

Vantage Report

User's Guide

Version 2.3
Edition 1
2/2006

ZyXEL

Copyright

Copyright © 2006 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 240](#).

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.

Customer Support

Please have the following information ready when you contact customer support.

- Product model.
- Warranty Information.
- Brief description of the problem and the steps you took to solve it.

LOCATION	METHOD	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
		SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)		support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
		sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC		info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Česká Republika
		info@cz.zyxel.com	+420-241-091-359		
DENMARK		support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Søborg Denmark
		sales@zyxel.dk	+45-39-55-07-07		
FINLAND		support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
		sales@zyxel.fi	+358-9-4780 8448		
FRANCE		info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
			+33-4-72-52-19-20		
GERMANY		support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
		sales@zyxel.de	+49-2405-6909-99		
HUNGARY		support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldomb Str. H-1025, Budapest Hungary
		info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN		http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
		sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA		support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
		sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY		support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway
		sales@zyxel.no	+47-22-80-61-81		
POLAND		info@pl.zyxel.com	+48-22-5286603	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
			+48-22-5206701		

METHOD	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

a. "+" is the (prefix) number you enter to make an international telephone call.

•

Table of Contents

Copyright	2
ZyXEL Limited Warranty	3
Customer Support.....	4
Table of Contents	6
Preface	20
Chapter 1	
Introducing Vantage Report	22
1.1 Introduction	22
1.2 Key Features	22
1.3 Versions	23
Chapter 2	
The Vantage Report Server	26
2.1 Starting and Stopping the Vantage Report Server	26
2.2 E-Mail in the Vantage Report Server	26
2.3 Time in the Vantage Report Server	27
2.4 ZyXEL Device Configuration and Source Data	28
Chapter 3	
The Web Configurator.....	30
3.1 Web Configurator Requirements	30
3.2 Web Configurator Access	30
3.3 Title Bar	32
3.4 Device Window	32
3.5 Function Window	35
3.6 Report Window	40
3.6.1 Monitor Layout	40
3.6.2 Statistical Report Layout	42
Chapter 4	
Monitor	44
4.1 Bandwidth Monitor	44
4.2 Service Monitor	45
4.3 Attack Monitor	46
4.4 Intrusion Monitor	47

4.5 Anti-Virus Monitor	48
4.6 Anti-Spam Monitor	49
Chapter 5	
Traffic	52
5.1 Bandwidth	52
5.1.1 Bandwidth Summary.....	52
5.1.2 Bandwidth Summary Drill-Down	54
5.1.3 Bandwidth Top Protocols	56
5.1.4 Bandwidth Top Protocols Drill-Down.....	58
5.1.5 Top Bandwidth Hosts	60
5.1.6 Top Bandwidth Hosts Drill-Down	62
5.2 Web Traffic	63
5.2.1 Top Web Sites.....	63
5.2.2 Top Web Sites Drill-Down	65
5.2.3 Top Web Hosts	67
5.2.4 Top Web Hosts Drill-Down	68
5.3 FTP Traffic	70
5.3.1 Top FTP Sites	70
5.3.2 Top FTP Sites Drill-Down.....	72
5.3.3 Top FTP Hosts	74
5.3.4 Top FTP Hosts Drill-Down	75
5.4 Mail Traffic	77
5.4.1 Top Mail Sites	77
5.4.2 Top Mail Sites Drill-Down.....	79
5.4.3 Top Mail Hosts	81
5.4.4 Top Mail Hosts Drill-Down.....	82
5.5 VPN Traffic	84
5.5.1 Top VPN Peer Gateways	84
5.5.2 Top VPN Peer Gateways Drill-Down	86
5.5.3 Top VPN Hosts	88
5.5.4 Top VPN Hosts Drill-Down.....	90
5.6 Other Traffic	92
5.6.1 Service Settings.....	92
5.6.2 Top Destinations of Other Traffic	93
5.6.3 Top Destinations of Other Traffic Drill-Down.....	95
5.6.4 Top Sources of Other Traffic	97
5.6.5 Top Sources of Other Traffic Drill-Down	99
Chapter 6	
Network Attack	102
6.1 Attack	102
6.1.1 Attack Summary	102

6.1.2 Attack Summary Drill-Down	104
6.1.3 Top Attack Sources	106
6.1.4 Top Attack Sources Drill-Down	107
6.1.5 Top Attack Categories	109
6.1.6 Top Attack Categories Drill-Down	111
6.2 Intrusion	113
6.2.1 Intrusion Summary	113
6.2.2 Intrusion Summary Drill-Down	115
6.2.3 Top Intrusion Signatures	117
6.2.4 Top Intrusion Signatures Drill-Down	119
6.2.5 Top Intrusion Sources	121
6.2.6 Top Intrusion Sources Drill-Down	123
6.2.7 Top Intrusion Destinations	125
6.2.8 Top Intrusion Destinations Drill-Down	127
6.2.9 Intrusion Severities	129
6.2.10 Intrusion Severities Drill-Down	131
6.3 AntiVirus	133
6.3.1 Virus Summary	133
6.3.2 Virus Summary Drill-Down	135
6.3.3 Top Viruses	137
6.3.4 Top Viruses Drill-Down	139
6.3.5 Top Virus Sources	141
6.3.6 Top Virus Sources Drill-Down	143
6.3.7 Top Virus Destinations	145
6.4 AntiSpam	147
6.4.1 Spam Summary	147
6.4.2 Spam Summary Drill-Down	149
6.4.3 Top Spam Senders	151
6.4.4 Top Spam Sources	153
6.4.5 Top Spam Scores	155

Chapter 7

Security Policy 158

7.1 Blocked Web Accesses	158
7.1.1 Web Block Summary	158
7.1.2 Web Block Summary Drill-Down	160
7.1.3 Top Blocked Web Sites	162
7.1.4 Top Blocked Web Sites Drill-Down	163
7.1.5 Top Blocked Web Hosts	165
7.1.6 Top Blocked Web Hosts Drill-Down	167
7.1.7 Top Blocked Web Categories	169
7.1.8 Top Blocked Web Categories Drill-Down	170
7.2 Allowed Web Accesses	172

7.2.1 Web Allowed Summary	172
7.2.2 Web Allowed Summary Drill-Down	174
7.2.3 Top Allowed Web Sites	176
7.2.4 Top Allowed Web Sites Drill-Down	177
7.2.5 Top Allowed Web Hosts	179
7.2.6 Top Allowed Web Hosts Drill-Down	181
Chapter 8	
Authentication	184
8.1 Successful Login Screen	184
8.2 Failed Login Screen	185
Chapter 9	
Log Viewer	188
9.1 Regular Log Viewer	188
9.2 Critical Log Viewer	190
Chapter 10	
Schedule Report.....	194
10.1 Scheduled Report Summary Screen	194
10.2 Customize Daily Report Screen	195
10.3 Customize Weekly Report Screen	197
10.4 Customize Overtime Report Screen	199
Chapter 11	
System	202
11.1 General Configuration Screen	202
11.2 Server Configuration Screen	203
11.3 User Maintenance Screens	204
11.3.1 User Maintenance Summary Screen	205
11.3.2 Add/Edit User Account Screen	205
11.4 Data Maintenance Screens	206
11.4.1 Data Backup and Data Restore Screen	207
11.4.2 Device List Export and Device List Import Screen	207
11.5 Upgrade Screen	208
11.6 Registration Screens	209
11.6.1 Registration Summary Screen	209
11.6.2 Registration Screen	211
11.7 About Screen	212
Appendix A	
Troubleshooting.....	214
Appendix B	

Product Specifications	216
Appendix C	
Setting up Your Computer's IP Address.....	218
Windows 2000/NT/XP	218
Verifying Settings	222
Appendix D	
Log Descriptions.....	224
Appendix E	
Open Software Announcements.....	240
Notice	240
Index.....	276

List of Figures

Figure 1 Typical Vantage Report Application	22
Figure 2 Web Configurator Login Screen	31
Figure 3 Web Configurator Main Screen	31
Figure 4 Device Window	33
Figure 5 Add Device, Edit Device, and Device Information Screens	34
Figure 6 Device Window Right-Click Menu	35
Figure 7 Function Window	35
Figure 8 Function Window Right-Click Menu	39
Figure 9 Report Window: Monitor and Statistical Report Examples	40
Figure 10 Typical Monitor Layout	41
Figure 11 Report Window Right-Click Menu	42
Figure 12 Typical Statistical Report Layout	42
Figure 13 Report Window Right-Click Menu	43
Figure 14 Monitor > Bandwidth	44
Figure 15 Monitor > Service	45
Figure 16 Monitor > Attack	47
Figure 17 Monitor > Intrusion	48
Figure 18 Monitor > AntiVirus	49
Figure 19 Monitor > AntiSpam	50
Figure 20 Traffic > Bandwidth > Summary	53
Figure 21 Traffic > Bandwidth > Summary > Drill-Down	55
Figure 22 Traffic > Bandwidth > Top Protocol	57
Figure 23 Traffic > Bandwidth > Top Protocol > Drill-Down	59
Figure 24 Traffic > Bandwidth > Top Hosts	60
Figure 25 Traffic > Bandwidth > Top Hosts > Drill-Down	62
Figure 26 Traffic > WEB > Top Sites	64
Figure 27 Traffic > WEB > Top Sites > Drill-Down	66
Figure 28 Traffic > WEB > Top Hosts	67
Figure 29 Traffic > WEB > Top Hosts > Drill-Down	69
Figure 30 Traffic > FTP > Top Sites	71
Figure 31 Traffic > FTP > Top Sites > Drill-Down	73
Figure 32 Traffic > FTP > Top Hosts	74
Figure 33 Traffic > FTP > Top Hosts > Drill-Down	76
Figure 34 Traffic > MAIL > Top Sites	78
Figure 35 Traffic > MAIL > Top Sites > Drill-Down	80
Figure 36 Traffic > MAIL > Top Hosts	81

Figure 37 Traffic > MAIL > Top Hosts > Drill-Down	83
Figure 38 Traffic > VPN > Top Peer Gateways	85
Figure 39 Traffic > VPN > Top Peer Gateways > Drill-Down	87
Figure 40 Traffic > VPN > Top Hosts	89
Figure 41 Traffic > VPN > Top Hosts > Drill-Down	91
Figure 42 Service > Customization > Customization	92
Figure 43 Traffic > Customization > Top Destinations	94
Figure 44 Traffic > Customization > Top Destinations > Drill-Down	96
Figure 45 Traffic > Customization > Top Sources	97
Figure 46 Traffic > Customization > Top Sources > Drill-Down	99
Figure 47 Network Attack > Attack > Summary	103
Figure 48 Network Attack > Attack > Summary > Drill-Down	105
Figure 49 Network Attack > Attack > Top Sources	106
Figure 50 Network Attack > Attack > Top Sources > Drill-Down	108
Figure 51 Network Attack > Attack > By Category	110
Figure 52 Network Attack > Attack > By Category > Drill-Down	112
Figure 53 Network Attack > Intrusion > Summary	114
Figure 54 Network Attack > Intrusion > Summary > Drill-Down	116
Figure 55 Network Attack > Intrusion > Top Intrusions	118
Figure 56 Network Attack > Intrusion > Top Intrusions > Drill-Down	120
Figure 57 Network Attack > Intrusion > Top Sources	122
Figure 58 Network Attack > Intrusion > Top Sources > Drill-Down	124
Figure 59 Intrusion > Top Destinations	126
Figure 60 Network Attack > Intrusion > Top Destinations > Drill-Down	128
Figure 61 Network Attack > Intrusion > By Severity	130
Figure 62 Network Attack > Intrusion > By Severity > Drill-Down	132
Figure 63 Network Attack > AntiVirus > Summary	134
Figure 64 Network Attack > AntiVirus > Summary > Drill-Down	136
Figure 65 Network Attack > AntiVirus > Top Viruses	138
Figure 66 Network Attack > AntiVirus > Top Viruses > Drill-Down	140
Figure 67 Network Attack > AntiVirus > Top Sources	142
Figure 68 Network Attack > AntiVirus > Top Sources > Drill-Down	144
Figure 69 Network Attack > AntiVirus > Top Destinations	146
Figure 70 Network Attack > AntiSpam > Summary	148
Figure 71 Network Attack > AntiSpam > Summary > Drill-Down	150
Figure 72 Network Attack > AntiSpam > Top Senders	152
Figure 73 Network Attack > AntiSpam > Top Sources	154
Figure 74 Network Attack > AntiSpam > By Score	156
Figure 75 Security Policy > WEB Blocked > Summary	159
Figure 76 Security Policy > WEB Blocked > Summary > Drill-Down	161
Figure 77 Security Policy > WEB Blocked > Top Sites	162
Figure 78 Security Policy > WEB Blocked > Top Sites > Drill-Down	164
Figure 79 Security Policy > WEB Blocked > Top Hosts	166

Figure 80 Security Policy > WEB Blocked > Top Hosts > Drill-Down	168
Figure 81 Security Policy > WEB Blocked > By Category	169
Figure 82 Security Policy > WEB Blocked > By Category > Drill-Down	171
Figure 83 Security Policy > WEB Allowed > Summary	173
Figure 84 Security Policy > WEB Allowed > Summary > Drill-Down	175
Figure 85 Security Policy > WEB Allowed > Top Sites	176
Figure 86 Security Policy > WEB Allowed > Top Sites > Drill-Down	178
Figure 87 Security Policy > WEB Allowed > Top Hosts	180
Figure 88 Security Policy > WEB Allowed > Top Hosts > Drill-Down	182
Figure 89 Event > Device Login > Successful Login	184
Figure 90 Event > Device Login > Failed Login	185
Figure 91 Log Viewer > All Logs	189
Figure 92 Log Viewer > Critical Logs	191
Figure 93 Schedule Reports > Schedule Reports	194
Figure 94 Schedule Reports > Schedule Reports > Add (Daily Report)	196
Figure 95 Schedule Reports > Schedule Reports > Add (Weekly Report)	198
Figure 96 Schedule Reports > Schedule Reports > Add (Overtime Report)	200
Figure 97 System > General Configuration	203
Figure 98 System > Server Configuration	204
Figure 99 System > User Maintenance	205
Figure 100 Add/Edit User Account Screen	206
Figure 101 System > Data Maintenance > Configuration Backup & Restore	207
Figure 102 System > Data Maintenance > Device List Import & Export	208
Figure 103 System > Upgrade	209
Figure 104 System > Registration	210
Figure 105 Registration Screen	211
Figure 106 System > About	212
Figure 107 Windows XP: Start Menu	219
Figure 108 Windows XP: Control Panel	219
Figure 109 Windows XP: Control Panel: Network Connections: Properties	220
Figure 110 Windows XP: Local Area Connection Properties	220
Figure 111 Windows XP: Advanced TCP/IP Settings	221
Figure 112 Windows XP: Internet Protocol (TCP/IP) Properties	222

List of Tables

Table 1 Differences Between Standard Version and Professional Version	24
Table 2 Processing Times by Menu Item	27
Table 3 Configuration Requirements for ZyXEL Devices by Menu Item	28
Table 4 Title Bar	32
Table 5 Device Window	33
Table 6 Function Window	36
Table 7 Typical Monitor Features	41
Table 8 Typical Statistical Report Features	42
Table 9 Monitor > Bandwidth	44
Table 10 Monitor > Service	46
Table 11 Monitor > Attack	47
Table 12 Monitor > Intrusion	48
Table 13 Monitor > AntiVirus	49
Table 14 Monitor > AntiSpam	50
Table 15 Traffic > Bandwidth > Summary	53
Table 16 Traffic > Bandwidth > Summary > Drill-Down	55
Table 17 Traffic > Bandwidth > Top Protocol	57
Table 18 Traffic > Bandwidth > Top Protocol > Drill-Down	59
Table 19 Traffic > Bandwidth > Top Hosts	61
Table 20 Traffic > Bandwidth > Top Hosts > Drill-Down	63
Table 21 Traffic > WEB > Top Sites	64
Table 22 Traffic > WEB > Top Sites > Drill-Down	66
Table 23 Traffic > WEB > Top Hosts	68
Table 24 Traffic > WEB > Top Hosts > Drill-Down	69
Table 25 Traffic > FTP > Top Sites	71
Table 26 Traffic > FTP > Top Sites > Drill-Down	73
Table 27 Traffic > FTP > Top Hosts	75
Table 28 Traffic > FTP > Top Hosts > Drill-Down	76
Table 29 Traffic > MAIL > Top Sites	78
Table 30 Traffic > MAIL > Top Sites > Drill-Down	80
Table 31 Traffic > MAIL > Top Hosts	82
Table 32 Traffic > MAIL > Top Hosts > Drill-Down	83
Table 33 Traffic > VPN > Top Peer Gateways	85
Table 34 Traffic > VPN > Top Peer Gateways > Drill-Down	87
Table 35 Traffic > VPN > Top Hosts	89
Table 36 Traffic > VPN > Top Hosts > Drill-Down	91

Table 37 Service > Customization > Customization	93
Table 38 Traffic > Customization > Top Destinations	94
Table 39 Traffic > Customization > Top Destinations > Drill-Down	96
Table 40 Traffic > Customization > Top Sources	98
Table 41 Traffic > Customization > Top Sources > Drill-Down	99
Table 42 Network Attack > Attack > Summary	103
Table 43 Network Attack > Attack > Summary > Drill-Down	105
Table 44 Network Attack > Attack > Top Sources	107
Table 45 Network Attack > Attack > Top Sources > Drill-Down	108
Table 46 Network Attack > Attack > By Category	110
Table 47 Network Attack > Attack > By Category > Drill-Down	112
Table 48 Network Attack > Intrusion > Summary	114
Table 49 Network Attack > Intrusion > Summary > Drill-Down	116
Table 50 Network Attack > Intrusion > Top Intrusions	118
Table 51 Network Attack > Intrusion > Top Intrusions > Drill-Down	120
Table 52 Network Attack > Intrusion > Top Sources	122
Table 53 Network Attack > Intrusion > Top Sources > Drill-Down	124
Table 54 Intrusion > Top Destinations	126
Table 55 Network Attack > Intrusion > Top Destinations > Drill-Down	128
Table 56 Network Attack > Intrusion > By Severity	130
Table 57 Network Attack > Intrusion > By Severity > Drill-Down	132
Table 58 Network Attack > AntiVirus > Summary	134
Table 59 Network Attack > AntiVirus > Summary > Drill-Down	136
Table 60 Network Attack > AntiVirus > Top Viruses	138
Table 61 Network Attack > AntiVirus > Top Viruses > Drill-Down	140
Table 62 Network Attack > AntiVirus > Top Sources	142
Table 63 Network Attack > AntiVirus > Top Sources > Drill-Down	144
Table 64 Network Attack > AntiVirus > Top Destinations	146
Table 65 Network Attack > AntiSpam > Summary	148
Table 66 Network Attack > AntiSpam > Summary > Drill-Down	150
Table 67 Network Attack > AntiSpam > Top Senders	152
Table 68 Network Attack > AntiSpam > Top Sources	154
Table 69 Network Attack > AntiSpam > By Score	156
Table 70 Security Policy > WEB Blocked > Summary	159
Table 71 Security Policy > WEB Blocked > Summary > Drill-Down	161
Table 72 Security Policy > WEB Blocked > Top Sites	163
Table 73 Security Policy > WEB Blocked > Top Sites > Drill-Down	164
Table 74 Security Policy > WEB Blocked > Top Hosts	166
Table 75 Security Policy > WEB Blocked > Top Hosts > Drill-Down	168
Table 76 Security Policy > WEB Blocked > By Category	170
Table 77 Security Policy > WEB Blocked > By Category > Drill-Down	171
Table 78 Security Policy > WEB Allowed > Summary	173
Table 79 Security Policy > WEB Allowed > Summary > Drill-Down	175

Table 80 Security Policy > WEB Allowed > Top Sites	177
Table 81 Security Policy > WEB Allowed > Top Sites > Drill-Down	178
Table 82 Security Policy > WEB Allowed > Top Hosts	180
Table 83 Security Policy > WEB Allowed > Top Hosts > Drill-Down	182
Table 84 Event > Device Login > Successful Login	184
Table 85 Event > Device Login > Failed Login	186
Table 86 Log Viewer > All Logs	189
Table 87 Log Viewer > Critical Logs	192
Table 88 Schedule Reports > Schedule Reports	195
Table 89 Schedule Reports > Schedule Reports > Add (Daily Report)	197
Table 90 Schedule Reports > Schedule Reports > Add (Weekly Report)	199
Table 91 Schedule Reports > Schedule Reports > Add (Overtime Report)	201
Table 92 System > General Configuration	203
Table 93 System > Server Configuration	204
Table 94 System > User Maintenance	205
Table 95 Add/Edit User Account Screen	206
Table 96 System > Data Maintenance > Configuration Backup & Restore	207
Table 97 System > Data Maintenance > Device List Import & Export	208
Table 98 System > Upgrade	209
Table 99 System > Registration	210
Table 100 Registration Screen	211
Table 101 Web Configurator Specifications	216
Table 102 System Notifications Specifications	216
Table 103 Feature Specifications	216
Table 104 System Maintenance Logs	224
Table 105 System Error Logs	225
Table 106 Access Control Logs	225
Table 107 TCP Reset Logs	226
Table 108 Packet Filter Logs	226
Table 109 ICMP Logs	226
Table 110 CDR Logs	227
Table 111 PPP Logs	227
Table 112 UPnP Logs	228
Table 113 Content Filtering Logs	228
Table 114 Attack Logs	229
Table 115 IPSec Logs	230
Table 116 IKE Logs	230
Table 117 PKI Logs	233
Table 118 Certificate Path Verification Failure Reason Codes	234
Table 119 802.1X Logs	235
Table 120 ACL Setting Notes	236
Table 121 ICMP Notes	236
Table 122 Syslog Logs	237

Table 123 RFC-2408 ISAKMP Payload Types 237

Preface

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.

About This User's Guide

This manual is designed to guide you through the configuration of Vantage Report for its various applications.

Related Documentation

- Included CD
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away.
- 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.

User Guide Feedback

Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

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 **Traffic > WEB > Top Hosts** means first click **Traffic**, then click **WEB** and finally click **Top Hosts**.

CHAPTER 1

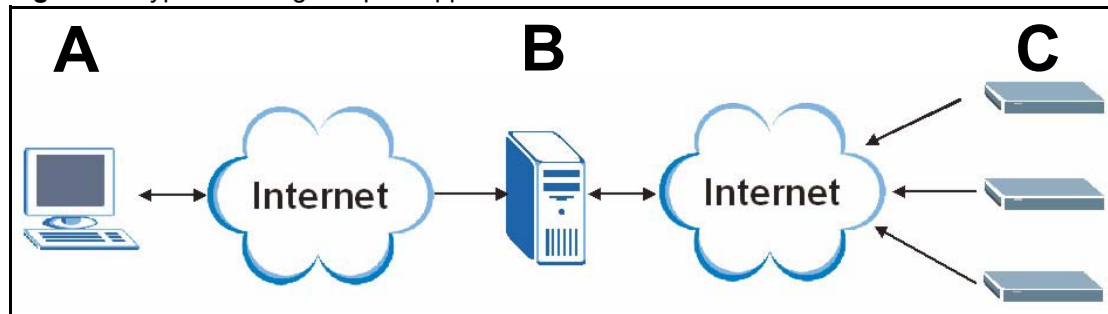
Introducing Vantage Report

Please see the Quick Start Guide for Vantage Report setup requirements, installation, and access. This chapter introduces Vantage Report and its key features.

1.1 Introduction

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 Key Features

- **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 thirty minutes, worst-case.

- **Statistical Reports**

Generate reports for historical analysis. These reports include bandwidth usage, service usage, VPN usage, web filter (blocked sites), attack, intrusion, anti-virus, anti-spam, and authentication 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.

- **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.

1.3 Versions

There are two versions of Vantage Report, standard version and professional version. When you install Vantage Report, you get the standard version. The professional version requires a license key, which you usually have to purchase.

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

The following table shows some of the differences between the standard and professional version.

Table 1 Differences Between Standard Version and Professional Version

FEATURE	STANDARD	PROFESSIONAL
number of supported devices	1	up to 25
number of scheduled reports	20	500
supported formats for scheduled reports	PDF	PDF, HTML
drill-down reports	no	yes
reverse DNS lookup	no	yes
web usage by category	no	yes
AntiVirus	no	yes
AntiSpam	no	yes

There is also a free trial of the professional version. The trial version is the same as the professional version except that it only supports one device. You can get the trial version by registering Vantage Report. See [section 11.6 on page 209](#) for more information

CHAPTER 2

The Vantage Report Server

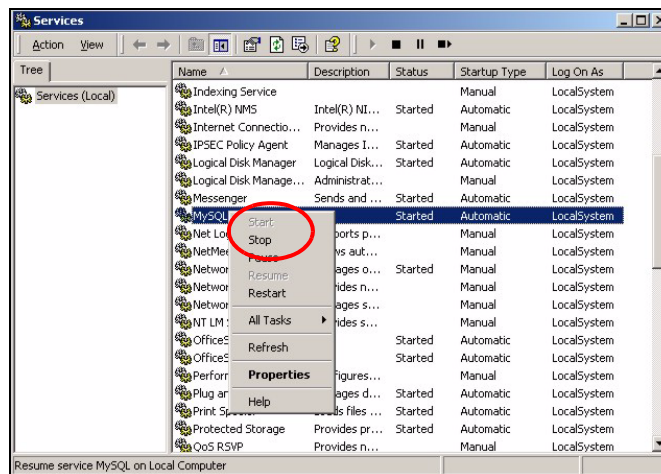
This chapter explains several characteristics of the Vantage Report server.

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 Right-click on **Vantage Report**. A menu appears.
- 3 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 11.2 on page 203](#) 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 11.3 on page 204](#)). 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 10 on page 194](#) 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 B on page 216](#) for a list of parameters and threshold values. One of the threshold values can be configured. See [section 11.1 on page 202](#).
- **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 30](#) 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 11.2 on page 203](#) 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
Traffic, Network Attack, Security Policy, Authentication	5
Log Viewer > All Logs	30
Log Viewer > Critical Logs	1

2.4 ZyXEL Device Configuration and Source Data

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

Table 3 Configuration Requirements for ZyXEL Devices by Menu Item

MENU ITEM(S)	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	--
Traffic (except VPN)	traffic statistics	--	--
Traffic > VPN	log entries	IPSec	--
Network Attack > Attack	log entries	Attack	--
Network Attack > Intrusion	log entries	IDP	IDP > Signature
Network Attack > AntiVirus	log entries	Anti-Virus	Anti-Virus > General
Network Attack > AntiSpam	log entries	Anti-Spam	--
Security Policy > WEB Blocked	log entries	Blocked Web Sites	--
Security Policy > WEB Allowed	log entries	Forward Web Sites	--
Event > Device Login	log entries	System Maintenance	--
Log Viewer > All Logs	log entries	**	**
Log Viewer > Critical Logs	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.

CHAPTER 3

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 7 or later
- Recommended screen resolution: 1024 x 768 pixels

3.2 Web Configurator Access

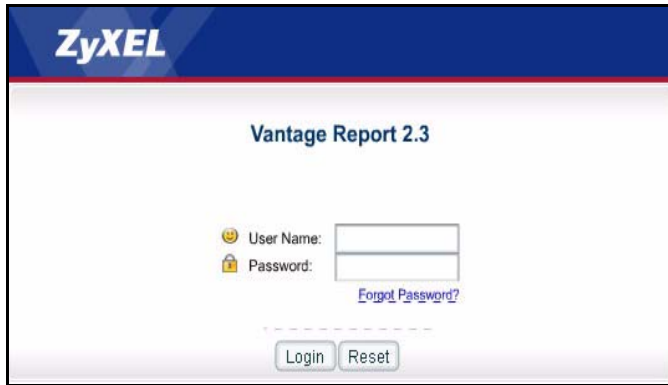
To access the web configurator, follow these steps:

- 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`.
 - [xxxxx](#) is the port number you entered during installation.

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 2 Web Configurator Login Screen



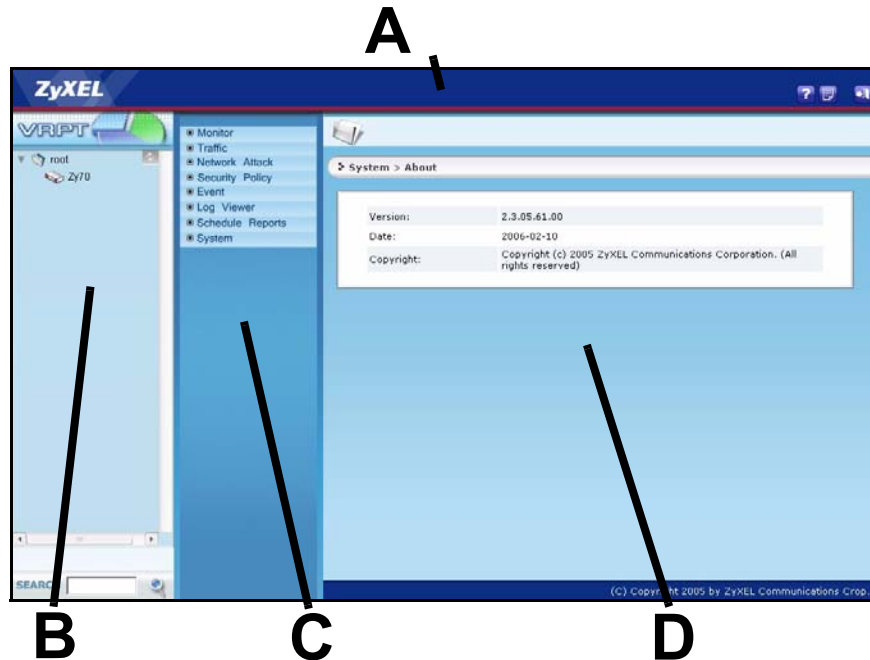
Note: If you forget your password, enter your user name, and click **Forget Password?**. Vantage Report sends your password to the e-mail address (if any) for your **User Name**. See [section 2.2 on page 26](#) for more information about e-mail in Vantage Report and [section 11.3 on page 204](#) for more information about SMTP configuration.

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

Note: See [section 11.3 on page 204](#) to change the password.

4 Click the **Login** button. The main screen in Vantage Report appears.

Figure 3 Web Configurator Main Screen



The main screen is divided into four parts: the title bar (**A**), the device window (**B**), the function window (**C**), and the report window (**D**). The title bar provides some icons that are useful anytime. The device window displays and organizes the ZyXEL devices that can provide information to Vantage Report. The function window lists the reports you can generate and organizes these reports into categories. Last, the report window shows the selected report for the selected device(s).




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 Title Bar

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

Table 4 Title Bar

ICON	DESCRIPTION
	This icon opens the help page for the current screen in Vantage Report.
	This icon provides the version of Vantage Report.
	This icon logs you out of Vantage Report.

3.4 Device Window

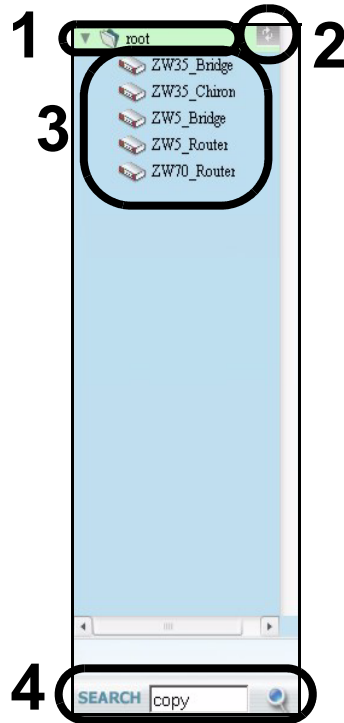
Use the device window to select which device(s) you want to include in a report, add devices to Vantage Report, and remove devices from Vantage Report.

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 4](#) shows an example.

Figure 4 Device Window



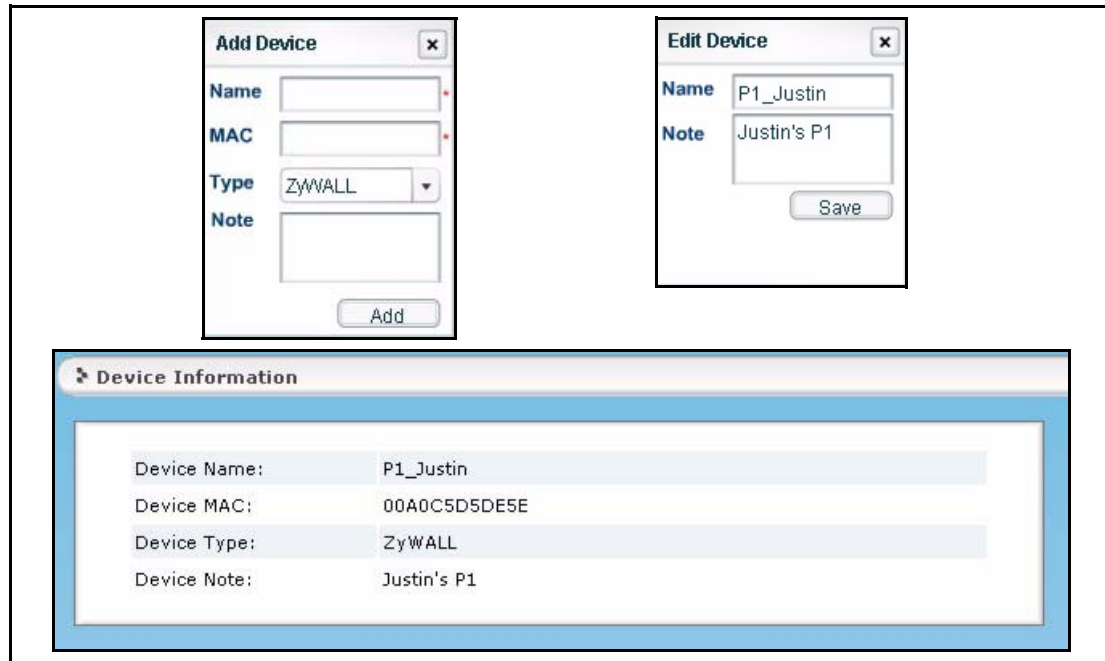
Each numbered section above is described in the following table.

Table 5 Device Window

SECTION	DESCRIPTION
1	<p>To add a device to Vantage report,</p> <ul style="list-style-type: none"> right click on root, and select Add Device. The Add Device screen appears in the device window. (See Figure 5.)
2	<p>To update the device window,</p> <ul style="list-style-type: none"> click the Refresh button.
3	<p>To select which device is included in a report</p> <ul style="list-style-type: none"> click on the device. <p>To look at the basic information about a device,</p> <ul style="list-style-type: none"> click on the device. The Device Information screen appears in the report window. (See Figure 5.) <p>To edit the basic information about a device,</p> <ul style="list-style-type: none"> right-click on the device, and select Edit Device. The Edit Device screen appears in the device window. (See Figure 5.) <p>To remove a device from Vantage Report,</p> <ul style="list-style-type: none"> right-click on the device, and select Delete Device. Vantage Report confirms you want to delete it before doing so.
4	<p>To search for a device,</p> <ul style="list-style-type: none"> type any part of the name, MAC address, or note in the SEARCH field, and click the magnifying glass. If a match is found, Vantage Report highlights the device in the device window, but the report 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 window. 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 5](#).

Figure 5 Add Device, Edit Device, and Device Information Screens



Each field is explained in the following table.

LABEL	DESCRIPTION
Name	Enter the name of the device 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 in Vantage Report, and it has to be different than other device names in Vantage Report. You can use the system name of the device.
MAC	This field is not available in the Edit Device screen. Enter the LAN MAC address of the device you want to add. 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: ZyWALL , Prestige , and IDP 10 .
Note	Enter any additional notes you want to make for the device 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, the following menu appears. If you right-click on a device, you can see the following menu items at the end of the menu.

Figure 6 Device Window Right-Click Menu



Click **About Macromedia Flash Player 7...** to get information about the current version of Flash.

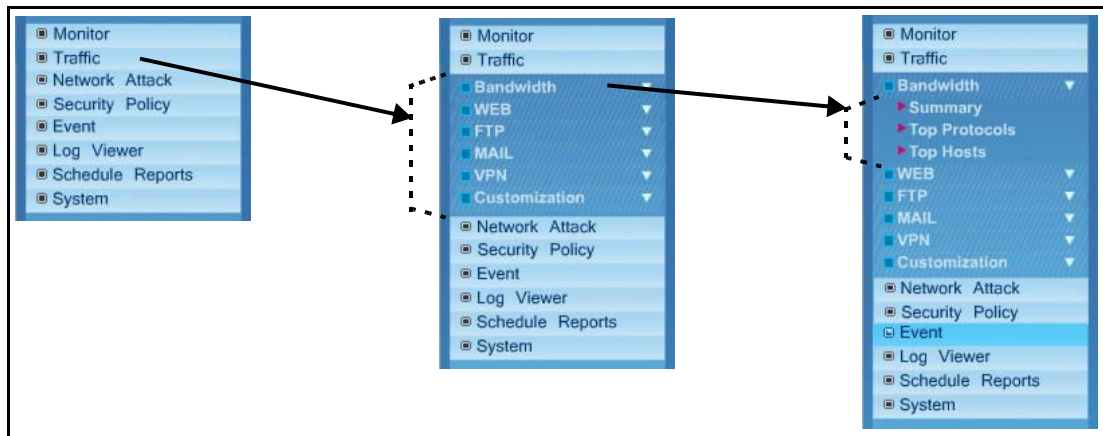
3.5 Function Window

Use the function window 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 7](#)

Figure 7 Function Window



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 6 expands the function window and introduces each monitor, statistical report, and screen. In addition, it also indicates if you can drill down into each statistical report.

Table 6 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
Monitor		Use monitors to check the status of ZyXEL devices.
Bandwidth		Use this report to monitor the total amount of traffic handled by the selected device.
Service		Use this report to monitor the amount of traffic generated by web, FTP, mail, or VPN services in the selected device.
Attack		Use this report to monitor the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall.
Intrusion		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.
AntiSpam		Use this report to monitor the number of spam messages stopped by the selected device.
Traffic		Use these reports to look at how much traffic was handled by ZyXEL devices or who used the most bandwidth in a ZyXEL device. You can also look at traffic in various directions.
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 Protocol	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.
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.
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.
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.

Table 6 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
VPN	Summary	Use these reports to look at the top sources and destinations of traffic in VPN tunnels.
	Top Peer Gateways	Use this report to look at the top destinations of VPN traffic. You can also use this report to look at the top sources of VPN traffic for any top destination.
	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.
Customization	Customization	Use the Service Settings screen to add, edit, or remove services whose traffic you can view in the other Service > Customization reports.
	Top Destination	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.
Network Attack		Use these reports to look at Denial-of-Service (DoS) attacks that were detected by the ZyXEL device's firewall.
Attack	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 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 Category	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		Use these reports to 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.
	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.

Table 6 Function Window

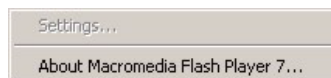
LEVEL 1/2	LEVEL 3	FUNCTION
AntiVirus		Use these reports to look at viruses that were detected by the ZyXEL device's anti-virus feature.
	Summary	Use this report to look at the number of virus occurrences by time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences.
AntiSpam		Use these reports to 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.
	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.
	By Score	Use this report to look at the top scores calculated for spam messages by number of messages.
Security Policy		Use these reports to look at the top sources and destinations of traffic that is forwarded or blocked based on each device's content filtering settings. You can also look at the amount of traffic forwarded or blocked by time interval.
WEB 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 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.
WEB Allowed	Summary	Use this report to look at the number of attempts to access allowed web sites by time interval. You can also use this report to look at the top sources of attempts to access allowed web sites in a specific time interval.
	Top Sites	Use this report to look at the top destinations of attempts to access allowed web sites by number of attempts. You can also use this report to look at the top sources of attempts to access allowed web sites for any top destination.
	Top Hosts	Use this report to look at the top sources of attempts to access allowed web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access allowed web sites for any top source.
Event		

Table 6 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
User	Device Login	Use these screens to look at who successfully logged into the ZyXEL device (for management or monitoring purposes) or who tried to log in but failed.
	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.
Log Viewer		Use these screens to look at all log entries or critical log entries for the selected ZyXEL device.
All Logs		Use the log viewer screens to look at all the log entries for the selected ZyXEL device.
Critical Logs		Use the log viewer screens to look at critical log entries for the selected ZyXEL device. Critical log entries are important and may require immediate attention. They are also updated more frequently than regular log entries.
Schedule Reports		
Schedule Reports		Use these screens to set up and maintain daily, weekly, and overtime (one-time) reports that Vantage Report sends by e-mail.
System		The root account can use all of the following screens. Other users can use the About screen and some features in User Maintenance .
General		Use this screen to maintain global reporting settings, such as how many days of logs to keep and default chart type.
Server		Use this screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports.
User		The root account can use these screens to view, add, edit, or remove Vantage Report users. Other users can only use these screens to look at and edit their user settings, including their password.
Data Maintenance	Configuration Backup & Restore	You can use this screen to backup or restore the settings in the General Configuration , Server Configuration , and User Maintenance screens. (The format is XML.)
	Device List Import & Export	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 professional version.
Registration		Use this screen to get the trial version, upgrade to the professional version, or increase the number of devices Vantage Report supports.
About		Use this screen to get the current release and copyright for Vantage Report.

