [%s]	%s is the remote name. The device sent a request to enter Main Mode.
Send Aggressive Mode request to [%s]	%s is the remote name. The device sent a request to enter Aggressive Mode.
Send DPD request to "%s:%s"	%s:%s is peer IP:Port. The device sent a Dead Peer Detection request to the peer.
Send DPD response to "%s:%s"	%s:%s is peer IP:Port. The device sent a DPD response sent to the peer.
Send: [ID]%s[SA]%s[KE] %s[ID]%s[CERT]%s[CR]%s[HASH] %s[SIG]%s[NONCE] %s[DEL] %s[VID]%s[ATTR] %s[	This is a combined message for outgoing IKE packets.
Start Phase 2: Quick Mode	Indicates the beginning of phase 2 using quick mode.
The cookie pair is : 0x%08x%08x / 0x%08x%08x	Indicates the initiator/responder cookie pair.
The IPSec tunnel "%s" is already established	%s is the tunnel name. When dialing a tunnel, the tunnel is already dialed.
Tunnel [%s] built successfully	%s is the tunnel name. The phase-2 tunnel negotiation is complete.
Tunnel [%s] Phase 1 pre-shared key mismatch	%s is the tunnel name. When negotiating phase-1, the pre-shared key did not match.
Tunnel [%s] Recving IKE request	%s is the tunnel name. The device received an IKE request.
Tunnel [%s] Sending IKE request	%s is the tunnel name. The device sent an IKE request.

Table 276 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Tunnel [%s] IKE Negotiation is in process	%s is the tunnel name. When IKE request is already sent but still attempting to dial a tunnel.
VPN gateway %s was disabled	%s is the gateway name. An administrator disabled the VPN gateway.
VPN gateway %s was enabled	%s is the gateway name. An administrator enabled the VPN gateway.
XAUTH fail! My name: %s	%s is the my xauth name. This indicates that my name is invalid.
XAUTH fail! Remote user: %s	%s is the remote xauth name. This indicates that a remote user's name is invalid.
XAUTH succeed! My name: %s	%s is the my xauth name. This indicates that my name is valid.
XAUTH succeed! Remote user: %s	%s is the remote xauth name. This indicate that a remote user's name is valid
Dynamic Tunnel [%s:%s:0x%x:%s] built successfully	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
Dynamic Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
Tunnel [%s:%s:0x%x:%s] built successfully	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
Tunnel [%s:%s] Phase 1 pre-shared key mismatch	The variables represent the phase 1 name and tunnel name. When negotiating phase-1, the pre-shared keys did not match.
Tunnel [%s:%s] Recving IKE request	The variables represent the phase 1 name and tunnel name. The device received an IKE request.
Tunnel [%s:%s] Sending IKE request	The variables represent the phase 1 name and tunnel name. The device sent an IKE request.
Tunnel [%s:0x%x] is disconnected	The variables represent the tunnel name and the SPI of a tunnel that was disconnected.
Tunnel [%s] rekeyed successfully	%s is the tunnel name. The tunnel was rekeyed successfully.

Table 277 IPsec Logs

LOG MESSAGE	DESCRIPTION
Corrupt packet, Inbound transform operation fail	The device received corrupt IPsec packets and could not process them.
Encapsulated packet too big with length	An outgoing packet needed to be transformed but was longer than 65535.
Get inbound transform fail	When performing inbound processing for incoming IPSEC packets and ICMPs related to them, the engine cannot obtain the transform context.
Get outbound transform fail	When outgoing packet need to be transformed, the engine cannot obtain the transform context.
Inbound transform operation fail	After encryption or hardware accelerated processing, HWAccel dropped packet (resource shortage, corrupt packet, invalid MAC, and so on).
Outbound transform operation fail	After encryption or hardware accelerated processing, Hwaccel dropped packet (e.g., resource overflow, corrupt packet, and so on).
Packet too big with Fragment Off	An outgoing packet needed to be transformed, but the fragment flag was off and the packet was too big.
SPI:0x%x SEQ:0x%x Execute transform step fail, ret=%d	The variables represent the SPI, sequence number and the error number. When trying to perform transforming, the engine returned an error.
SPI:0x%x SEQ:0x%x No rule found, Dropping packet	The variables represent the SPI and the sequence number. The packet did not match the tunnel policy and was dropped.
SPI:0x%x SEQ:0x%x Packet Anti-Replay detected	The variables represent the SPI and the sequence number. The device received a packet again (that it had already received).
VPN connection %s was disabled.	%s is the VPN connection name. An administrator disabled the VPN connection.
VPN connection %s was enabled.	%s is the VPN connection name. An administrator enabled the VPN connection.

Table 278 Firewall Logs

LOG MESSAGE	DESCRIPTION
priority:%lu, from %s to %s, service %s, %s	1st variable is the global index of rule, 2nd is the from zone, 3rd is the to zone, 4th is the service name, 5th is ACCEPT/DROP/REJECT.
%s:%d: in %s():	Firewall is dead, trace to %s is which file, %d is which line, %s is which function
Firewall has been %s.	%s is enabled/disabled

Table 278 Firewall Logs (continued)

LOG MESSAGE	DESCRIPTION
Firewall rule %d has been moved to %d.	1st %d is the old global index of rule, 2nd %d is the new global index of rule
Firewall rule %d has been deleted.	%d is the global index of rule
Firewall rules have been flushed.	Firewall rules were flushed
Firewall rule %d was %s.	%d is the global index of rule, %s is appended/inserted/modified
Firewall %s %s rule %d was %s.	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule 3rd %s is appended/inserted/modified
Firewall %s %s rule %d has been moved to %d.	1st %s is from zone, 2nd %s is to zone, 1st %d is the old index of the rule 2nd %d is the new index of the rule
Firewall %s %s rule %d has been deleted.	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule
Firewall %s %s rules have been flushed.	1st %s is from zone, 2nd %s is to zone
abnormal TCP flag attack detected	Abnormal TCP flag attack detected
invalid state detected	Invalid state detected
The Asymmetrical Route has been enabled.	Asymmetrical route has been turned on.
The Asymmetrical Route has been disabled.	Asymmetrical Route has been turned off.

Table 279 Sessions Limit Logs

LOG MESSAGE	DESCRIPTION
Maximum sessions per host (%d) was exceeded.	%d is maximum sessions per host.

Table 280 Policy Route Logs

LOG MESSAGE	DESCRIPTION
Cann't open bwm_entries	Policy routing can't activate BWM feature.
Cann't open link_down	Policy routing can't detect link up/down status.

Table 280 Policy Route Logs (continued)

LOG MESSAGE	DESCRIPTION
Cannot get handle from UAM, user-aware PR is disabled	User-aware policy routing is disabled due to some reason.
mblock: allocate memory failed!	Allocating policy routing rule fails: insufficient memory.
pt: allocate memory failed!	Allocating policy routing rule fails: insufficient memory.
To send message to policy route daemon failed!	Failed to send control message to policy routing manager.
The policy route %d allocates memory fail!	Allocating policy routing rule fails: insufficient memory. %d: the policy route rule number
The policy route %d uses empty user group!	Use an empty object group. %d: the policy route rule number
The policy route %d uses empty source address group!	Use an empty object group. %d: the policy route rule number
The policy route %d uses empty destination address group!	Use an empty object group. %d: the policy route rule number
The policy route %d uses empty service group	Use an empty object group. %d: the policy route rule number
Policy-route rule %d was inserted.	Rules is inserted into system. %d: the policy route rule number
Policy-route rule %d was appended.	Rules is appended into system. %d: the policy route rule number
Policy-route rule %d was modified.	Rule is modified. %d: the policy route rule number
Policy-route rule %d was moved to %d.	Rule is moved. 1st %d: the original policy route rule number 2nd %d: the new policy route rule number
Policy-route rule %d was deleted.	Rule is deleted. %d: the policy route rule number
Policy-route rules were flushed.	Policy routing rules are cleared.

Table 281 Built-in Services Logs

LOG MESSAGE	DESCRIPTION
User on %u.%u.%u.%u has been denied access from %s	HTTP/HTTPS/TELNET/SSH/FTP/SNMP access to the device was denied. %u.%u.%u.%u is IP address %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET
HTTPS certificate:%s does not exist. HTTPS service will not work.	An administrator assigned a nonexistent certificate to HTTPS. %s is certificate name assigned by user
HTTPS port has been changed to port %s.	An administrator changed the port number for HTTPS. %s is port number
HTTPS port has been changed to default port.	An administrator changed the port number for HTTPS back to the default (443).
HTTP port has changed to port %s.	An administrator changed the port number for HTTP. %s is port number assigned by user
HTTP port has changed to default port.	An administrator changed the port number for HTTP back to the default (80).
SSH port has been changed to port %s.	An administrator changed the port number for SSH. %s is port number assigned by user
SSH port has been changed to default port.	An administrator changed the port number for SSH back to the default (22).
SSH certificate:%s does not exist. SSH service will not work.	An administrator assigned a nonexistent certificate to SSH. %s is certificate name assigned by user
SSH certificate:%s format is wrong. SSH service will not work.	After an administrator assigns a certificate for SSH, the device needs to convert it to a key used for SSH. %s is certificate name assigned by user
TELNET port has been changed to port %s.	An administrator changed the port number for TELNET. %s is port number assigned by user
TELNET port has been changed to default port.	An administrator changed the port number for TELNET back to the default (23).
FTP certificate:%s does not exist.	An administrator assigned a nonexistent certificate to FTP. %s is certificate name assigned by user
FTP port has been changed to port %s.	An administrator changed the port number for FTP. %s is port number assigned by user
FTP port has been changed to default port.	An administrator changed the port number for FTP back to the default (21).