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

Figure 8 Function Window Right-Click Menu

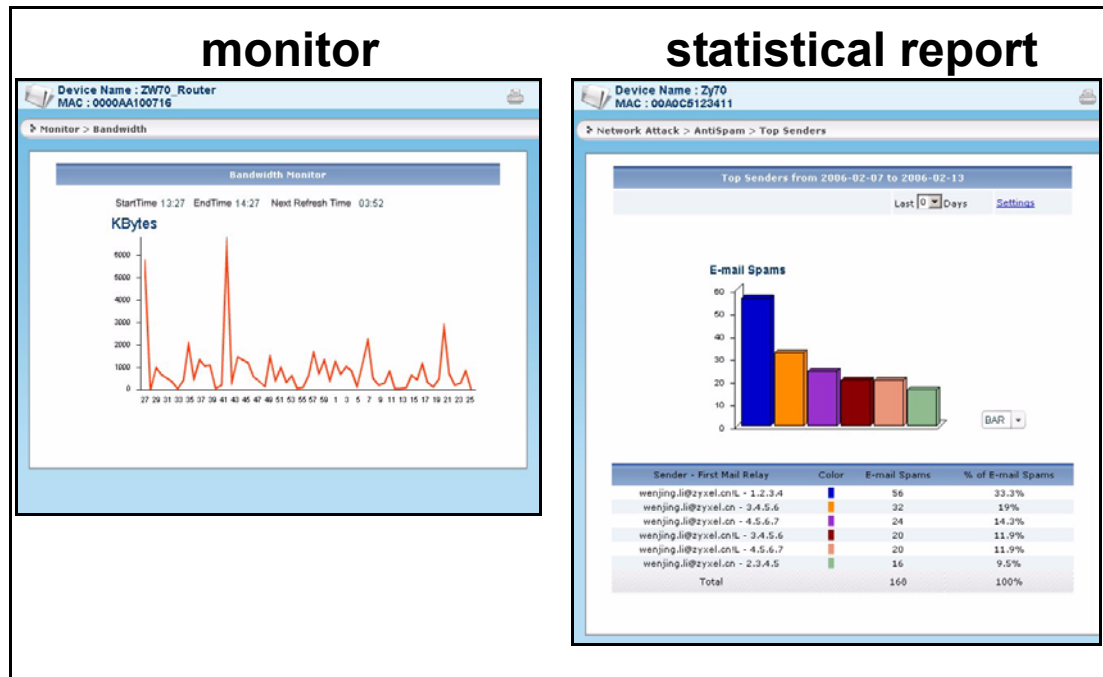


Click **About Macromedia Flash Player 7...** to get information about the current version of Flash.

3.6 Report Window

The report window displays the monitor, statistical report, or screen that you select in the device window and the function window. The layout in the report 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 9](#).

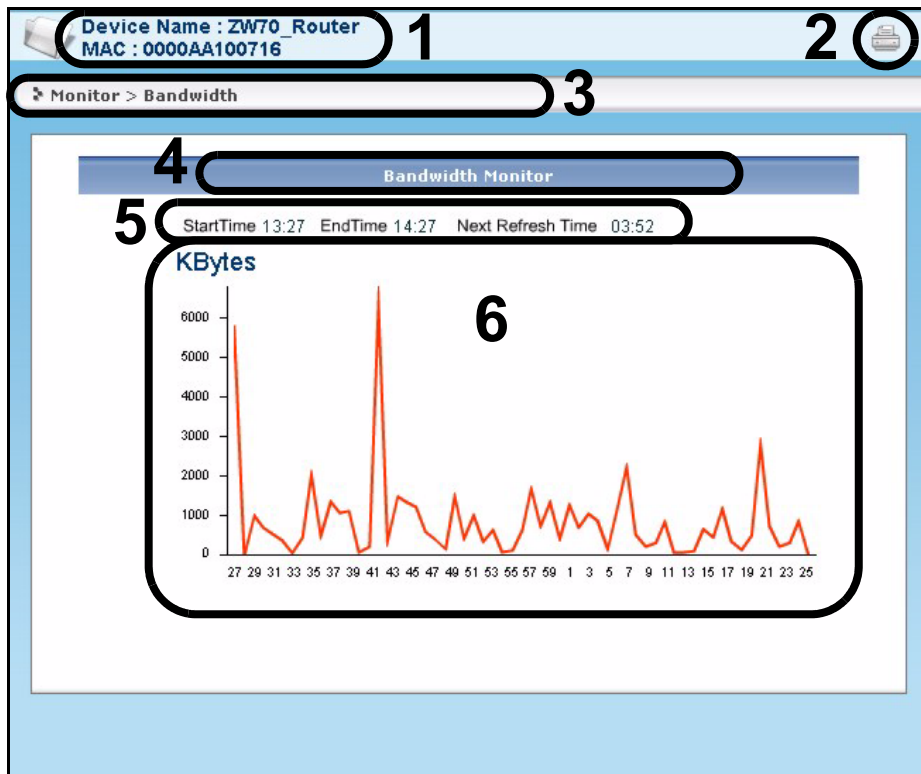
Figure 9 Report Window: Monitor and Statistical Report Examples



3.6.1 Monitor Layout

A typical monitor is shown in [Figure 4](#).

Figure 10 Typical Monitor Layout



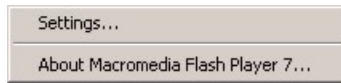
Each numbered section above is described in the following table.

Table 7 Typical Monitor Features

SECTION	DESCRIPTION
1	Device Name, MAC: These fields are the same ones you entered when you added the device. (See “Device Window.”)
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.
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. Next Refresh Time: This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time that is discussed in section 2.3 on page 27 .
6	The graph shows how the status changes over time. The X-axis (horizontal) is time. See section 2.3 on page 27 for more information about clock time in Vantage Report. The Y-axis (vertical) depends on the type of monitor you select. In Figure 10 , the y-axis is the number of kilobytes of traffic handled by the device each minute. See section 2.4 on page 28 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 11 Report Window Right-Click Menu

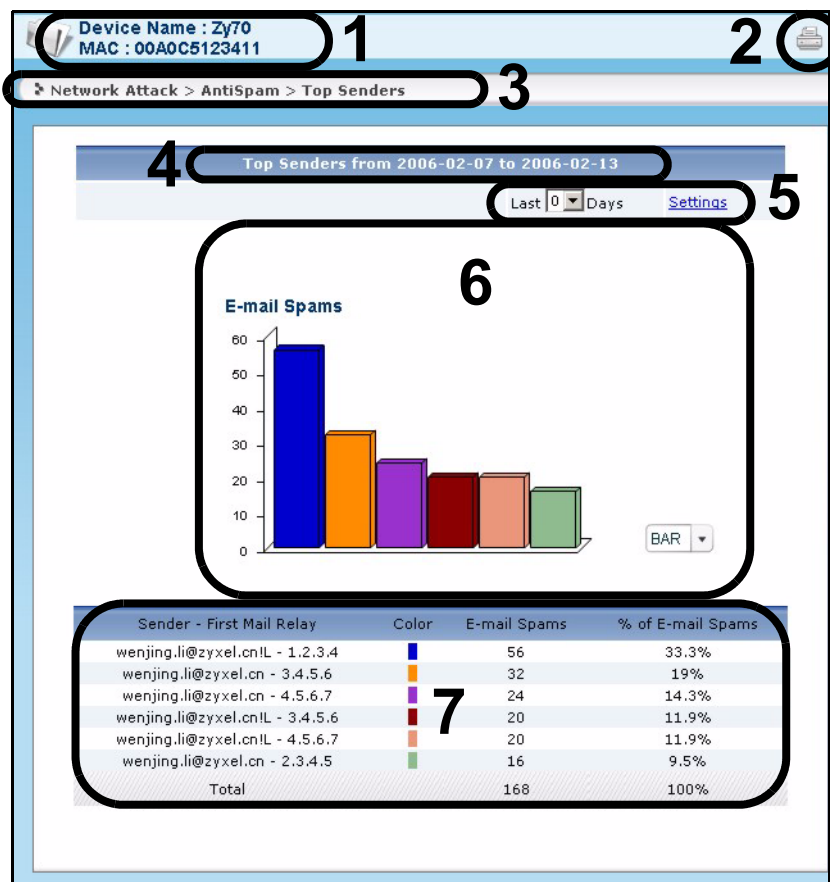


Click **Settings...** if you want to change the Flash settings on the Vantage Report server. In most cases, this is unnecessary. Click **About Macromedia Flash Player 7...** to get information about the current version of Flash.

3.6.2 Statistical Report Layout

A typical statistical report is shown in [Figure 12](#).

Figure 12 Typical Statistical Report Layout



Each numbered section above is described in the following table.

Table 8 Typical Statistical Report Features

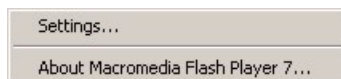
SECTION	DESCRIPTION
1	Device Name, MAC: These fields are the same ones you entered when you added the device. (See Figure 5 on page 34.)
2	Print icon: Click this icon to print the current screen.

Table 8 Typical Statistical Report Features

SECTION	DESCRIPTION
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.
5	<p>Last Days, Settings: Use one of these fields to specify what historical information is included in the report.</p> <ul style="list-style-type: none"> • Select how many days, ending (and including) today, in the Last Days drop-down list. • Click Settings, and 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. See section 11.1 on page 202. <p>When you change any of these fields, the report updates automatically. The Last Days field returns to zero, regardless of your selection. This way, you can refresh the report by selecting Last Days again. You can see the current date range in the title (section 4). Both the Last Days and Settings fields reset to the default values when you click a menu item in the function window (including the menu item for the same report). They do not reset when you open or close drill-down reports.</p> <p>These fields are not available in drill-down reports because these reports use the same historical information as the main report.</p> <p>See section 2.3 on page 27 for more information about time in these screens.</p>
6	<p>The graph displays the specified report visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. You can specify the Default Chart Type in System > General Configuration. See section 11.1 on page 202. • Move your mouse over a slice in the pie chart or a bar in the bar chart. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little. <p>See section 2.4 on page 28 for more information about the source data used by the statistical report.</p>
7	<p>In the table,</p> <ul style="list-style-type: none"> • 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 > General Configuration, the table displays the domain name, if identifiable, with IP addresses (for example, "www.yahoo.com/200.100.20.10"). See section 11.1 on page 202. • Some reports provide extra information (for example, number of traffic events) in the table. See each report for more information. <p>See section 2.4 on page 28 for more information about the source data used by the statistical report.</p>

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 13 Report 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 Macromedia Flash Player 7...** to get information about the current version of Flash.

CHAPTER 4

Monitor

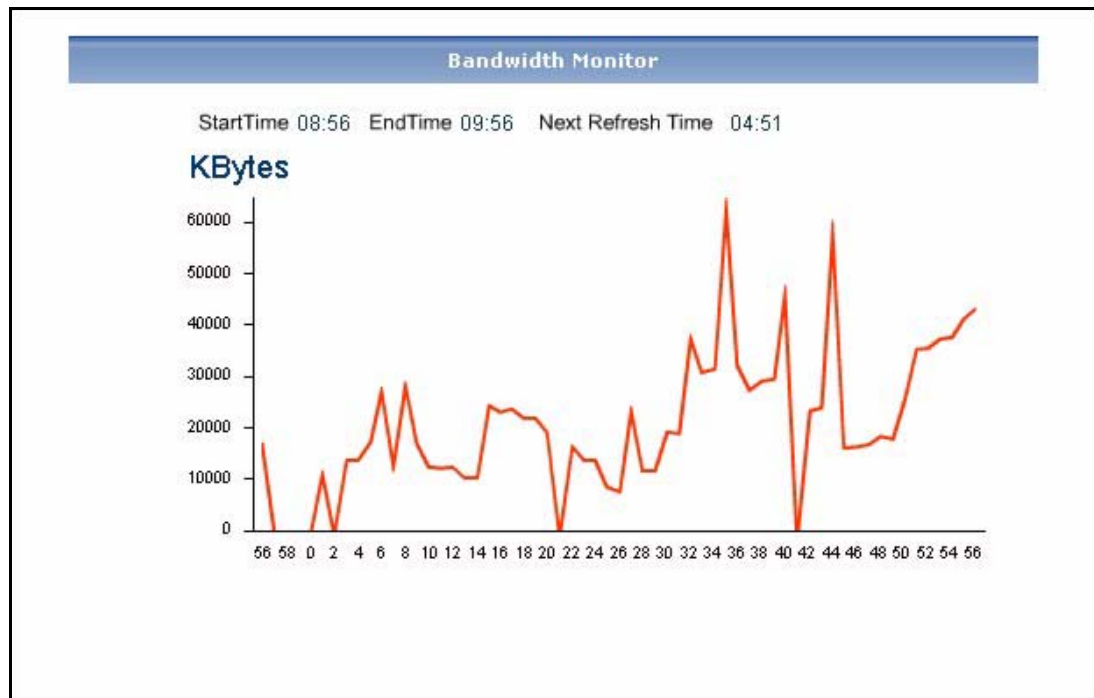
Use monitors to check the status of ZyXEL devices. See [section 2.3 on page 27](#) for a related discussion about time.

4.1 Bandwidth Monitor

Use this report to monitor the total amount of traffic handled by the selected device.

Click **Monitor** > **Bandwidth** to open this screen.

Figure 14 Monitor > Bandwidth



Each field is described in the following table.

Table 9 Monitor > Bandwidth

LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.

Table 9 Monitor > Bandwidth

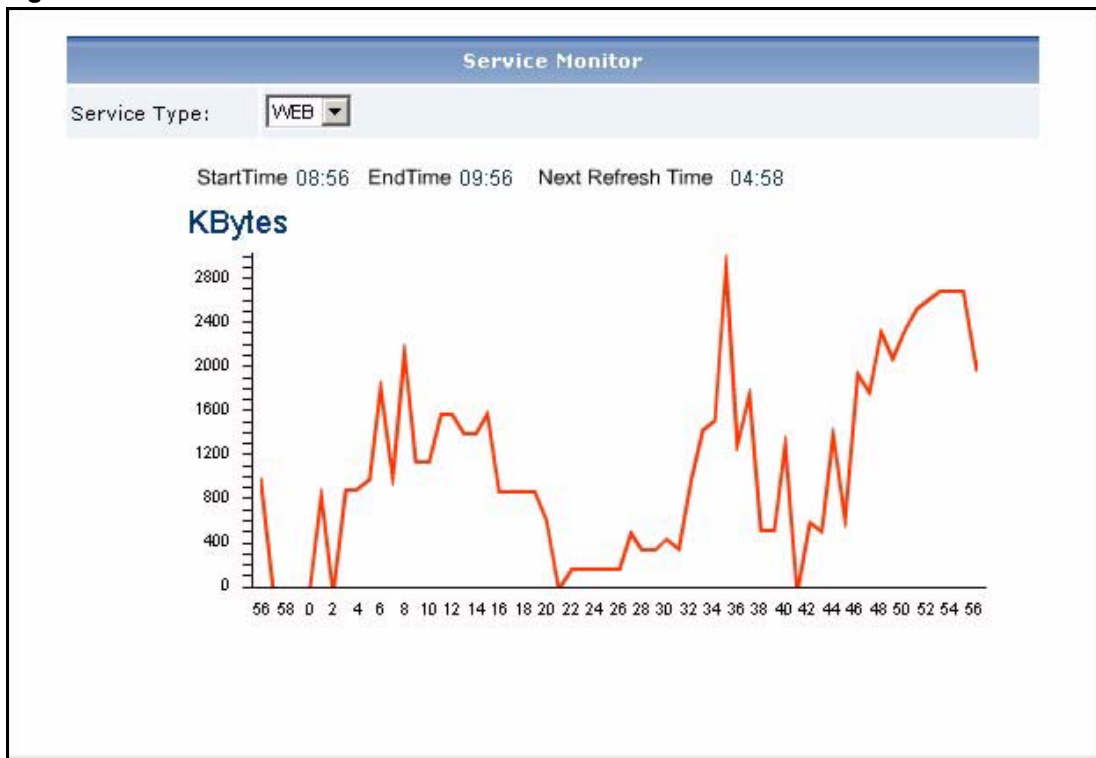
LABEL	DESCRIPTION
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next Refresh Time	This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time.
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 . For example, if the start time is 13:27 and end time is 14:27, then "39" means 13:39 and "5" means 14:05.

4.2 Service Monitor

Use this report to monitor the amount of traffic generated by web, FTP, mail, or VPN services in the selected device.

Click **Monitor > Service** to open this screen.

Figure 15 Monitor > Service



Each field is described in the following table.

Table 10 Monitor > Service

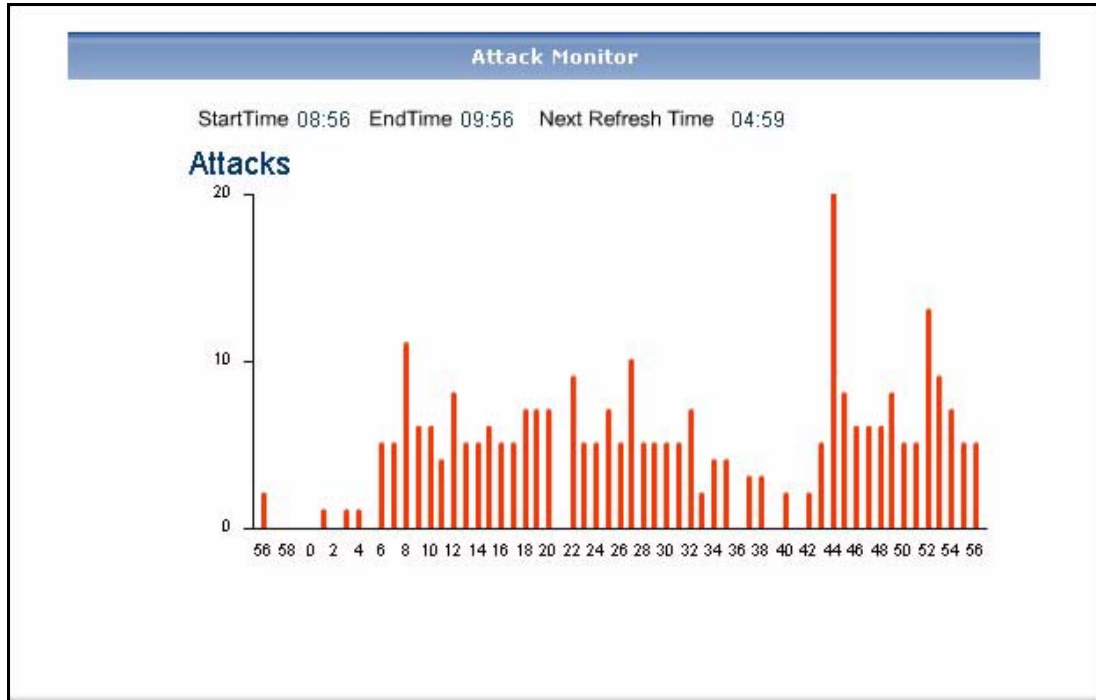
LABEL	DESCRIPTION
title	This field displays the title of the monitor. It does not include the service you select in the Service Type field.
Service Type	Select the service whose traffic you want to look at. Choices are: WEB - Look at the amount of traffic generated by HTTP/HTTPS services. FTP - Look at the amount of traffic generated by FTP services. MAIL - Look at the amount of traffic generated by POP3/SMTP services. VPN - Look at the amount of traffic generated by IPSec/VPN services.
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.
Next Refresh Time	This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time.
graph	The graph shows how the status changes over time. Y-axis (vertical): how much traffic from the selected service 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 . For example, if the start time is 13:27 and end time is 14:27, then "39" means 13:39 and "5" means 14:05.

4.3 Attack Monitor

Use this report to monitor the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall.

Click **Monitor > Attack** to open this screen.

Figure 16 Monitor > Attack



Each field is described in the following table.

Table 11 Monitor > Attack

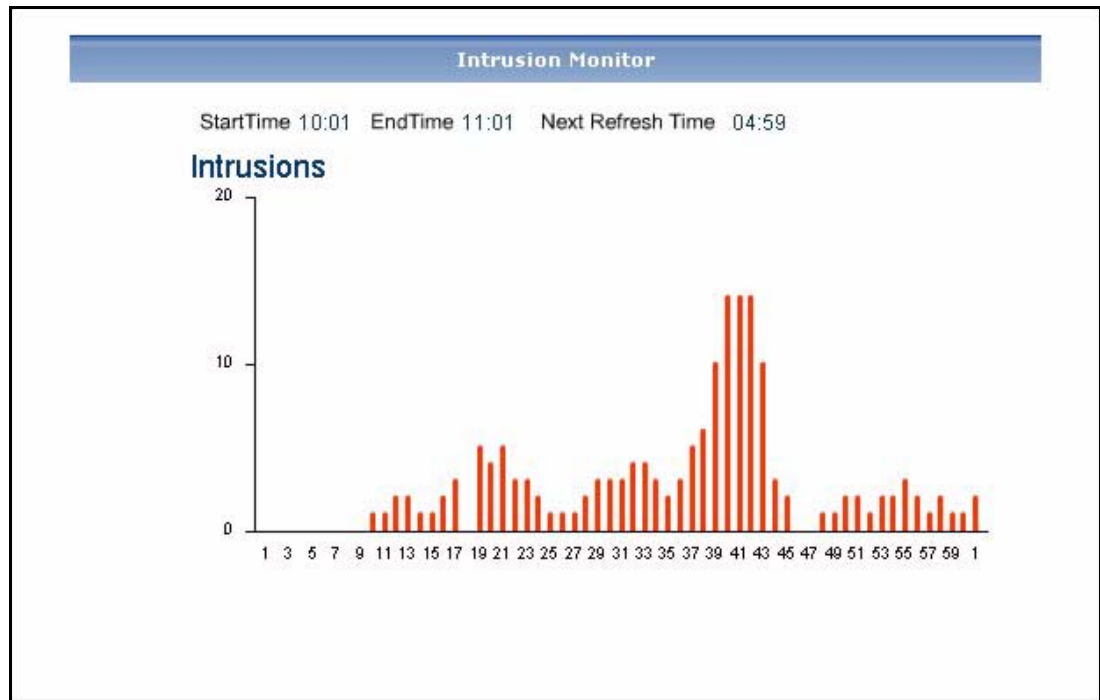
LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next Refresh Time	This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time.
graph	The graph shows how the status changes over time. Y-axis (vertical): the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall each minute. X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the Start Time and End Time . For example, if the start time is 13:27 and end time is 14:27, then "39" means 13:39 and "5" means 14:05.

4.4 Intrusion Monitor

Use this report to monitor the number of intrusions detected by the selected device's IDP feature.

Click **Monitor > Intrusion** to open this screen.

Figure 17 Monitor > Intrusion



Each field is described in the following table.

Table 12 Monitor > Intrusion

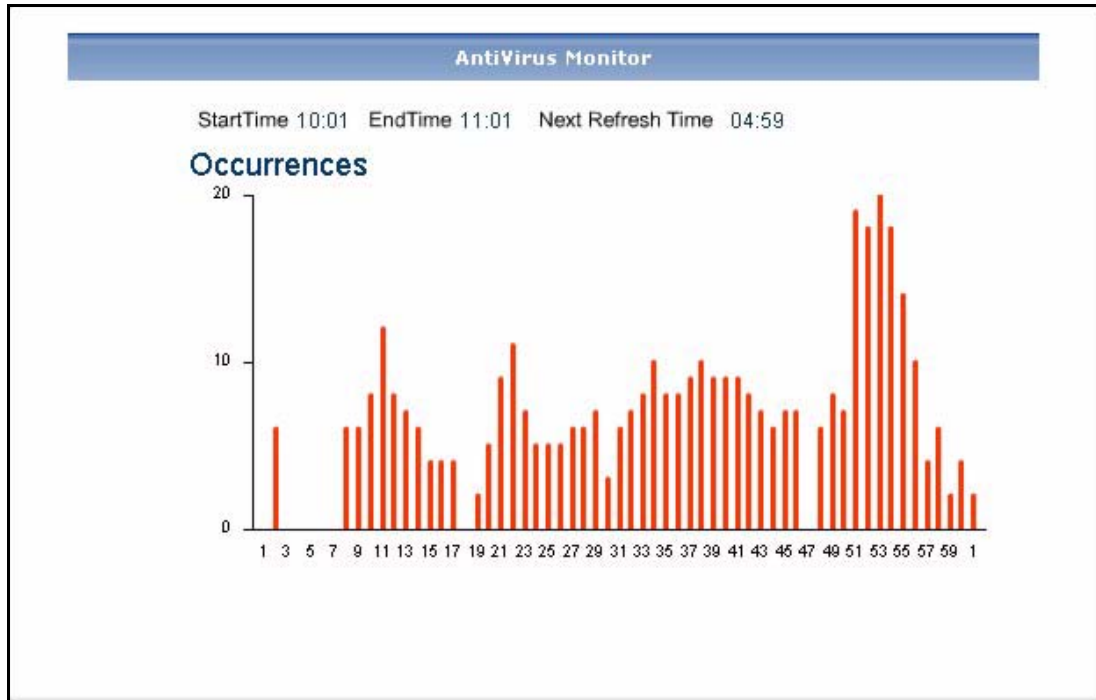
LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next Refresh Time	This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time.
graph	The graph shows how the status changes over time. Y-axis (vertical): the number of intrusions detected by the selected device's IDP feature each minute. X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the Start Time and End Time . For example, if the start time is 13:27 and end time is 14:27, then "39" means 13:39 and "5" means 14:05.

4.5 Anti-Virus Monitor

Use this report to monitor the number of virus occurrences prevented by the selected device.

Click **Monitor** > **AntiVirus** to open this screen.

Figure 18 Monitor > AntiVirus



Each field is described in the following table.

Table 13 Monitor > AntiVirus

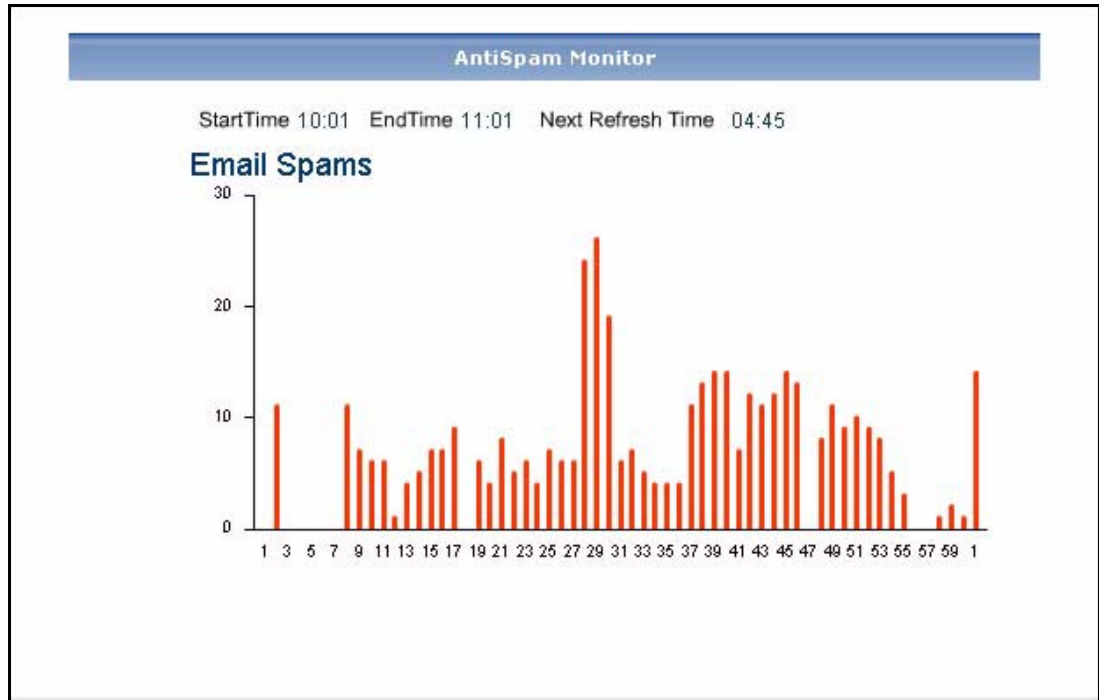
LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next Refresh Time	This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time.
graph	The graph shows how the status changes over time. Y-axis (vertical): the number of virus occurrences prevented by the selected device each minute. X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the Start Time and End Time . For example, if the start time is 13:27 and end time is 14:27, then "39" means 13:39 and "5" means 14:05.

4.6 Anti-Spam Monitor

Use this report to monitor the number of spam messages stopped by the selected device.

Click **Monitor** > **AntiSpam** to open this screen.

Figure 19 Monitor > AntiSpam



Each field is described in the following table.

Table 14 Monitor > AntiSpam

LABEL	DESCRIPTION
title	This field displays the title of the monitor.
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.
Next Refresh Time	This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time.
graph	The graph shows how the status changes over time. Y-axis (vertical): the number of spam messages stopped by the selected device each minute. X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the Start Time and End Time . For example, if the start time is 13:27 and end time is 14:27, then "39" means 13:39 and "5" means 14:05.

CHAPTER 5

Traffic

Use these reports to look at the top sources and destinations of traffic for web, FTP, POP3/SMTP, and other protocols.

5.1 Bandwidth

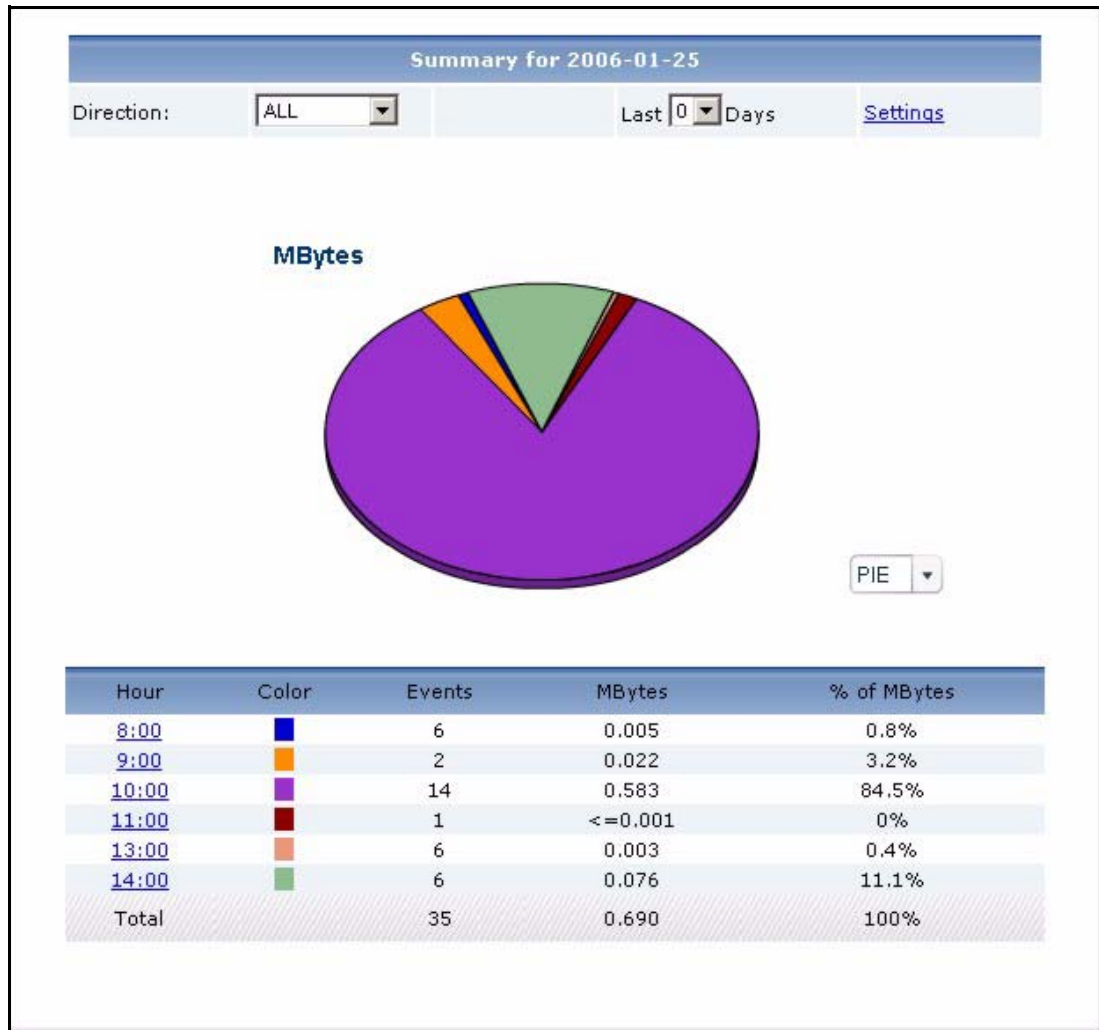
Use these reports to look at how much traffic was handled by ZyXEL devices, who used the most bandwidth in a ZyXEL device, and which protocols were used. You can also look at traffic in various directions.

5.1.1 Bandwidth Summary

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

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

Figure 20 Traffic > Bandwidth > Summary



Each field is described in the following table.

Table 15 Traffic > Bandwidth > 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. It does not include the Direction you select.
Direction	This field is displayed if there are any traffic statistics for the selected report. Select which kind of traffic, by direction, you want to look at. The options depend on which directions have traffic. If there is no traffic in a specific direction, the option is not available. 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

Table 15 Traffic > Bandwidth > Summary

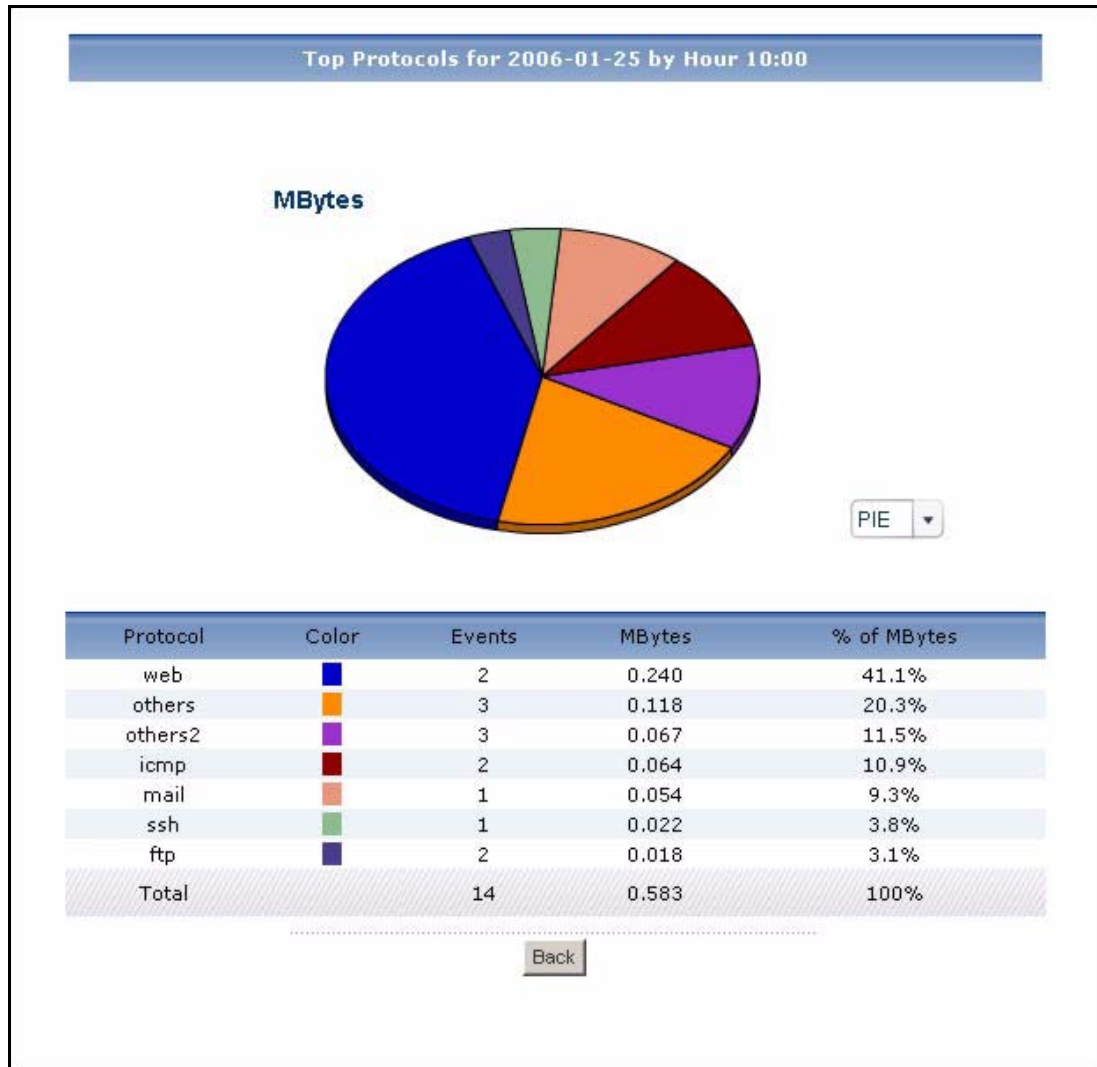
LABEL	DESCRIPTION
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="841 598 1166 737" style="text-align: center;"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top services by amount of traffic in the selected time interval. The Bandwidth Summary Drill-Down report appears.</p>
Color	This field displays what color represents each time interval in the graph.
Events	This field displays the number of traffic events in each interval.
MBytes	This field displays how much traffic (in megabytes) the device handled in each time interval.
% of MBytes	This field displays what percentage of all traffic was handled in each time interval.
Total	This entry displays the totals for the time intervals 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 **Traffic > Bandwidth > Summary** to open this screen.

Figure 21 Traffic > Bandwidth > Summary > Drill-Down



Each field is described in the following table.

Table 16 Traffic > Bandwidth > 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. It does not include the Direction you select.
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.

Table 16 Traffic > Bandwidth > Summary > Drill-Down

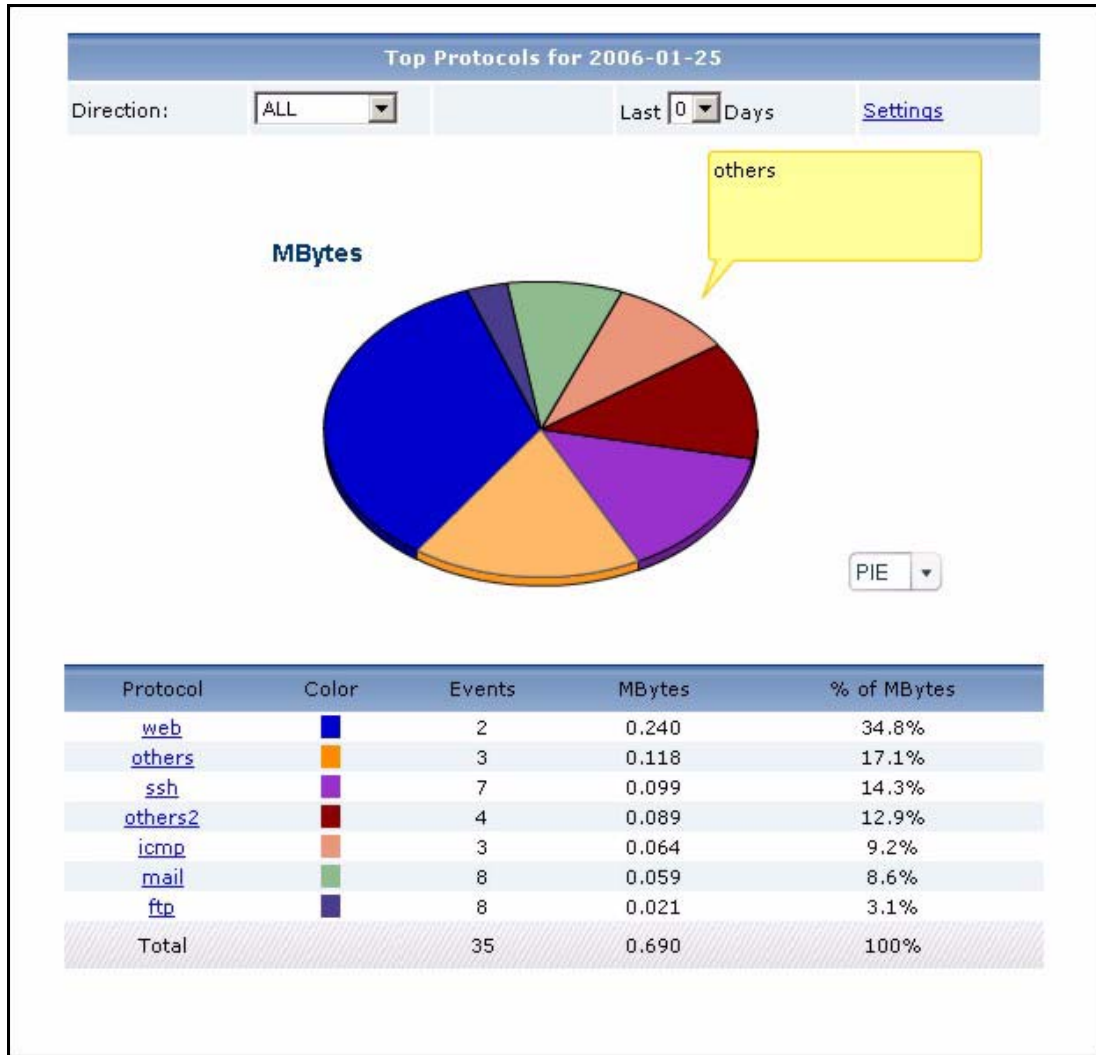
LABEL	DESCRIPTION
Color	This field displays what color represents each service in the graph.
Events	This field displays the number of traffic events for each service in the selected time interval.
MBytes	This field displays how much traffic (in megabytes) the device handled for each service in the selected time interval.
% of MBytes	This field displays what percentage of all traffic in the selected time interval was attributed to each service.
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 **Traffic > Bandwidth > Top Protocol** to open this screen.

Figure 22 Traffic > Bandwidth > Top Protocol



Each field is described in the following table.

Table 17 Traffic > Bandwidth > Top Protocol

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.
Direction	This field is displayed if there are any traffic statistics for the selected report. Select which kind of traffic, by direction, you want to look at. The options depend on which directions have traffic. If there is no traffic in a specific direction, the option is not available. 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

Table 17 Traffic > Bandwidth > Top Protocol

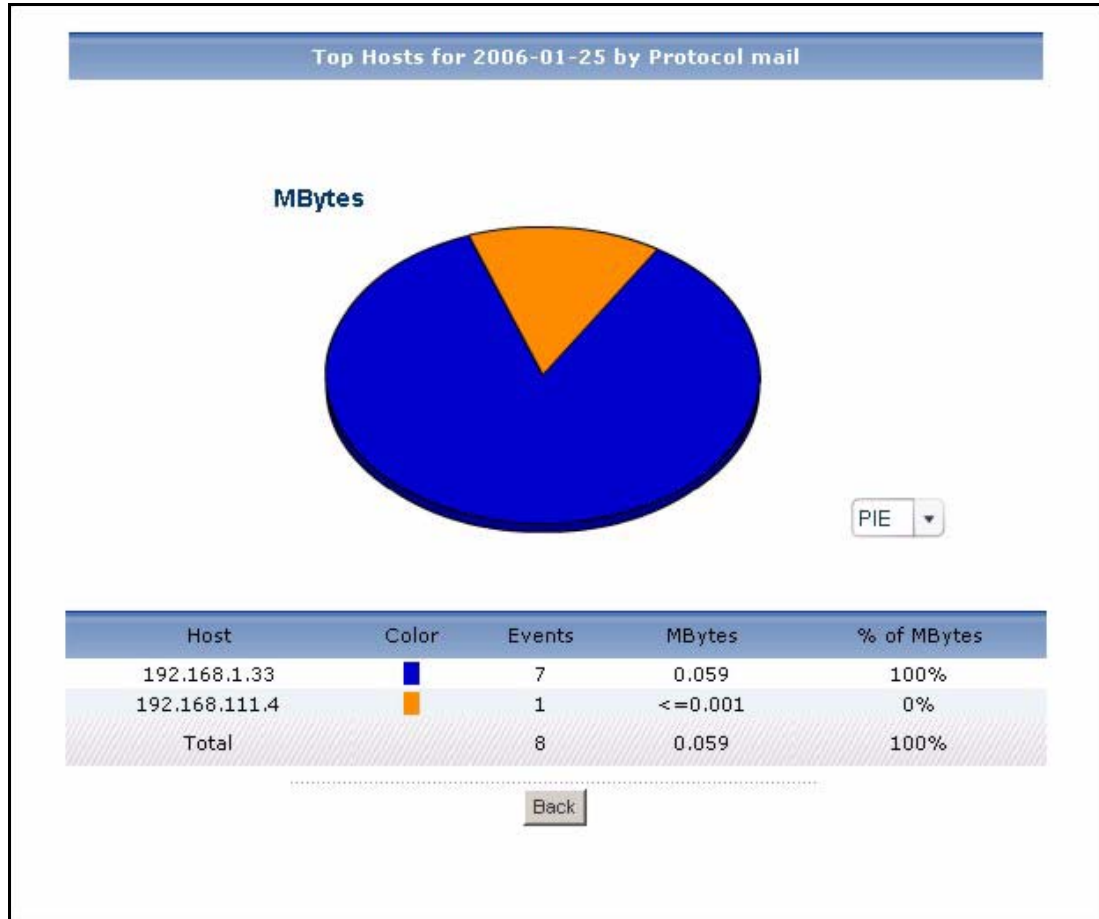
LABEL	DESCRIPTION
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="841 598 1166 737" data-label="Image"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	<p>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 sources may be different than the ones you manage in the Service Settings screen.</p> <p>Click on a service to look at the top sources of traffic for the selected service. The Bandwidth Top Protocols Drill-Down report appears.</p>
Color	This field displays what color represents each service in the graph.
Events	This field displays the number of traffic events for each service.
MBytes	This field displays how much traffic (in megabytes) each service generated through the selected device.
% of MBytes	This field displays what percentage of all traffic each service generated through the selected device.
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 **Traffic > Bandwidth > Top Protocol** to open this screen.

Figure 23 Traffic > Bandwidth > Top Protocol > Drill-Down



Each field is described in the following table.

Table 18 Traffic > Bandwidth > Top Protocol > 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. It does not include the Direction you select.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events each source generated using the selected service.
MBytes	This field displays how much traffic (in megabytes) each source generated using the selected service.

Table 18 Traffic > Bandwidth > Top Protocol > Drill-Down

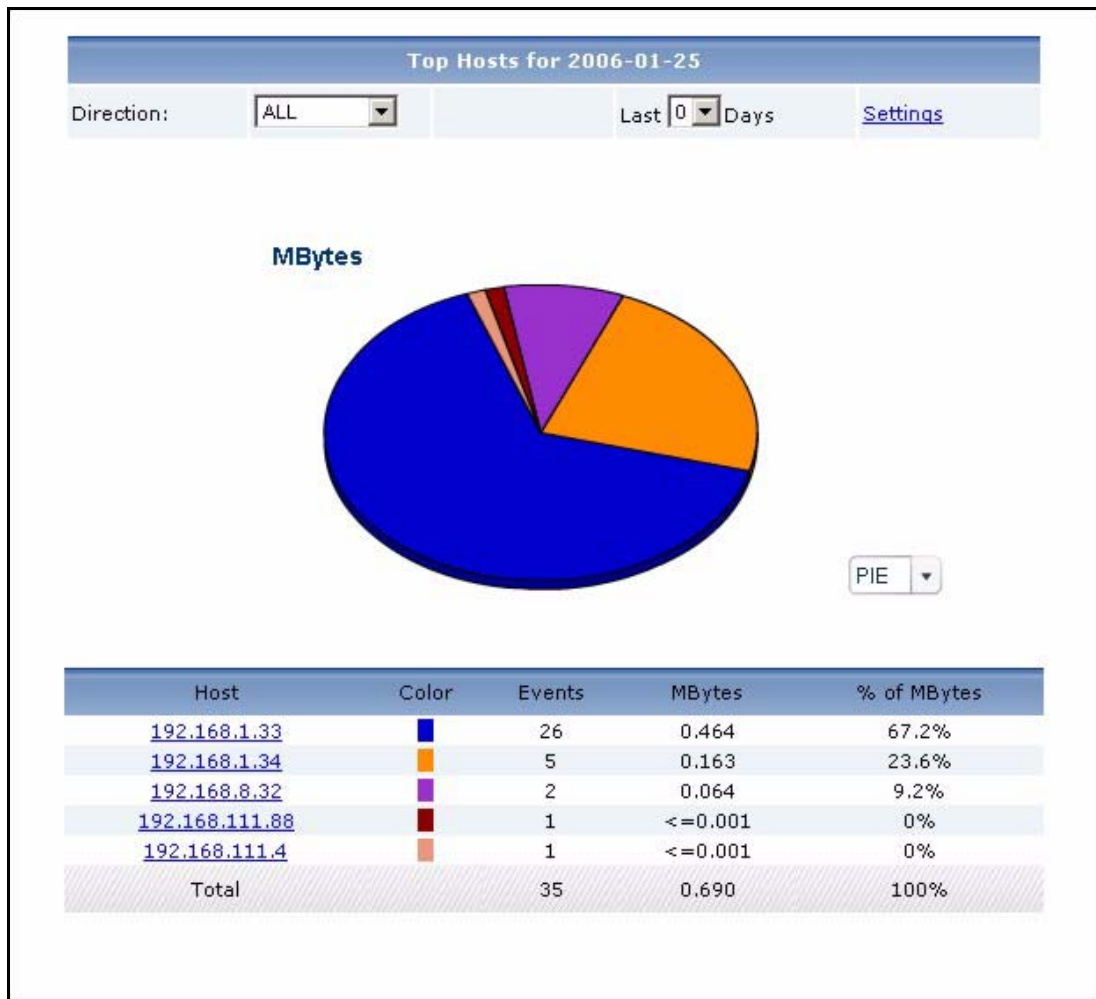
LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of the selected service's traffic was generated by each source.
Total	This entry displays the totals for the sources above. If the number of sources generating traffic using the selected service is greater than the maximum number of records 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 **Traffic > Bandwidth > Top Hosts** to open this screen.

Figure 24 Traffic > Bandwidth > Top Hosts



Each field is described in the following table.

Table 19 Traffic > Bandwidth > 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. It does not include the Direction you select.
Direction	<p>This field is displayed if there are any traffic statistics for the selected report. Select which kind of traffic, by direction, you want to look at. The options depend on which directions have traffic. If there is no traffic in a specific direction, the option is not available. In addition, the following options may appear.</p> <p>All - all traffic, regardless of direction Inbound - all traffic routed from the WAN Outbound - all traffic routed to the WAN</p>
Last ... Days	<p>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. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="837 999 1166 1136" data-label="Image"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>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.</p> <p>Click on a source to look at the top services by amount of traffic for the selected source. The Bandwidth Top Hosts Drill-Down report appears.</p>
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events for each source.
MBytes	This field displays how much traffic (in megabytes) the device handled for each source.

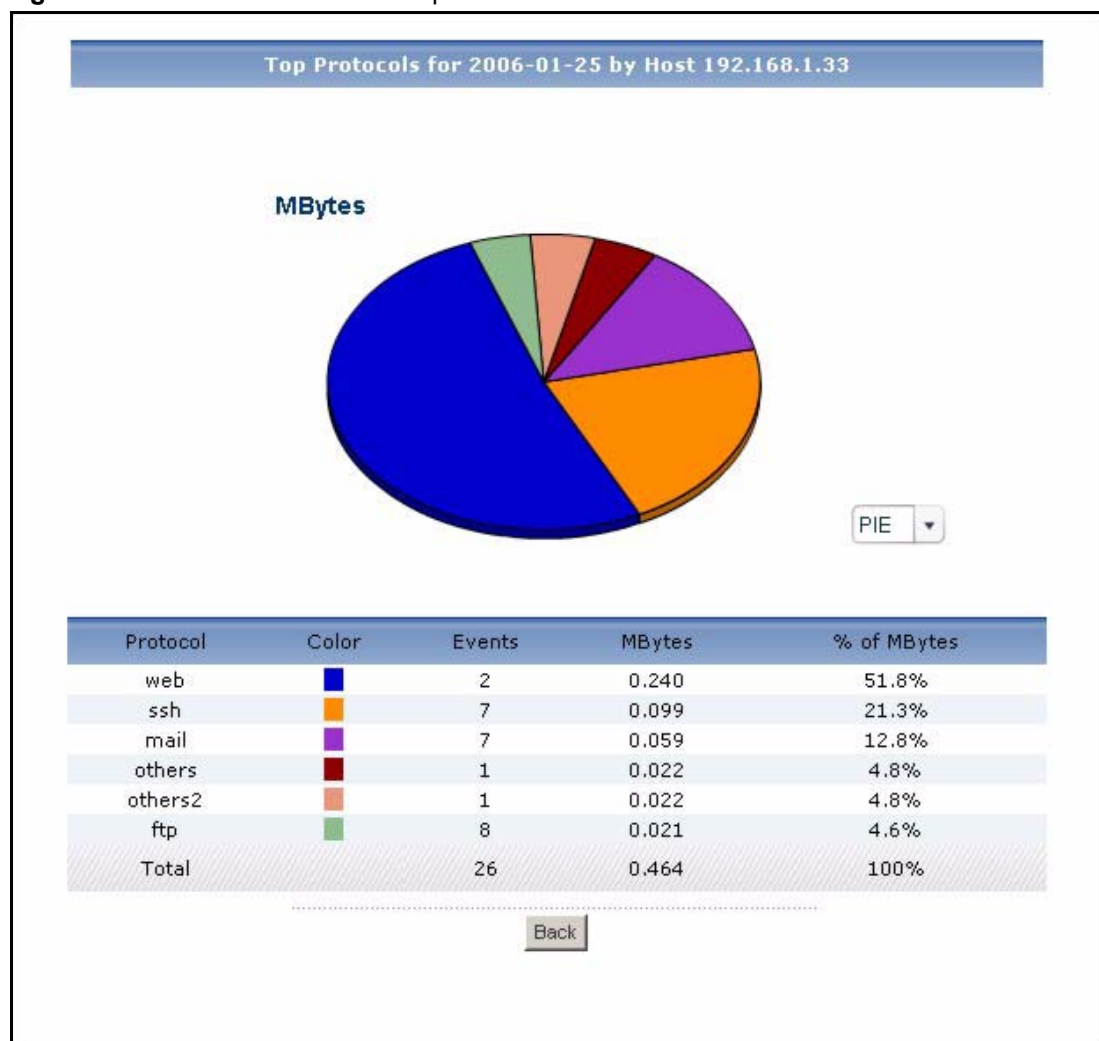
Table 19 Traffic > Bandwidth > Top Hosts

LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of all traffic the device handled for each source.
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 **Traffic > Bandwidth > Top Hosts** to open this screen.

Figure 25 Traffic > Bandwidth > Top Hosts > Drill-Down

Each field is described in the following table.

Table 20 Traffic > Bandwidth > 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. It does not include the Direction you select.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none">• Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar.• 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.
Color	This field displays what color represents each service in the graph.
Events	This field displays the number of traffic events the selected source generated using each service.
MBytes	This field displays how much traffic (in megabytes) the selected source generated using each service.
% of MBytes	This field displays what percentage of the selected source's traffic was generated using each service.
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.

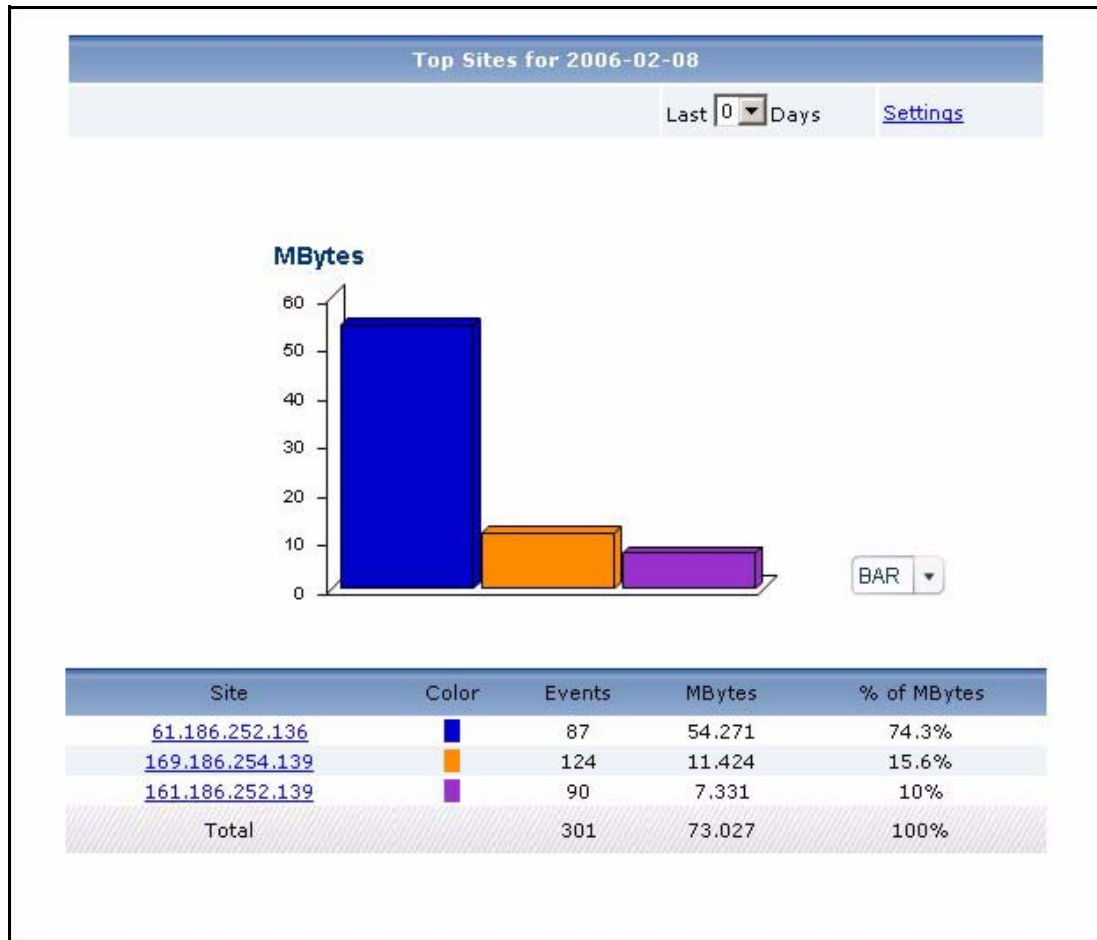
5.2 Web Traffic

Use this report to 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 **Traffic > WEB > Top Sites** to open this screen.

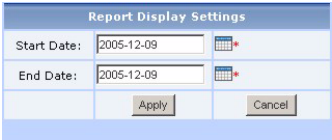
Figure 26 Traffic > WEB > Top Sites

Each field is described in the following table.

Table 21 Traffic > WEB > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

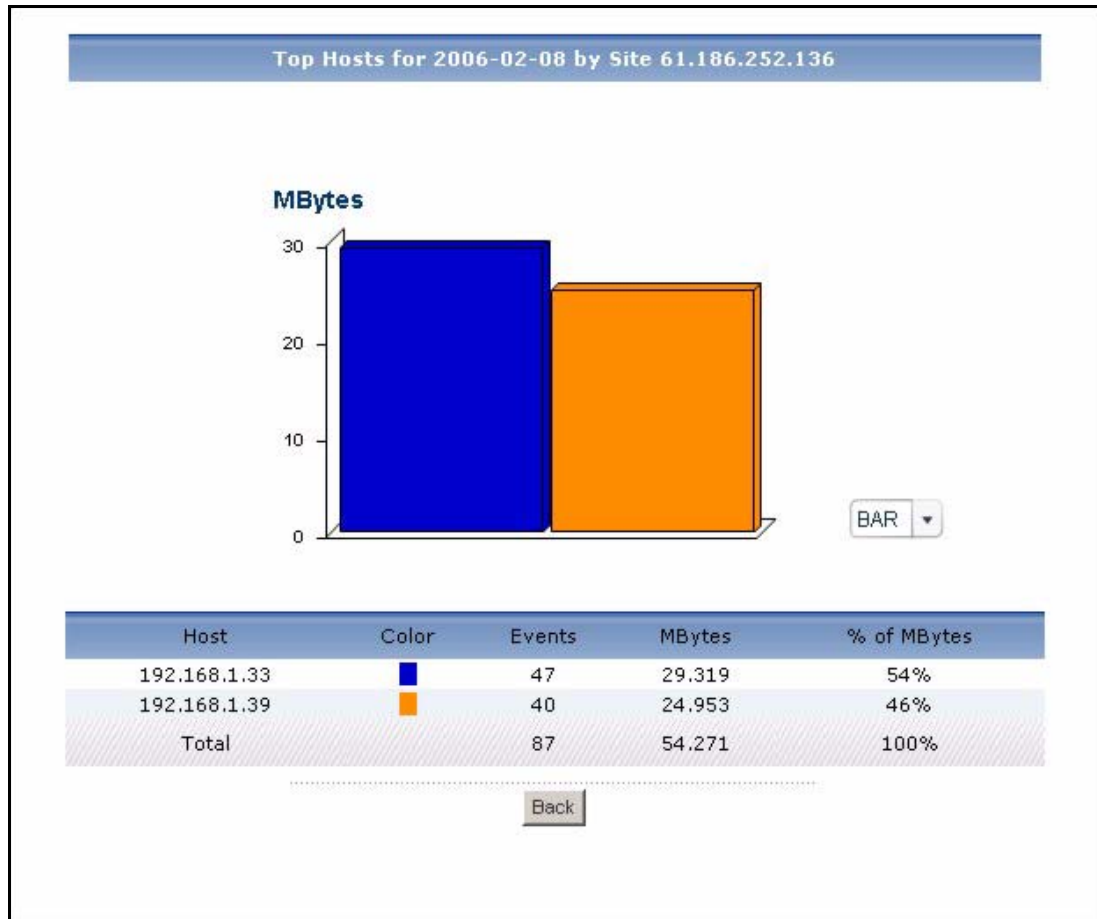
Table 21 Traffic > WEB > Top Sites

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	<p>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.</p> <p>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").</p> <p>Click on a destination to look at the top sources of web traffic for the selected destination. The Top Web Sites Drill-Down report appears.</p>
Color	This field displays what color represents each destination in the graph.
Events	This field displays the number of traffic events for each destination.
MBytes	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes	This field displays what percentage of web traffic the device handled for each destination.
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 **Traffic > WEB > Top Sites** to open this screen.

Figure 27 Traffic > WEB > Top Sites > Drill-Down

Each field is described in the following table.

Table 22 Traffic > WEB > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events from each source to the selected destination.
MBytes	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.

Table 22 Traffic > WEB > Top Sites > Drill-Down

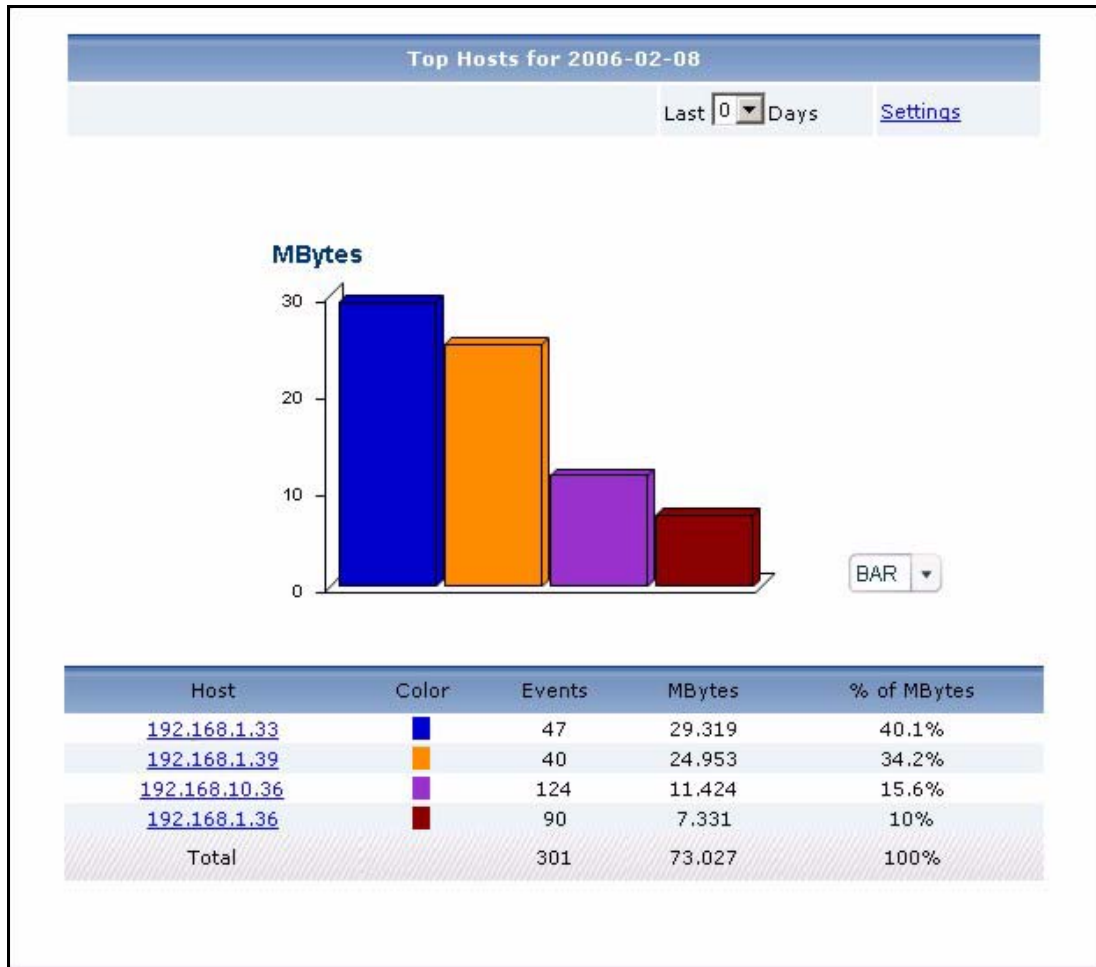
LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of the selected destination's web traffic was generated from each source.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
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.

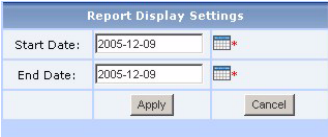
Click **Traffic > WEB > Top Hosts** to open this screen.

Figure 28 Traffic > WEB > Top Hosts



Each field is described in the following table.

Table 23 Traffic > WEB > Top Hosts

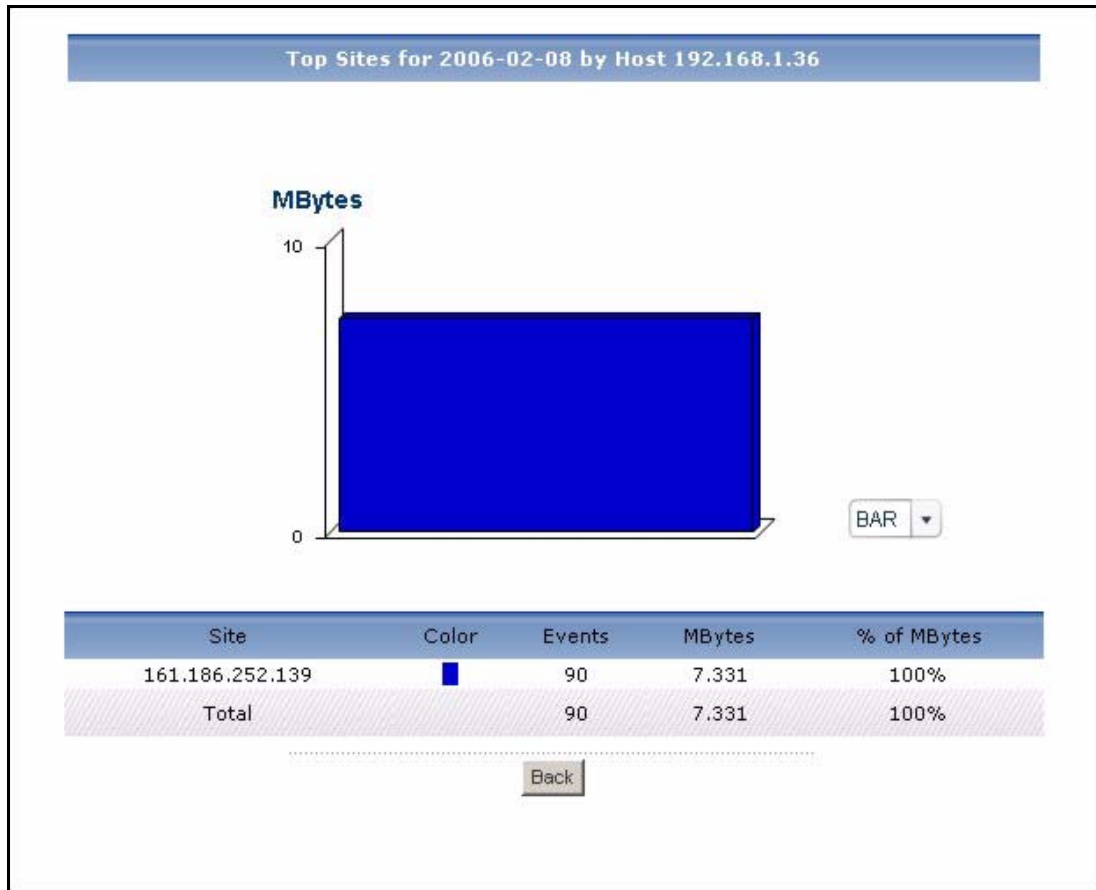
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>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. Click on a source to look at the top destinations of web traffic for the selected source. The Top Web Hosts Drill-Down report appears.</p>
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events for each source.
MBytes	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes	This field displays what percentage of web traffic the device handled for each source.
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 **Traffic > WEB > Top Hosts** to open this screen.

Figure 29 Traffic > WEB > Top Hosts > Drill-Down



Each field is described in the following table.

Table 24 Traffic > WEB > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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").
Color	This field displays what color represents each destination in the graph.

Table 24 Traffic > WEB > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Events	This field displays the number of traffic events from the selected source to each destination.
MBytes	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes	This field displays what percentage of the selected source's web 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.
Back	Click this to return to the main report.

5.3 FTP Traffic

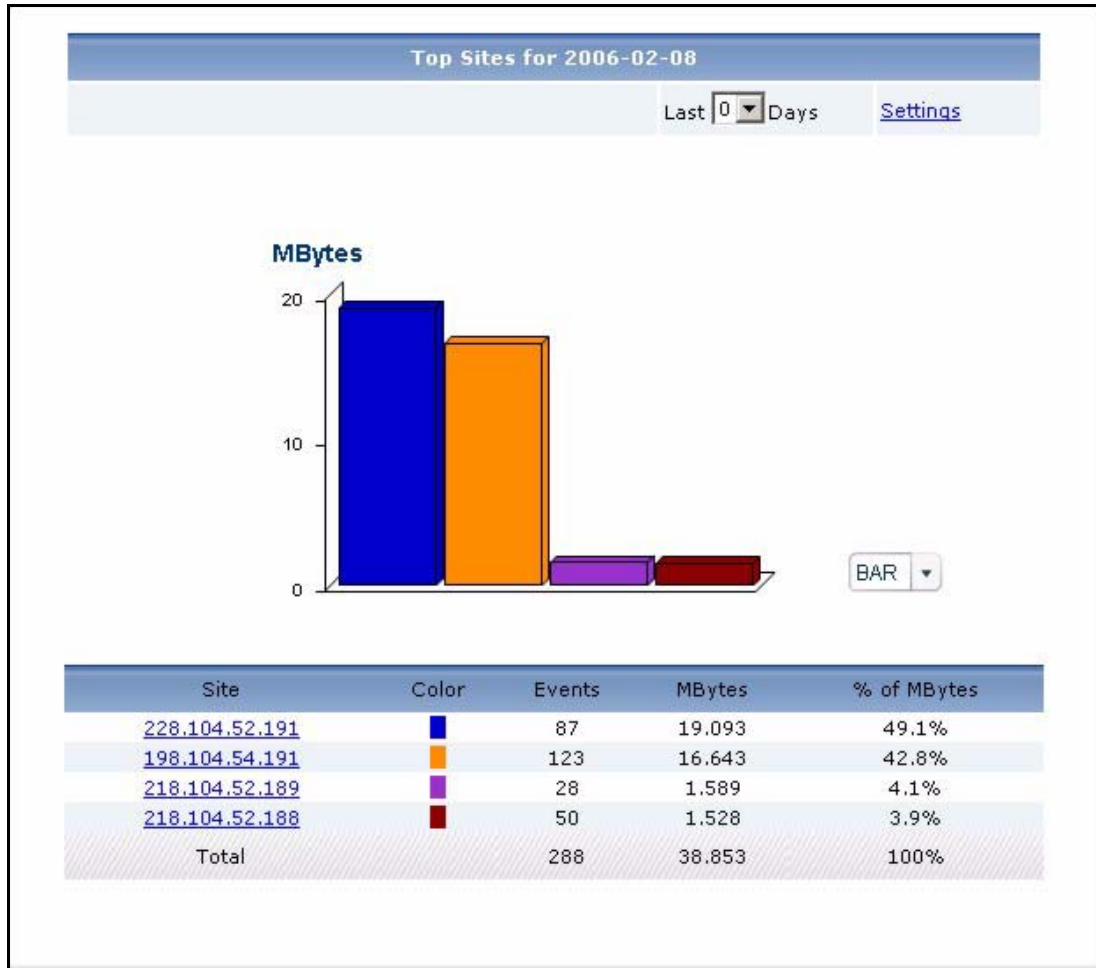
Use this report to look at the top destinations and sources of FTP traffic.

5.3.1 Top FTP Sites

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

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

Figure 30 Traffic > FTP > Top Sites

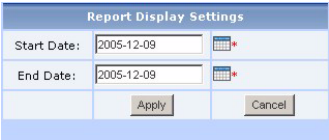


Each field is described in the following table.

Table 25 Traffic > FTP > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 25 Traffic > FTP > Top Sites

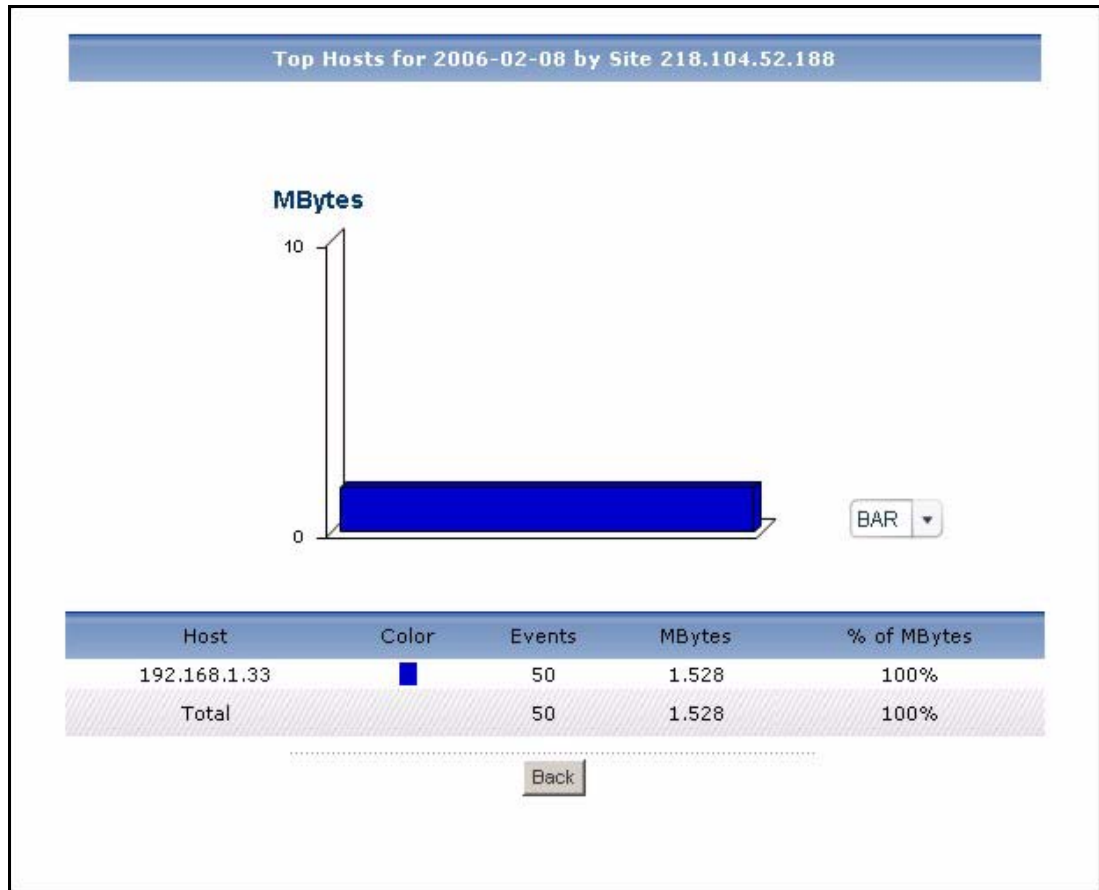
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	<p>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.</p> <p>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").</p> <p>Click on a destination to look at the top sources of FTP traffic for the selected destination. The Top FTP Sites Drill-Down report appears.</p>
Color	This field displays what color represents each destination in the graph.
Events	This field displays the number of traffic events for each destination.
MBytes	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes	This field displays what percentage of FTP traffic the device handled for each destination.
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 **Traffic > FTP > Top Sites** to open this screen.

Figure 31 Traffic > FTP > Top Sites > Drill-Down



Each field is described in the following table.

Table 26 Traffic > FTP > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events from each source to the selected destination.
MBytes	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.

Table 26 Traffic > FTP > Top Sites > Drill-Down

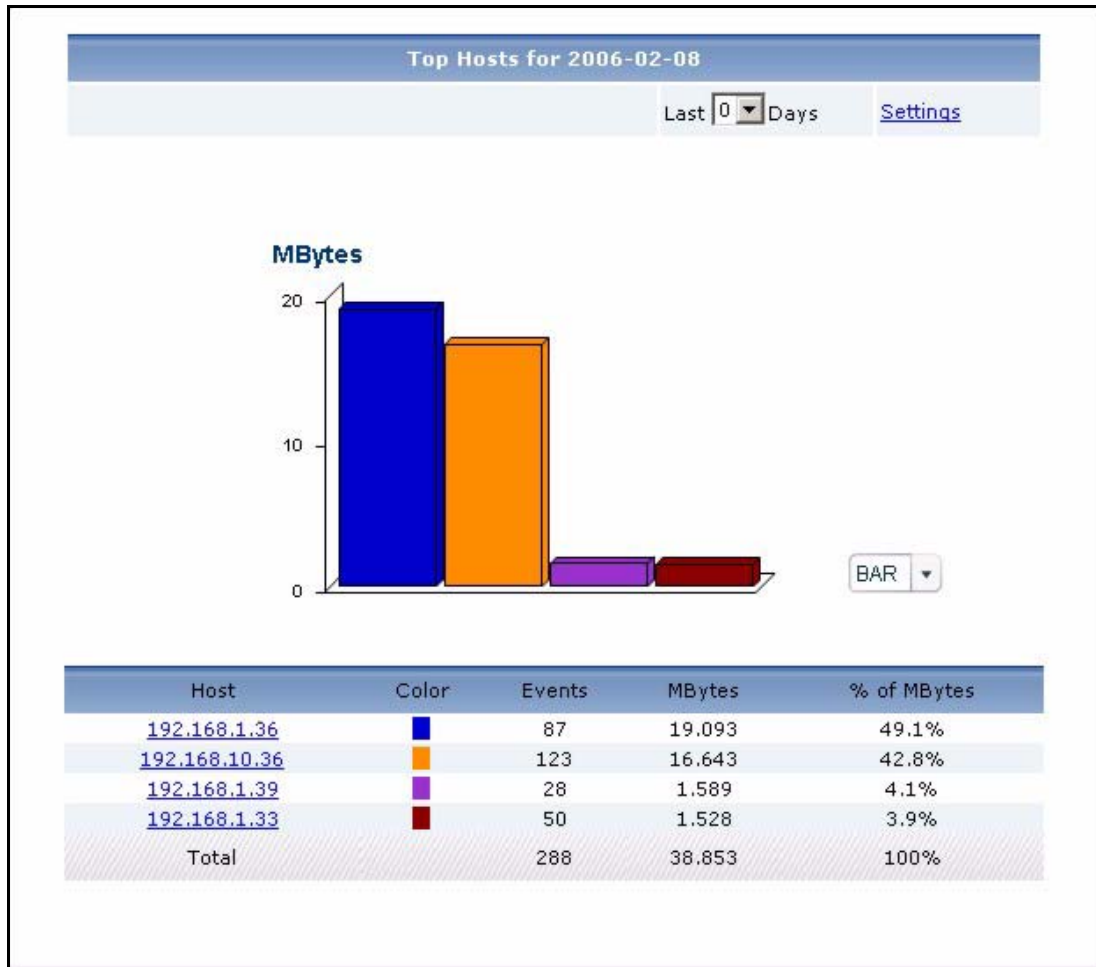
LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of the selected destination's FTP traffic was generated from each source.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
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 **Traffic > FTP > Top Hosts** to open this screen.

Figure 32 Traffic > FTP > Top Hosts



Each field is described in the following table.

Table 27 Traffic > FTP > Top Hosts

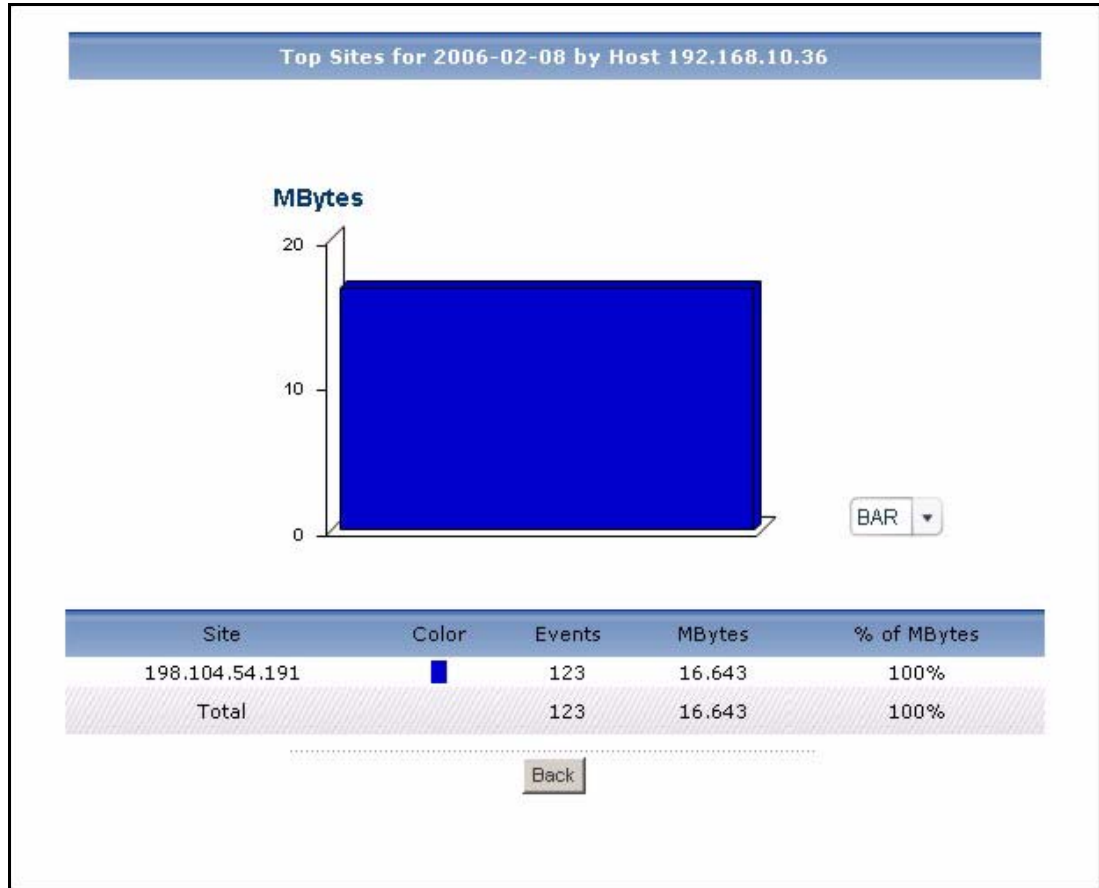
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="836 737 1166 877" style="text-align: center;"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>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. Click on a source to look at the top destinations of FTP traffic for the selected source. The Top FTP Hosts Drill-Down report appears.</p>
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events for each source.
MBytes	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes	This field displays what percentage of FTP traffic the device handled for each source.
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 **Traffic > FTP > Top Hosts** to open this screen.