Table 281 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
SNMP port has been changed to port %s.	An administrator changed the port number for SNMP. %s is port number assigned by user
SNMP port has been changed to default port.	An administrator changed the port number for SNMP back to the default (161).
Console baud has been changed to %s.	An administrator changed the console port baud rate. %s is baud rate assigned by user
Console baud has been reset to %d.	An administrator changed the console port baud rate back to the default (115200). %d is default baud rate
DHCP Server on Interface %s will not work due to Device HA status is Stand-By	If interface is stand-by mode for device HA, DHCP server can't be run. Otherwise it has conflict with the interface in master mode. %s is interface name
DHCP Server on Interface %s will be reapplied due to Device HA status is Active	When an interface has become the HA master, the DHCP server needs to start operating. %s is interface name
DHCP's DNS option:%s has changed.	DHCP pool's DNS option support from WAN interface. If this interface is unlink/disconnect or link/connect, this log will be shown. %s is interface name. The DNS option of DHCP pool has retrieved from it
Set timezone to %s.	An administrator changed the time zone. %s is time zone value
Set timezone to default.	An administrator changed the time zone back to the default (0).
Enable daylight saving.	An administrator turned on daylight saving.
Disable daylight saving.	An administrator turned off daylight saving.
DNS access control rules have been reached the maximum number.	An administrator tried to add more than the maximum number of DNS access control rules (64).
DNS access control rule %u of DNS has been appended.	An administrator added a new rule. %u is rule number
DNS access control rule %u has been inserted.	An administrator inserted a new rule. %u is rule number

Table 281 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
DNS access control rule %u has been appended	An administrator appended a new rule. %u is rule number
DNS access control rule %u has been modified	An administrator modified the rule %u. %u is rule number
DNS access control rule %u has been deleted.	An administrator removed the rule %u. %u is rule number
DNS access control rule %u has been moved to %d.	An administrator moved the rule %u to index %d. %u is previous index %d variable is current index
The default record of Zone Forwarder have reached the maximum number of 128 DNS servers.	The default record DNS servers is more than 128.
Interface %s ping check is successful. Zone Forwarder adds DNS servers in records.	Ping check ok, add DNS servers in bind. %s is interface name
Interface %s ping check is failed. Zone Forwarder removes DNS servers in records.	Ping check failed, remove DNS servers from bind. %s is interface name
Interface %s ping check is disabled. Zone Forwarder adds DNS servers in records.	Ping check disabled, add DNS servers in bind. %s is interface name
Wizard apply DNS server failed.	Wizard apply DNS server failed.
Wizard adds DNS server %s failed because DNS zone setting has conflictd.	Wizard apply DNS server failed because DNS zone conflictd. %s is the IP address of the DNS server
Wizard adds DNS server %s failed because Zone Forwarder numbers have reached the maximum number of 32.	Wizard apply DNS server fail because the device already has the maximum number of DNS records configured. %s is IP address of the DNS server.
Access control rules of %s have reached the maximum number of %u	The maximum number of allowable rules has been reached. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. %u is the maximum number of access control rules.

Table 281 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
Access control rule %u of %s was appended.	A new built-in service access control rule was appended. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %u of %s was inserted.	An access control rule was inserted successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %u of %s was modified.	An access control rule was modified successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %u of %s was deleted.	An access control rule was removed successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %d of %s was moved to %d.	An access control rule was moved successfully. 1st %d is the previous index . %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. 2nd %d is current previous index.
SNMP trap can not be sent successfully	Cannot send a SNMP trap to a remote host due to network error

Table 282 System Logs

LOG MESSAGE	DESCRIPTION
Port %d is up!!	When LINK is up, %d is the port number.
Port %d is down!!	When LINK is down, %d is the port number.
%s is dead at %s	A daemon (process) is gone (was killed by the operating system). 1st %s: Daemon Name, 2nd %s: date+time
%s process count is incorrect at %s	The count of the listed process is incorrect. 1st %s: Daemon Name, 2nd %s: date+time

Table 282 System Logs (continued)

LOG MESSAGE	DESCRIPTION
%s becomes Zombie at %s	A process is present but not functioning. 1st %s: Daemon Name, 2nd %s: date+time When memory usage exceed threshold-max, memory usage reaches %d%% :mem-threshold-max. When disk usage exceeds threshold-max, %s: Partition name file system usage reaches %d%%: disk-threshold-max. When memory usage drops below threshold-min, System Memory usage drops below the threshold of %d%%: mem-threshold-min. When disk usage drops below threshold-min, %s: partition_name file system drops below the threshold of %d%%: disk-threshold-min.
DHCP Server executed with cautious mode enabled	DHCP Server executed with cautious mode enabled.
DHCP Server executed with cautious mode disabled	DHCP Server executed with cautious mode disabled.
Received packet is not an ARP response packet	A packet was received but it is not an ARP response packet.
Receive an ARP response	The device received an ARP response.
Receive ARP response from %s (%s)	The device received an ARP response from the listed source.
The request IP is: %s, sent from %s	The device accepted a request.
Received ARP response NOT for the request IP address	The device received an ARP response that is NOT for the requested IP address.
Receive an ARP response from the client issuing the DHCP request	The device received an ARP response from the client issuing the DHCP request.
Receive an ARP response from an unknown client	The device received an ARP response from an unknown client.
In total, received %d arp response packets for the requested IP address	The device received the specified total number of ARP response packets for the requested IP address.
Clear arp cache successfully.	The ARP cache was cleared successfully.
Client MAC address is not an Ethernet address	A client MAC address is not an Ethernet address.

Table 282 System Logs (continued)

LOG MESSAGE	DESCRIPTION
DHCP request received via interface %s (%s:%s), src_mac: %s with requested IP: %s	The device received a DHCP request through the specified interface.
IP confliction is detected. Send back DHCP-NAK.	IP conflict was detected. Send back DHCP-NAK.
Clear ARP cache done	Clear ARP cache done.
NTP update successful, current time is %s	The device successfully synchronized with a NTP time server. %s is the time format.
NTP update failed	The device was not able to synchronize with the NTP time server successfully.
Device is rebooted by administrator!	An administrator restarted the device.
Insufficient memory.	Cannot allocate system memory.
Connect to dyndns server has failed.	Cannot connect to members.dyndns.org to update DDNS.
Update the profile %s has failed because of strange server response.	Update profile failed because the response was strange, %s is the profile name.
Update the profile %s has succeeded because the IP address of FQDN %s was not changed.	Update profile succeeded, because the IP address of profile is unchanged, %s is the profile name.
Update the profile %s has succeeded.	Update profile succeeded, %s is the profile name.
Update the profile %s has failed because the FQDN %s is invalid.	Update profile failed because FQDN for the profile is invalid for DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because the FQDN %s is malformed.	The FQDN format is malformed for DynDNS server, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because the FQDN %s is not under your control.	The owner of this FQDN is not the user, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because the FQDN %s was blocked for abuse.	The FQDN is blocked by DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because of authentication fail.	Try to update profile, but failed, because of authentication fail, %s is the profile name.

Table 282 System Logs (continued)

LOG MESSAGE	DESCRIPTION
Update the profile %s has failed because of invalid system parameters.	Some system parameters are invalid to update FQDN, %s is the profile name.
Update the profile %s has failed because the FQDN %s was blocked.	The FQDN is blocked by DynDNS , 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because too many or too few hosts found.	%s is the profile name.
Update the profile %s has failed because of dyndns internal error	Update profile failed because of a dyndns internal error, %s is the profile name.
Update the profile %s has failed because the feature requested is only available to donators.	Update profile failed because the feature requested is only available to donators, %s is the profile name.
Update the profile %s has failed because of error response.	Update profile failed because the response is incorrect, %s is the profile name.
Update the profile %s has failed because %s.	Update profile failed, and show the response message, 1st %s is the profile name, 2nd %s is the reason.
Update the profile %s has failed because of unknown error.	Update profile failed because unknown error. Sometimes, the force authentication will result in this error, 1st %s is the profile name.
Update the profile %s has failed because Username was empty.	DDNS profile needs username, %s is the profile name.
Update the profile %s has failed because Password was empty.	DDNS profile needs password, %s is the profile name.
Update the profile %s has failed because Domain name was empty.	DDNS profile needs domain name, %s is the profile name.
Update the profile %s has failed because Custom IP was empty.	The DDNS profile's IP select type is custom, and a custom IP was not defined, %s is the profile name.
Update the profile %s has failed because WAN interface was empty.	If the DDNS profile's IP select type is iface, it needs a WAN iface, %s is the profile name.
The profile %s has been paused because the VRRP status of WAN interface was standby.	The profile is paused by device-HA, because the VRRP status of that iface is standby, %s is the profile name.