Figure 33 Traffic > FTP > Top Hosts > Drill-Down



Each field is described in the following table.

Table 28 Traffic > FTP > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.

Table 28 Traffic > FTP > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Events	This field displays the number of traffic events from the selected source to each destination.
MBytes	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes	This field displays what percentage of the selected source's FTP 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.
Back	Click this to return to the main report.

5.4 Mail Traffic

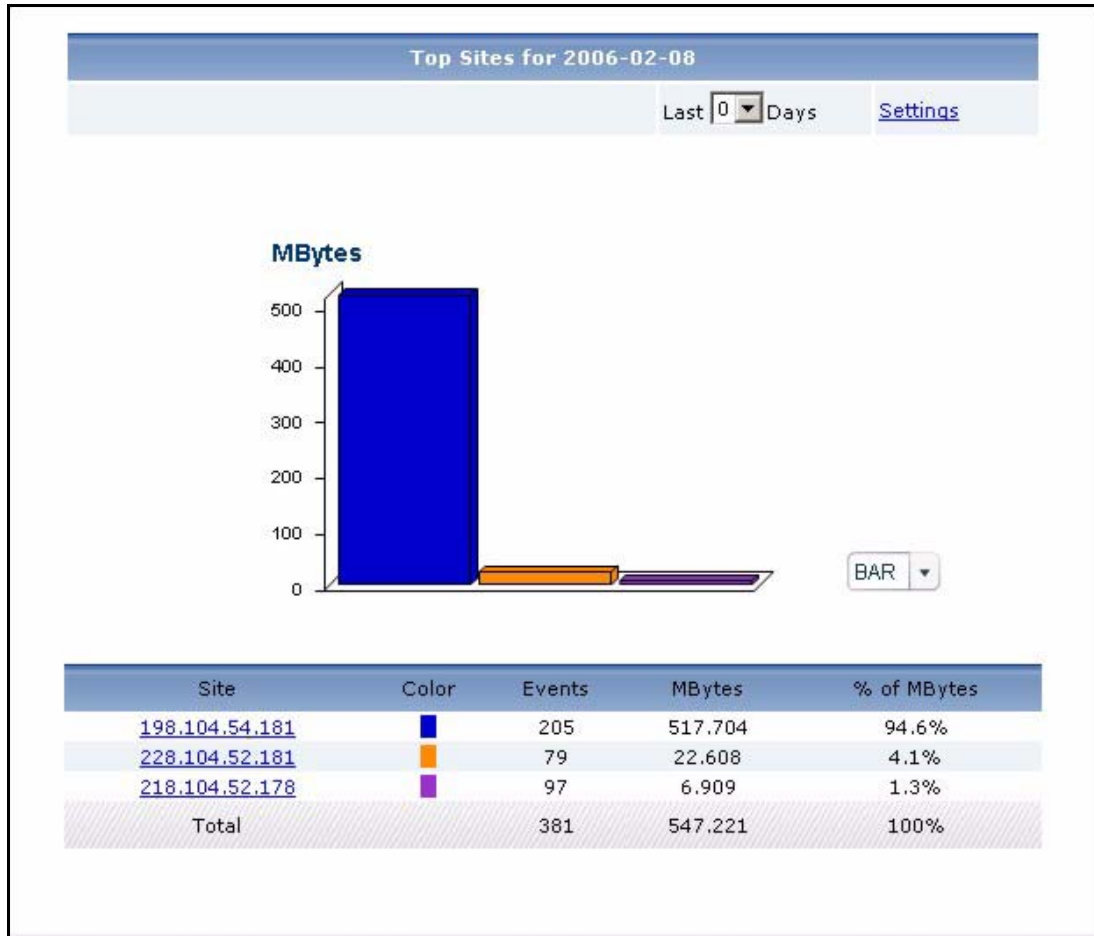
Use this report to look at the top destinations and sources of mail traffic.

5.4.1 Top Mail Sites

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

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

Figure 34 Traffic > MAIL > Top Sites

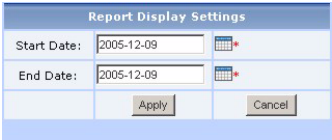


Each field is described in the following table.

Table 29 Traffic > MAIL > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

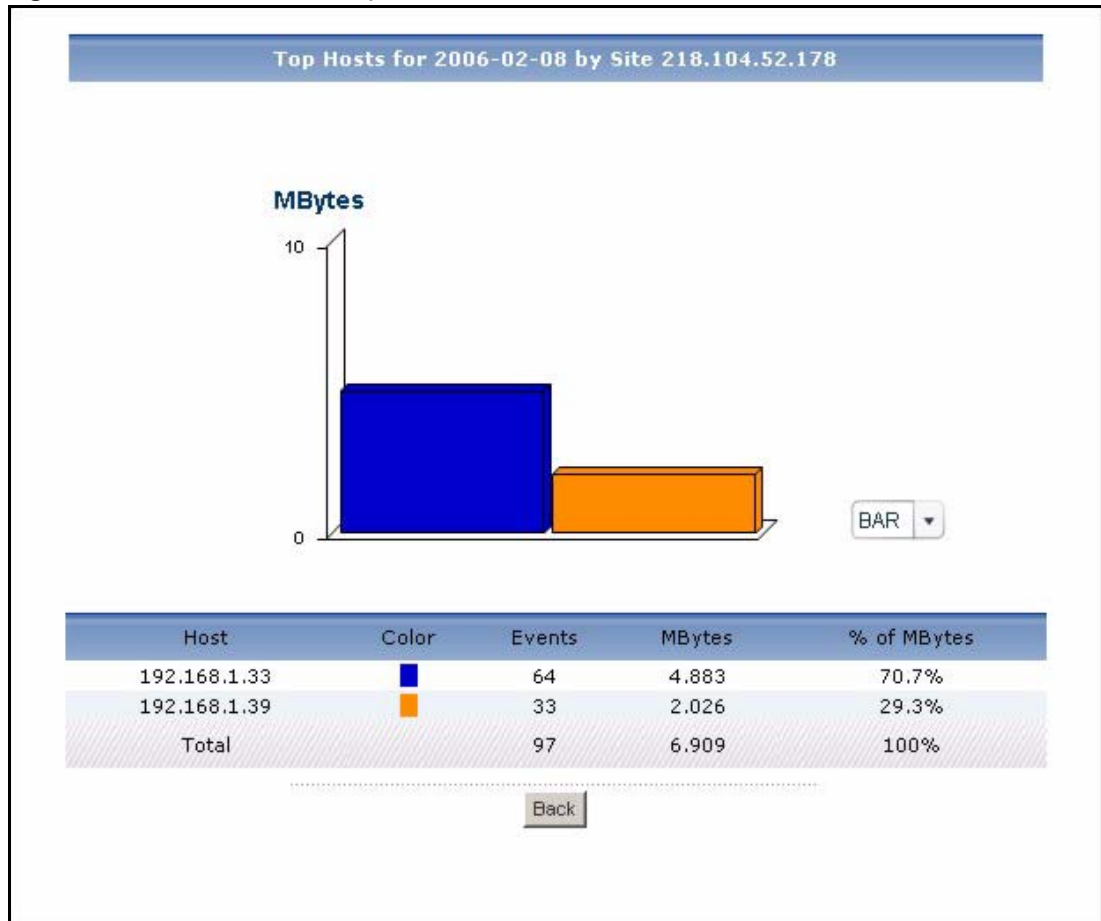
Table 29 Traffic > MAIL > Top Sites

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	<p>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.</p> <p>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").</p> <p>Click on a destination to look at the top sources of mail traffic for the selected destination. The Top Mail Sites Drill-Down report appears.</p>
Color	<p>This field displays what color represents each destination in the graph.</p>
Events	<p>This field displays the number of traffic events for each destination.</p>
MBytes	<p>This field displays how much traffic (in megabytes) the device handled for each destination.</p>
% of MBytes	<p>This field displays what percentage of mail traffic the device handled for each destination.</p>
Total	<p>This entry displays the totals for the destinations above.</p>

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 **Traffic > MAIL > Top Sites** to open this screen.

Figure 35 Traffic > MAIL > Top Sites > Drill-Down

Each field is described in the following table.

Table 30 Traffic > MAIL > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events from each source to the selected destination.
MBytes	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.

Table 30 Traffic > MAIL > Top Sites > Drill-Down

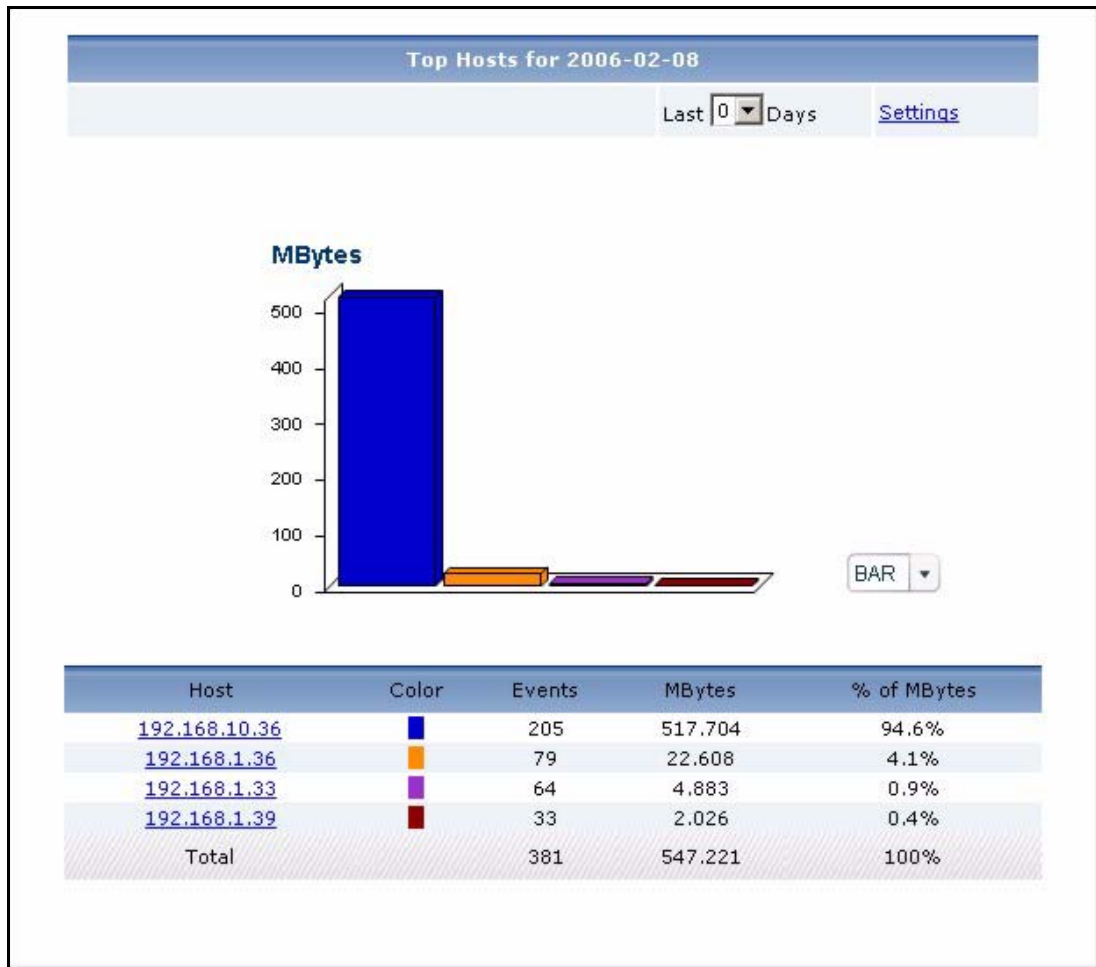
LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of the selected destination's mail traffic was generated from each source.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
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.

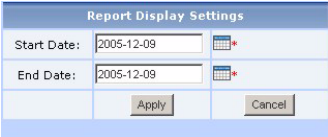
Click **Traffic > MAIL > Top Hosts** to open this screen.

Figure 36 Traffic > MAIL > Top Hosts



Each field is described in the following table.

Table 31 Traffic > MAIL > Top Hosts

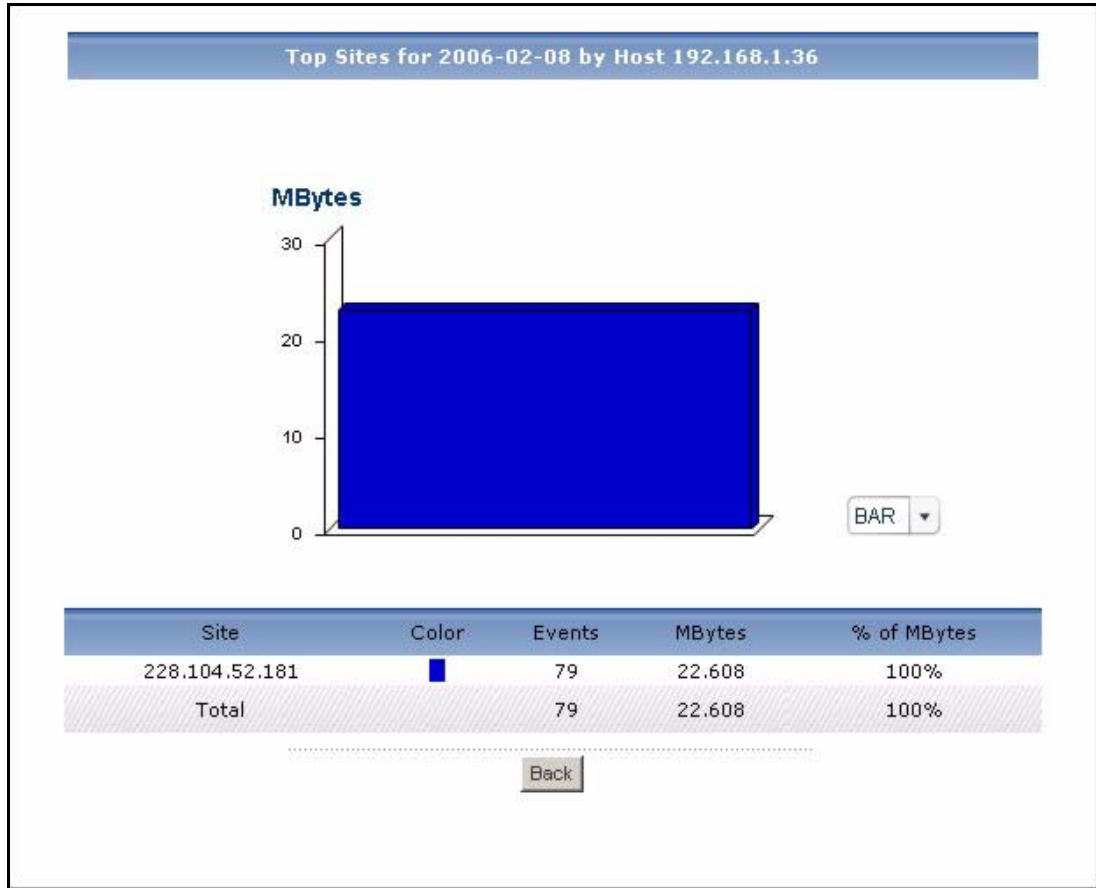
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>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. Click on a source to look at the top destinations of mail traffic for the selected source. The Top Mail Hosts Drill-Down report appears.</p>
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events for each source.
MBytes	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes	This field displays what percentage of mail traffic the device handled for each source.
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 **Traffic > MAIL > Top Hosts** to open this screen.

Figure 37 Traffic > MAIL > Top Hosts > Drill-Down



Each field is described in the following table.

Table 32 Traffic > MAIL > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.

Table 32 Traffic > MAIL > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Events	This field displays the number of traffic events from the selected source to each destination.
MBytes	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes	This field displays what percentage of the selected source'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.
Back	Click this to return to the main report.

5.5 VPN Traffic

Use these reports to look at the top sources and destinations of traffic in VPN tunnels.

Note: To look at VPN usage reports, each ZyXEL device must record forwarded IPSec VPN 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.

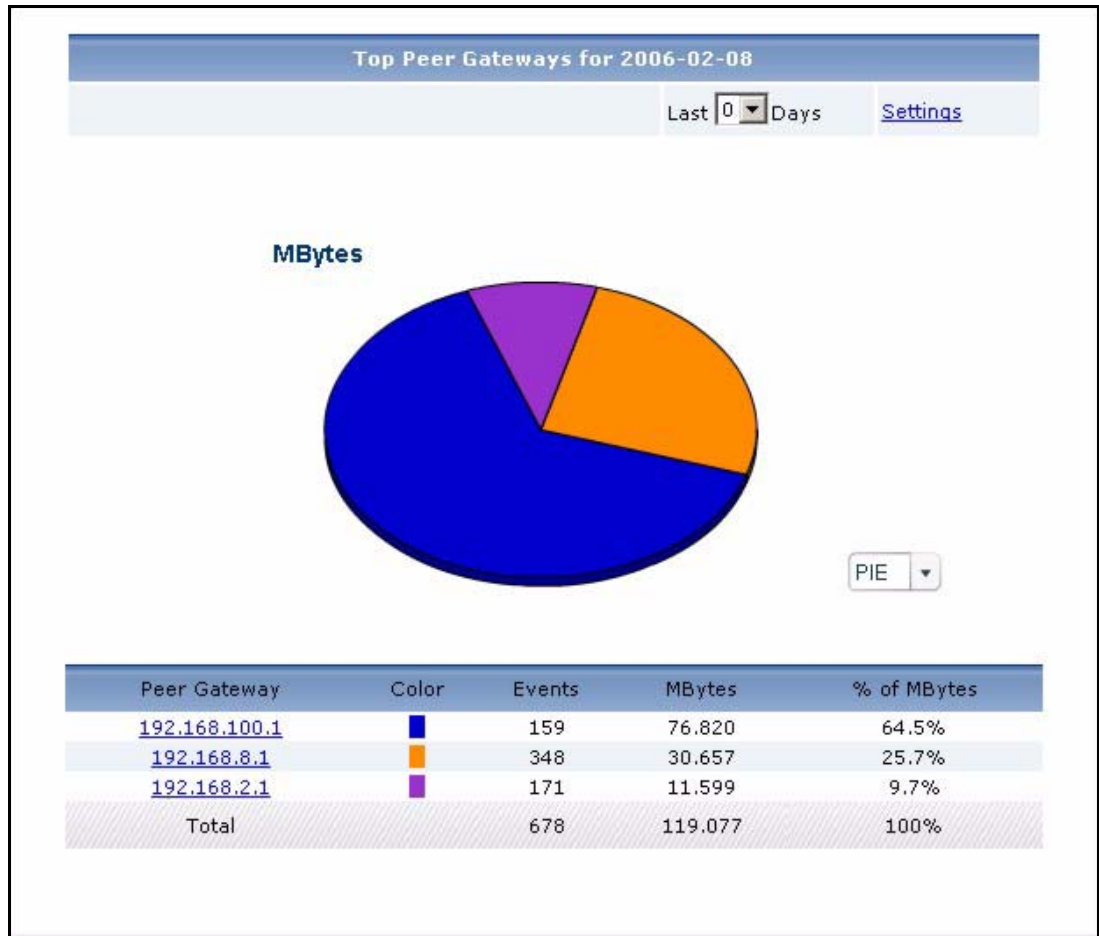
5.5.1 Top VPN Peer Gateways

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

Note: To look at VPN usage reports, each ZyXEL device must record forwarded IPSec VPN 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.

Click **Traffic > VPN > Top Peer Gateways** to open this screen.

Figure 38 Traffic > VPN > Top Peer Gateways

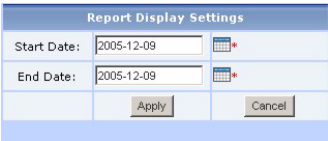


Each field is described in the following table.

Table 33 Traffic > VPN > Top Peer Gateways

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 33 Traffic > VPN > Top Peer Gateways

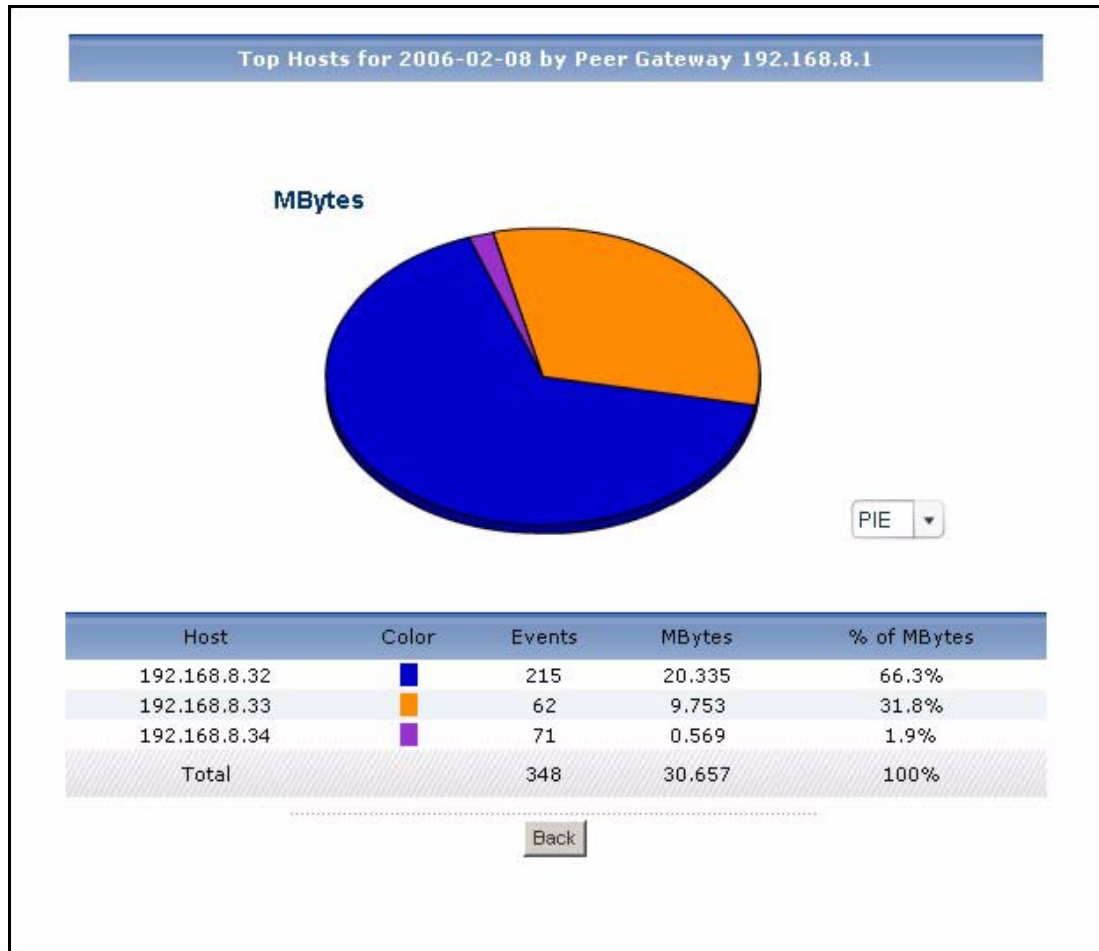
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Peer Gateway	<p>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.</p> <p>Each destination is identified by the IP address of the remote gateway. Click on a destination to look at the top sources of VPN traffic for the selected destination. The Top VPN Peer Gateways Drill-Down report appears.</p>
Color	This field displays what color represents each destination in the graph.
Events	This field displays the number of traffic events for each destination.
MBytes	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes	This field displays what percentage of VPN traffic the device handled for each destination.
Total	This entry displays the totals for the destinations above.

5.5.2 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 **Traffic > VPN > Top Peer Gateways** to open this screen.

Figure 39 Traffic > VPN > Top Peer Gateways > Drill-Down



Each field is described in the following table.

Table 34 Traffic > VPN > Top Peer Gateways > 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. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events from each source to the selected destination.

Table 34 Traffic > VPN > Top Peer Gateways > Drill-Down

LABEL	DESCRIPTION
MBytes	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.
% of MBytes	This field displays what percentage of the selected destination's VPN traffic was generated 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.
Back	Click this to return to the main report.

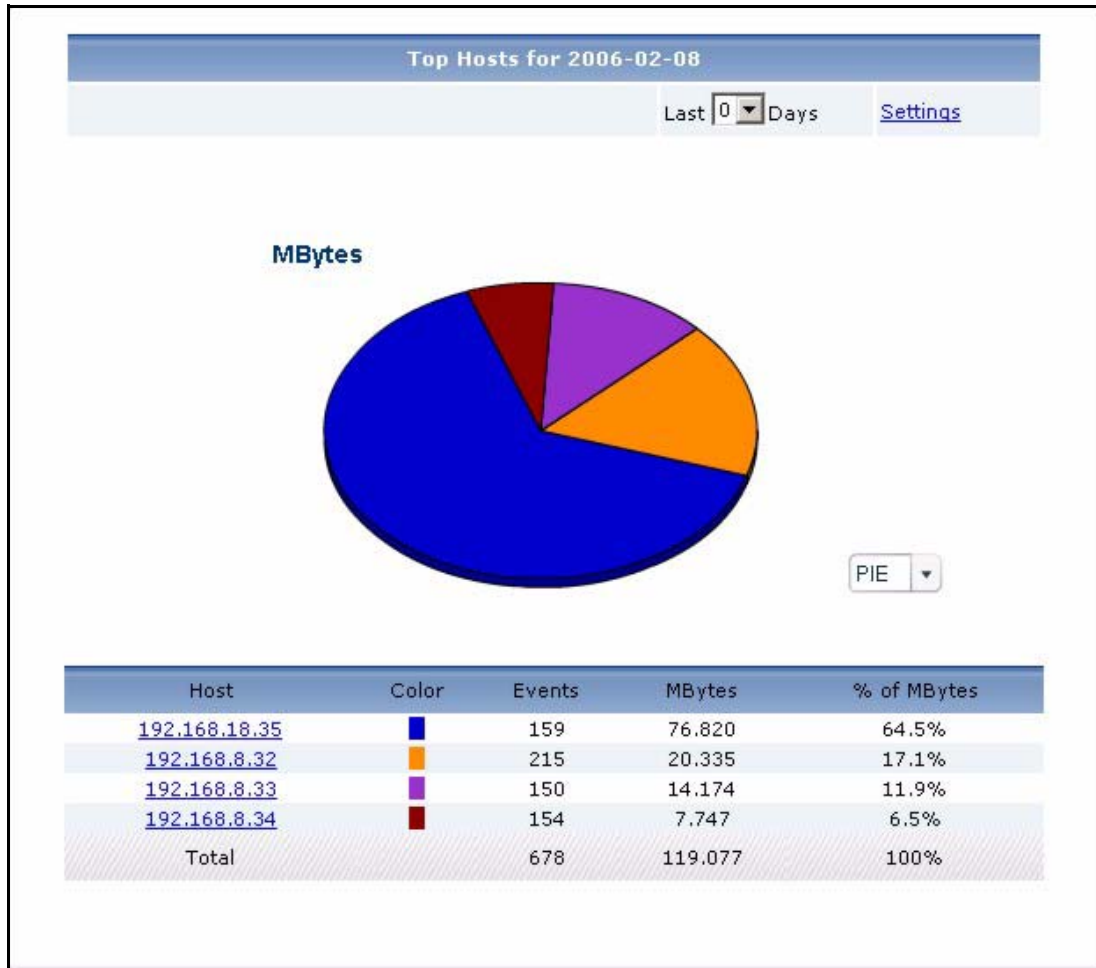
5.5.3 Top VPN Hosts

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

Note: To look at VPN usage reports, each ZyXEL device must record forwarded IPSec VPN 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.

Click **Traffic > VPN > Top Hosts** to open this screen.

Figure 40 Traffic > VPN > Top Hosts

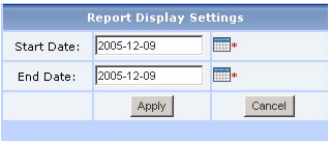


Each field is described in the following table.

Table 35 Traffic > VPN > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 35 Traffic > VPN > Top Hosts

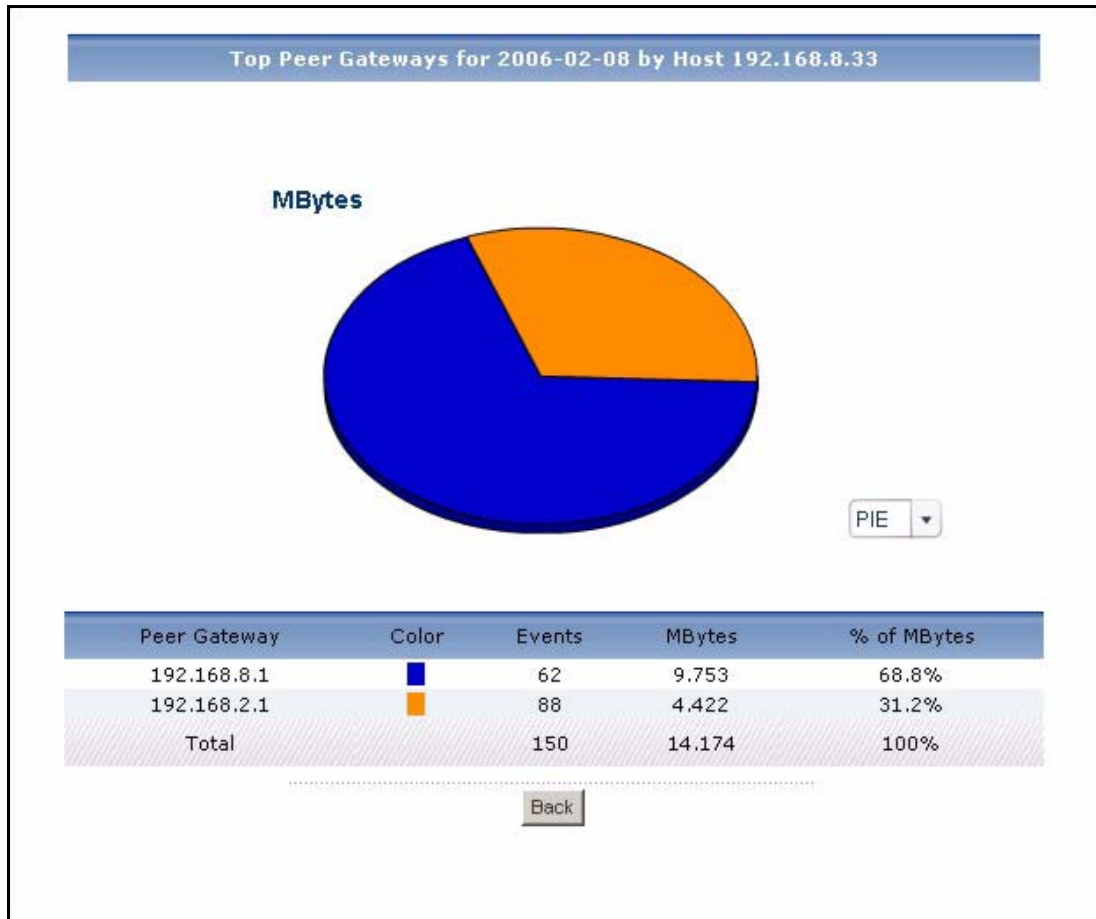
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>This field displays the top sources of VPN 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.</p> <p>Each source is identified by its IP address. Click on a source to look at the top destinations of VPN traffic for the selected source. The Top VPN Hosts Drill-Down report appears.</p>
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events for each source.
MBytes	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes	This field displays what percentage of VPN traffic the device handled for each source.
Total	This entry displays the totals for the sources above.

5.5.4 Top VPN Hosts Drill-Down

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

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

Figure 41 Traffic > VPN > Top Hosts > Drill-Down



Each field is described in the following table.

Table 36 Traffic > VPN > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Peer Gateway	This field displays the top destinations of VPN 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.
Events	This field displays the number of traffic events from the selected source to each destination.
MBytes	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.

Table 36 Traffic > VPN > Top Hosts > Drill-Down

LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of the selected source's VPN 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.
Back	Click this to return to the main report.

5.6 Other Traffic

Use these reports to look at the top sources and destinations of any kind of traffic.

5.6.1 Service Settings

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.

Click **Traffic > Customization > Customization** to open the **Service Settings** screen.

Figure 42 Service > Customization > Customization

The screenshot shows the 'Service Settings' interface. At the top, there is a header 'Service Settings'. Below it, there are two main sections. The first section is 'Add a Known Service:' with a dropdown menu currently showing '[Customized Service]'. To the right of this is a 'Customized Service:' label. Below this is a list box containing two entries: 'news(tcp:144)' and 'syslog(udp:514)'. The second section is 'Add a Customized Service', which contains four input fields: 'Name:' (an empty text box), 'Port Range (1-65535):' (two empty text boxes separated by a hyphen), and 'Protocol:' (a dropdown menu currently showing 'tcp'). At the bottom of the form, there are two buttons: 'Add' and 'Delete'.

Each field is described in the following table.

Table 37 Service > Customization > Customization

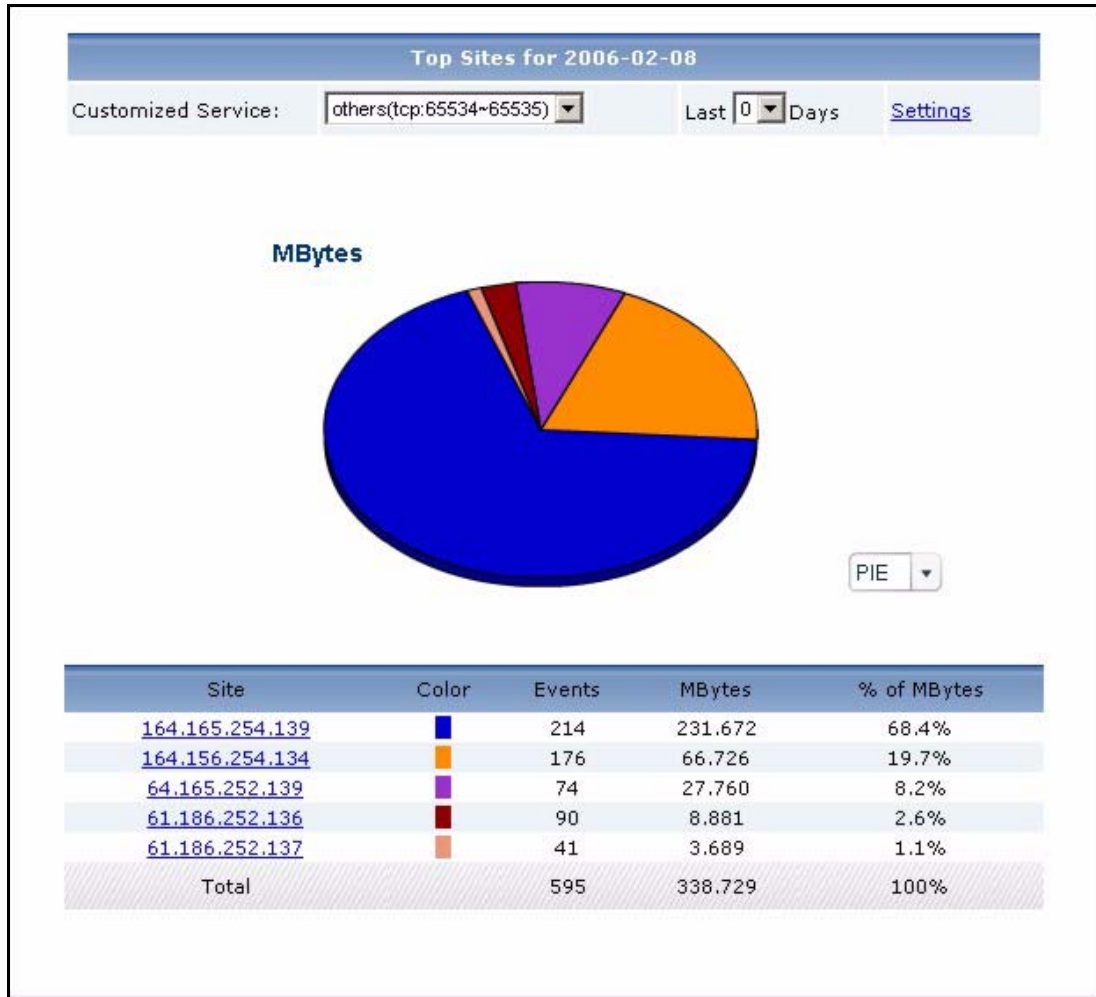
LABEL	DESCRIPTION
Add a Known Service	<p>Use this drop-down box to add a service to the Customized Service drop-down box.</p> <ul style="list-style-type: none"> • Select a pre-defined service from the drop-down list box, and click the Add button; or • Select [Customized Service], fill in the Add a Customized Service section, and click the Add button. <p>This drop-down box does not include web, mail, or FTP services.</p>
Add a Customized Service	<p>Use this section to create new TCP/UDP services that are not in the pre-defined list. You cannot edit pre-defined services.</p>
Name	<p>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.</p>
Port range	<p>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.</p>
Protocol	<p>Select the protocol used by the service. Choices are tcp, udp and tcp/udp.</p>
Customized Service	<p>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.</p> <p>To remove a service from the Customized Service drop-down box, click on the service in this list box, and click the Delete button.</p> <p>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.</p>
Add	<p>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.</p>
Delete	<p>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.</p>

5.6.2 Top Destinations of Other Traffic

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

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

Figure 43 Traffic > Customization > Top Destinations

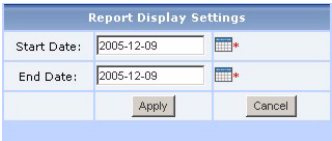


Each field is described in the following table.

Table 38 Traffic > Customization > Top Destinations

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.
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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

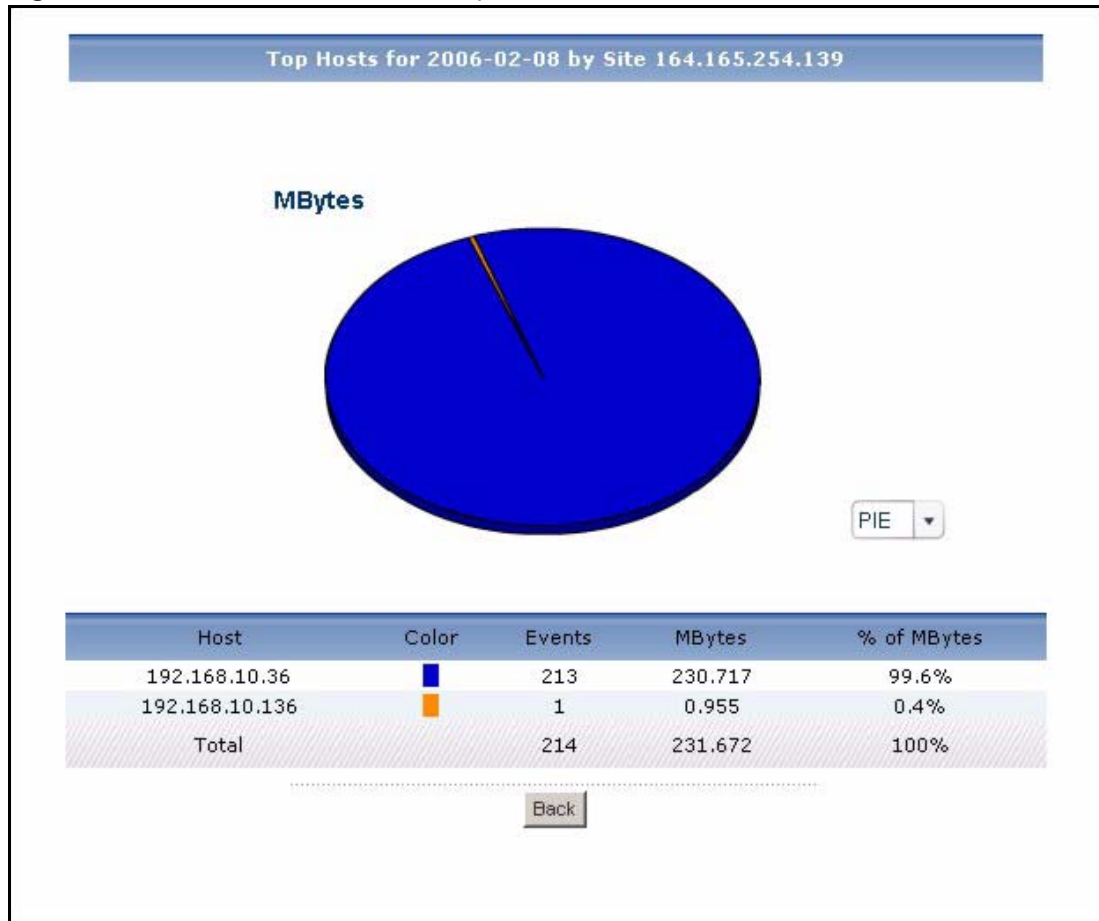
Table 38 Traffic > Customization > Top Destinations

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	<p>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.</p> <p>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. The Top Sites for Other Services Drill-Down report appears.</p>
Color	This field displays what color represents each destination in the graph.
Events	This field displays the number of traffic events for each destination.
MBytes	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes	This field displays what percentage of the selected service's traffic the device handled for each destination.
Total	This entry displays the totals for the destinations above.

5.6.3 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 **Traffic > Customization > Top Destinations** to open this screen.

Figure 44 Traffic > Customization > Top Destinations > Drill-Down

Each field is described in the following table.

Table 39 Traffic > Customization > Top Destinations > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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 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.
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events from each source to the selected destination.
MBytes	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.

Table 39 Traffic > Customization > Top Destinations > Drill-Down

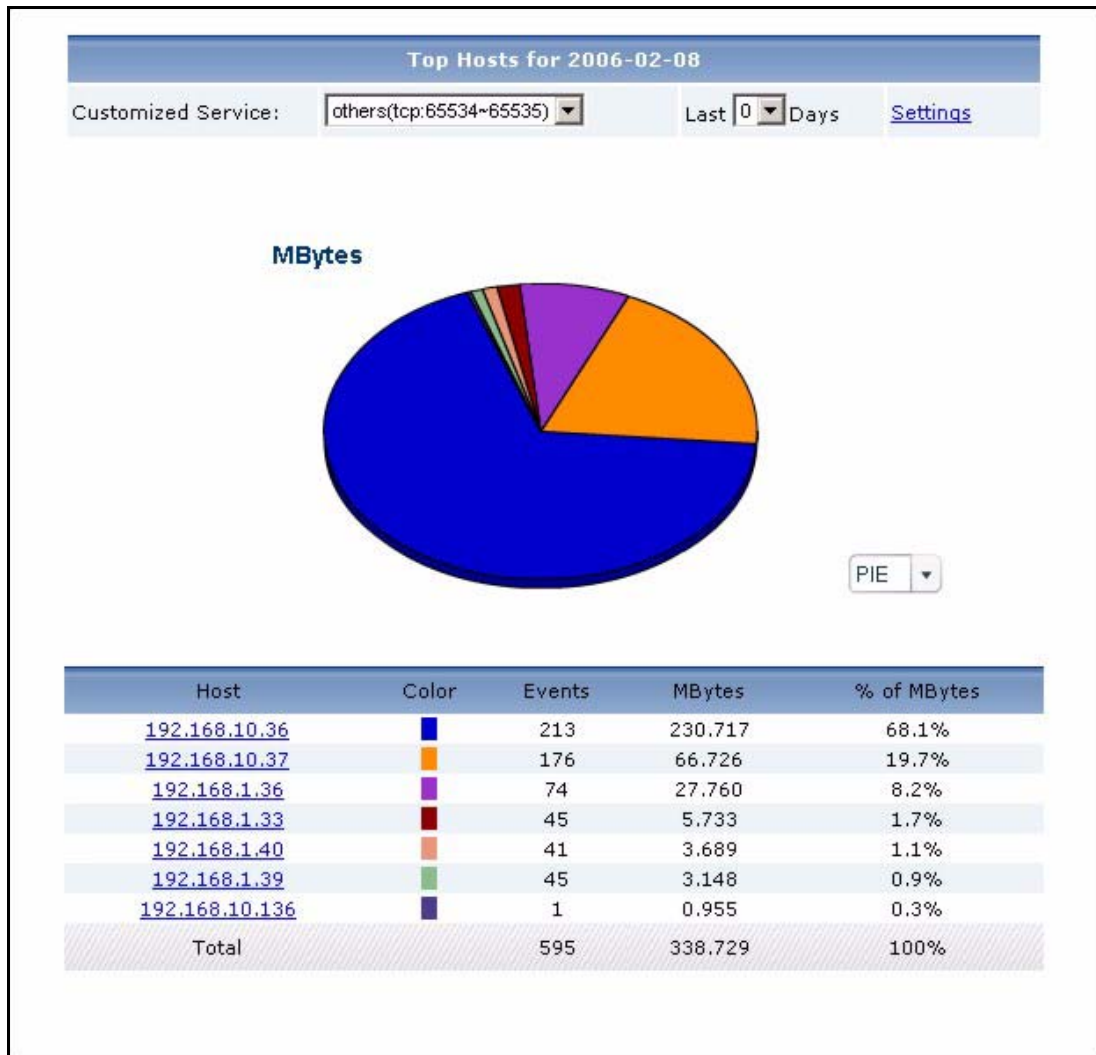
LABEL	DESCRIPTION
% of MBytes	This field displays what percentage of the selected destination's traffic using the selected service was generated from each source.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.6.4 Top Sources of Other Traffic

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

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

Figure 45 Traffic > Customization > Top Sources



Each field is described in the following table.

Table 40 Traffic > Customization > Top Sources

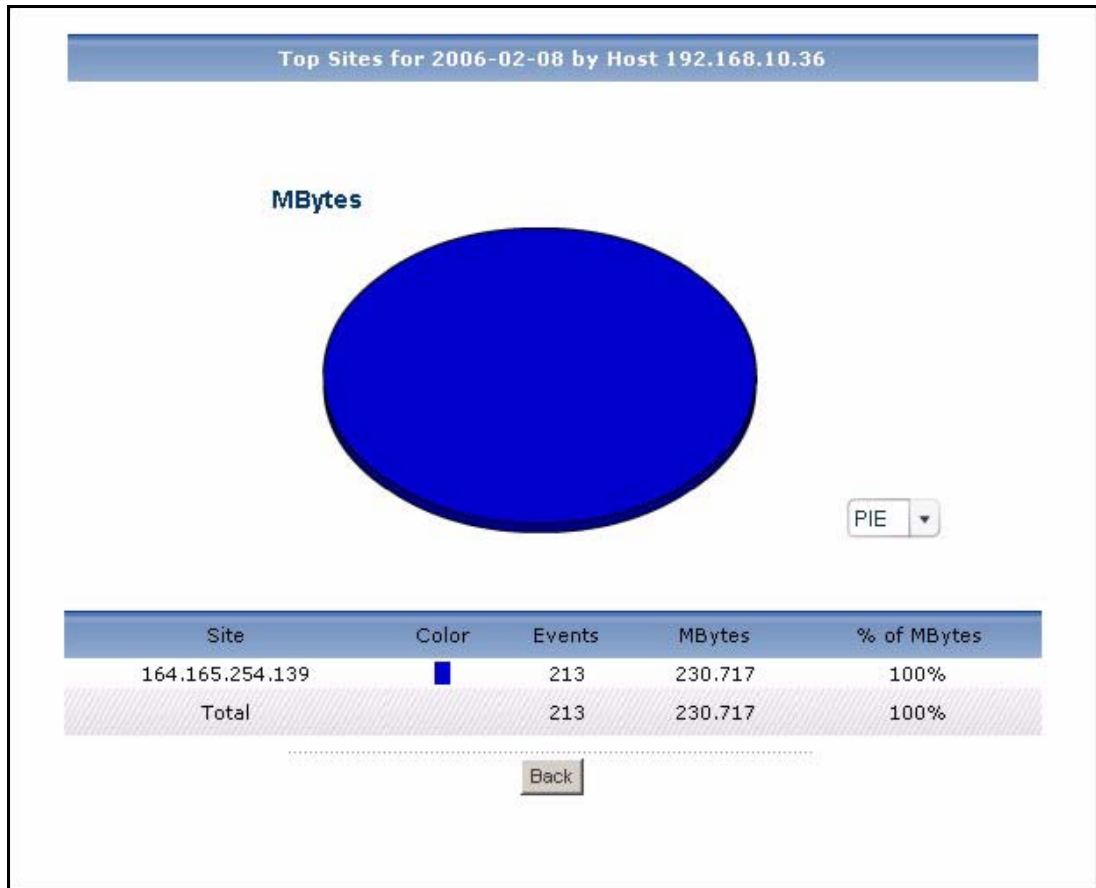
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Customized Service	Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the Service Settings screen.
Last ... Days	<p>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. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="841 808 1166 947" data-label="Image"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>This field displays the top sources 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.</p> <p>Each source is identified by its IP address. Click on a source to look at the top destinations of the selected service's traffic for the selected source. The Top Hosts for Other Services Drill-Down report appears.</p>
Color	This field displays what color represents each source in the graph.
Events	This field displays the number of traffic events for each source.
MBytes	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes	This field displays what percentage of the selected service's traffic the device handled for each source.
Total	This entry displays the totals for the sources above.

5.6.5 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 **Traffic > Customization > Top Sources** to open this screen.

Figure 46 Traffic > Customization > Top Sources > Drill-Down



Each field is described in the following table.

Table 41 Traffic > Customization > Top Sources > 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	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 41 Traffic > Customization > Top Sources > Drill-Down

LABEL	DESCRIPTION
Site	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.
Events	This field displays the number of traffic events from the selected source to each destination.
MBytes	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.
% of MBytes	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.
Back	Click this to return to the main report.

CHAPTER 6

Network Attack

Use these reports to look at Denial-of-Service (DoS) attacks that were detected by the ZyXEL device's firewall.

6.1 Attack

Use this report to look at the number of DoS attacks by time interval, top sources and by category.

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.

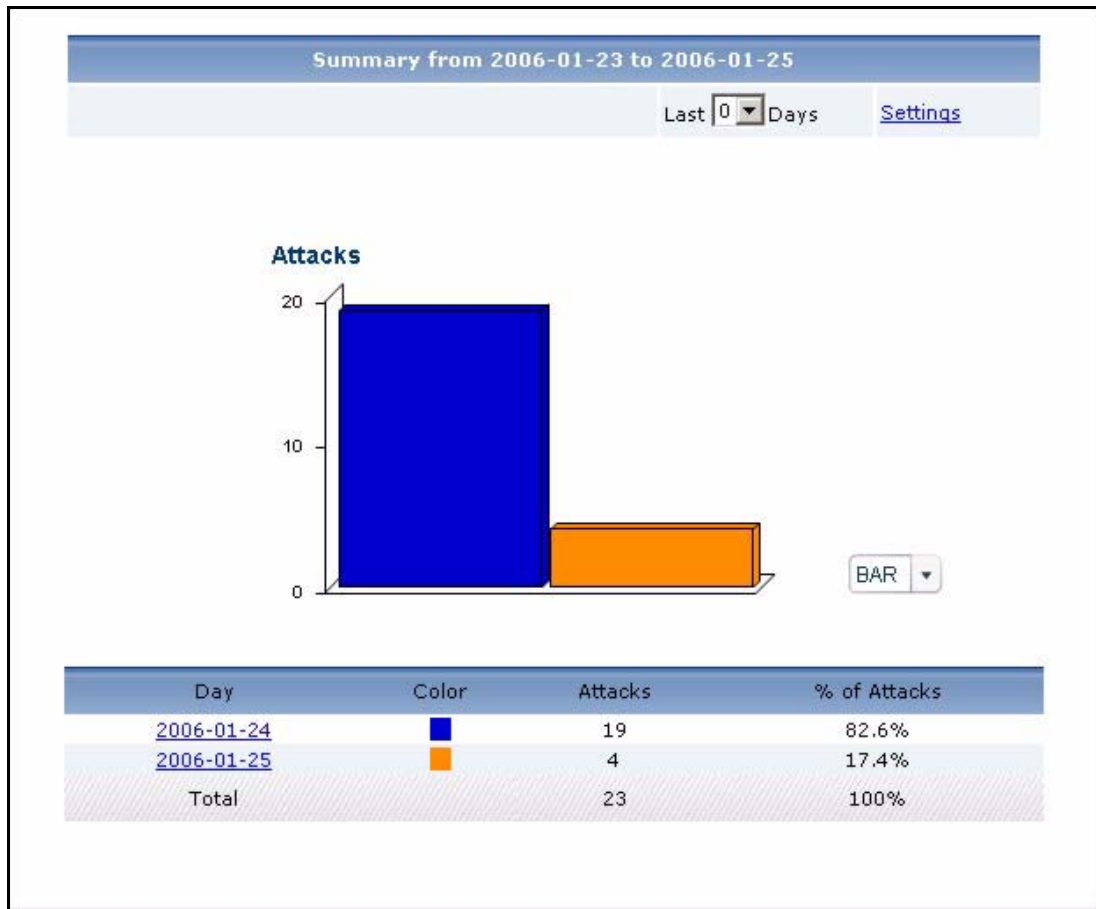
6.1.1 Attack Summary

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 **Network Attack > Attack > Summary** to open this screen.

Figure 47 Network Attack > Attack > Summary

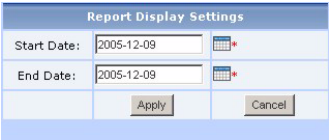


Each field is described in the following table.

Table 42 Network Attack > Attack > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 42 Network Attack > Attack > Summary

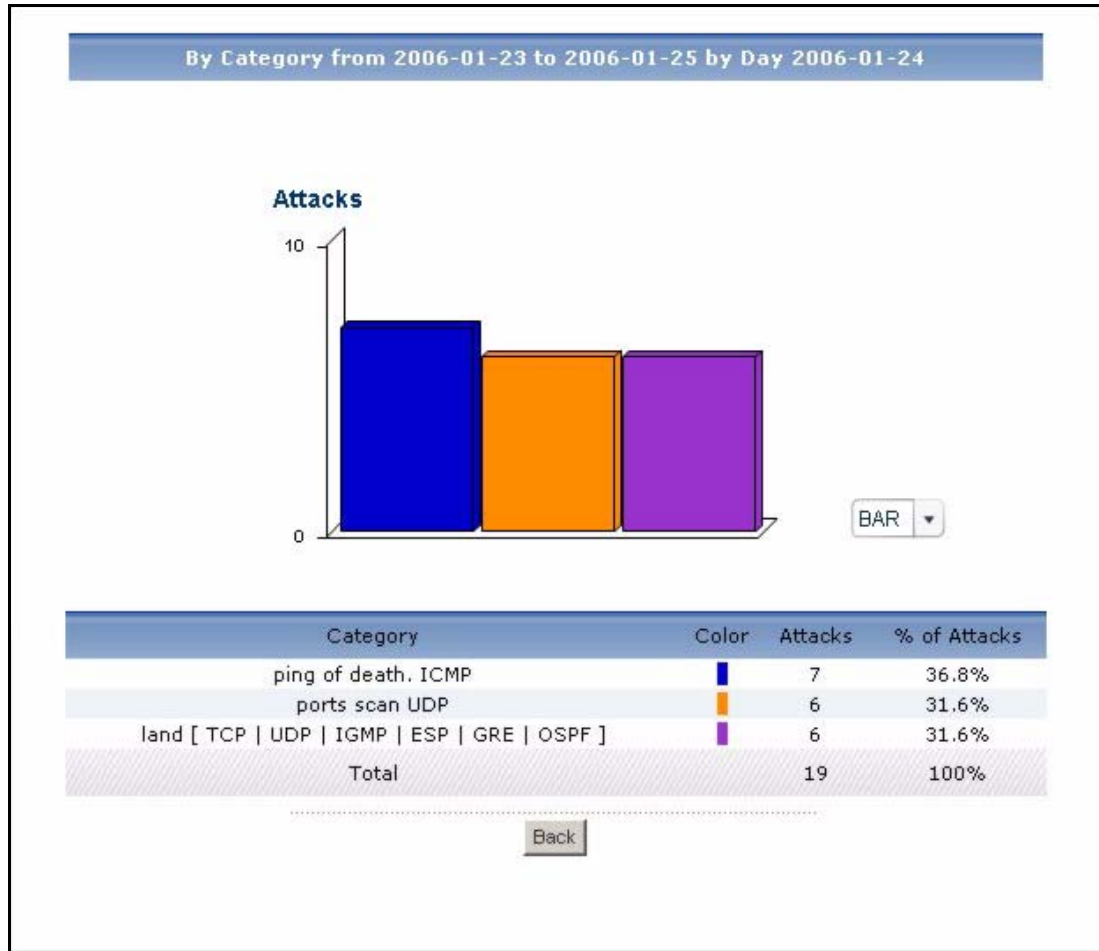
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top categories of attacks in the selected time interval. The Attack Summary Drill-Down report appears.</p>
Color	<p>This field displays what color represents each time interval in the graph.</p>
Attacks	<p>This field displays the number of DoS attacks in the selected time interval.</p>
% of Attacks	<p>This field displays what percentage of all DoS attacks was handled in each time interval.</p>
Total	<p>This entry displays the totals for the time intervals above.</p>

6.1.2 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 **Network Attack > Attack > Summary** to open this screen.

Figure 48 Network Attack > Attack > Summary > Drill-Down



Each field is described in the following table.

Table 43 Network Attack > Attack > 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. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	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.

Table 43 Network Attack > Attack > Summary > Drill-Down

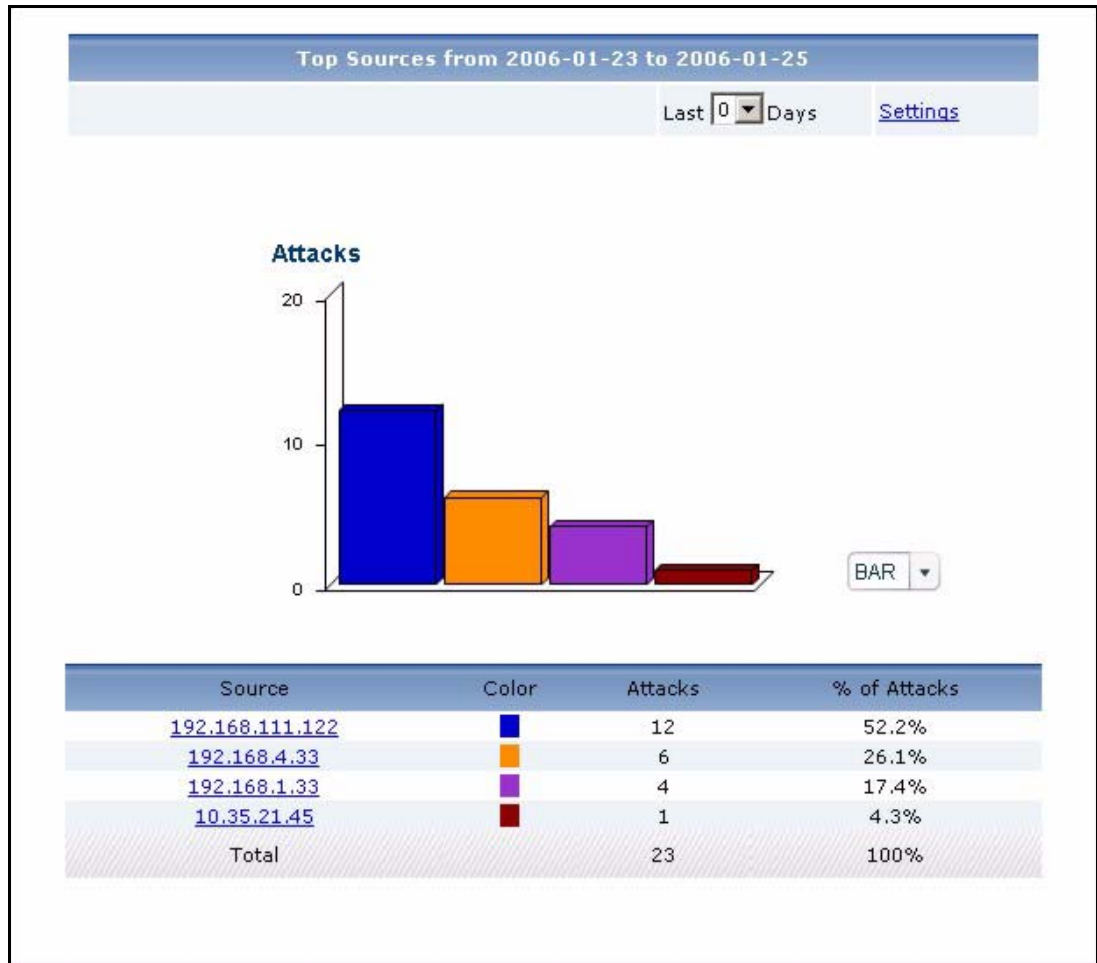
LABEL	DESCRIPTION
Total	This entry displays the totals for the categories above. If the number of categories in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

6.1.3 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 **Network Attack > Attack > Top Sources** to open this screen.

Figure 49 Network Attack > Attack > Top Sources

Each field is described in the following table.

Table 44 Network Attack > Attack > Top Sources

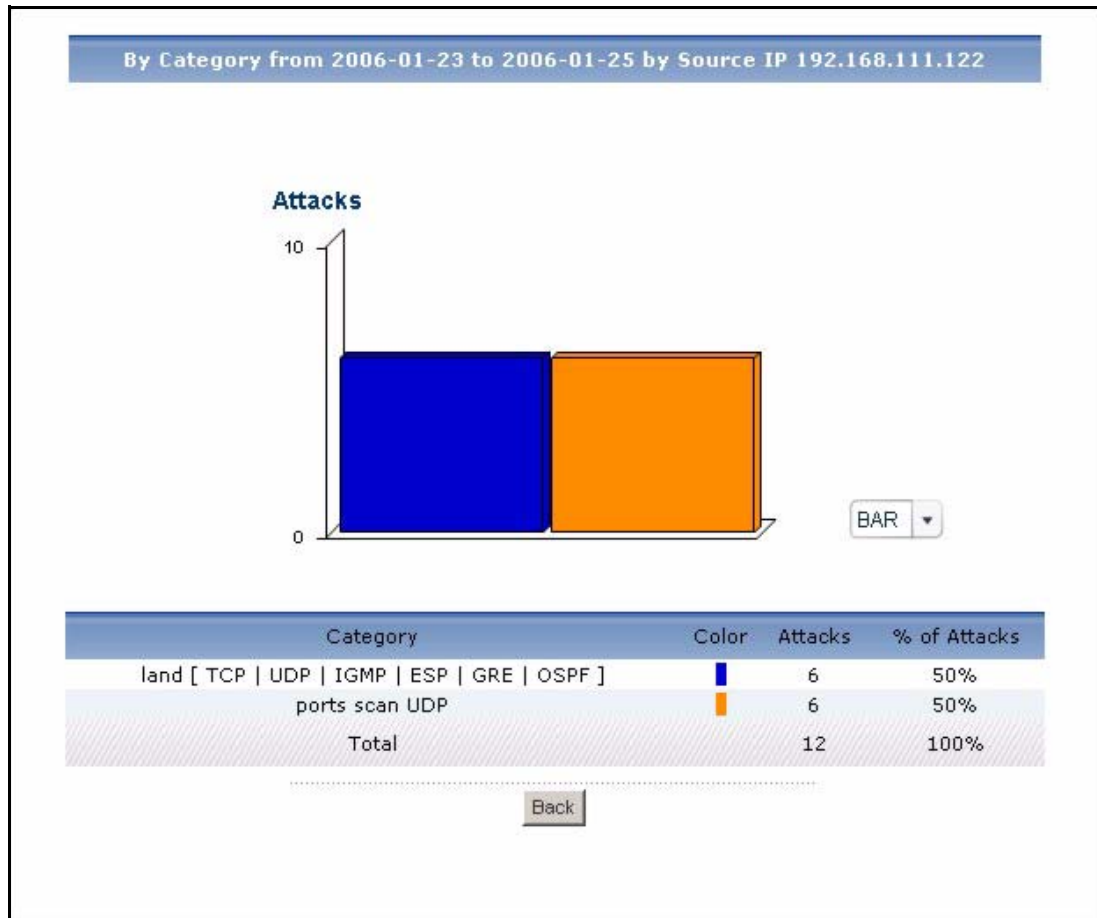
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="836 737 1166 877" style="text-align: center;"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	<p>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.</p> <p>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").</p> <p>Click on a source to look at the top categories of DoS attacks by the selected source. The Top Attack Sources Drill-Down report appears.</p>
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.
Total	This entry displays the totals for the sources above.

6.1.4 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 **Network Attack > Attack > Top Sources** to open this screen.

Figure 50 Network Attack > Attack > Top Sources > Drill-Down



Each field is described in the following table.

Table 45 Network Attack > Attack > Top Sources > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. Click on a slice in the pie chart to move it away from the pie chart a little.
Category	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 in each category that occurred from the selected source.

Table 45 Network Attack > 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.
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.

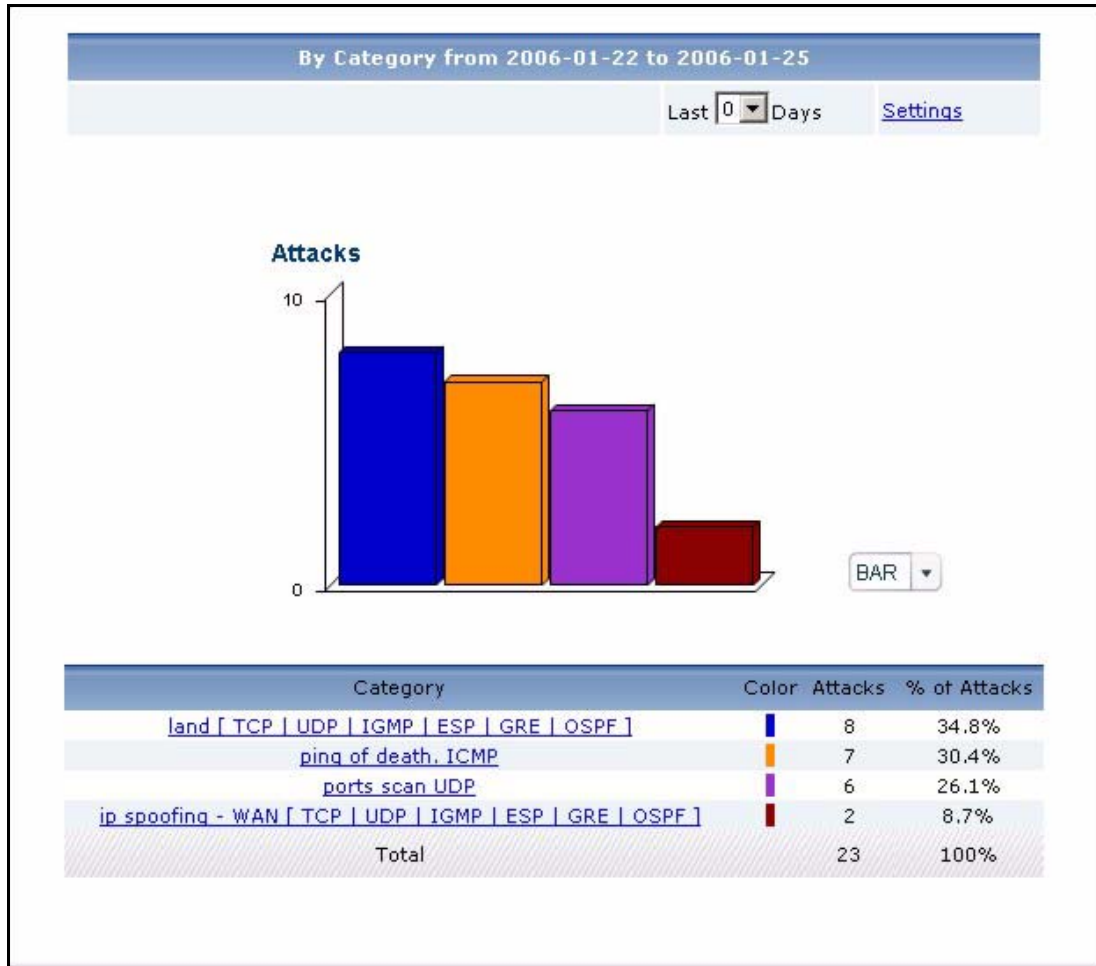
6.1.5 Top Attack Categories

Use this report to look at the top 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 **Network Attack > Attack > By Category** to open this screen.

Figure 51 Network Attack > Attack > By Category

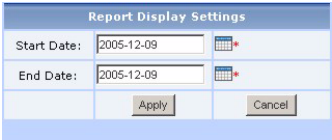


Each field is described in the following table.

Table 46 Network Attack > Attack > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

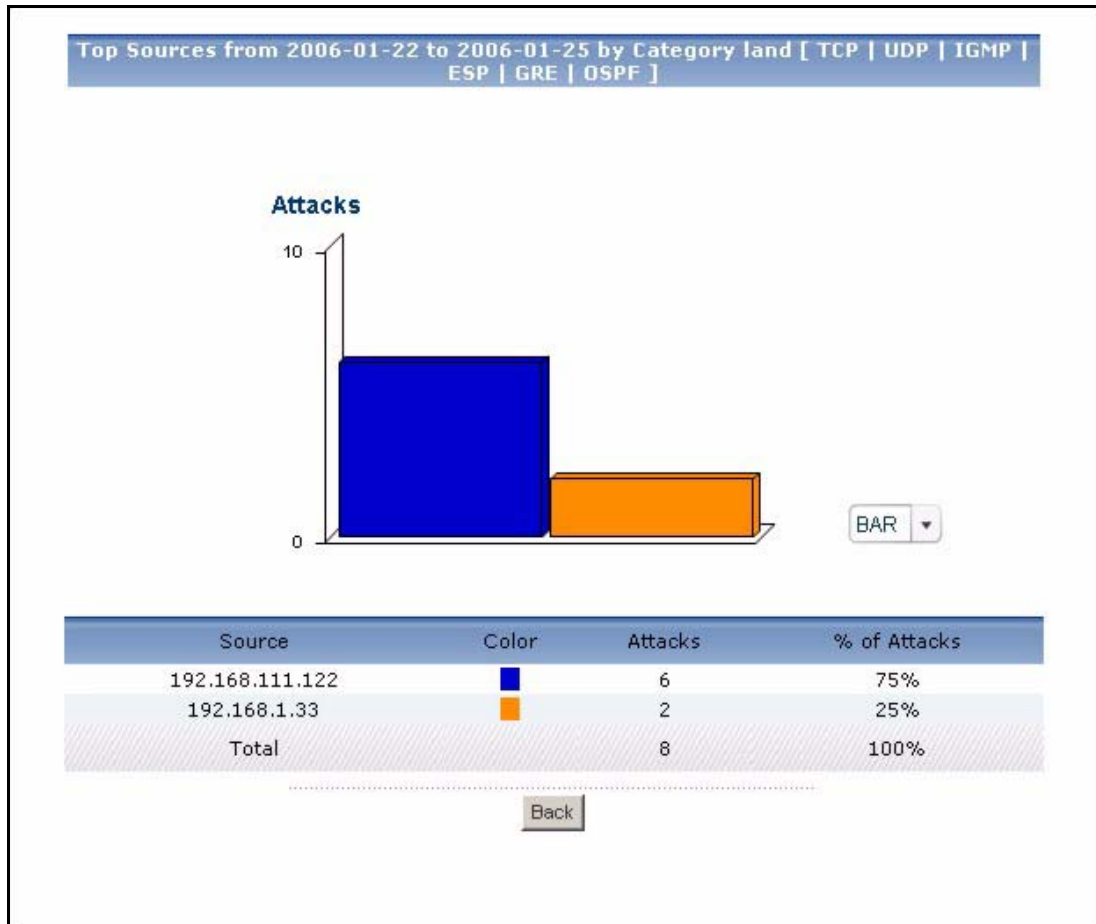
Table 46 Network Attack > Attack > By Category

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	<p>This field displays the top categories of DoS attacks in the selected device, sorted by the number of attacks by each one. If the number of categories is less than the maximum number of records displayed in this table, every category is displayed.</p> <p>Click on a category to look at the top sources of DoS attacks in the selected category. The Top Attack Categories Drill-Down report appears.</p>
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks in each category the device stopped.
% of Attacks	This field displays what percentage of all DoS attacks come from each category.
Total	This entry displays the totals for the categories above.

6.1.6 Top Attack Categories Drill-Down

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

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

Figure 52 Network Attack > Attack > By Category > Drill-Down

Each field is described in the following table.

Table 47 Network Attack > Attack > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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 DoS attacks in the selected category, sorted by the number of attacks by each one. 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.
Attacks	This field displays the number of DoS attacks by each source in the selected category.

Table 47 Network Attack > Attack > By Category > Drill-Down

LABEL	DESCRIPTION
% of Attacks	This field displays what percentage of all DoS attacks in the selected category were made by each source.
Total	This entry displays the totals for the sources above. If the number of sources in the selected category 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.

6.2 Intrusion

Use these reports to 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 selected device's IDP feature.

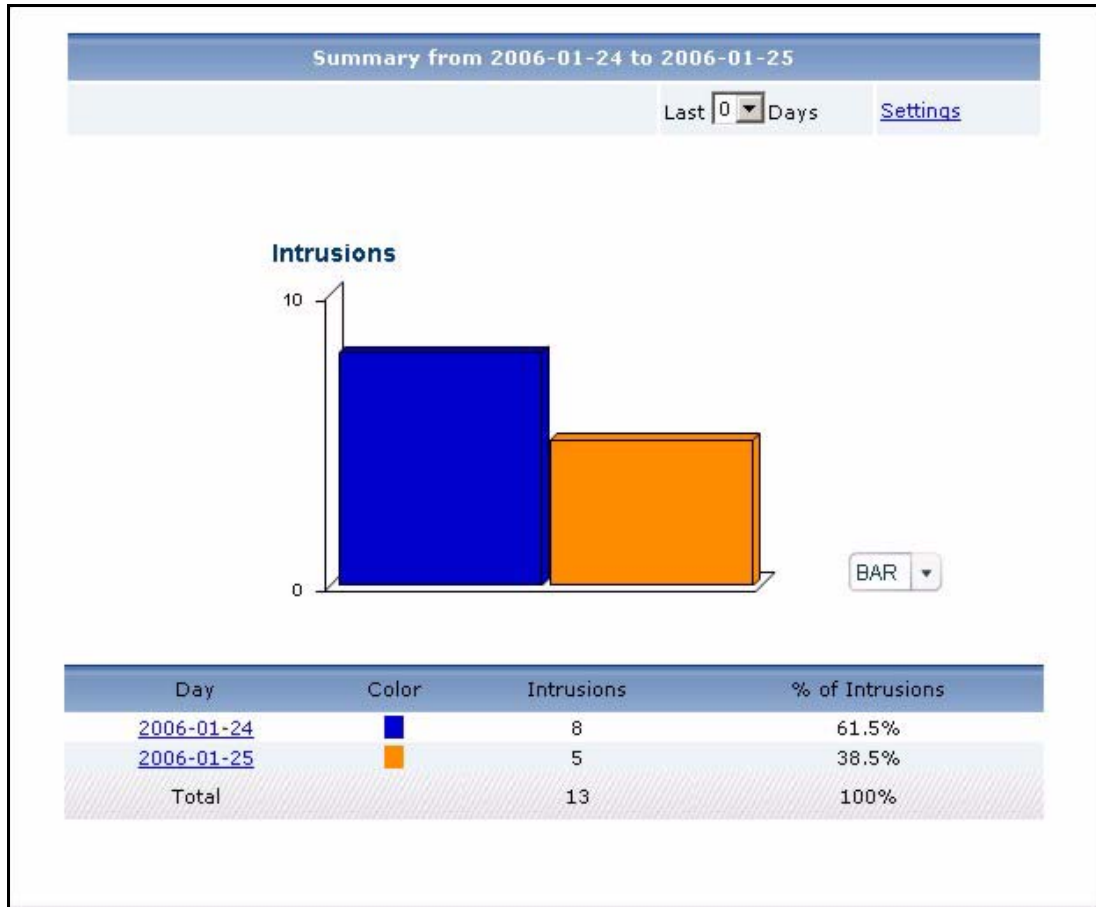
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP > Signature**, and make sure the ZyXEL device logs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

6.2.1 Intrusion Summary

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

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.

Click **Network Attack > Intrusion > Summary** to open this screen.

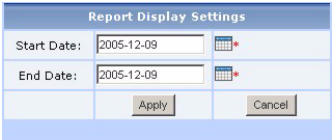
Figure 53 Network Attack > Intrusion > Summary

Each field is described in the following table.

Table 48 Network Attack > Intrusion > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

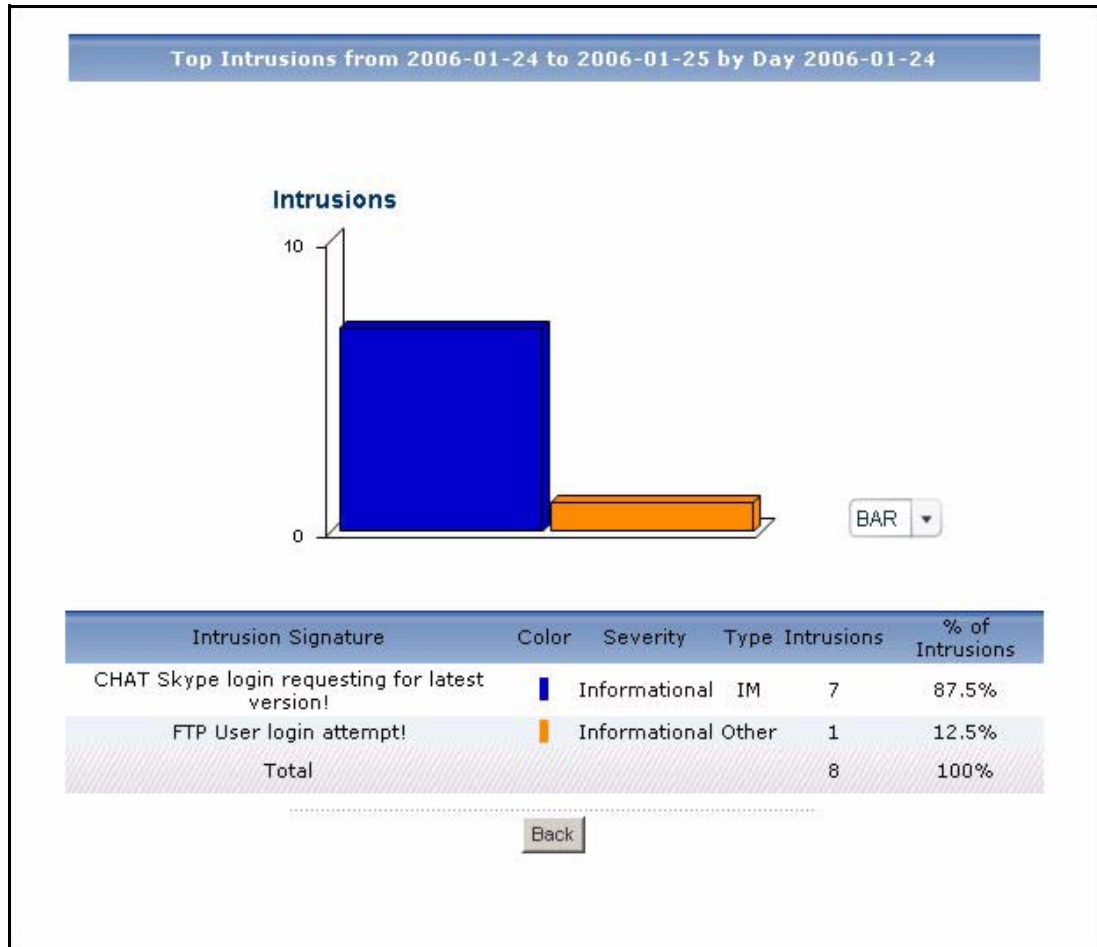
Table 48 Network Attack > Intrusion > Summary

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top intrusion signatures in the selected time interval. The Intrusion Summary Drill-Down report appears.</p>
Color	<p>This field displays what color represents each time interval in the graph.</p>
Intrusions	<p>This field displays the number of intrusions in the selected time interval.</p>
% of Intrusions	<p>This field displays what percentage of all intrusions was made in each time interval.</p>
Total	<p>This entry displays the totals for the time intervals above.</p>

6.2.2 Intrusion Summary Drill-Down

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

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

Figure 54 Network Attack > Intrusion > Summary > Drill-Down

Each field is described in the following table.

Table 49 Network Attack > Intrusion > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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 categories of intrusions in the selected time interval, sorted by the number of attempts 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 how many intrusions occurred in the selected time interval.

Table 49 Network Attack > Intrusion > Summary > Drill-Down

LABEL	DESCRIPTION
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
Total	This entry displays the totals for the intrusion signatures above. If the number of signatures 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.

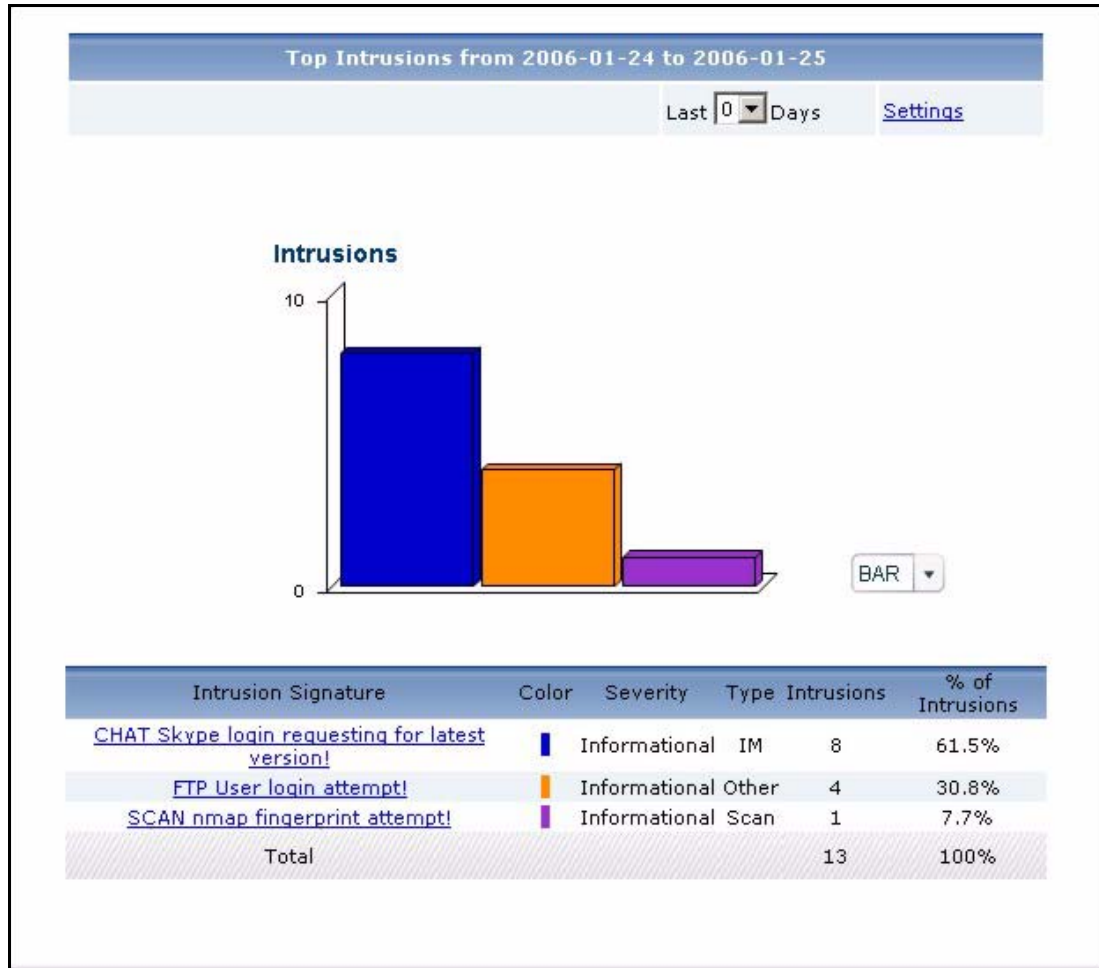
6.2.3 Top Intrusion Signatures

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

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.