Table 282 System Logs (continued)

LOG MESSAGE	DESCRIPTION
Update the profile %s has failed because WAN interface was link-down.	DDNS profile cannot be updated for WAN IP because WAN iface is link-down, %s is the profile name.
Update the profile %s has failed because WAN interface was not connected.	DDNS profile cannot be updated for WAN IP because WAN iface is PPP and not connected, %s is the profile name.
Update the profile %s has failed because IP address of WAN interface was empty.	DDNS profile cannot be updated because the IP of WAN iface is 0.0.0.0, 1st %s is the profile name.
Update the profile %s has failed because ping-check of WAN interface has failed.	DDNS profile cannot be updated because the ping-check for WAN iface failed , %s is the profile name.
The profile %s has been paused because the HA interface of VRRP status was standby.	The profile is paused by Device-HA, because the VRRP status of that HA iface is standby, %s is the profile name.
Update the profile %s has failed because HA interface was link-down.	DDNS profile cannot be updated for HA IP address because HA iface is link-down, %s is the profile name.
Update the profile %s has failed because the HA interface was not connected.	DDNS profile cannot be updated for HA IP address because HA iface is PPP and not connected, %s is the profile name.
Update the profile %s has failed because IP address of HA interface was empty.	DDNS profile cannot be updated because the IP address of HA iface is 0.0.0.0, %s is the profile name.
Update the profile %s has failed because ping-check of HA interface has failed.	DDNS profile cannot be updated because the fail of ping-check for HA iface, %s is the profile name
DDNS has been disabled by Device-HA.	DDNS is disabled by Device-HA, because all VRRP groups are standby.
DDNS has been enabled by Device-HA.	DDNS is enabled by Device-HA, because one of VRRP groups is active.
Disable DDNS has succeeded.	Disable DDNS.
Enable DDNS has succeeded.	Enable DDNS.
DDNS profile %s has been renamed as %s.	Rename DDNS profile, 1st %s is the original profile name, 2nd %s is the new profile name.

Table 282 System Logs (continued)

LOG MESSAGE	DESCRIPTION
DDNS profile %s has been deleted.	Delete DDNS profile, %s is the profile name,
DDNS Initialization has failed.	Initialize DDNS failed,
All DDNS profiles are deleted	All DDNS profiles have been removed.

Table 283 Connectivity Check Logs

LOG MESSAGE	DESCRIPTION
Can't open link_up2	Can not recover routing status which is link-down.
Can not open %s.pid	Can not open connectivity check process ID file. %s: interface name
Can not open %s.arg	Can not open configuration file for connectivity check process. %s: interface name
The connectivity-check is activate for %s interface	The link status of interface is still activate after check of connectivity check process. %s: interface name
The connectivity-check is fail for %s interface	The link status of interface is fail after check of connectivity check process. %s: interface name
Can't get gateway IP of %s interface	The connectivity check process can't get the gateway IP address for the specified interface. %s: interface name
Can't alloc memory	The connectivity check process can't get memory from OS.
Can't load %s module	The connectivity check process can't load module for check link-status. %s: the connectivity module, currently only ICMP available.
Can't handle 'isalive' function of %s module	The connectivity check process can't execute 'isalive' function from module for check link-status. %s: the connectivity module, currently only ICMP available.
Create socket error	The connectivity check process can't get socket to send packet.
Can't get IP address of %s interface	The connectivity check process can't get IP address of interface. %s: interface name.

Table 283 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
Can't get flags of %s interface	The connectivity check process can't get interface configuration. %s: interface name
Can't get remote address of %s interface	The connectivity check process can't get remote address of PPP interface %s: interface name
Can't get NETMASK address of %s interface	The connectivity check process can't get netmask address of interface. %s: interface name
Can't get BROADCAST address of %s interface	The connectivity check process can't get broadcast address of interface %s: interface name
Can't use MULTICAST IP for destination	The connectivity check process can't use multicast address to check link-status.
The destination is invalid, because destination IP is broadcast IP	The connectivity check process can't use broadcast address to check link-status.
Can't get MAC address of %s interface!	The connectivity check process can't get MAC address of interface. %s: interface name
To send ARP REQUEST error!	The connectivity check process can't send ARP request packet.
The %s routing status seted to DEAD by connectivity-check	The interface routing can't forward packet. %s: interface name
The %s routing status seted ACTIVATE by connectivity-check	The interface routing can forward packet. %s: interface name

Table 284 Device HA Logs

LOG MESSAGE	DESCRIPTION
Device HA VRRP Group %s has been added.	An VRRP group has been created, %s: the name of VRRP group.
Device HA VRRP group %s has been modified.	An VRRP group has been modified, %s: the name of VRRP group.
Device HA VRRP group %s has been deleted.	An VRRP group has been deleted, %s: the name of VRRP group.

Table 284 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
Device HA VRRP interface %s for VRRP Group %s has changed.	Configuration of an interface that belonged to a VRRP group has been changed, 1st %s: VRRP interface name, 2nd %s: %s: the name of VRRP group.
Device HA syncing from %s starts.	Device HA Syncing from Master starts when user click "Sync Now" using Auto Sync, %s: The IP of FQDN of Master.
%s has no file to sync, Skip syncing it for %s.	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2nd %s: The feature name for the syncing object.
Master configuration is the same with Backup. Skip updating it.	The System Startup configuration file synchronized from the Master is the same with the one in the Backup, so the configuration does not have to be updated.
%s file not existed, Skip syncing it for %s	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2nd %s: The feature name for the syncing object.
Master firmware version can not be recognized. Stop syncing from Master.	Synchronizing stopped because the firmware version file was not found in the Master. A Backup device only synchronizes from the Master if the firmware versions are the same between the Master and the Backup.
Device HA Sync has failed when syncing %s for %s due to bad \"Sync Password\".	The synchronization password was incorrect when attempting to synchronize a certain object (AV/AS/IDP/Certificate/System Configuration). 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Device HA Sync has failed when syncing %s for %s due to bad \"Sync From\" or \"Sync Port\".	The Sync From IP address or Sync Port may be incorrect when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration).
Device HA Sync has failed when syncing %s for %s.	Synchronization failed when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration) due to an unknown reason, 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Sync Failed: Cannot connect to Master when syncing %s for %s.	Synchronization failed because the Backup could not connect to the Master. The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Backup firmware version can not be recognized. Stop syncing from Master.	The firmware version on the Backup cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.

Table 284 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
Sync failed: Remote Firmware Version Unknown	The firmware version on the Master cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Master firmware version should be the same with Backup.	The Backup and Master have different firmware versions. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Update %s for %s has failed.	Updating a certain object failed when updating (AS/AV/IDP/Certificate/System Configuration). 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Update %s for %s has failed: %s.	Updating a certain object failed when updating (AS/AV/IDP/Certificate/System Configuration) due to some reason. 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Device HA has skipped syncing %s since %s is %s.	A certain service has no license or the license is expired, so it was not synchronized from the Master. 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized, 3rd %s: unlicensed or license expired.
Device HA authentication type for VRRP group %s maybe wrong.	A VRRP group's Authentication Type (Md5 or IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Device HA authentication string of text for VRRP group %s maybe wrong.	A VRRP group's Simple String (Md5) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Device HA authentication string of AH for VRRP group %s maybe wrong.	A VRRP group's AH String (IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Retrying to update %s for %s. Retry: %d.	An update failed. Retrying to update the failed object again. 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized, %d: the retry count.
Recovering to Backup original state for %s has failed.	An update failed. The device will try to recover the failed update feature to the original state before Device HA synchronizes the specified object.
Recovering to Backup original state for %s has succeeded.	Recovery succeeded when an update for the specified object failed.
One of VRRP groups has became active. Device HA Sync has aborted from Master %s.	%s: IP or FQDN of Master
Master configuration file does not exist. Skip updating ZySH Startup Configuration.	

Table 284 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
System internal error: %s. Skip updating %s.	1st %s: error string, 2ed %s: the syncing object
Master configuration file is empty. Skip updating ZySH Startup Configuration.	
Device HA Sync has failed when syncing %s for %s due to transmission timeout.	1st %s: the syncing object, 2ed %s: the feature name for the syncing object

Table 285 Routing Protocol Logs

LOG MESSAGE	DESCRIPTION
RIP on interface %s has been stopped because Device-HA binds this interface.	Device-HA is currently running on the interface %s, so all the local service have to be stopped including RIP. %s: Interface Name
RIP on all interfaces have been stopped	Got the CLI command 'no router rip' to shut down RIP on all interfaces
Invalid RIP md5 authentication	RIP md5 authentication has been set without setting md5 authentication id and key first
Invalid RIP text authentication.	RIP text authentication has been set without setting authentication key first
RIP on interface %s has been activated.	RIP on interface %s has been activated. %s: Interface Name
RIP direction on interface %s has been changed to In-Only.	RIP direction on interface %s has been changed to In-Only. %s: Interface Name
RIP direction on interface %s has been changed to Out-Only.	RIP direction on interface %s has been changed to Out-Only. %s: Interface Name
RIP authentication mode has been changed to %s.	RIP authentication mode has been changed to text or md5.
RIP text authentication key has been changed.	RIP text authentication key has been changed.
RIP md5 authentication id and key have been changed.	RIP md5 authentication id and key have been changed.
RIP global version has been changed to %s.	RIP global version has been changed to version 1 or 2.