Click **Network Attack > Intrusion > Top Intrusions** to open this screen.

Figure 55 Network Attack > Intrusion > Top Intrusions

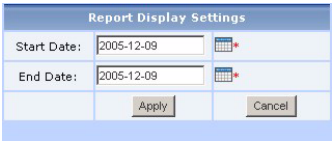


Each field is described in the following table.

Table 50 Network Attack > Intrusion > Top Intrusions

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

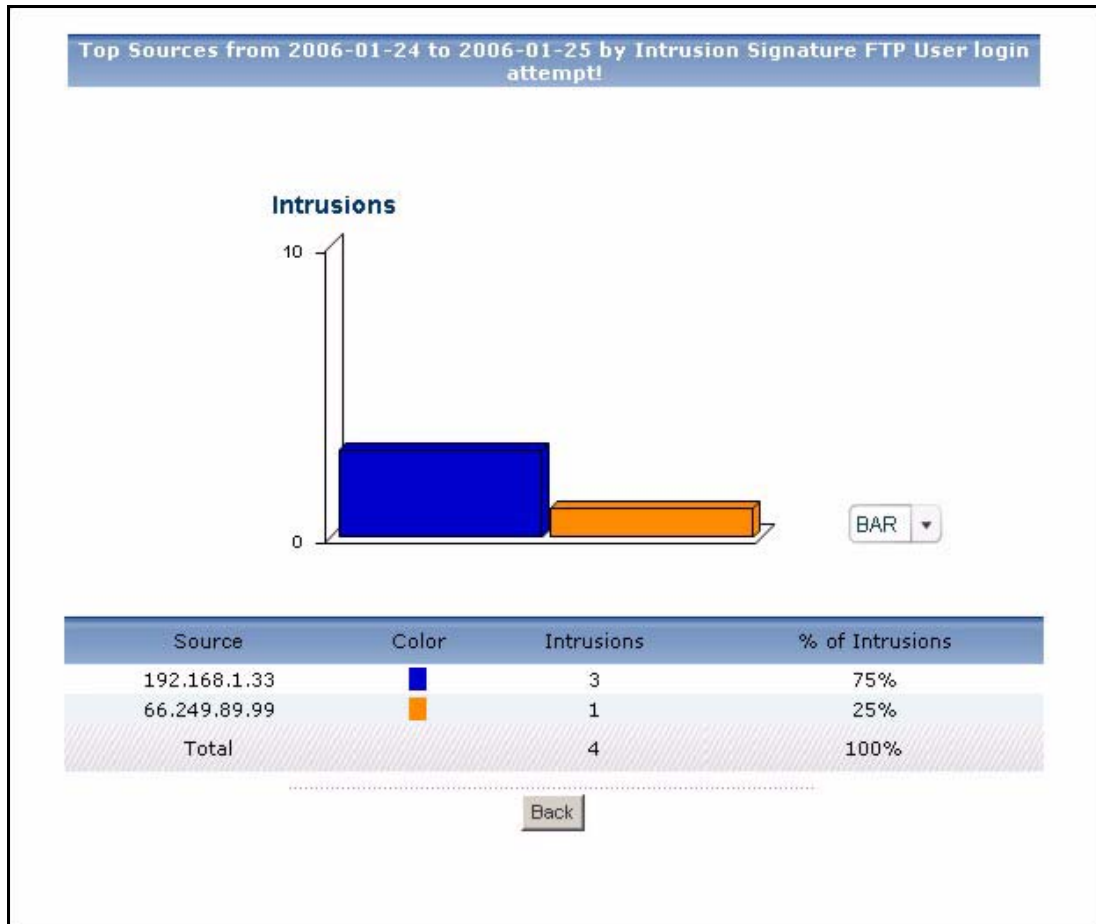
Table 50 Network Attack > Intrusion > Top Intrusions

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	<p>This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one.</p> <p>Click on an intrusion signature to look at the top sources for the selected signature. The Top Intrusion Signatures Drill-Down report appears.</p>
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 each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
Total	This entry displays the totals for the intrusion signatures above.

6.2.4 Top Intrusion 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 **Network Attack > Intrusion > Top Intrusions** to open this screen.

Figure 56 Network Attack > Intrusion > Top Intrusions > Drill-Down

Each field is described in the following table.

Table 51 Network Attack > Intrusion > Top Intrusions > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.

Table 51 Network Attack > Intrusion > Top Intrusions > Drill-Down

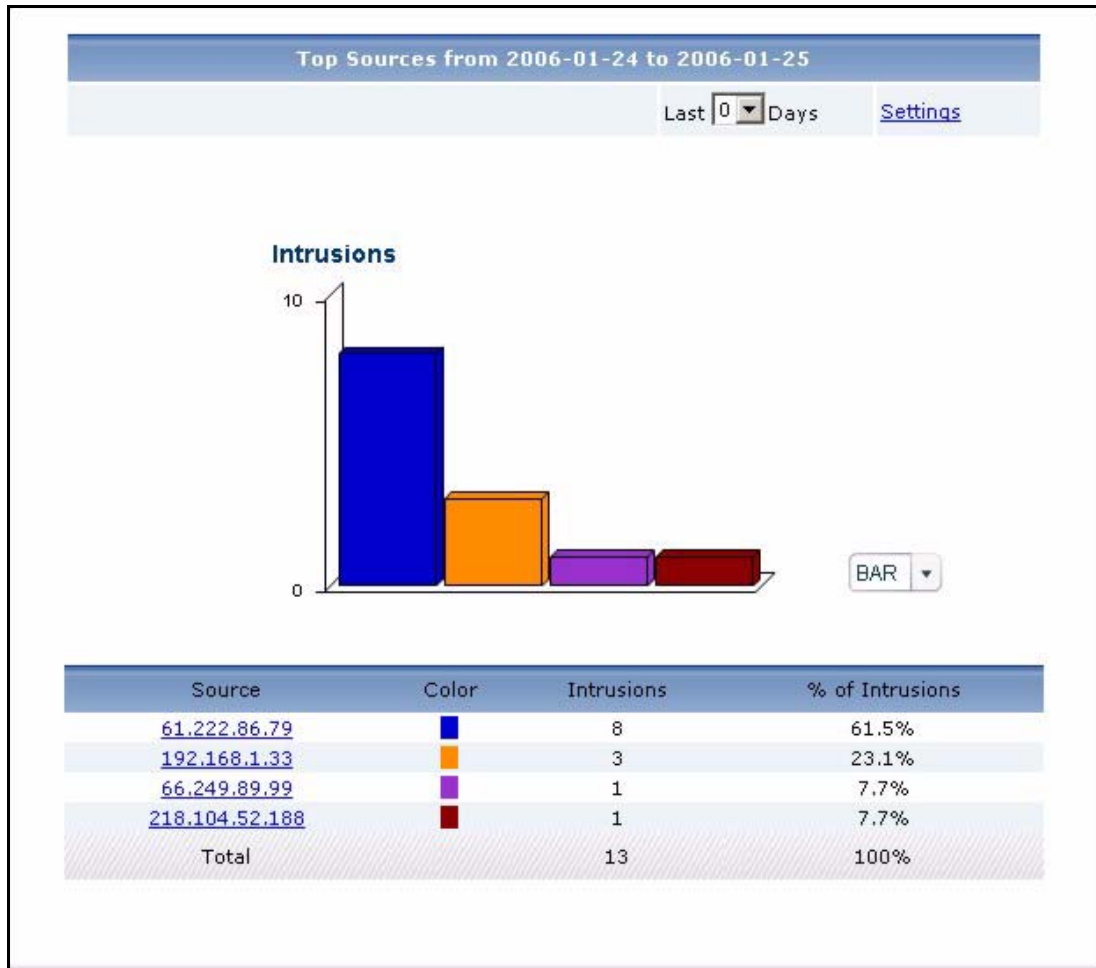
LABEL	DESCRIPTION
% of Intrusions	This field displays what percentage of all intrusions using the selected intrusion signature was made by each source.
Total	This entry displays the totals for the sources above. If the number of sources of the selected intrusion signature is greater than the maximum 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.

6.2.5 Top Intrusion Sources

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

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.

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

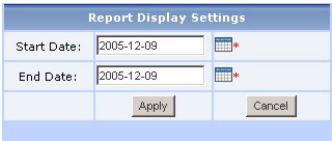
Figure 57 Network Attack > Intrusion > Top Sources

Each field is described in the following table.

Table 52 Network Attack > Intrusion > Top Sources

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

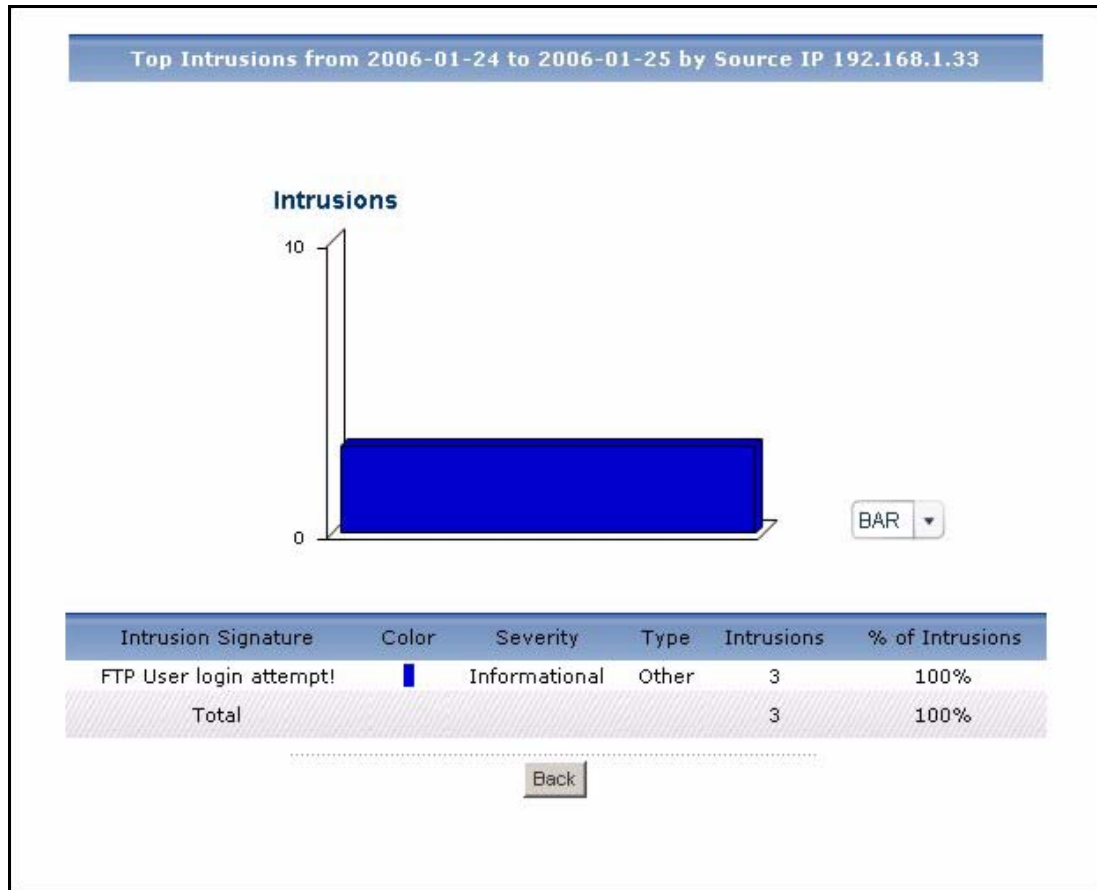
Table 52 Network Attack > Intrusion > Top Sources

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	<p>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.</p> <p>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").</p> <p>Click on a source to look at the top intrusion signatures for the selected source. The Top Intrusion Sources Drill-Down report appears.</p>
Color	<p>This field displays what color represents each source in the graph.</p>
Intrusions	<p>This field displays the number of intrusions by each source.</p>
% of Intrusions	<p>This field displays what percentage of all intrusions was made by each source.</p>
Total	<p>This entry displays the totals for the sources above.</p>

6.2.6 Top Intrusion Sources Drill-Down

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

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

Figure 58 Network Attack > Intrusion > Top Sources > Drill-Down

Each field is described in the following table.

Table 53 Network Attack > Intrusion > Top Sources > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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 53 Network Attack > Intrusion > 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.
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.

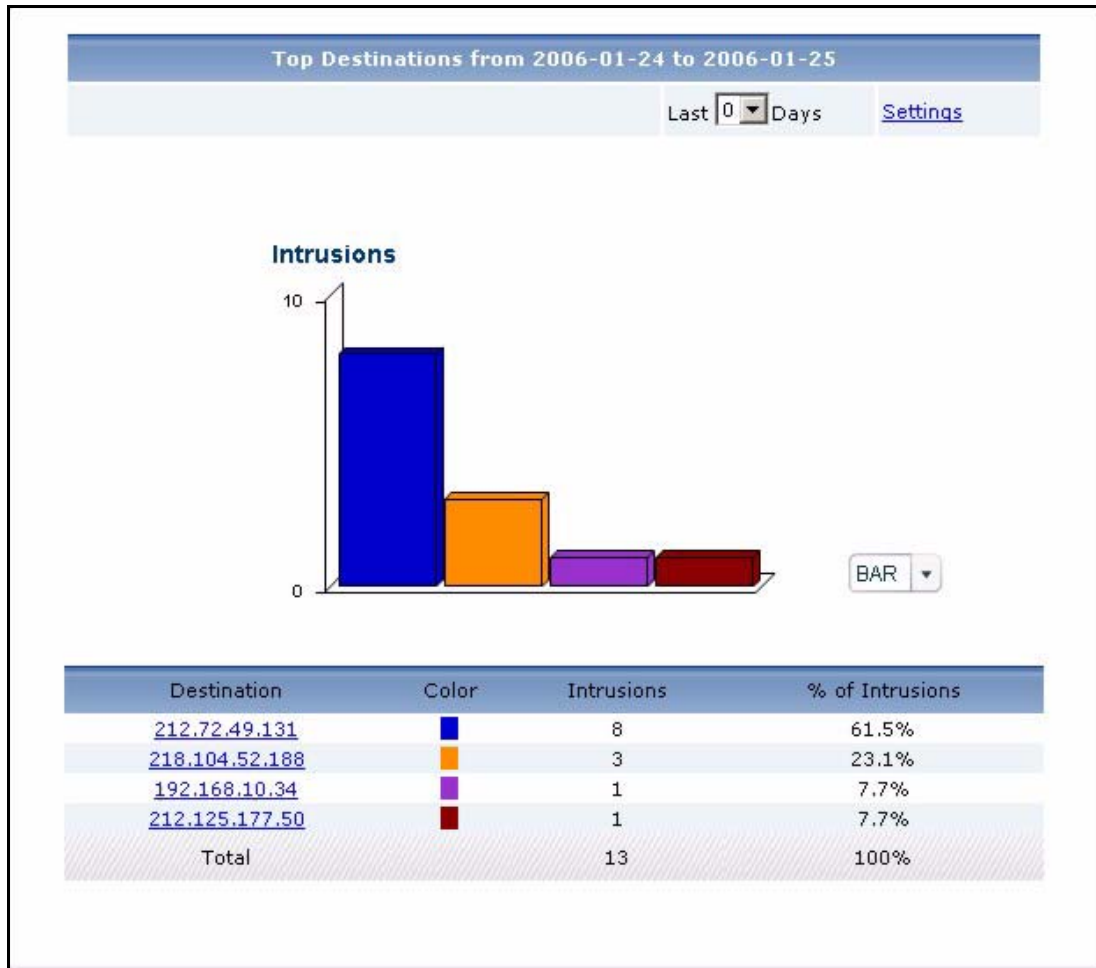
6.2.7 Top Intrusion Destinations

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

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.

Click **Network Attack > Intrusion > Top Destinations** to open this screen.

Figure 59 Intrusion > Top Destinations

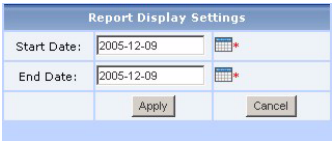


Each field is described in the following table.

Table 54 Intrusion > Top Destinations

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

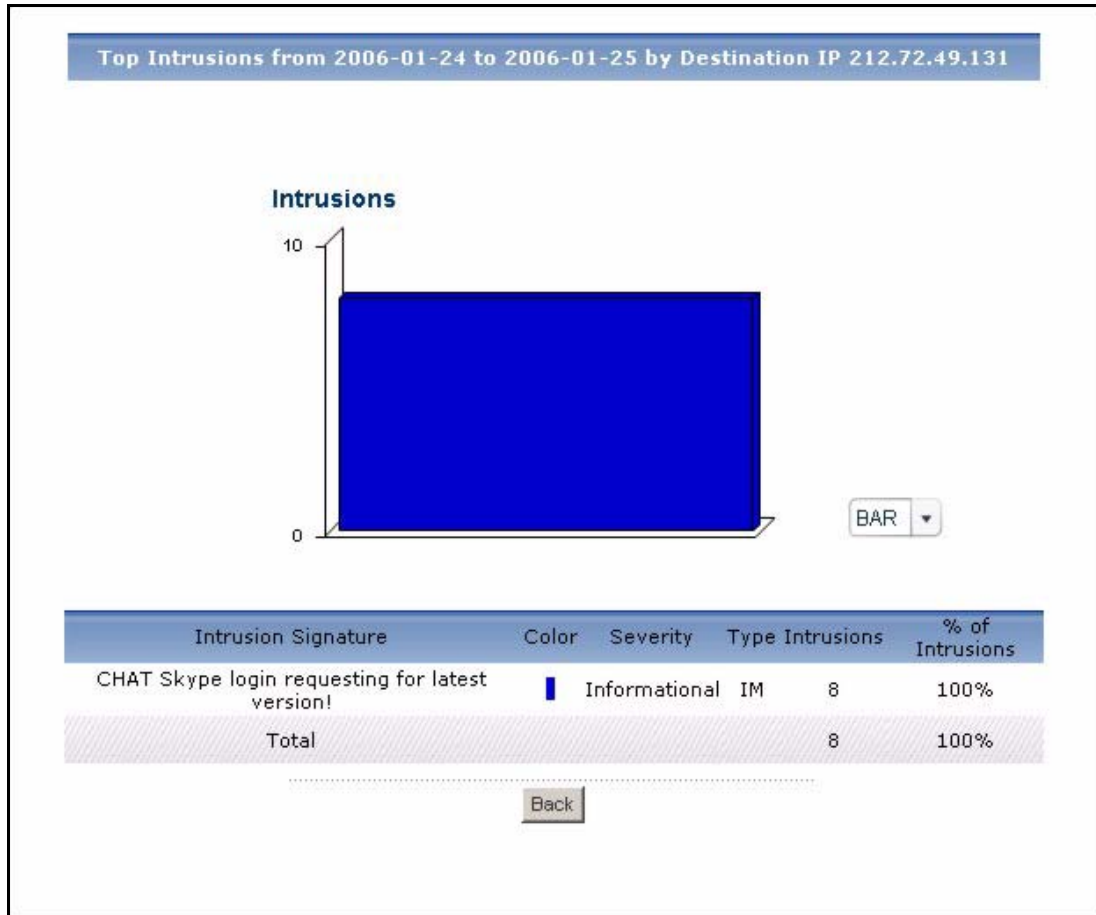
Table 54 Intrusion > Top Destinations

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	<p>This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed.</p> <p>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").</p> <p>Click on a destination to look at the top intrusion signatures for the selected destination. The Top Intrusion Destinations Drill-Down report appears.</p>
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions at each destination.
% of Intrusions	This field displays what percentage of all intrusions went to each destination.
Total	This entry displays the totals for the destinations above.

6.2.8 Top Intrusion Destinations Drill-Down

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

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

Figure 60 Network Attack > Intrusion > Top Destinations > Drill-Down

Each field is described in the following table.

Table 55 Network Attack > Intrusion > Top Destinations > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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 at 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 at the selected destination using each intrusion signature.

Table 55 Network Attack > Intrusion > Top Destinations > Drill-Down

LABEL	DESCRIPTION
% of Intrusions	This field displays what percentage of all intrusions at the selected destination was made by each intrusion signature.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures at 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.

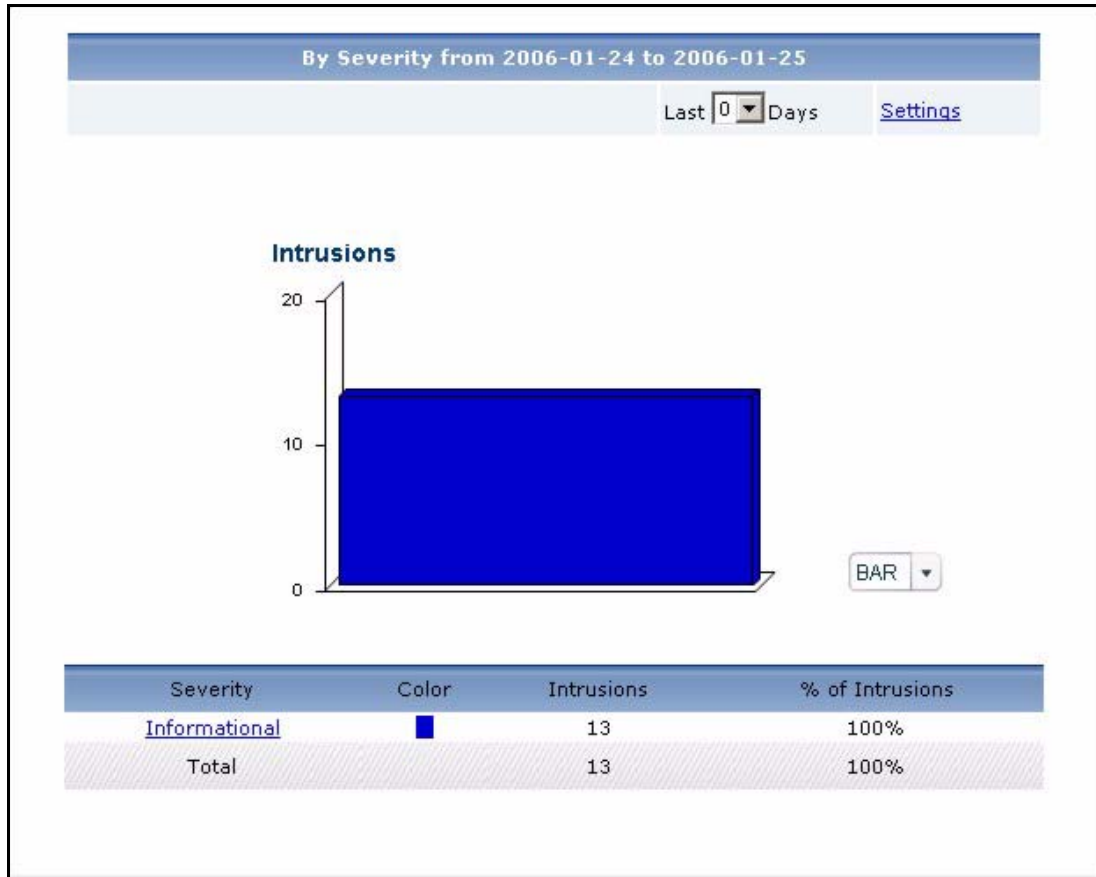
6.2.9 Intrusion Severities

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.

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.

Click **Network Attack > Intrusion > By Severity** to open this screen.

Figure 61 Network Attack > Intrusion > By Severity

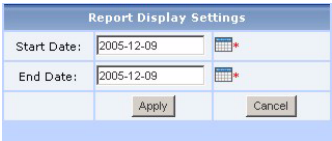


Each field is described in the following table.

Table 56 Network Attack > Intrusion > By Severity

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 56 Network Attack > Intrusion > By Severity

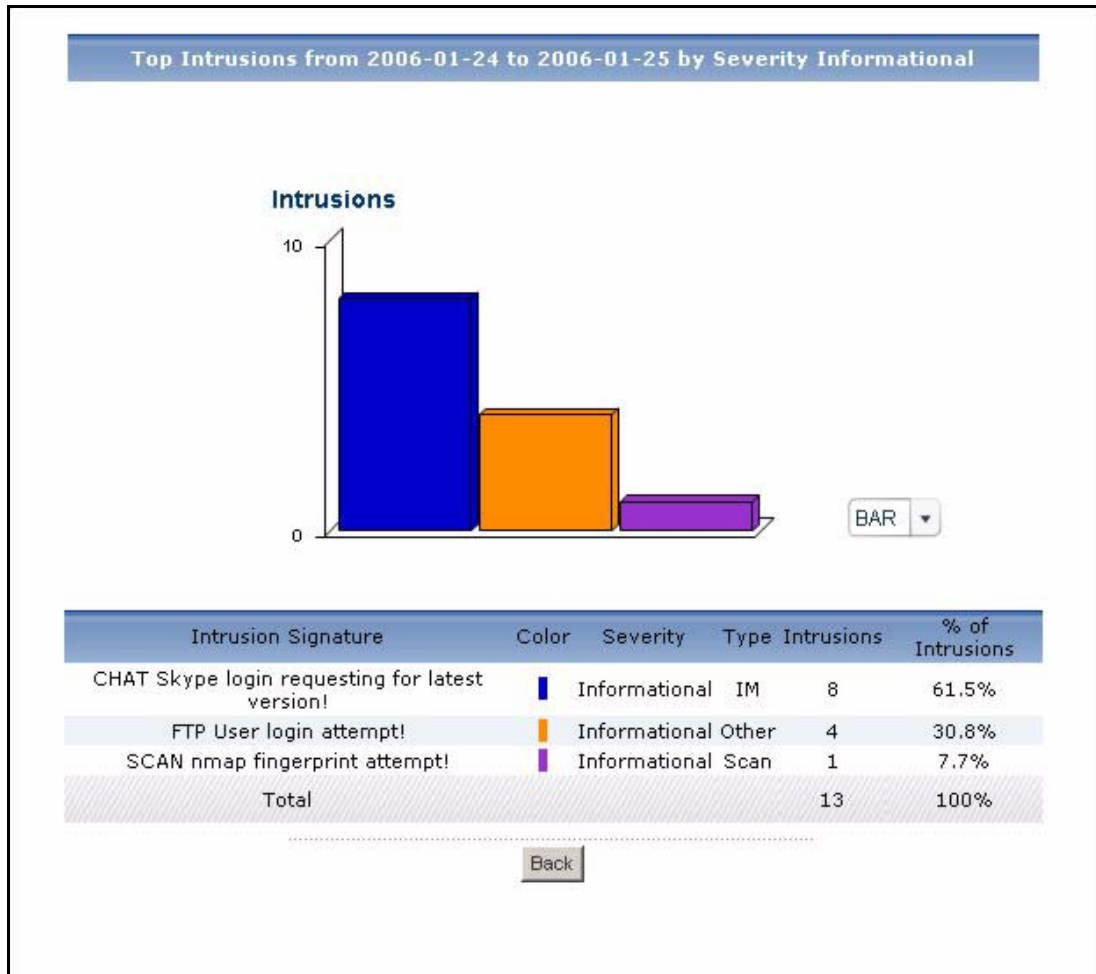
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	<p>This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level.</p> <p>Click on a severity to look at the top intrusion signatures for the selected severity. The Intrusion Severities Drill-Down report appears.</p>
Color	<p>This field displays what color represents each level of severity in the graph.</p>
Intrusions	<p>This field displays the number of intrusions of each level of severity.</p>
% of Intrusions	<p>This field displays what percentage of all intrusions are at each level of severity.</p>
Total	<p>This entry displays the totals for the severities above.</p>

6.2.10 Intrusion Severities Drill-Down

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

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

Figure 62 Network Attack > Intrusion > By Severity > Drill-Down



Each field is described in the following table.

Table 57 Network Attack > Intrusion > By Severity > 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. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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 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 57 Network Attack > Intrusion > 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.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures of the selected severity 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.

6.3 AntiVirus

Use these reports to look at viruses that were detected by the ZyXEL device's anti-virus feature.

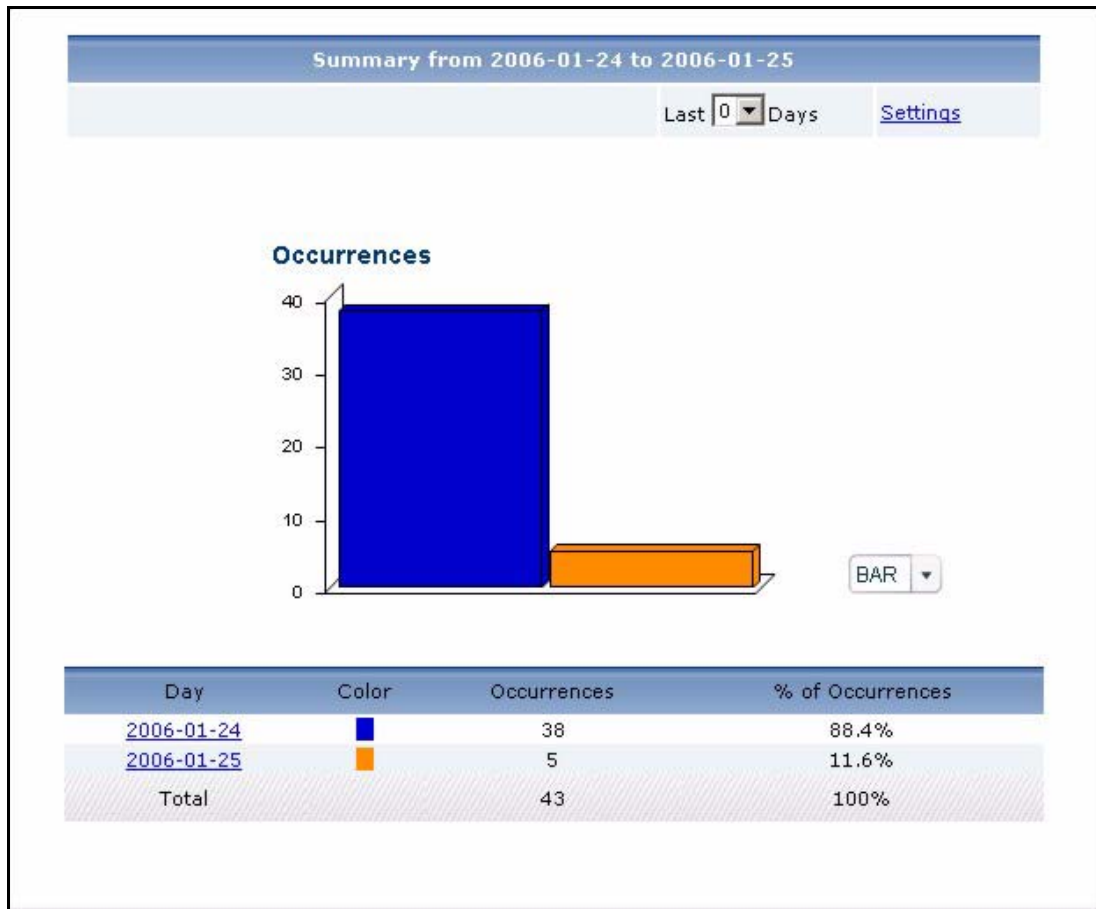
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs > Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus > General**. ZyXEL devices 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.

6.3.1 Virus Summary

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

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.

Click **Network Attack > AntiVirus > Summary** to open this screen.

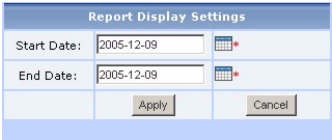
Figure 63 Network Attack > AntiVirus > Summary

Each field is described in the following table.

Table 58 Network Attack > AntiVirus > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

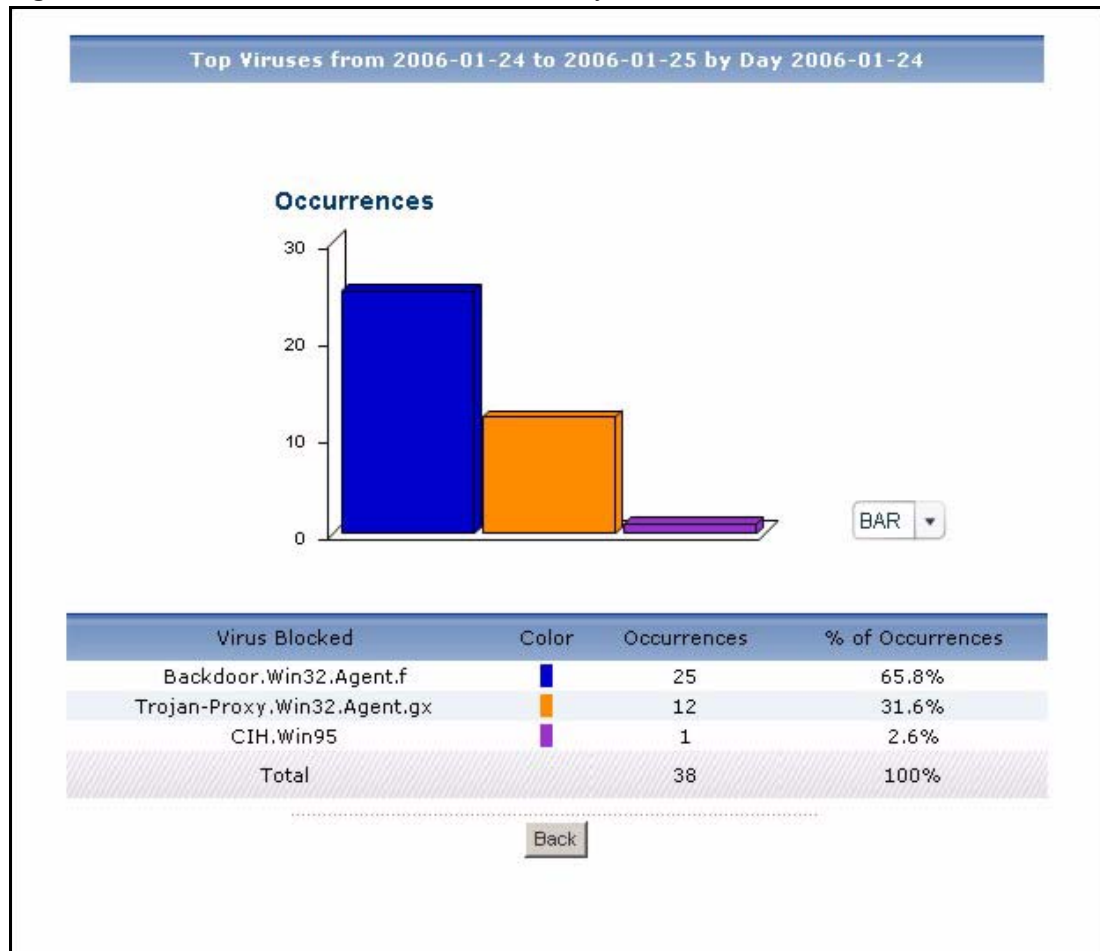
Table 58 Network Attack > AntiVirus > Summary

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top viruses in the selected time interval. The Virus Summary Drill-Down report appears.</p>
Color	<p>This field displays what color represents each time interval in the graph.</p>
Occurrences	<p>This field displays the number of occurrences in the selected time interval.</p>
% of Occurrences	<p>This field displays what percentage of all occurrences was made in each time interval.</p>
Total	<p>This entry displays the totals for the time intervals above.</p>

6.3.2 Virus Summary Drill-Down

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

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

Figure 64 Network Attack > AntiVirus > Summary > Drill-Down

Each field is described in the following table.

Table 59 Network Attack > AntiVirus > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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 time interval, 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 by 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 59 Network Attack > AntiVirus > Summary > Drill-Down

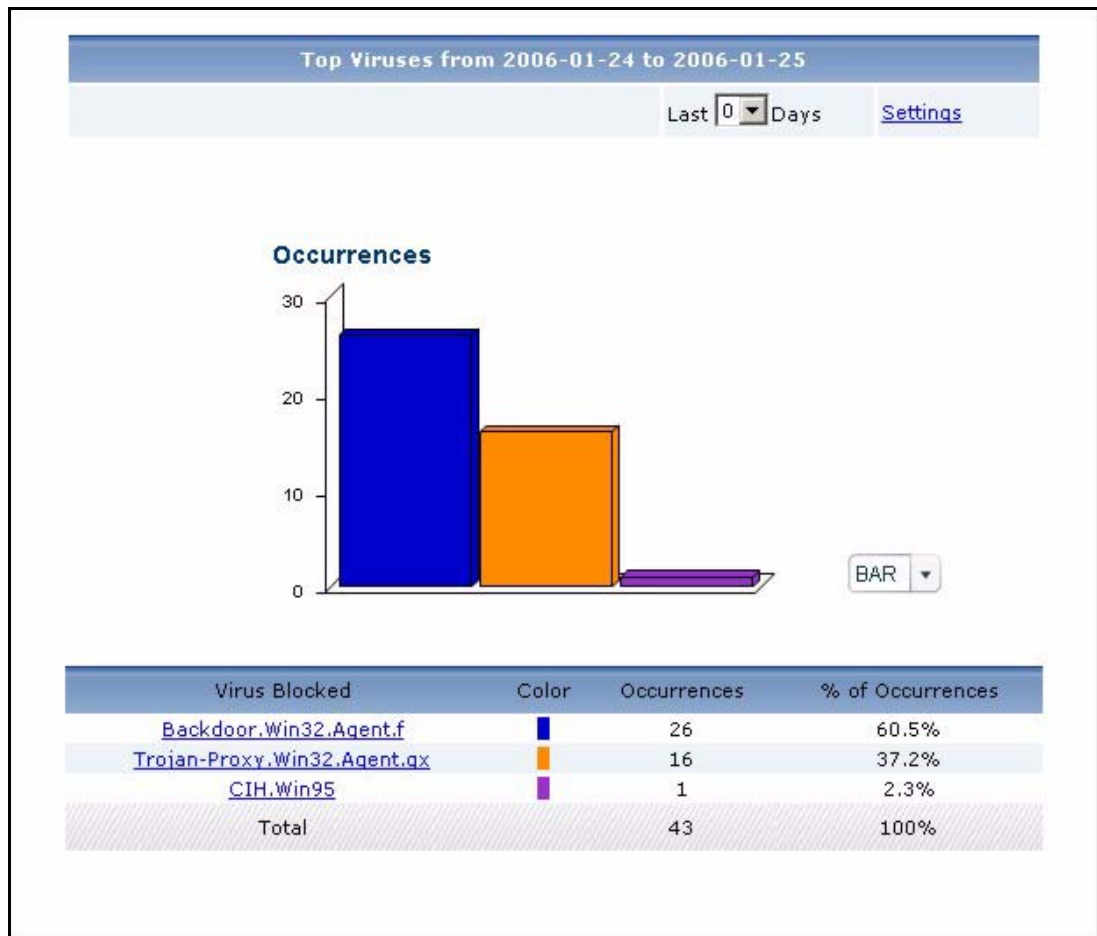
LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

6.3.3 Top Viruses

Use this report to look at the top viruses by number of occurrences.

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.

Click **Network Attack > AntiVirus > Top Viruses** to open this screen.

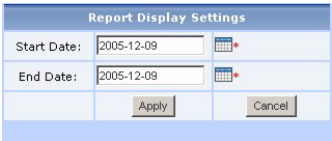
Figure 65 Network Attack > AntiVirus > Top Viruses

Each field is described in the following table.

Table 60 Network Attack > AntiVirus > Top Viruses

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

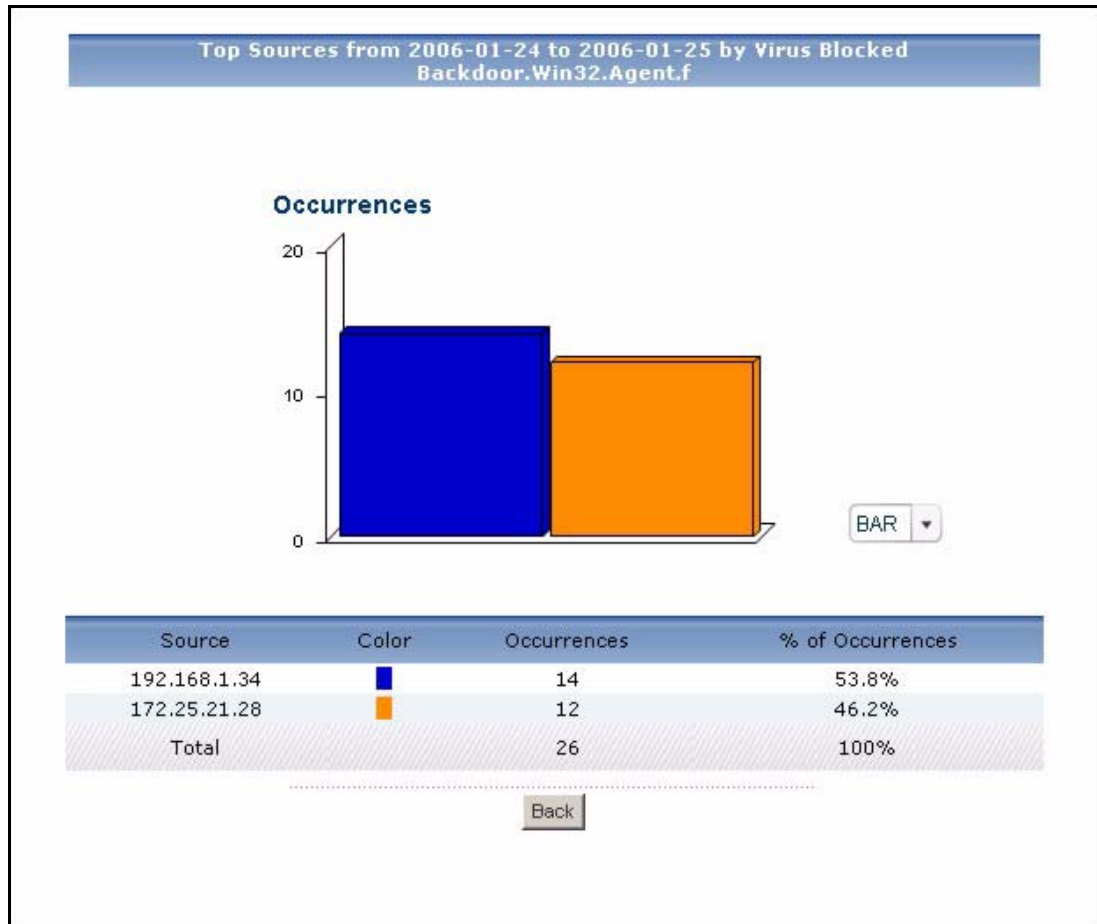
Table 60 Network Attack > AntiVirus > Top Viruses

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	<p>This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one.</p> <p>Click on a virus to look at the top sources for the selected virus. The Top Viruses Drill-Down report appears.</p>
Color	<p>This field displays what color represents each virus in the graph.</p>
Occurrences	<p>This field displays the number of occurrences by each virus.</p>
% of Occurrences	<p>This field displays what percentage of all occurrences was made by each virus.</p>
Total	<p>This entry displays the totals for the viruses above.</p>

6.3.4 Top Viruses Drill-Down

Use this report to look at the top sources of any top virus.