Table 285 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
RIP redistribute OSPF routes has been enabled.	RIP redistribute OSPF routes has been enabled.
RIP redistribute static routes has been enabled.	RIP redistribute static routes has been enabled.
RIP on interface %s has been deactivated. %s: Interface Name	RIP on interface %s has been deactivated. %s: Interface Name
RIP direction on interface %s has been changed to BiDir. %s: Interface Name	RIP direction on interface %s has been changed to BiDir. %s: Interface Name
RIP authentication has been disabled.	RIP text or md5 authentication has been disabled.
RIP text authentication key has been deleted.	RIP text authentication key has been deleted.
RIP md5 authentication id and key have been deleted.	RIP md5 authentication id and key have been deleted.
RIP global version has been deleted.	RIP global version has been deleted.
RIP redistribute OSPF routes has been disabled.	RIP redistribute OSPF routes has been disabled.
RIP redistribute static routes has been disabled.	RIP redistribute static routes has been disabled.
RIP v2-broadcast on interface %s has been enabled. %s: Interface Name.	RIP v2-broadcast on interface %s has been enabled. %s: Interface Name.
RIP send-version on interface %s has been changed to %s. %s: Interface Name.	RIP send-version on interface %s has been changed to version 1 or 2 or both 1 2. %s: Interface Name.
RIP receive-version on interface %s has been changed to %s. 2nd%s: Interface Name.	RIP receive-version on interface %s has been changed to version 1 or 2 or both 1 2. 2nd%s: Interface Name.
RIP send-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP Version	RIP send-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP Version
RIP receive-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP	RIP receive-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP
RIP v2-broadcast on interface %s has been disabled. %s: Interface Name	RIP v2-broadcast on interface %s has been disabled. %s: Interface Name

Table 285 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
OSPF on interface %s has been stopped because Device-HA binds this interface.	Device-HA is currently running on the interface %s, so all the local service have to be stopped including OSPF. %s: Interface Name
Area %s cannot be removed. This area is in use.	One or more interfaces are still using this area, so area %s cannot be removed. %s: OSPF Area
Invalid OSPF %s authentication of area %s.	OSPF md5 or text authentication has been set without setting md5 authentication id and key, or text authentication key first.
Invalid OSPF virtual-link %d md5 authentication of area %s.	Virtual-link %s md5 authentication has been set without setting md5 authentication id and key first. %s: Virtual-Link ID
Invalid OSPF virtual-link %s text authentication of area %s.	Virtual-link %s text authentication has been set without setting text authentication key first. %s: Virtual-Link ID
Invalid OSPF virtual-link %s authentication of area %s.	Virtual-link %s authentication has been set to same-as-area but the area has invalid authentication configuration. %s: Virtual-Link ID
Invalid OSPF md5 authentication on interface %s.	Invalid OSPF md5 authentication is set on interface %s. %s: Interface Name
Invalid OSPF text authentication on interface %s.	Invalid OSPF text authentication is set on interface %s. %s: Interface Name
Interface %s does not belong to any OSPF area.	Interface %s has been set OSPF authentication same-as-area, however the interface does not belong to any OSPF area. %s: Interface Name
Invalid OSPF authentication of area %s on interface %s.	Interface %s has been set OSPF authentication same-as-area, however the area has invalid text authentication configuration. %s: Interface Name

Table 286 NAT Logs

LOG MESSAGE	DESCRIPTION
The NAT range is full	The NAT mapping table is full.
%s FTP ALG has succeeded.	The FTP Application Layer Gateway (ALG) has been turned on or off. %s: Enable or Disable
Extra signal port of FTP ALG has been modified.	Extra FTP ALG port has been changed.

Table 286 NAT Logs (continued)

LOG MESSAGE	DESCRIPTION
Signal port of FTP ALG has been modified.	Default FTP ALG port has been changed.
%s H.323 ALG has succeeded.	The H.323 ALG has been turned on or off. %s: Enable or Disable
Extra signal port of H.323 ALG has been modified.	Extra H.323 ALG port has been changed.
Signal port of H.323 ALG has been modified.	Default H.323 ALG port has been changed.
%s SIP ALG has succeeded.	The SIP ALG has been turned on or off. %s: Enable or Disable
Extra signal port of SIP ALG has been modified.	Extra SIP ALG port has been changed.
Signal port of SIP ALG has been modified.	Default SIP ALG port has been changed.
Register SIP ALG extra port=%d failed.	SIP ALG apply additional signal port failed. %d: Port number
Register SIP ALG signal port=%d failed.	SIP ALG apply signal port failed. %d: Port number
Register H.323 ALG extra port=%d failed.	H323 ALG apply additional signal port failed. %d: Port number
Register H.323 ALG signal port=%d failed.	H323 ALG apply signal port failed. %d: Port number
Register FTP ALG extra port=%d failed.	FTP ALG apply additional signal port failed. %d: Port number
Register FTP ALG signal port=%d failed.	FTP ALG apply signal port failed. %d: Port number

Table 287 PKI Logs

LOG MESSAGE	DESCRIPTION
Generate X509certificate "%s" successfully	The router created an X509 format certificate with the specified name.
Generate X509 certificate "%s" failed, errno %d	The router was not able to create an X509 format certificate with the specified name. See Table 256 on page 637 for details about the error number.

Table 287 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Generate certificate request "%s" successfully	The router created a certificate request with the specified name.
Generate certificate request "%s" failed, errno %d	The router was not able to create a certificate request with the specified name. See Table 256 on page 637 for details about the error number.
Generate PKCS#12 certificate "%s" successfully	The router created a PKCS#12 format certificate with the specified name.
Generate PKCS#12 certificate "%s" failed, errno %d	The router was not able to create anPKCS#12 format certificate with the specified name. See Table 256 on page 637 for details about the error number.
Prepare to import "%s" into "My Certificate"	%s is the name of a certificate request.
Prepare to import "%s" into Trusted Certificate"	%s is the name of a certificate request.
CMP enrollment "%s" successfully, CA "%s", URL "%s"	The device used CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
CMP enrollment "%s" failed, CA "%s", URL "%s"	The device was unable to use CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
SCEP enrollment "%s" successfully, CA "%s", URL "%s"	The device used SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
SCEP enrollment "%s" failed, CA "%s", URL "%s"	The device was unable to use SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
Import X509 certificate "%s" into My Certificate successfully	The device imported a x509 format certificate into My Certificates. %s is the certificate request name.
Import X509 certificate "%s" into Trusted Certificate successfully	The device imported a x509 format certificate into Trusted Certificates. %s is the certificate request name.
Import PKCS#12 certificate "%s" into "My Certificate" successfully	The device imported a PKCS#12 format certificate into My Certificates. %s is the certificate request name.
Import PKCS#7 certificate "%s" into "My Certificate" successfully	The device imported a PKCS#7 format certificate into My Certificates. %s is the certificate request name.

Table 287 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Import PKCS#7 certificate "%s" into "Trusted Certificate" successfully	The device imported a PKCS#7 format certificate into Trusted Certificates. %s is the certificate request name.
Decode imported certificate "%s" failed	The device was not able to decode an imported certificate. %s is certificate the request name
Export PKCS#12 certificate "%s" from "My Certificate" successfully	The device exported a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
Export PKCS#12 certificate "%s" from "My Certificate" failed	The device was not able to export a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "My Certificate" failed	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "Trusted Certificate" failed	The device was not able to export a x509 format certificate from Trusted Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "My Certificate" successfully	The device exported a x509 format certificate from My Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "Trusted Certificate" successfully	The device exported a x509 format certificate from Trusted Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "My Certificate" failed	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
Import PKCS#12 certificate "%s" with incorrect password	An administrator used the wrong password when trying to import a PKCS#12 format certificate. %s is the certificate name.
Cert trusted: %s	%s is the subject.
Due to %d, cert not trusted: %s	%d is an error number (see Table 256 on page 637), %s is the certificate subject.

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.

CODE	DESCRIPTION
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 288 Interface Logs

LOG MESSAGE	DESCRIPTION
Interface %s has been deleted.	An administrator deleted an interface. %s is the interface name.
AUX Interface dialing failed. This AUX interface is not enabled.	A user tried to dial the AUX interface, but the AUX interface is not enabled.
AUX Interface disconnecting failed. This AUX interface is not enabled.	The AUX interface is not enabled and a user tried to use the disconnect aux command.

Table 288 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
Please type phone number of interface AUX first then dial again.	A user tried to dial the AUX interface, but the AUX interface does not have a phone number set.
Please type phone number of Interface AUX first then disconnect again.	The AUX interface does not have a phone number set and a user tried to use the disconnect aux command.
Interface %s will reapply because Device HA become active status.	Device-ha became active and is using a PPP base interface, the PPP interface must reapply, %s is the interface name.
Interface %s will reapply because Device HA is not running.	Device-ha was deleted and free PPP base interface, PPP interface must reapply, %s is the interface name.
Interface %s will stop connect because Device HA become standby status.	When device-ha is stand-by and use PPP base interface, PPP interface connection will stop, %s: interface name.
Create interface %s has been failed.	When PPP can't running fail, %s: interface name.
Base interface %s is disabled. Interface %s is disabled now.	When user disable ethernet, vlan or bridge interface and this interface is base interface of PPP or virtual interface. PPP and virtual will disable too. 1st %s is interface name, 2nd %s is interface.
Interface %s has been changed.	An administrator changed an interface's configuration. %s: interface name.
Interface %s has been added.	An administrator added a new interface. %s: interface name.
Interface %s is enabled.	An administrator enabled an interface. %s: interface name.
Interface %s is disabled.	An administrator disabled an interface. %s: interface name.
%s MTU > (%s MTU - 8), %s may not work correctly.	An administrator configured a PPP interface, PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and peer will not receive correct PPP packets. 1st %s: PPP interface name, 2nd %s: ethernet interface name.
(%s MTU - 8) < %s MTU, %s may not work correctly.	An administrator configured ethernet, vlan or bridge and this interface is base interface of PPP interface. PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and peer will not receive correct PPP packets. 1st %s: Ethernet interface name, 2nd %s: PPP interface name.
Interface %s links down. Default route will not apply until interface %s links up.	An administrator set a static gateway in interface but this interface is link down. At this time the configuration will be saved but route will not take effect until the link becomes up. 1st %s: interface name, 2nd %s: interface name.

Table 288 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
name=%s,status=%s,TxPkts=%u,RxPkts=%u,Colli.=%u,TxB/s=%u,RxB/s=%u,UpTime=%s	Port statistics log. This log will be sent to the VRPT server. 1st %s: physical port name, 2nd %s: physical port status, 1st %u: physical port Tx packets, 2nd %u: physical port Rx packets, 3rd %u: physical port packets collisions, 4th %u: physical port Tx Bytes/s, 5th %u: physical port Rx Bytes/s, 3rd %s: physical port up time.
name=%s,status=%s,TxPkts=%u,RxPkts=%u,Colli.=%u,TxB/s=%u,RxB/s=%u	Interface statistics log. This log will be sent to the VRPT server. 1st %s: interface name, 2nd %s: interface status, 1st %u variable: interface Tx packets, 2nd %u variable: interface Rx packets, 3rd %u: interface packets collisions, 4th %u: interface Tx Bytes/s, 5th %u: interface Rx Bytes/s.
Interface %s start dialing.	A PPP or aux interface started dialing to a server. %s: interface name.
Interface %s connect failed: Connect to server failed.	A PPTP interface failed to connect to the PPTP server. %s: interface name.
Interface %s connection terminated.	A PPP or AUX connection will terminate. %s: interface name.
Interface %s connection terminated: idle timeout.	An idle PPP or AUX connection timed out.1%s: interface name.
Interface %s connect failed: MS-CHAPv2 mutual authentication failed.	MS-CHAPv2 authentication failed (the server must support mS-CHAPv2 and verify that the authentication failed, this does not include cases where the servers does not support MS-CHAPv2). %s: interface name.
Interface %s connect failed: MS-CHAP authentication failed.	MS-CHAP authentication failed (the server must support MS-CHAP and verify that the authentication failed, this does not include cases where the server does not support MS-CHAP). %s: interface name.
Interface %s connect failed: CHAP authentication failed.	CHAP authentication failed (the server must support CHAP and verify that the authentication failed, this does not include cases where the server does not support CHAP). CHAP: interface name.
Interface %s is connected.	A PPP or AUX interface connected successfully. %s: interface name.
Interface %s is disconnected.	A PPP or AUX interface disconnected successfully. %s: interface name.
Interface %s connect failed: Peer not responding.	The interface's connection will be terminated because the server did not send any LCP packets.
Interface %s connect failed: PAP authentication failed.	PAP authentication failed (the server must support PAP and verify verify that the authentication failed, this does not include cases where the server does not support PAP). %s: PPP interface name.

Table 288 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
Interface %s connect failed: Connect timeout.	A PPPOE connection timed out due to a lack of response from the PPPOE server. %s: PPP interface name.
Interface %s create failed because has no member.	A bridge interface has no member. %s: bridge interface name.
Interface %s has been renamed from '%s' to '%s'	An interface was renamed. 1st %s: the interface's system name (gex), 2nd %s: current interface name, 3rd %s: new interface name.

Table 289 Account Logs

LOG MESSAGE	DESCRIPTION
Account %s %s has been deleted.	A user deleted an ISP account profile. 1st %s: profile type, 2nd %s: profile name.
Account %s %s has been changed.	A user changed an ISP account profile's options. 1st %s: profile type, 2nd %s: profile name.
Account %s %s has been added.	A user added a new ISP account profile. 1st %s: profile type, 2nd %s: profile name.

Table 290 Port Grouping Logs

LOG MESSAGE	DESCRIPTION
Interface %s links up because of changing Port Group. Enable DHCP client.	An administrator used port-grouping to assign a port to a representative Interface and this representative interface is set to DHCP client and only has one member. In this case the DHCP client will be enabled. %s: interface name.
Interface %s links down because of changing Port Group. Disable DHCP client.	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has no members in its group. In this case the DHCP client will be disabled. %s: interface name.
Port Group on %s is changed. Renew DHCP client.	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has more than one member in its group. In this case the DHCP client will renew. %s: interface name.
Port Grouping %s has been changed.	An administrator configured port-grouping, %s: interface name.

Table 291 Force Authentication Logs

LOG MESSAGE	DESCRIPTION
Force User Authentication will be enabled due to http server is enabled.	Force user authentication will be turned on because HTTP server was turned on.
Force User Authentication will be disabled due to http server is disabled.	Force user authentication will be turned off because HTTP server was turned off.
Force User Authentication may not work properly!	

Table 292 File Manager Logs

LOG MESSAGE	DESCRIPTION
ERROR: # %s, %s	Apply configuration failed, this log will be what CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
WARNING: # %s, %s	Apply configuration failed, this log will be what CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
ERROR: # %s, %s	Run script failed, this log will be what wrong CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
WARNING: # %s, %s	Run script failed, this log will be what wrong CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
Resetting system...	Before apply configuration file.
System reseted. Now apply %s..	After the system reset, it started to apply the configuration file. %s is configuration file name.
Running %s...	An administrator ran the listed shell script. %s is script file name.

Table 293 EPS Logs

LOG MESSAGE	DESCRIPTION
'EPS' signature data of Auth. policy %d has been updated.	EPS profile settings were changed and have been re-applied to the associated authentication policy. %d is the authentication profile name.
'EPS' signature data of SSL policy %d has been updated.	EPS profile settings were changed and have been re-applied to the associated SSL VPN rule. %d is the SSL VPN rule name.
EPS profile %s has been modified.	An EPS profile was modified. %s is the EPS profile name.
'EPS' signature file is replaced with default one.	An administrator reset EPS signatures back to the factory defaults.
Missing EPS signature default tools, ret = %d.	An error occurred when reloading the factory default EPS signatures.
Windows service pack check fail in %s	A user's computer failed to pass an EPS checking item, the failed item is about the Windows service pack version.
'Windows auto update check fail in %s	A user's computer failed to pass an EPS checking item, the failed item is about Windows Auto Update settings.
Windows security patch check fail in %s	A user's computer failed to pass an EPS checking item about Windows service patches.
Antivirus check fail in %s	A user's computer failed to pass an EPS checking item about anti-virus installation and activation.
Personal firewall check fail in %s	A user's computer failed to pass an EPS checking item about personal firewall installation and activation.
Windows registry check fail in %s	A user's computer failed to pass an EPS checking item about Windows registry settings.
Trusted process check fail in %s	A user's computer failed to pass an EPS checking item about processes that the user's computer must execute.
Forbidden process check fail in %s	A user's computer failed to pass an EPS checking item about processes that the user's computer cannot execute.
Files information check fail in %s	A user's computer failed to pass an EPS checking item about the size and version of specific files.
OS type check fail in %s	A user's computer failed to pass an EPS checking item about the Operating System.
Windows version check fail in %s	A user's computer failed to pass an EPS checking item about the Windows version.
EPS checking result is pass.	A user's computer passed all the EPS checking items.

ZyNOS Log Descriptions

This appendix provides descriptions of example log messages for ZyNOS-based devices. Log messages vary by device.

Table 294 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful SMT login	Someone has logged on to the router's SMT interface.
SMT login failed	Someone has failed to log on to the router's SMT interface.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via FTP.
FTP login failed	Someone has failed to log on to the router via FTP.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.

Table 294 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
SMT Session Begin	An SMT management session has started.
SMT Session End	An SMT management session has ended.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.
DNS server %s was not responding to last 32 consecutive queries...	The specified DNS server did not respond to the last 32 consecutive queries.
DDNS update IP:%s (host %d) successfully	The device updated the IP address of the specified DDNS host name.
SMTP successfully	The device sent an e-mail.
myZyXEL.com registration successful	Registration of the device with myZyXEL.com was successful.
Trial service registration successful	Registration for a trial service was successful.
Service upgrade successful	Registration for a service upgrade was successful.
Service refresh successful.	The device successfully refreshed service information from myZyXEL.com.
Content Filter trial service activation successfully	The content filtering trial service was successfully activated for this device.
Anti-Spam trial service activation successfully	The anti-spam trial service was successfully activated for this device.
IDP/Anti-Virus trial service activation successfully	The IDP and anti-virus trial service was successfully activated for this device.
%s	The myZyXEL.com service registration failed due to the error listed. If you are unable to register for services at myZYXEL.com, the error message displayed in this log may be useful when contacting customer support.