Click on a specific virus in **Network Attack > AntiVirus > Top Viruses** to open this screen.

Figure 66 Network Attack > AntiVirus > Top Viruses > Drill-Down

Each field is described in the following table.

Table 61 Network Attack > AntiVirus > Top Viruses > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.

Table 61 Network Attack > AntiVirus > Top Viruses > Drill-Down

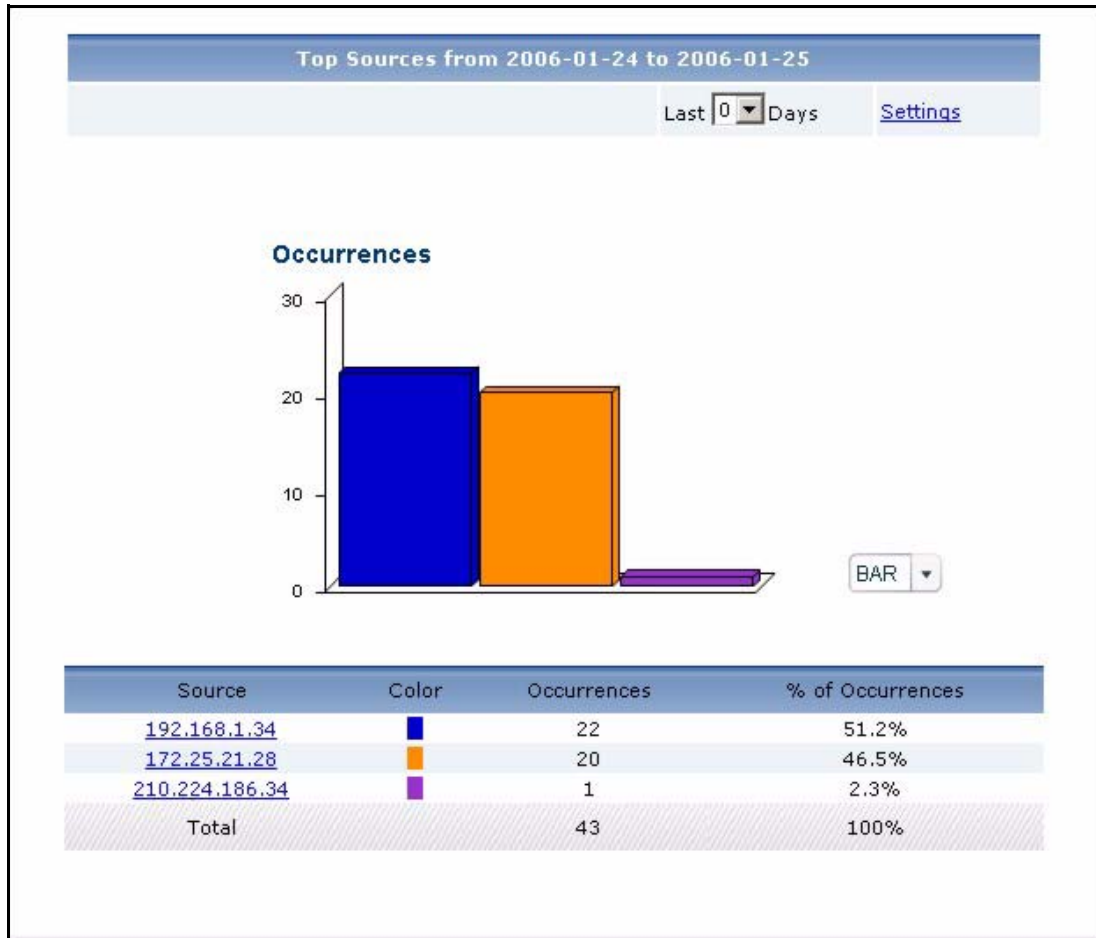
LABEL	DESCRIPTION
Occurrences	This field displays the number of occurrences of the selected virus from each source.
% of Occurrences	This field displays what percentage of all occurrences of the selected virus comes from each source.
Total	This entry displays the totals for the sources above. If the 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.

6.3.5 Top Virus Sources

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

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.

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

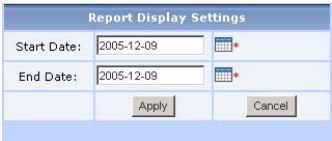
Figure 67 Network Attack > AntiVirus > Top Sources

Each field is described in the following table.

Table 62 Network Attack > AntiVirus > Top Sources

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

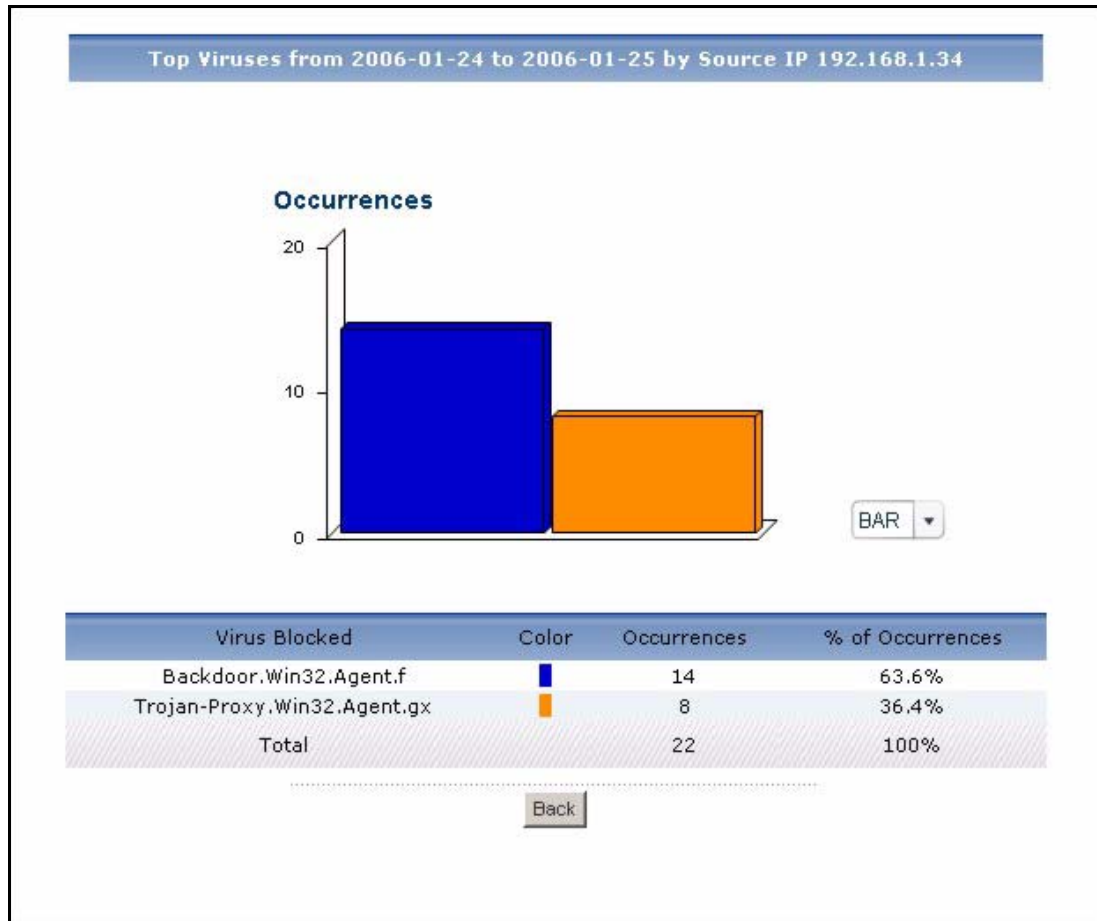
Table 62 Network Attack > AntiVirus > Top Sources

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	<p>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.</p> <p>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").</p> <p>Click on a source to look at the top viruses for the selected source. The Top Virus Sources Drill-Down report appears.</p>
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.
Total	This entry displays the totals for the sources above.

6.3.6 Top Virus Sources Drill-Down

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

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

Figure 68 Network Attack > AntiVirus > Top Sources > Drill-Down

Each field is described in the following table.

Table 63 Network Attack > AntiVirus > Top Sources > 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. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.

Table 63 Network Attack > AntiVirus > Top Sources > Drill-Down

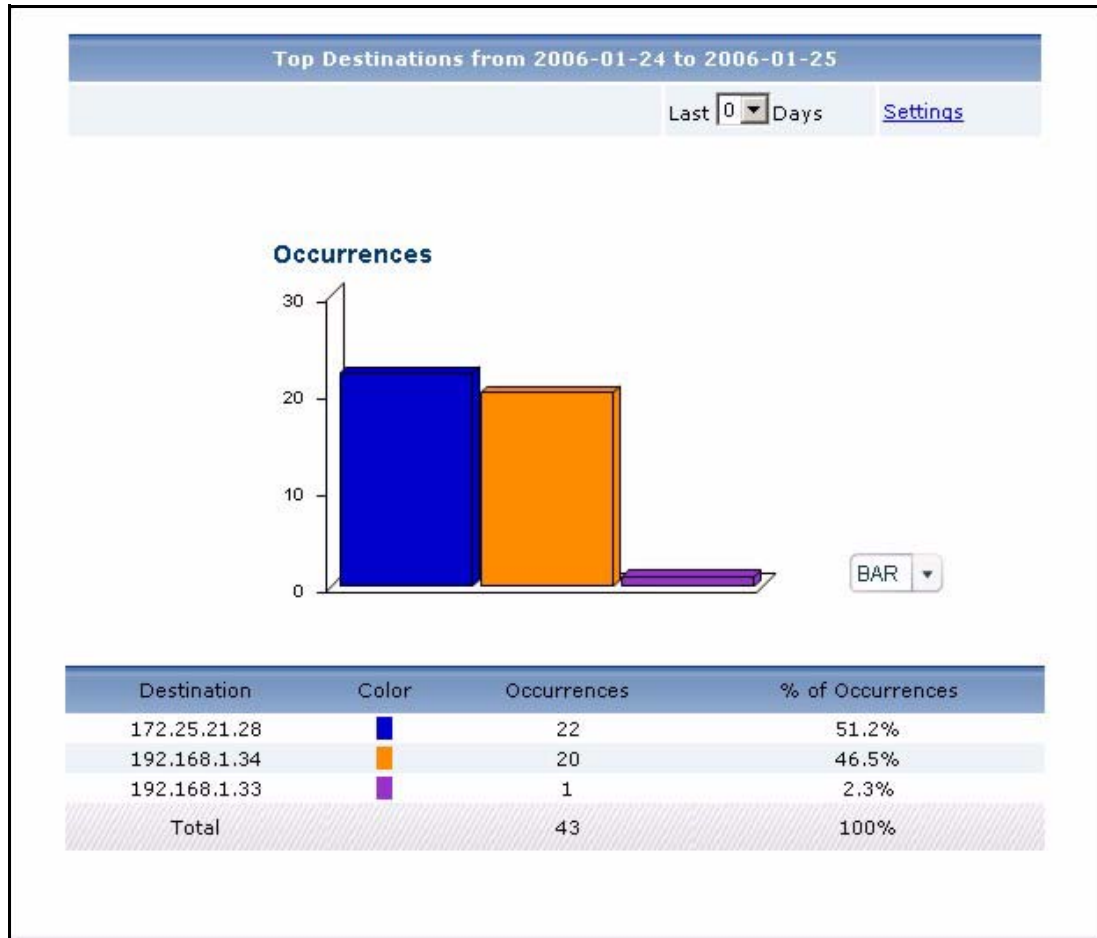
LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

6.3.7 Top Virus Destinations

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

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.

Click **Network Attack > AntiVirus > Top Destinations** to open this screen.

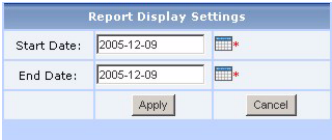
Figure 69 Network Attack > AntiVirus > Top Destinations

Each field is described in the following table.

Table 64 Network Attack > AntiVirus > Top Destinations

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report).

Table 64 Network Attack > AntiVirus > Top Destinations

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report).</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	<p>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.</p> <p>Each destination is identified by its IP address.</p>
Color	<p>This field displays what color represents each destination in the graph.</p>
Occurrences	<p>This field displays the number of occurrences at each destination if the selected device had not blocked the virus.</p>
% of Occurrences	<p>This field displays what percentage of all occurrences were going to each destination.</p>
Total	<p>This entry displays the totals for the destinations above.</p>

6.4 AntiSpam

Use these reports to 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.

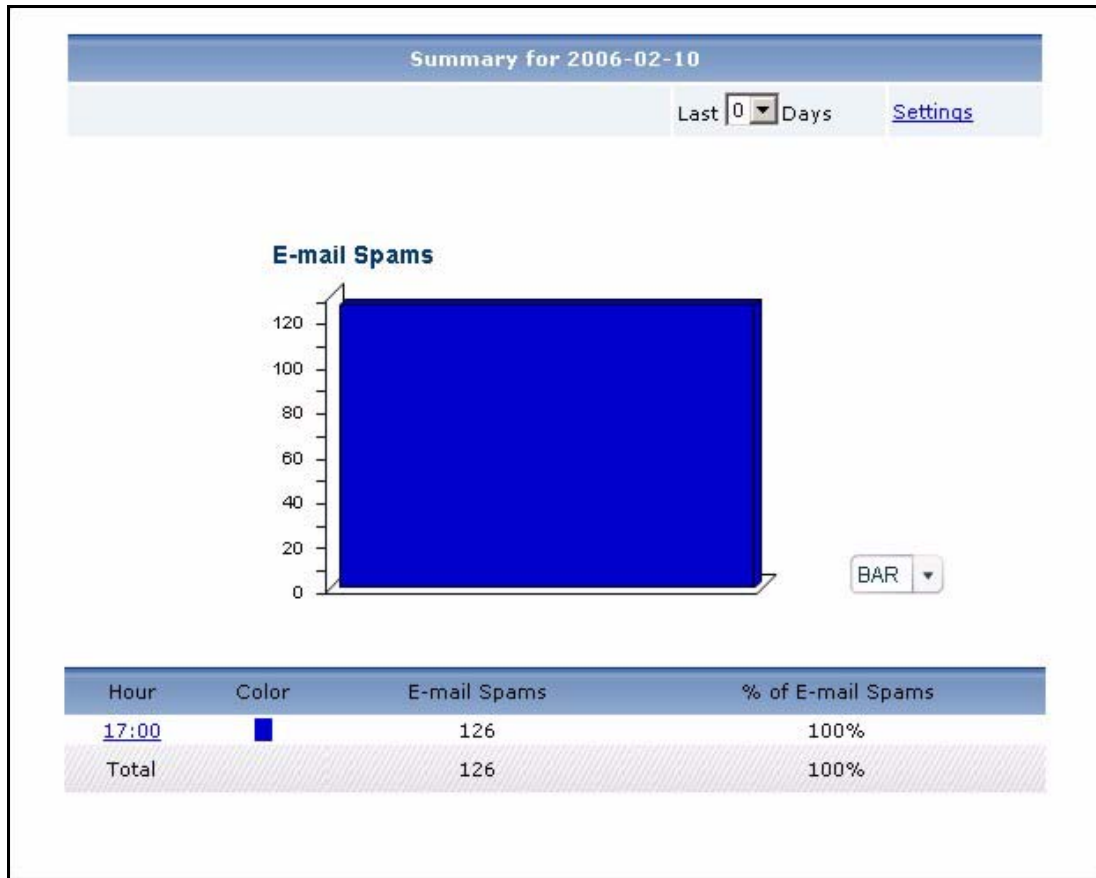
6.4.1 Spam Summary

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

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.

Click **Network Attack > AntiSpam > Summary** to open this screen.

Figure 70 Network Attack > AntiSpam > Summary

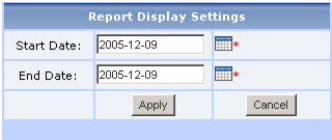


Each field is described in the following table.

Table 65 Network Attack > AntiSpam > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

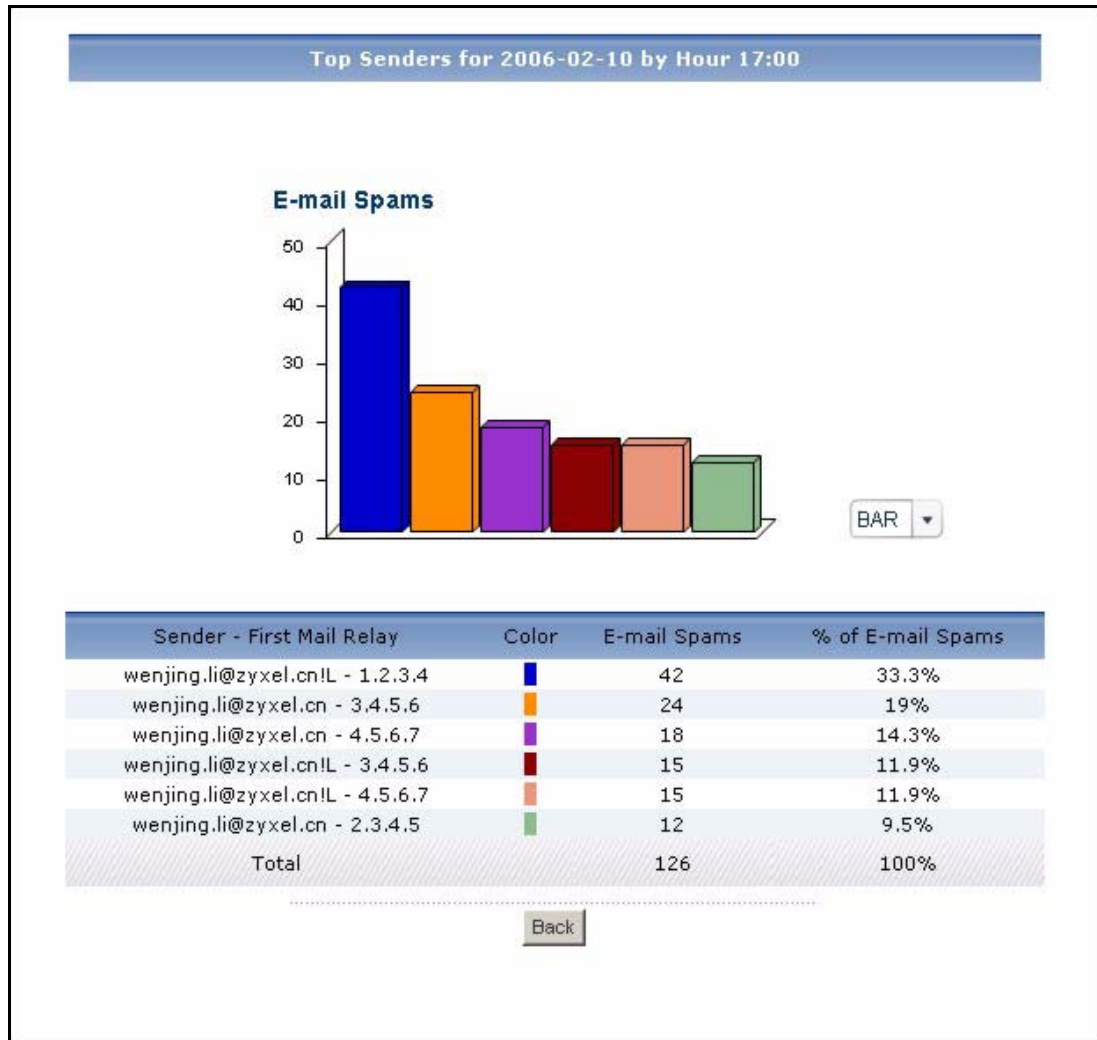
Table 65 Network Attack > AntiSpam > Summary

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top spam messages in the selected time interval. The Spam Summary Drill-Down report appears.</p>
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.
Total	This entry displays the totals for the time intervals above.

6.4.2 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 **Network Attack > AntiSpam > Summary** to open this screen.

Figure 71 Network Attack > AntiSpam > Summary > Drill-Down

Each field is described in the following table.

Table 66 Network Attack > AntiSpam > 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	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 66 Network Attack > AntiSpam > Summary > Drill-Down

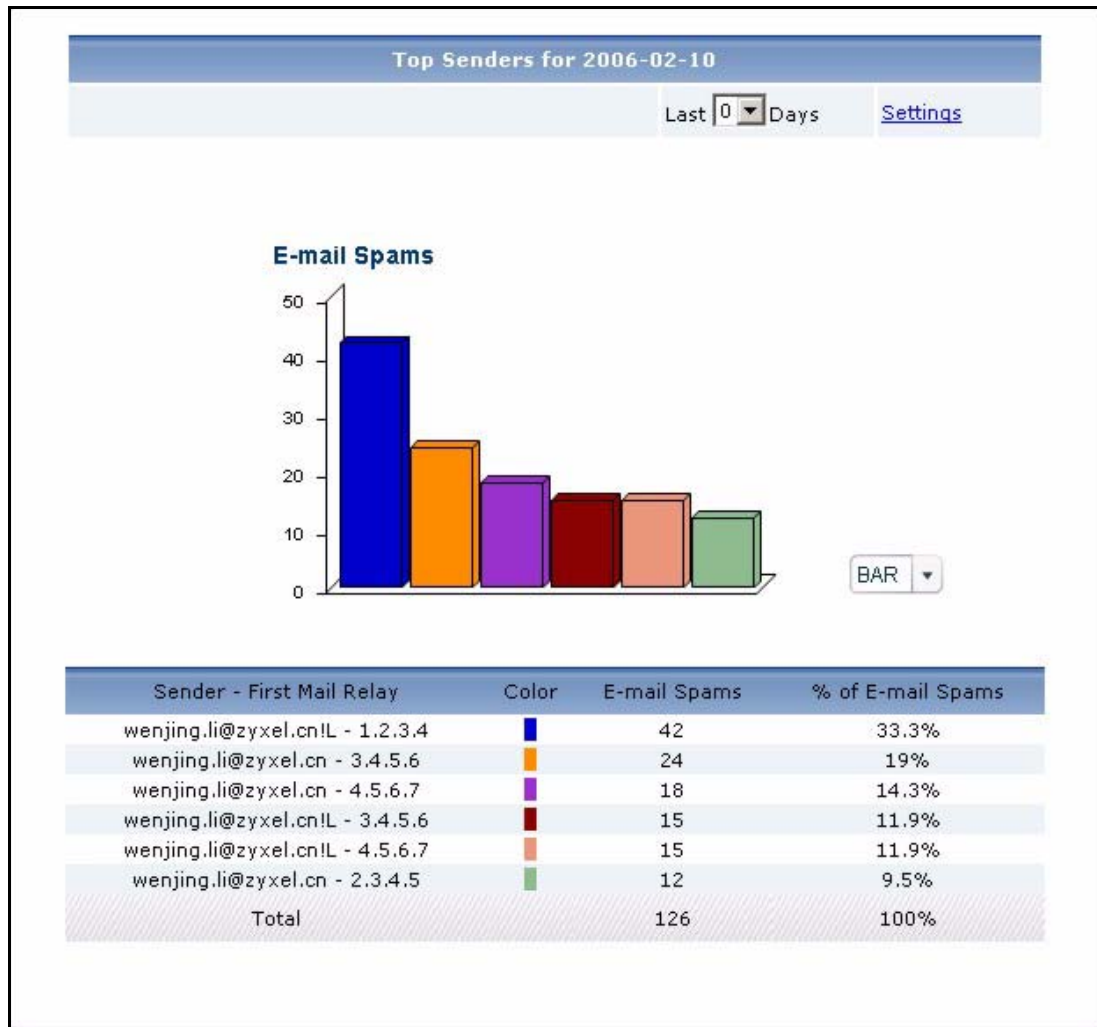
LABEL	DESCRIPTION
Sender - First Mail Relay	This field displays the top combinations of senders of spam and the first SMTP server to which spam is sent in the selected time interval, sorted by the number of spam messages sent for each combination. Each sender is identified by its e-mail address. Each 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.
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.

6.4.3 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.

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.

Click **Network Attack > AntiSpam > Top Senders** to open this screen.

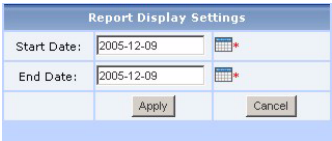
Figure 72 Network Attack > AntiSpam > Top Senders

Each field is described in the following table.

Table 67 Network Attack > AntiSpam > Top Senders

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report).

Table 67 Network Attack > AntiSpam > Top Senders

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report).</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Sender - First Mail Relay	<p>This field displays the top combinations of senders of spam and the first SMTP server to which spam is sent using the selected device, sorted by the number of spam messages sent for each combination.</p> <p>Each sender is identified by its e-mail address.</p> <p>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").</p>
Color	<p>This field displays what color represents each sender in the graph.</p>
E-mail Spams	<p>This field displays how many spam messages each sender sent.</p>
% of E-mail Spams	<p>This field displays what percentage of all spam messages was sent by each sender.</p>
Total	<p>This entry displays the totals for the senders above.</p>

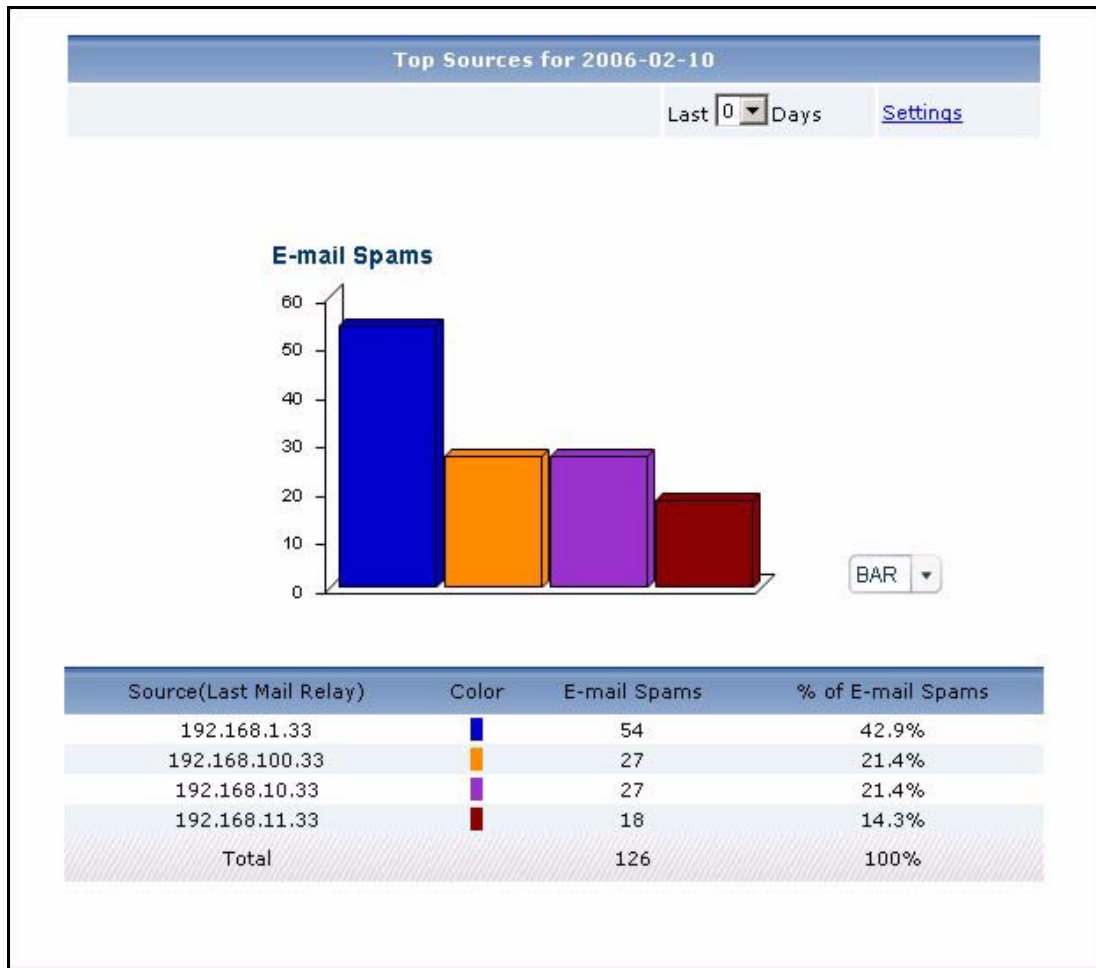
6.4.4 Top Spam Sources

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

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

Figure 73 Network Attack > AntiSpam > Top Sources

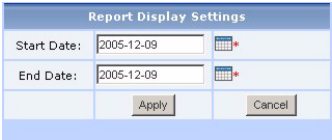


Each field is described in the following table.

Table 68 Network Attack > AntiSpam > Top Sources

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report).

Table 68 Network Attack > AntiSpam > Top Sources

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report).</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source (Last Mail Relay)	<p>This field displays the top SMTP servers that sent spam blocked by 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.</p> <p>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").</p>
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.
Total	This entry displays the totals for the sources above.

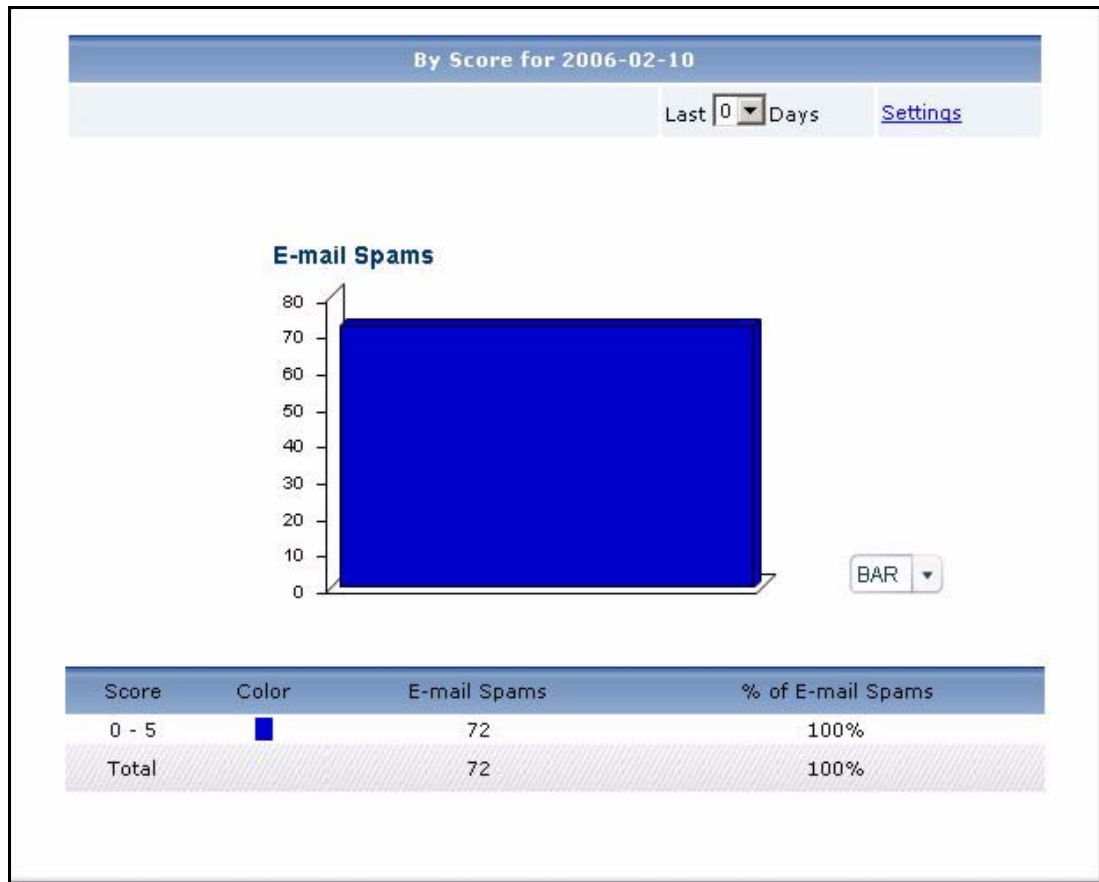
6.4.5 Top Spam Scores

Use this report to look at the top scores calculated for spam messages by number of 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.

Click **Network Attack > AntiSpam > By Score** to open this screen.

Figure 74 Network Attack > AntiSpam > By Score

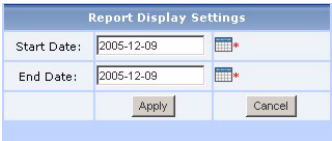


Each field is described in the following table.

Table 69 Network Attack > AntiSpam > By Score

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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report).

Table 69 Network Attack > AntiSpam > By Score

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report).</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Score	<p>This field displays the top 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.</p>
Color	<p>This field displays what color represents each score in the graph.</p>
E-mail Spams	<p>This field displays the number of spam messages from each score.</p>
% of E-mail Spams	<p>This field displays what percentage of all spam messages came from each score.</p>
Total	<p>This entry displays the totals for the scores above.</p>

CHAPTER 7

Security Policy

Use these reports to look at the top sources and destinations of traffic that is allowed or blocked based on each device's content filtering settings. You can also look at the amount of traffic forwarded or blocked by time interval.

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 **Allow Web Sites** and **Block Web Sites** are enabled.

7.1 Blocked Web Accesses

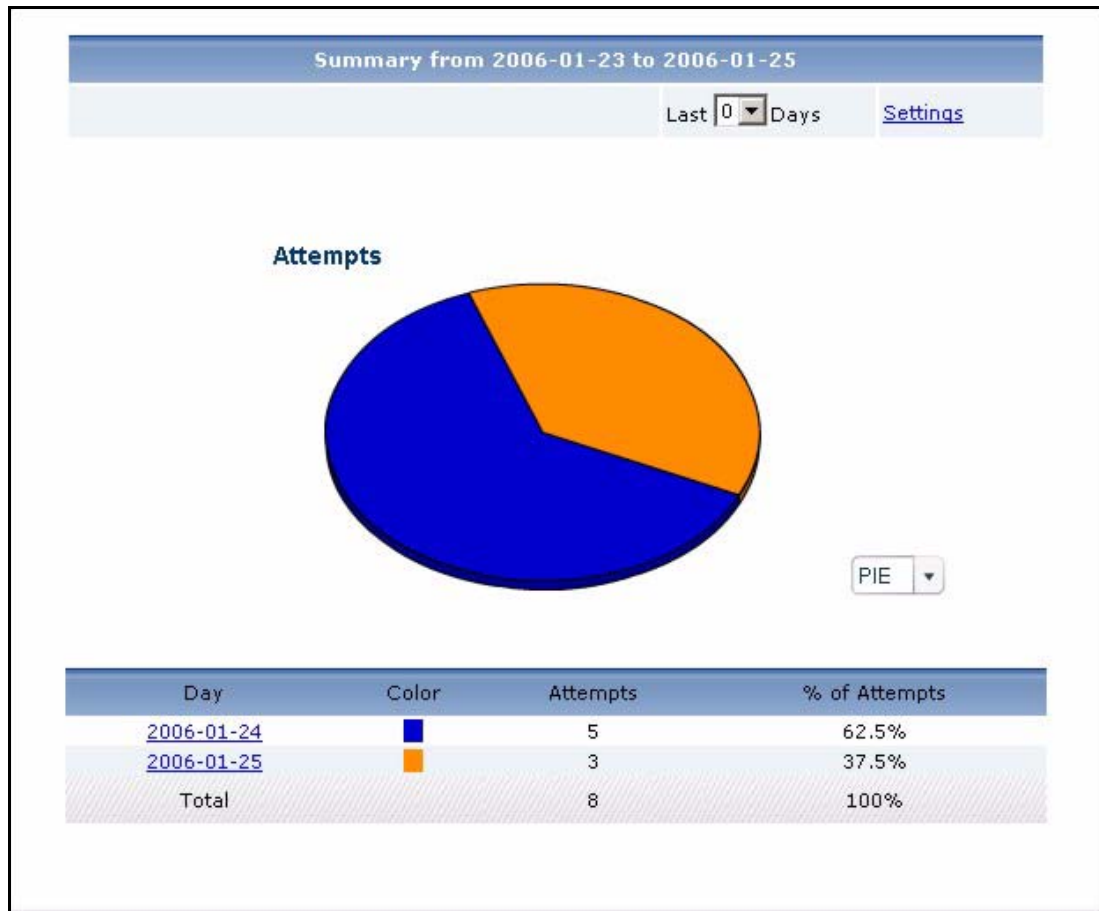
Use this report to look at the number of attempts to access blocked web sites by time interval as well as top blocked sites and hosts.

7.1.1 Web Block 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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Blocked > Summary** to open this screen.

Figure 75 Security Policy > WEB Blocked > Summary

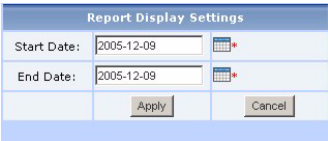


Each field is described in the following table.

Table 70 Security Policy > WEB 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 70 Security Policy > WEB Blocked > Summary

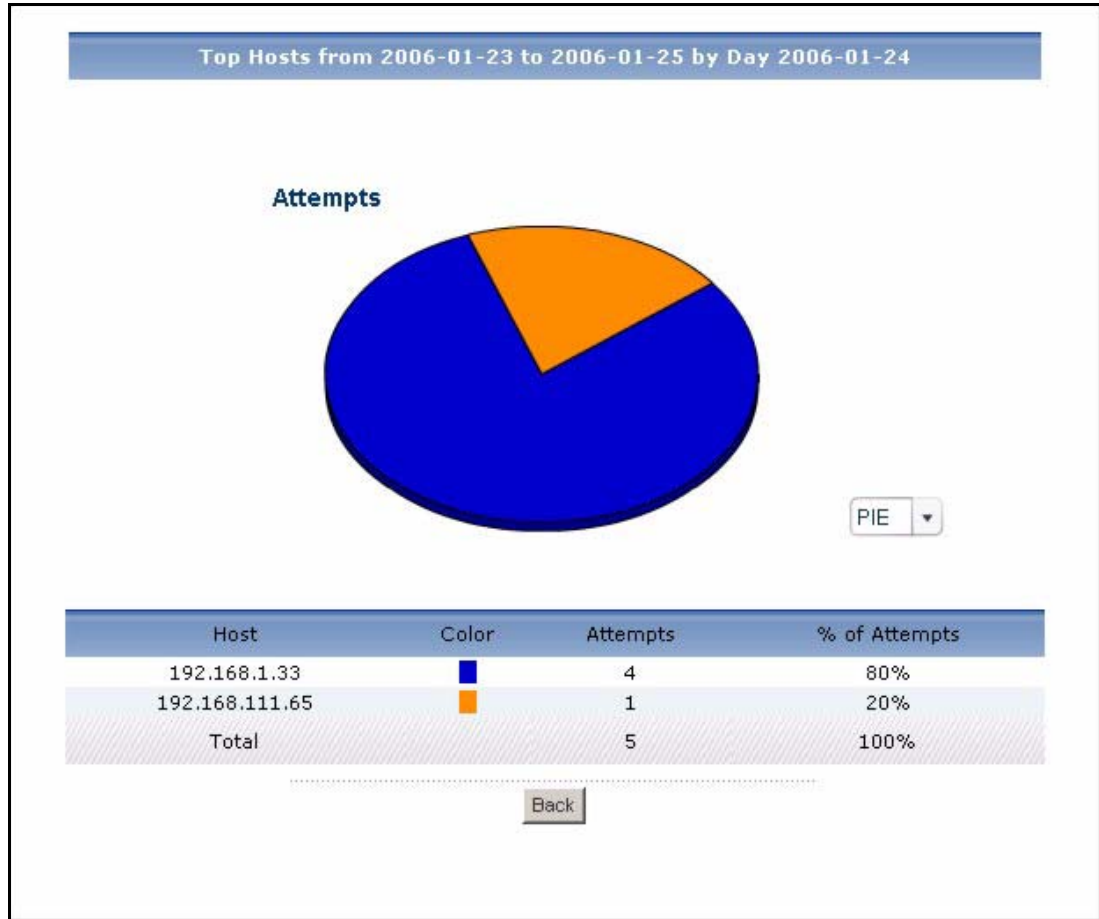
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval. The Web Block Summary Drill-Down report appears.</p>
Color	<p>This field displays what color represents each time interval in the graph.</p>
Attempts	<p>This field displays the number of attempts by each source to access blocked web sites in the selected time interval.</p>
% of Attempts	<p>This field displays what percentage of all attempts was handled in each time interval.</p>
Total	<p>This entry displays the totals for the time intervals above.</p>

7.1.2 Web Block 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 **Security Policy > WEB Blocked > Summary** to open this screen.

Figure 76 Security Policy > WEB Blocked > Summary > Drill-Down



Each field is described in the following table.

Table 71 Security Policy > WEB 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. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how much traffic (in megabytes) the device handled for each source in the selected time interval.
% of Attempts	This field displays what percentage of all traffic in the selected time interval was attributed to each source.