Table 295 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.
Dial Backup starts	Dial backup started working.
Dial Backup ends	Dial backup stopped working.
DHCP Server cannot assign the static IP %s (out of range).	The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid.
The DHCP static IP %s is conflict.	The static DHCP IP address conflicts with another host.
SMTP fail (%s)	The device failed to send an e-mail (error message included).
SMTP authentication fail (%s)	The device failed to authenticate with the SMTP server (error message included).
%s	The device will send a Gratuitous ARP to detect the IP collision. If the collision happens, there will be a log in centralized log.

Table 296 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP UDP IGMP ESP GRE OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP UDP IGMP ESP GRE OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP UDP IGMP ESP GRE OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP UDP IGMP ESP GRE OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.

Table 296 Access Control Logs (continued)

LOG MESSAGE	DESCRIPTION
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [TCP UDP]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.
Firewall matches a dynamic ACL rule of an ALG session	The firewall allowed access for a packet that matched a dynamic ACL rule of an ALG session.
Maximum number of dynamic ACL rules exceeded.	
Dynamic ACL rule, listening port : %d, peer port : %d already exists.	

Table 297 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to TCP Maximum Incomplete in the Firewall Attack Alerts screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds

Table 297 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

Table 298 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[TCP UDP ICMP IGMP Generic] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see [Table 312 on page 662](#).

Table 299 ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

Table 300 CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 301 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 302 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 303 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s: %s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s(cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s :%s(cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The Vantage Report cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The Vantage Report cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see [Table 312 on page 662](#).

Table 304 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.

Table 304 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
land [TCP UDP IGMP ESP GRE OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [TCP UDP IGMP ESP GRE OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP UDP IGMP ESP GRE OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.

Table 304 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
IP address in FTP port command is different from the client IP address. It maybe a bounce attack.	The IP address in an FTP port command is different from the client IP address. It may be a bounce attack.
Fragment packet size is smaller than the MTU size of output interface.	The fragment packet size is smaller than the MTU size of output interface.

Table 305 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: SNMP denied	Attempted use of SNMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

Table 306 Wireless Logs

LOG MESSAGE	DESCRIPTION
WLAN MAC Filter Fail	The MAC filter blocked a wireless station from connecting to the device.
WLAN MAC Filter Success	The MAC filter allowed a wireless station to connect to the device.
WLAN STA Association	A wireless station associated with the device.

Table 306 Wireless Logs

LOG MESSAGE	DESCRIPTION
WLAN STA Association List Full	The maximum number of associated wireless clients has been reached.
WLAN STA Association Again	The SSID and time of association were updated for an wireless station that was already associated.

Table 307 IPsec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPsec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the "MyIP" configured as "0.0.0.0" when the WAN IP address changed.
Inbound packet decryption failed	Please check the algorithm configuration.
Cannot find outbound SA for rule <%d>	A packet matches a rule, but there is no phase 2 SA for outbound traffic.
Rule [%s] sends an echo request to peer	The device sent a ping packet to check the specified VPN tunnel's connectivity.
Rule [%s] receives an echo reply from peer	The device received a ping response when checking the specified VPN tunnel's connectivity.
Delete all tunnels	The device disconnected all IPsec tunnels.

Table 308 IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.

Table 308 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> -<My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.

Table 308 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPsec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPsec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to %d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
XAUTH succeed! Remote user: <Username>	The router used extended authentication to authenticate the listed remote username.
XAUTH fail! Remote user: <Username>	The router was not able to use extended authentication to authenticate the listed remote username.
XAUTH succeed! My name: <Username>	The router used extended authentication to authenticate the listed username.
XAUTH fail! My name: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.

Table 308 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (PFS) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPSec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1 verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.

Table 308 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.
Remote Gateway Addr in rule [%s] is changed to %s"	The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address.
New My Vantage Report Addr in rule [%s] is changed to %s	The IP address for the domain name of the Vantage Report in the listed rule changed to the listed IP address.
Remote Gateway Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the remote gateway's IP address changed.
My Vantage Report Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the Vantage Report's IP address changed.

Table 309 PKI Logs

LOG MESSAGE	DESCRIPTION
Enrollment successful	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.

Table 309 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 226 on page 659 for the corresponding descriptions of the codes.

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).

CODE	DESCRIPTION
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 310 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.

Table 310 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 311 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets travelling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets travelling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets travelling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets travelling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets travelling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets travelling from the LAN to the DMZ.
(L to L/ZW)	LAN to LAN/ Vantage Report	ACL set for packets travelling from the LAN to the LAN or the Vantage Report.
(W to W/ZW)	WAN to WAN/ Vantage Report	ACL set for packets travelling from the WAN to the WAN or the Vantage Report.
(D to D/ZW)	DMZ to DMZ/ Vantage Report	ACL set for packets travelling from the DMZ to the DM or the Vantage Report.
(L to WL)	LAN to WLAN	ACL set for packets travelling from the LAN to the WLAN.
(WL to L)	WLAN to LAN	ACL set for packets travelling from the WLAN to the LAN.

Table 311 ACL Setting Notes (continued)

PACKET DIRECTION	DIRECTION	DESCRIPTION
(W to WL)	WAN to WLAN	ACL set for packets travelling from the WAN to the WLAN.
(WL to W)	WLAN to WAN	ACL set for packets travelling from the WLAN to the WAN.
(D to WL)	DMZ to WLAN	ACL set for packets travelling from the DMZ to the WLAN.
(WL to D)	WLAN to DMZ	ACL set for packets travelling from the WLAN to the DMZ.
(WL to WL)	WLAN to WLAN/ Vantage Report	ACL set for packets travelling from the WLAN to the WLAN or the Vantage Report.

Table 312 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded

Table 312 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 313 IDP Logs

LOG MESSAGE	DESCRIPTION
The buffer size is too small!	The buffer for holding IDP information such as the signature file version was too small to hold any more information.
The format of the user config file is incorrect!	There was a format error in the configuration backup file that someone attempted to load into the system.
The system is doing signature update now, please wait!	The device is updating the signature file.
No data!	The system could not find any IDP signatures that matched a search.
IDP %s!	The device detected an intrusion event in a connection. The format of %s is "ID" followed by the IDP ID signature number and the IDP signature name. For example, ID:10001,Window Ping.
Can not find the signature, please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.

Table 313 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
Signature update OK - New signature version: <Signature version> Release Date: <Release date>!	The device updated the signature file successfully. The signature file's version and release date are included.
The turbo card is not ready, please insert the card and reboot!	The turbo card is not installed.

Table 314 AV Logs

LOG MESSAGE	DESCRIPTION
HTTP Virus infected - %s!	The device detected a virus in an HTTP connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
FTPDATA Virus infected - %s!	The device detected a virus in a FTPDATA connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
SMTP Virus infected - %s!	The device detected a virus in a SMTP connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
POP3 Virus infected - %s!	The device detected a virus in a POP3 connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
HTTP Bypass - %s!	The device bypassed the scanning of files in HTTP connections. %s is the filename. For example, game.zip.
FTPDATA Bypass - %s!	The device bypassed the scanning of files in FTP data connections. %s is the filename. For example, game.zip.
SMTP Bypass - %s!	The device bypassed the scanning of files in SMTP connections. %s is the filename. For example, game.zip.
POP3 Bypass - %s!	The device bypassed the scanning of files in POP3 connections. %s is the filename. For example, game.zip.
Can not find the signature, please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.

Table 314 AV Logs (continued)

LOG MESSAGE	DESCRIPTION
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.
Update the signature file successfully.	The device updated the signature file successfully.
The turbo card is not ready, please insert the card and reboot!	The turbo card is not installed.
The system is doing signature update now, please wait!	The device is updating the signature file.
HTTP Block. The session is over maximum ZIP sessions - %s!	The system blocked scanning files in HTTP connections. The format of %s is %FILENAME%. For example, game.zip."
FTPDATA Block. The session is over maximum ZIP sessions - %s!	The system blocked scanning files in FTPDATA connections. The format of %s is %FILENAME%. For example, game.zip."
SMTP Block. The session is over maximum ZIP sessions - %s!	The system blocked scanning files in SMTP connections. The format of %s is %FILENAME%. For example, game.zip."
POP3 Block. The session is over maximum ZIP sessions - %s!	The system blocked scanning files in POP3 connections. The format of %s is %FILENAME%. For example, game.zip."
Zip file unsupported - %s!	The system destroyed unsupported zip files.

Table 315 AS Logs

LOG MESSAGE	DESCRIPTION
Mail is in the Black List - Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!%MAIL_DIRECTION%	An e-mail with the listed source and subject matched an anti-spam blacklist entry.
Mail score is higher than threshold - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!%MAIL_DIRECTION%	The spam score (listed) for the e-mail with the listed source and subject was higher than or equal to the spam score threshold.
Exceed maximum mail sessions (%d).%MAIL_DIRECTION%	The number of concurrent mail sessions went over the limit (%d).

Table 315 AS Logs (continued)

LOG MESSAGE	DESCRIPTION
Remove rating server [%Rating Server IP Address%] from server list!%MAIL_DIRECTION%	The listed server IP address has been removed from the list of anti-spam external database servers.
"This is a phishing mail - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!"%MAIL_DIRECTION%	The spam score (listed) for the e-mail with the listed source and subject was higher than the spam score threshold. The anti-spam external database identified the e-mail as a phishing mail.
Invalid parameter for AsEngine!	There was an internal AS system error. This type of error causes the device to restart.
Mail Parser buffer is overflow!%MAIL_DIRECTION%	There were too many characters in a single line of an e-mail header that the device was attempting to parse.
Initialized the link list for IP list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Initialized the link list for Email list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Initialized the link list for MIME list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Initialized the link list for subject list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Convert the string to the PCRE pattern failed - ret_code:%d	Convert the string to regular expression failed.
Compile the string for PCRE failed - rule:%d	Compile the regular expression by PCRE library failed.
Load the anti-spam fixed runtime settings failed - ret_code:%d	Load the anti-spam fixed runtime settings failed.
Load the anti-spam variable runtime settings failed - rule:%d, ret_code:%d	Load the anti-spam variable runtime settings failed.
AS checking bypassed as a mail header line exceeds 1024 characters!%MAIL_DIRECTION%	AS checking bypassed as a mail header line exceeds 1024 characters. See

Table 316 AS Directions for Multiple WAN Devices

FROM\TO	LAN	WAN1	DMZ	WAN2	WLAN
LAN	(L to L)	(L to W1)	(L to D)	(L to W2)	(L to WL)
WAN1	(W1 to L)	(W1 to W1)	(W1 to D)	(W1 to W2)	(W1 to WL)
DMZ	(D to L)	(D to W1)	(D to D)	(D to W2)	(D to WL)
WAN2	(W2 to L)	(W2 to W1)	(W2 to D)	(W2 to W2)	(W2 to WL)
WLAN	(WL to L)	(WL to W1)	(WL to D)	(WL to W2)	(WL to WL)

Table 317 AS Directions for Single WAN Devices

FROM/TO	LAN	WAN	DMZ	WLAN
LAN	(L to L)	(L to W)	(L to D)	(L to WL)
WAN	(W to L)	(W to W)	(W to D)	(W to WL)
DMZ	(D to L)	(D to W)	(D to D)	(D to WL)
WLAN	(WL to L)	(WL to W)	(WL to D)	(WL to WL)

Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 318 Syslog Logs

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU, LOGS, Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DMZ", "LAN:DEV" for example).

Table 318 Syslog Logs (continued)

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hh:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web MAIN MENU, LOGS, Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC.
Event Log: <Facility*8 + Severity>Mon dd hh:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0 1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu b64 >"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web MAIN MENU, LOGS, Log Settings page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hh:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid>" act="<idp action>" count="1"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web MAIN MENU, LOGS, Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hh:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Spam" 1stReIP="<IP>"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web MAIN MENU, LOGS, Log Settings page. The severity is the log's syslog class. 1stReIP is the IP address of the first mail relay server. The definition of messages and notes are defined in the Anti-Spam log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hh:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" act="<idp action>" sid="<idp sid>" count="1"	This message is sent by the "RAS" at the time when this syslog is generated. The facility is defined in the web MAIN MENU, LOGS, Log Settings page. The severity is the centralized log type. The definition of messages and notes are defined in the IDP categories.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 319 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Open Software Announcements

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes MySQL and Anomic under GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third-party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5.You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7.If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8.If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so t hat distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9.The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10.If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11.BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/ OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,

THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

ONE LINE TO GIVE THE PROGRAM'S NAME AND A BRIEF IDEA OF WHAT IT DOES.

Copyright (C) YYYY NAME OF AUTHOR

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19YY NAME OF AUTHOR

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

SIGNATURE OF TY COON, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may consider it
more useful to permit linking proprietary

applications with the library. If this is what you want to do, use the GNU Library
General Public License instead of this License.

**This product includes Hibernate and Ifreechart under GNU LESSER
GENERAL PUBLIC LICENSE**

GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C)
1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston,
MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license
document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor
of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share
and change it. By contrast, the GNU General Public Licenses are intended to
guarantee your freedom to share and change free software--to make sure the
software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility

is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if

the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object

file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate

distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations

under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you

have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and a brief idea of what it does. Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!

This Product includes JDK under Binary Code License of Sun Microsystems, Inc.

Sun Microsystems, Inc. Binary Code License Agreement

for the JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files,

header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java 2 Platform Standard Edition (J2SE platform) platform on Java-enabled general purpose desktop computers and servers.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A

PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at <http://www.sun.com/policies/trademarks>. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that

arises or results from the use or distribution of any and all Programs and/or Software.

D. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as Java™ 2 Platform Standard Edition Development Kit 5.0; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2004, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (i) provides you prompt notice of the claim; (ii) gives you sole control of the defense and

settlement of the claim; (iii) provides you, at your expense, with all available information, assistance and authority to defend; and (iv) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A., Attention: Contracts Administration.

F. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

G. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#141623/Form ID#011801)

This Product includes Quartz

All source code, binaries, documentation and other files distributed with Quartz Enterprise Job Scheduler are subject to the following license terms, and are held under the following copyright, unless otherwise noted within the individual files.

Copyright James House (c) 2001-2004

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product uses and includes within its distribution, software developed by the Apache Software Foundation (<http://www.apache.org/>)

This Product includes Stuts and Tomcat under Apache License

Apache License Version 2.0, January 2004 <http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution

incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each

Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

NOTE: Some components of the Vantage VRPT 3.4 incorporate source code covered under the GPL, LGPL, Sun Microsystems, Inc. Binary Code License, Quartz License and Apache License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

This source code is free to download at <http://www.zyxel.com>

End-User License Agreement for "Vantage VRPT 3.4"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED \$1,000. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND

DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Note: Refer also to the [Open Software Announcements on page 671](#).

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

ZyXEL Limited Warranty

ZyXEL warrants that (a) the Vantage software (henceforth called the SOFTWARE) will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Support Services provided by ZyXEL shall be substantially as described in applicable written materials provided to you by ZyXEL, and ZyXEL support engineers will make commercially reasonable efforts to solve any problem issues. To the extent

allowed by applicable law, implied warranties on the SOFTWARE, if any, are limited to ninety (90) days.

CUSTOMER REMEDIES.

ZyXEL's and its suppliers' entire liability and your exclusive remedy shall be, at ZyXEL's option, either (a) return of the price paid, if any, or (b) repair or replacement of the SOFTWARE that does not meet ZyXEL's Limited Warranty and which is returned to ZyXEL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside Taiwan, neither these remedies nor any product support services offered by ZyXEL are available without proof of purchase from an authorized international source.

NO OTHER WARRANTIES

To the maximum extent permitted by applicable law, ZyXEL and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE, and the provision of or failure to provide Support Services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Please read the license screen in the installation wizard. You must accept the terms of the license in order to install Vantage.

Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

A

- about icon [37](#)
- access control [488](#)
- Add Device screen [40](#)
- additional ZyXEL device configuration [30](#)
- alerts, configuring rules [561](#), [563](#), [565](#)
- anti-virus
 - monitors [86](#)
 - statistical reports [315](#)
- authentication
 - failed login [445](#), [501](#)
 - successful login [499](#)
- authentication code [559](#)

B

- bandwidth
 - monitors [65](#)
- bandwidth. See device traffic.
- bar view icon [27](#)
- basic version license [22](#)
- browser types [33](#)

C

- clock time [25](#)
- common icons [27](#)
- common terms [25](#)
 - drill-down report [26](#)
 - incoming VPN traffic [26](#)
 - outgoing VPN traffic [26](#)
 - remote user [26](#)
 - remote VPN user [26](#)
 - ZLD-based ZyXEL devices [25](#)
 - ZyNOS-based ZyXEL devices [25](#)
- configuration
 - backup [555](#)

- e-mail [554](#)
 - general [549](#)
 - restore [555](#)
 - screens [549](#)
 - SMTP mail server [554](#)
 - users [555](#)
- content filter (all)
 - statistical reports [446](#)
- content filter (blocked)
 - statistical reports [467](#)
- copyright [709](#)
- CPU usage
 - monitors [71](#)
- customized report templates [522](#), [523](#)
- customized service field
 - where configured [168](#)
 - where it is used [171](#), [175](#), [179](#)
- customized service traffic. See other service traffic.

D

- dashboard [67](#)
- data backup [555](#)
- data restore [555](#)
- device information screen [53](#)
- device list
 - export [556](#)
- device traffic
 - direction in statistical reports [97](#)
- device window [36](#)
 - add device [38](#)
 - add folder [38](#)
 - editing device basic information [39](#)
 - editing folder information [39](#)
 - export [556](#)
 - moving device [39](#)
 - refresh [38](#)
 - removing device [39](#)
 - removing folder [39](#)

- right-click [40](#)
- searching device [39](#)
- viewing device basic information [39](#)

devices [591](#)

DNS reverse. See reverse DNS.

DoS (Denial-of-Service) [269](#)

drill-down [58](#), [590](#)

drill-down report [26](#)

E

Edit Device screen [40](#)

e-mail [24](#)

- forget password [25](#)
- low free disk mark [550](#)
- scheduled reports [24](#)
- SMTP settings [24](#), [554](#)
- system notification [24](#)
- test SMTP mail server [25](#), [555](#)

E-Mail anti-spam

- monitors [88](#)
- statistical reports [349](#)

E-Mail anti-virus

- monitors [87](#)
- statistical reports [333](#)

E-Mail intrusions

- monitors [89](#)
- signatures [363](#)

endpoint security, see EPS.

EPS [443](#)

events

- statistical reports [499](#)

F

failed login [445](#), [501](#)

features [591](#)

firmware

- platform [169](#)
- versions [591](#)

folder

- add [38](#)
- edit folder information [39](#)
- remove [39](#)

forget password [25](#), [34](#)

FTP traffic

- statistical reports [138](#)

full license version

- license key [22](#)

full version license [22](#)

function window [41](#)

- list of screens [42](#)

H

hardware requirement [22](#)

- log space required [22](#)

help icon [37](#)

host

- definition [26](#)

hostname reverse [550](#)

I

iCard [558](#)

idle timeout [36](#)

inactivity timeout [36](#)

interface usage

- monitors [75](#)

intrusions [291](#)

- monitors [85](#)
- signatures [294](#)

IPSec Secure Remote Access

- dynamic tunnel [222](#)
- Xauth [265](#)

J

JavaScript [33](#)

L

license key [22](#), [558](#)

license version

- full [22](#)
- license versions [22](#)
 - basic [22](#)
- list of screens [42](#)
- log descriptions
 - ZyNOS-based devices [645](#)
 - ZyWALL 1050 and USG Series [599](#)
- log entries [21](#)
 - archiving [538](#)
 - how used [30](#)
 - received by day [531](#)
 - received by device [533](#)
- log setting requirements [30](#)
- log space required
 - hardware [22](#)
- log viewer
 - processing time [25](#)
 - regular log entries. See regular log viewer.
- Login screen [34](#)
- logout icon [37](#)
- low free disk mark [550](#)

M

- MAC [40](#), [53](#)
- Macromedia flash player [33](#)
- mail traffic
 - statistical reports [153](#)
- main menu bar [36](#), [37](#)
- main screen [36](#)
 - parts of [36](#)
- memory usage
 - monitors [72](#)
- minimum hardware requirements [22](#)
- monitors [590](#)
 - anti-virus [86](#)
 - bandwidth [65](#)
 - CPU usage [71](#)
 - E-Mail anti-spam [88](#)
 - E-Mail anti-virus [87](#)
 - E-Mail intrusions [89](#)
 - end time [56](#)
 - graph [56](#)
 - interface usage [75](#)
 - intrusions [85](#)

- memory usage [72](#)
- next refresh time [56](#)
- port usage [74](#)
- printing [55](#)
- processing time [25](#)
- right-click [56](#)
- session usage [73](#)
- start time [56](#)
- typical layout [55](#)
- web security [90](#)
- web security anti-virus [91](#)
- web security intrusions [92](#)

N

- NetBIOS, enable settings [551](#)
- network security [269](#)
 - statistical reports [269](#)
- number of devices
 - currently allowed [559](#)
 - currently used [559](#)
 - increase allowed [558](#)
 - maximum allowed [559](#)

O

- operation system support [589](#)
- other service traffic
 - configure customized service field [168](#)
 - statistical reports [170](#)

P

- password
 - default value [34](#)
- pie view icon [27](#)
- platform [169](#)
- port number [23](#)
- port usage
 - monitors [74](#)
- print icon [27](#)
- printing
 - monitors [55](#)

- statistical reports [57](#)
- processing time [25](#)

Q

- Quick Start Guide [21](#)

R

- refresh icon [27](#)
- registration [590](#)
 - authentication code [559](#)
 - iCard [558](#)
 - license key [558](#)
 - upgrade [560](#)
- remote user [26](#)
- remote VPN user [26](#)
- report and setting window [36](#)
- report templates [522](#), [523](#)
- report window [52](#)
 - typical layouts [54](#)
- reports
 - processing time [25](#)
- reverse DNS [58](#), [550](#), [590](#)
- reverse hostname [590](#)

S

- scheduled reports [24](#), [590](#)
 - daily [510](#)
 - one-time [520](#)
 - overtime [520](#)
 - requirements [509](#)
 - store log days [509](#)
 - templates [522](#), [523](#)
 - weekly [518](#)
- Secure Remote Access
 - IPSec [222](#)
 - Site-to-Site [183](#)
 - SSL [242](#)
- security issues [296](#)
 - E-Mail [364](#)

- Web [423](#)
- security policy [443](#)
- security timeout [36](#)
- session usage
 - monitors [73](#)
- settings icon [27](#)
- Site-to-Site Secure Remote Access [183](#)
- SMTP mail server [24](#)
 - test [25](#), [555](#)
- software release
 - upgrade [557](#)
- source data [27](#)
 - how used in screens [30](#)
 - log entries [30](#)
 - traffic statistics [30](#)
- spam. See E-Mail anti-spam.
- specification
 - supported operation system [589](#)
- SSL Secure Remote Access
 - application [258](#)
 - authentication [242](#)
- Start Vantage Report [23](#)
- statistical reports [590](#)
 - anti-virus [315](#)
 - content filter (all) [446](#)
 - content filter (blocked) [467](#)
 - dates [57](#)
 - default chart type [58](#), [550](#)
 - E-Mail anti-spam [349](#)
 - E-Mail anti-virus [333](#)
 - E-Mail intrusions [361](#)
 - FTP traffic [138](#)
 - graph [58](#)
 - graph type [58](#)
 - last x days [58](#)
 - mail traffic [153](#)
 - mouse over [58](#)
 - network security [269](#)
 - other service traffic [170](#)
 - printing [57](#)
 - processing time [25](#)
 - right-click [58](#)
 - settings [58](#)
 - table [58](#)
 - title [57](#)
 - typical layout [57](#)
 - web security anti-virus [403](#)
 - web traffic [123](#)

- Stop Vantage Report [23](#)
- store log days
 - scheduled reports [509](#)
- submenu window [36](#)
- successful login [499](#)
- supported operation system [589](#)
- syntax conventions [5](#)
- system dashboard [59](#)
- system information summary [59](#)
- system notification [24](#)
 - low free disk mark setting [550](#)

T

- templates [522](#), [523](#)
- time [25](#)
 - clock time [25](#)
 - processing time [25](#)
- title bar [36](#)
- top level summary [67](#)
- traffic statistics
 - how used [30](#)
 - in typical application [21](#)
- typical application [21](#)

U

- upgrade
 - license version [558](#)
 - software release [557](#)
- user name
 - default value [34](#)
- users
 - account [579](#)
 - group [577](#)
 - on line vs off line [580](#)
 - screens [555](#)

V

- Vantage Report
 - about [37](#)

- license key [558](#)
- logs [536](#)
- settings [549](#)
- typical application [21](#)
- users. See users.

- Vantage Report server [21](#), [23](#)
 - as service [23](#), [590](#)
 - clock time in [25](#)
 - configuration. See configuration.
 - e-mail [24](#)
 - port number [23](#)
 - processing time [25](#)
 - source data [27](#)
 - starting [23](#)
 - stopping [23](#)
 - time [25](#)

- Vantage Report users. See users.

- version
 - license [22](#)
 - full [558](#)
 - upgrade [558](#)
- view detail icon [27](#)
- view logs icon [58](#)
- virus. See anti-virus.
- virus. See E-Mail anti-virus.
- virus. See web security anti-virus.
- VPN traffic
 - incoming [26](#)
 - outgoing [26](#)

W

- web configurator [33](#)
 - default password [34](#)
 - default user name [34](#)
 - in typical application [21](#)
 - minimum requirements [33](#)
 - screen resolution [33](#)
 - starting [33](#)
 - timeout [36](#)
 - URL [33](#)
- Web intrusions [418](#)
 - signatures [421](#)
- web security
 - monitors [90](#)
- web security anti-virus

- monitors [91](#)
- statistical reports [403](#)
- web security intrusions
 - monitors [92](#)
- web traffic
 - statistical reports [123](#)
- web users
 - statistical reports [133](#)

X

- Xauth [265](#)

Z

- ZLD [169](#)
- ZLD-based ZyXEL devices [25](#)
- ZyNOS [169](#)
- ZyNOS-based ZyXEL devices [25](#)
- ZyWALL 1050 [169](#)
 - feature support [591](#)
- ZyWALL USG series
 - feature support [591](#)
- ZyXEL device
 - add [38](#)
 - corresponding configuration [27](#)
 - device type setting [40](#)
 - edit basic information [39](#)
 - feature support [591](#)
 - MAC setting [40](#), [53](#)
 - model name [53](#)
 - move [39](#)
 - remove [39](#)
 - searching device [39](#)
 - select [39](#)
 - source data, see source data.
 - view basic information [39](#)
- ZyXEL devices
 - in typical application [21](#)