Table 71 Security Policy > WEB Blocked > Summary > Drill-Down

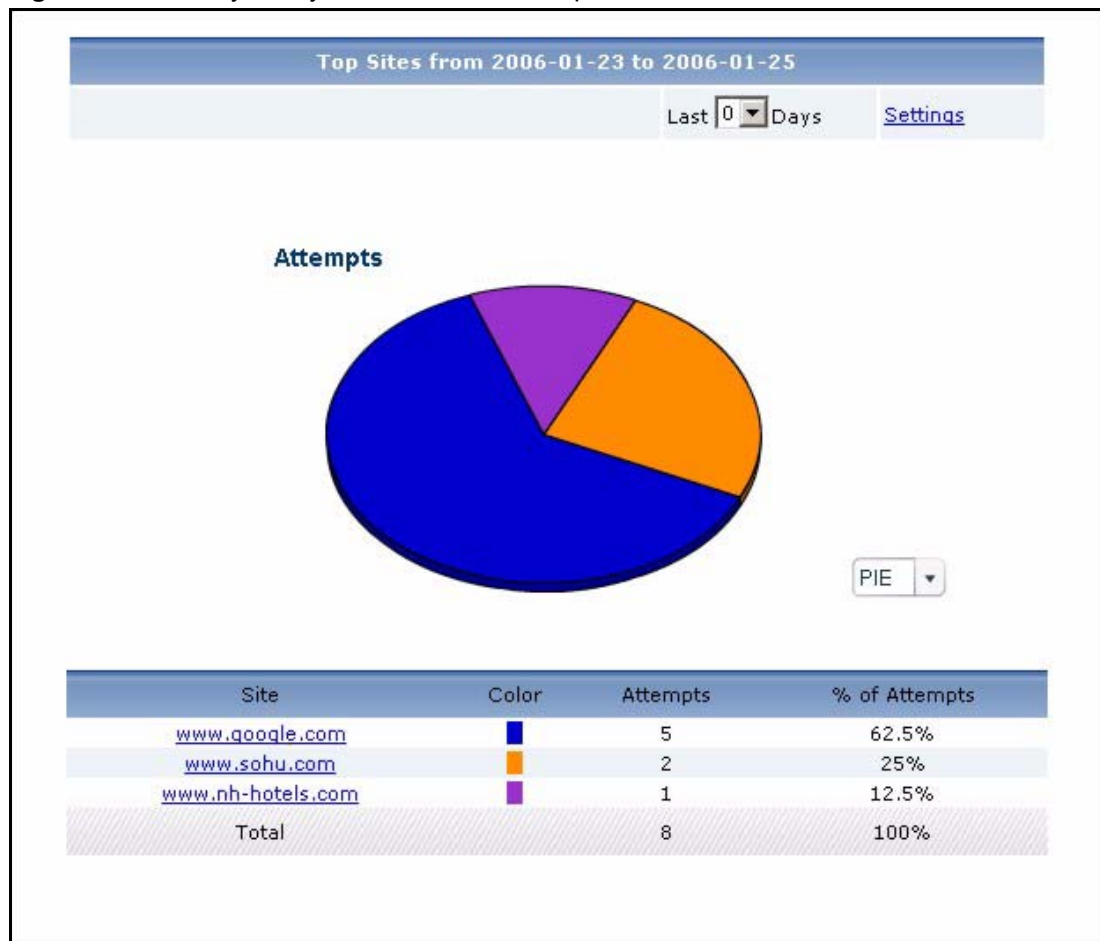
LABEL	DESCRIPTION
Total	This entry displays the totals for the sources above. If the number of sources in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.1.3 Top Blocked 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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Blocked > Top Sites** to open this screen.

Figure 77 Security Policy > WEB Blocked > Top Sites

Each field is described in the following table.

Table 72 Security Policy > WEB Blocked > Top Sites

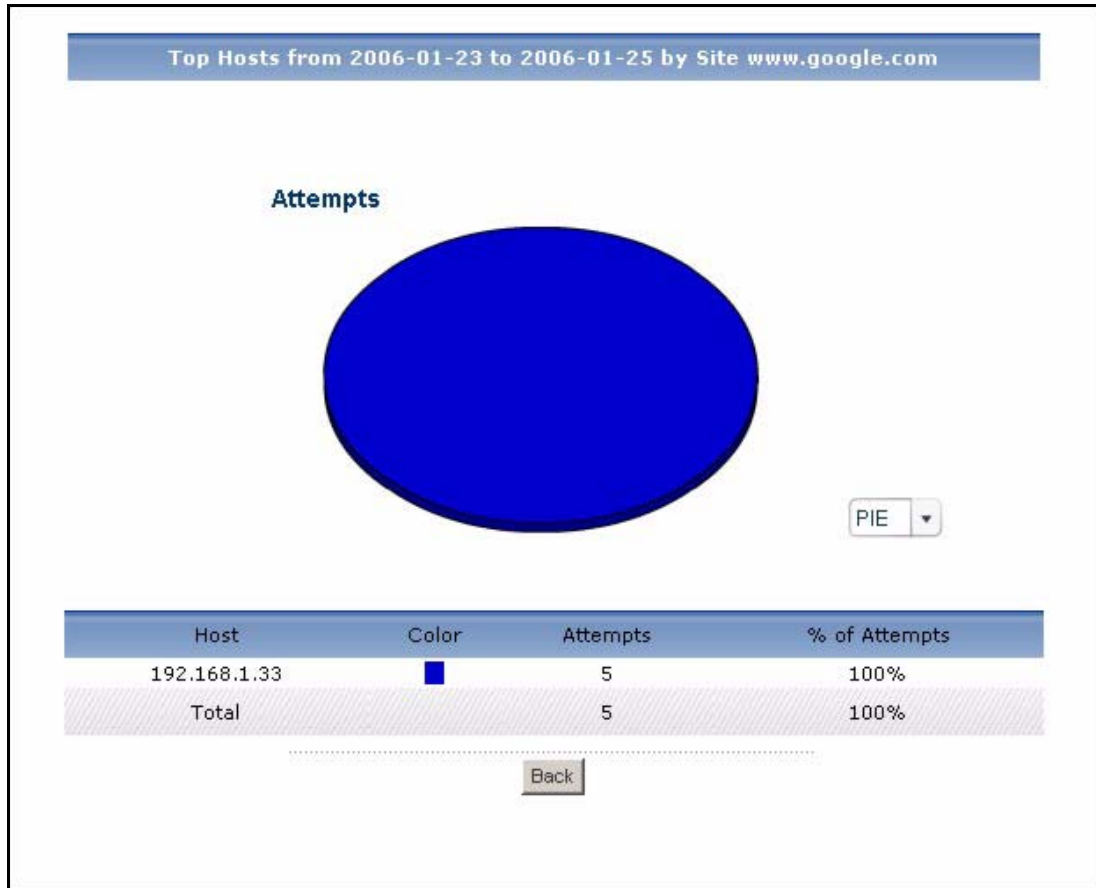
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="837 737 1166 877" data-label="Image"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	<p>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.</p> <p>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. The Top Blocked Web Sites Drill-Down report appears.</p>
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.
Total	This entry displays the totals for the destinations above.

7.1.4 Top Blocked Web 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 **Security Policy > WEB Blocked > Top Sites** to open this screen.

Figure 78 Security Policy > WEB Blocked > Top Sites > Drill-Down



Each field is described in the following table.

Table 73 Security Policy > WEB 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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.
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.

Table 73 Security Policy > WEB Blocked > Top Sites > Drill-Down

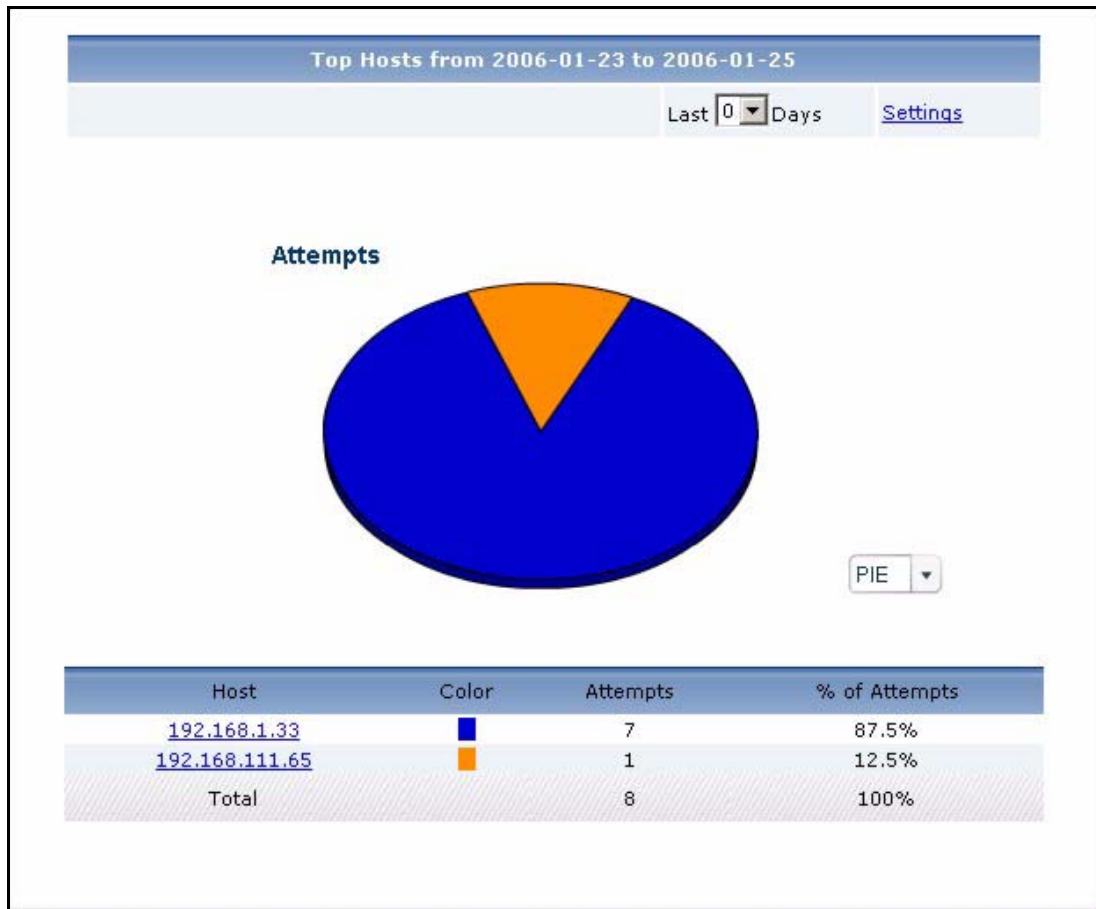
LABEL	DESCRIPTION
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by each source to the selected destination.
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater 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.

7.1.5 Top Blocked Web 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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Blocked > Top Hosts** to open this screen.

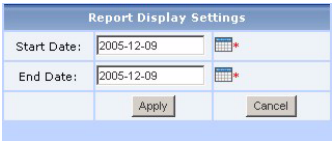
Figure 79 Security Policy > WEB Blocked > Top Hosts

Each field is described in the following table.

Table 74 Security Policy > WEB 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

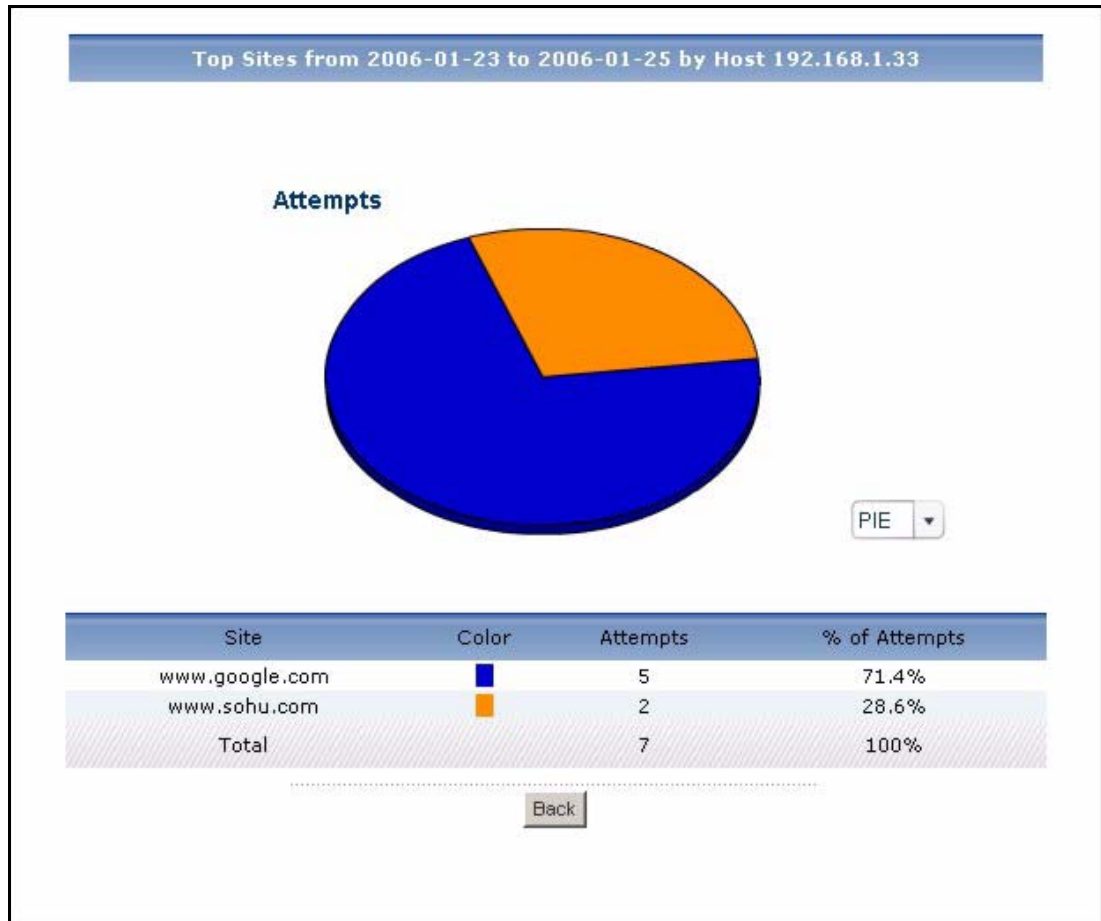
Table 74 Security Policy > WEB Blocked > Top Hosts

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>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.</p> <p>Each source is identified by its IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source. The Top Blocked Web Hosts Drill-Down report appears.</p>
Color	<p>This field displays what color represents each source in the graph.</p>
Attempts	<p>This field displays how much traffic (in megabytes) the device handled for each source.</p>
% of Attempts	<p>This field displays what percentage of all attempts to access blocked web sites was made from each source.</p>
Total	<p>This entry displays the totals for the sources above.</p>

7.1.6 Top Blocked Web 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 **Security Policy > WEB Blocked > Top Hosts** to open this screen.

Figure 80 Security Policy > WEB Blocked > Top Hosts > Drill-Down

Each field is described in the following table.

Table 75 Security Policy > WEB 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. 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.

Table 75 Security Policy > WEB Blocked > Top Hosts > Drill-Down

LABEL	DESCRIPTION
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.

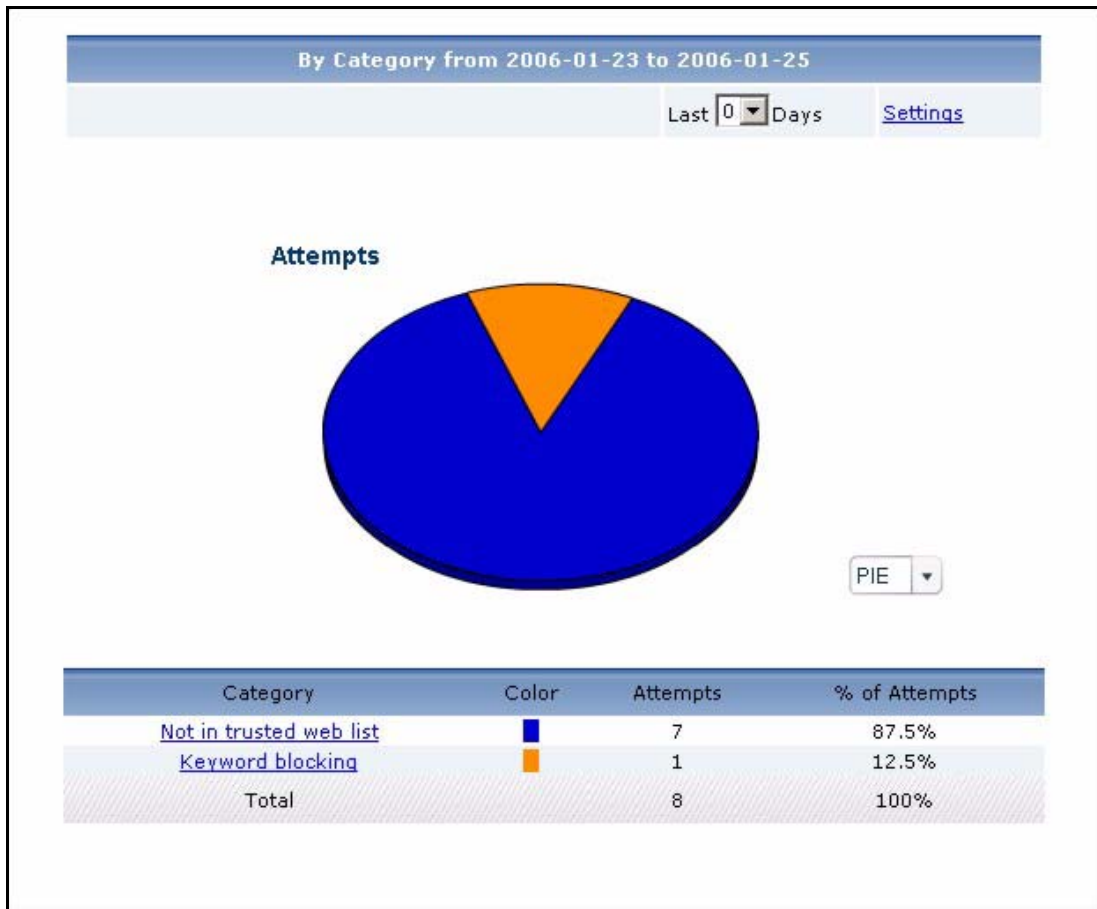
7.1.7 Top Blocked Web Categories

Use this report to look at the top 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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Blocked > By Category** to open this screen.

Figure 81 Security Policy > WEB Blocked > By Category



Each field is described in the following table.

Table 76 Security Policy > WEB Blocked > By Category

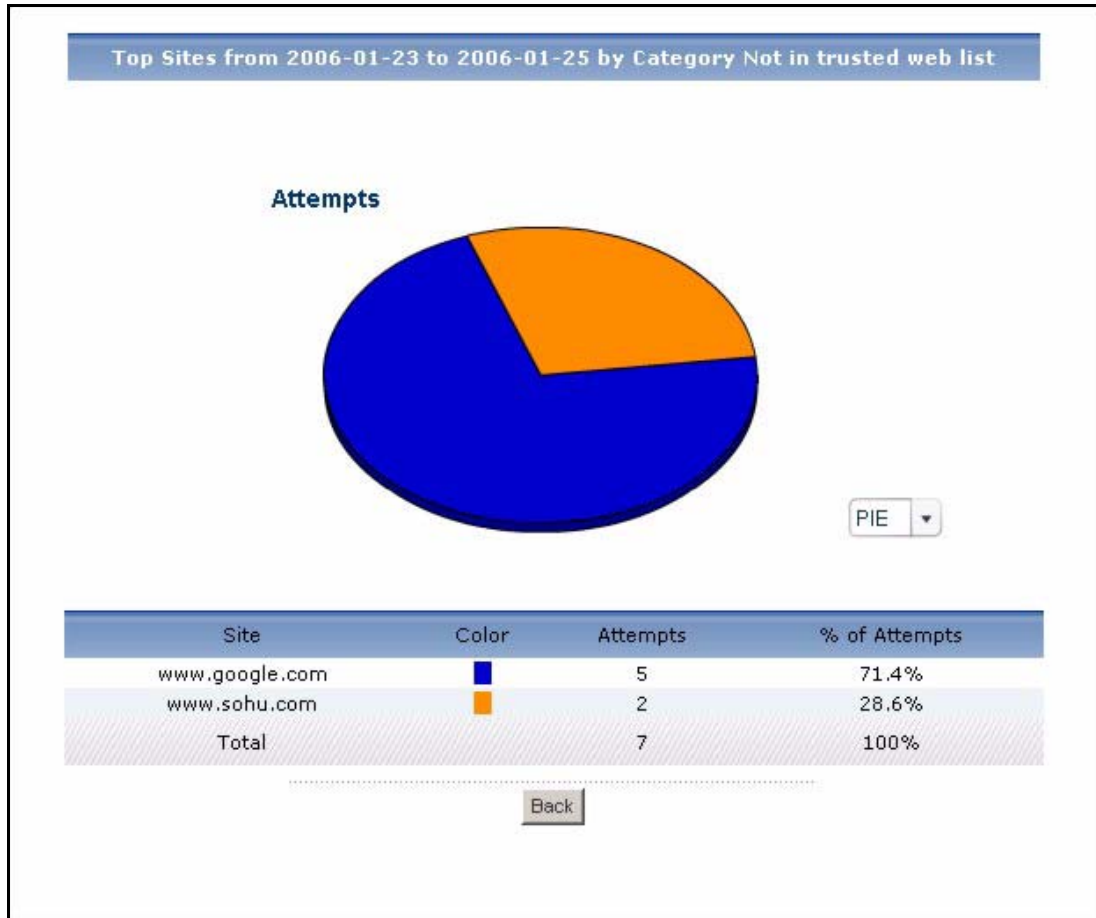
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="841 737 1166 877" style="text-align: center;"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	<p>This field displays the top categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of categories is less than the maximum number of records displayed in this table, every source is displayed.</p> <p>Click on a source to look at the top destinations of blocked web traffic for the selected category. The Top Blocked Web Categories Drill-Down report appears.</p>
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.
Total	This entry displays the totals for the categories above.

7.1.8 Top Blocked Web Categories Drill-Down

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

Click on a specific category in **Security Policy > WEB Blocked > By Category** to open this screen.

Figure 82 Security Policy > WEB Blocked > By Category > Drill-Down



Each field is described in the following table.

Table 77 Security Policy > WEB 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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 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 77 Security Policy > WEB Blocked > 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.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts in the selected category 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 Allowed Web Accesses

Use this report to look at the number of attempts to access allowed web sites by time interval as well as top allowed sites and hosts.

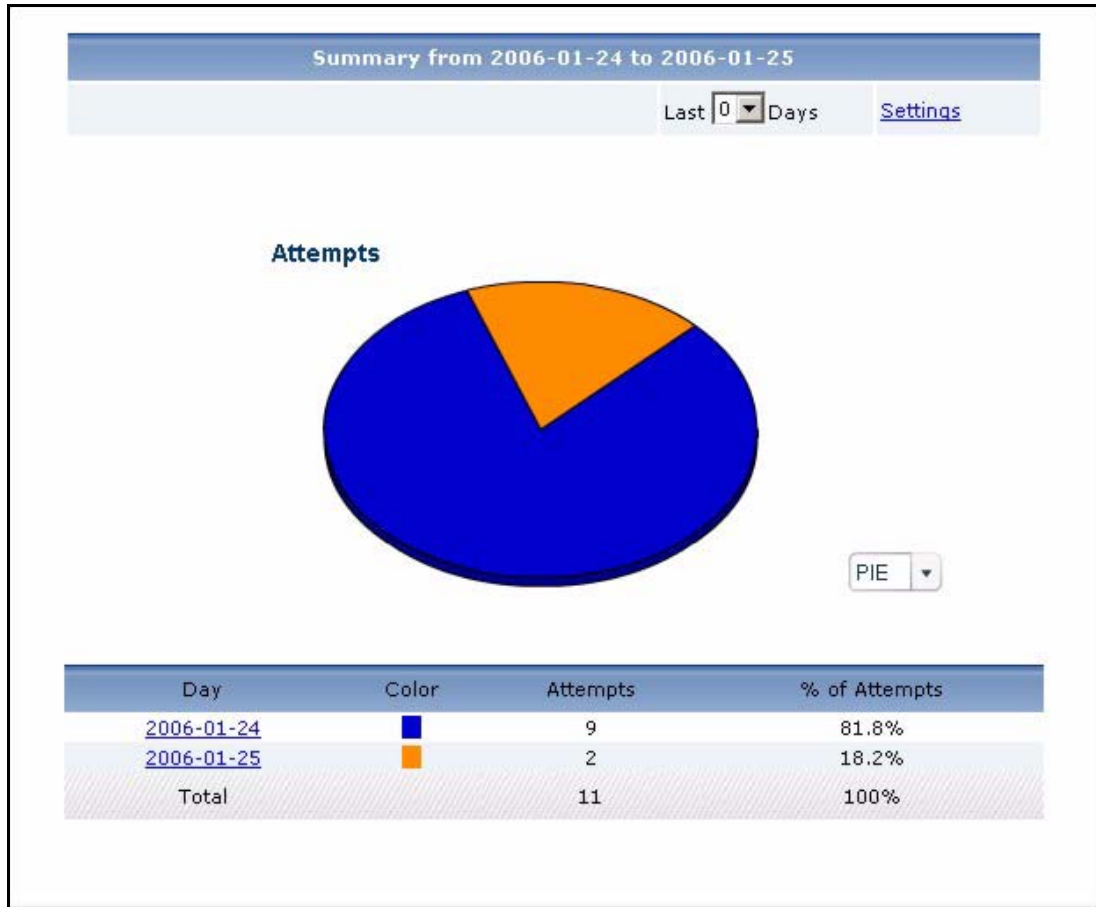
7.2.1 Web Allowed Summary

Use this report to look at the number of attempts to access allowed web sites by time interval.

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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Allowed > Summary** to open this screen.

Figure 83 Security Policy > WEB Allowed > Summary

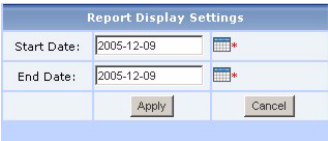


Each field is described in the following table.

Table 78 Security Policy > WEB Allowed > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 78 Security Policy > WEB Allowed > Summary

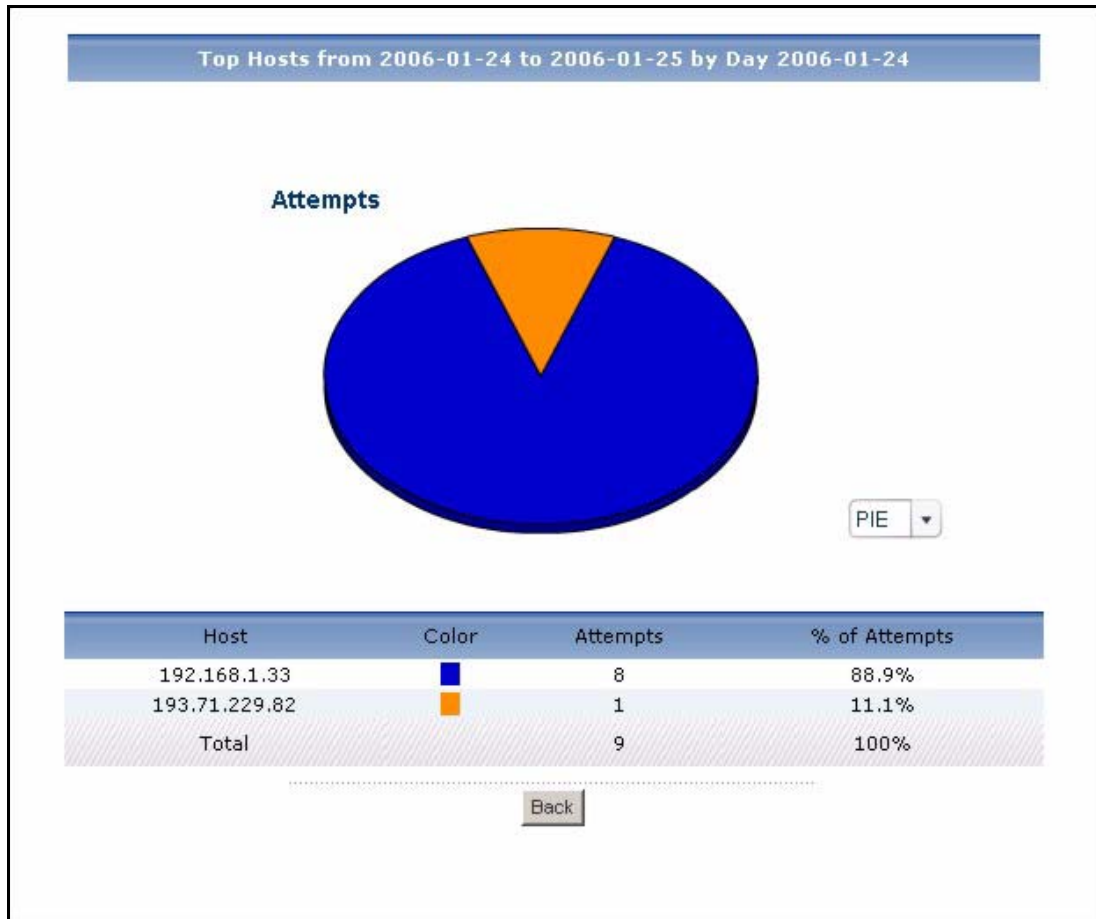
LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>Select a specific Start Date and End Date. The date range can be up to 30 days long, but you cannot include 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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	<p>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.</p> <p>Click on a time interval to look at the top sources of attempts to access allowed web sites in the selected time interval. The Web Allowed Summary Drill-Down report appears.</p>
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts to access allowed web sites in each time interval.
% of Attempts	This field displays the percentage of all attempts in each time interval.
Total	This entry displays the totals for the time intervals above.

7.2.2 Web Allowed Summary Drill-Down

Use this report to look at the top sources of attempts to access allowed web sites in a specific time interval.

Click on a specific time interval in **Security Policy > WEB Allowed > Summary** to open this screen.

Figure 84 Security Policy > WEB Allowed > Summary > Drill-Down



Each field is described in the following table.

Table 79 Security Policy > WEB Allowed > 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. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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 allowed web sites in the selected time interval, sorted by the number of attempts by each one. Each source is identified by its 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 allowed 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.

Table 79 Security Policy > WEB Allowed > Summary > Drill-Down

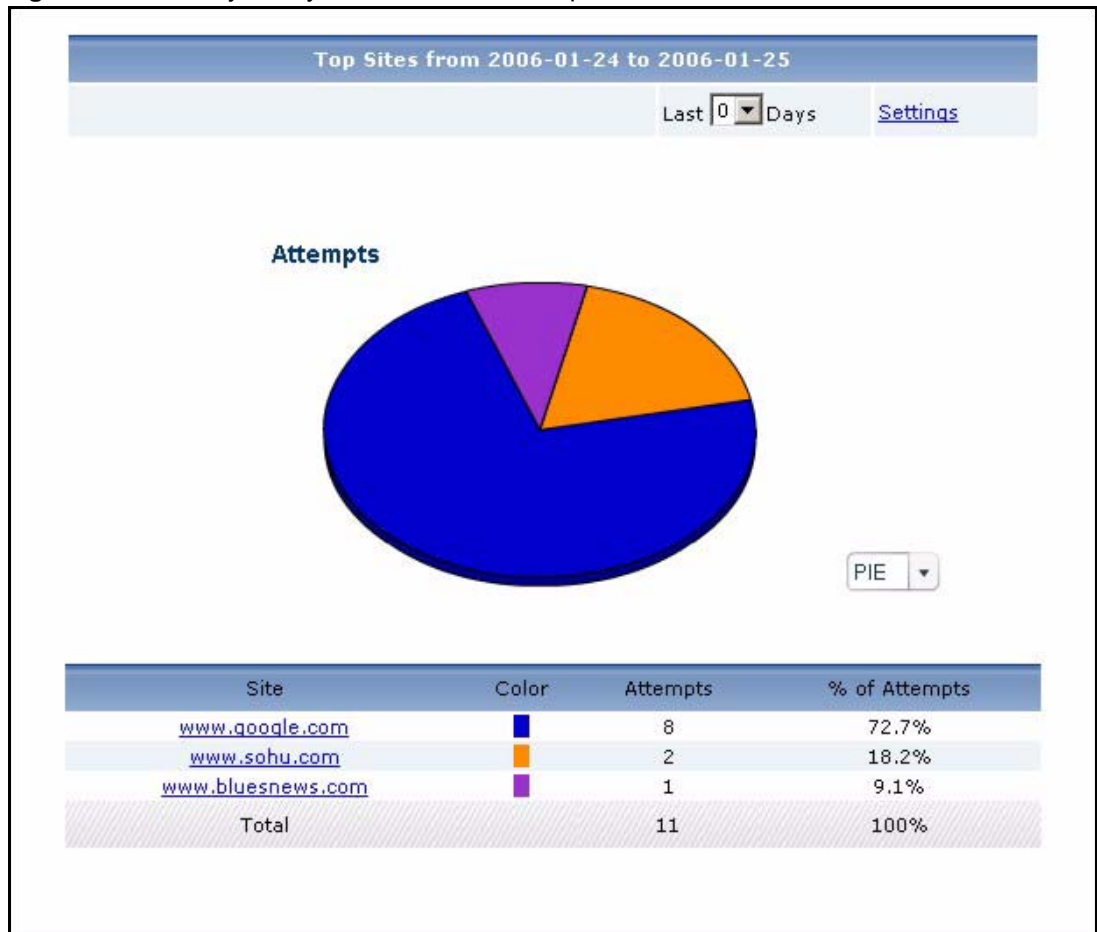
LABEL	DESCRIPTION
Total	This entry displays the totals for the sources above. If the number of sources in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

7.2.3 Top Allowed Web Sites

Use this report to look at the top destinations of forwarded 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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Allowed > Top Sites** to open this screen.

Figure 85 Security Policy > WEB Allowed > Top Sites

Each field is described in the following table.

Table 80 Security Policy > WEB Allowed > Top Sites

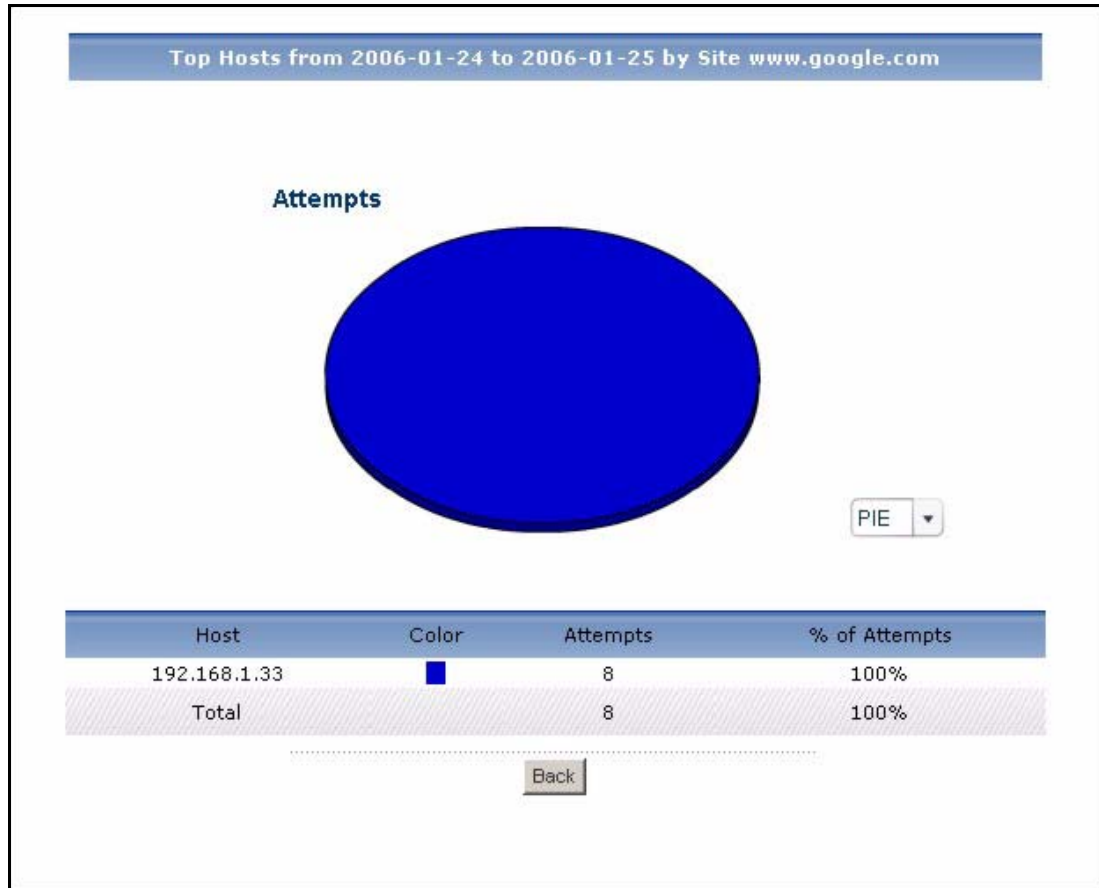
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the Last Days or Settings fields.
Last ... Days	<p>Use this field or Settings to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p> <div data-bbox="836 737 1166 877" style="text-align: center;"> </div> <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	<p>This field displays the top destinations of forwarded 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.</p> <p>Each destination is identified by its domain name. Click on a destination to look at the top sources of forwarded web traffic for the selected destination. The Top Forwarded Web Sites Drill-Down report appears.</p>
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 allowed web sites was made to each destination.
Total	This entry displays the totals for the destinations above.

7.2.4 Top Allowed Web Sites Drill-Down

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

Click on a specific destination in **Security Policy > WEB Allowed > Top Sites** to open this screen.

Figure 86 Security Policy > WEB Allowed > Top Sites > Drill-Down



Each field is described in the following table.

Table 81 Security Policy > WEB Allowed > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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 forwarded web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its 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.

Table 81 Security Policy > WEB Allowed > Top Sites > Drill-Down

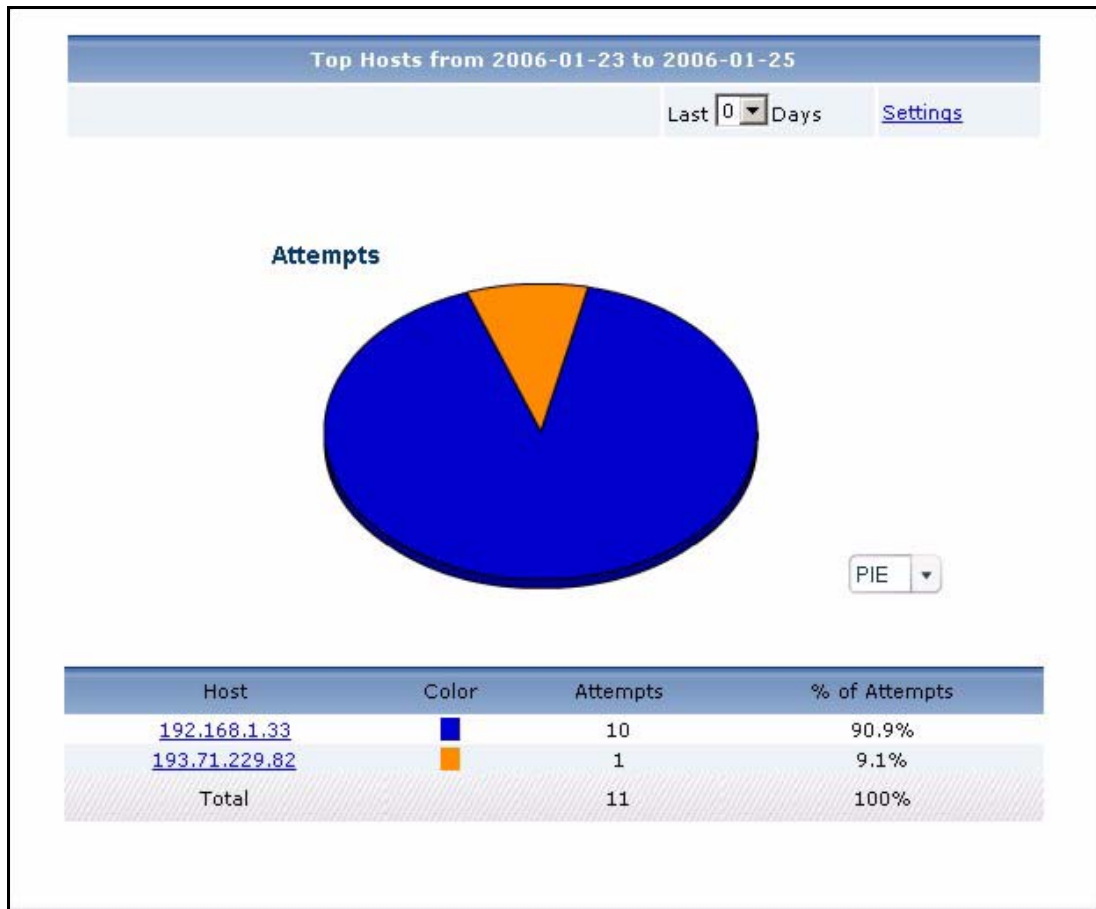
LABEL	DESCRIPTION
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made by each source to the selected destination.
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater 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.

7.2.5 Top Allowed Web Hosts

Use this report to look at the top sources of forwarded 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 **Allow Web Sites** and **Block Web Sites** are enabled.

Click **Security Policy > WEB Allowed > Top Hosts** to open this screen.

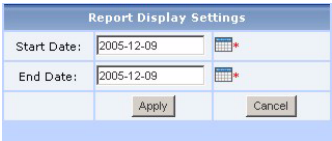
Figure 87 Security Policy > WEB Allowed > Top Hosts

Each field is described in the following table.

Table 82 Security Policy > WEB Allowed > 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. This field returns to zero, so you can refresh the report by selecting it again. 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 function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.

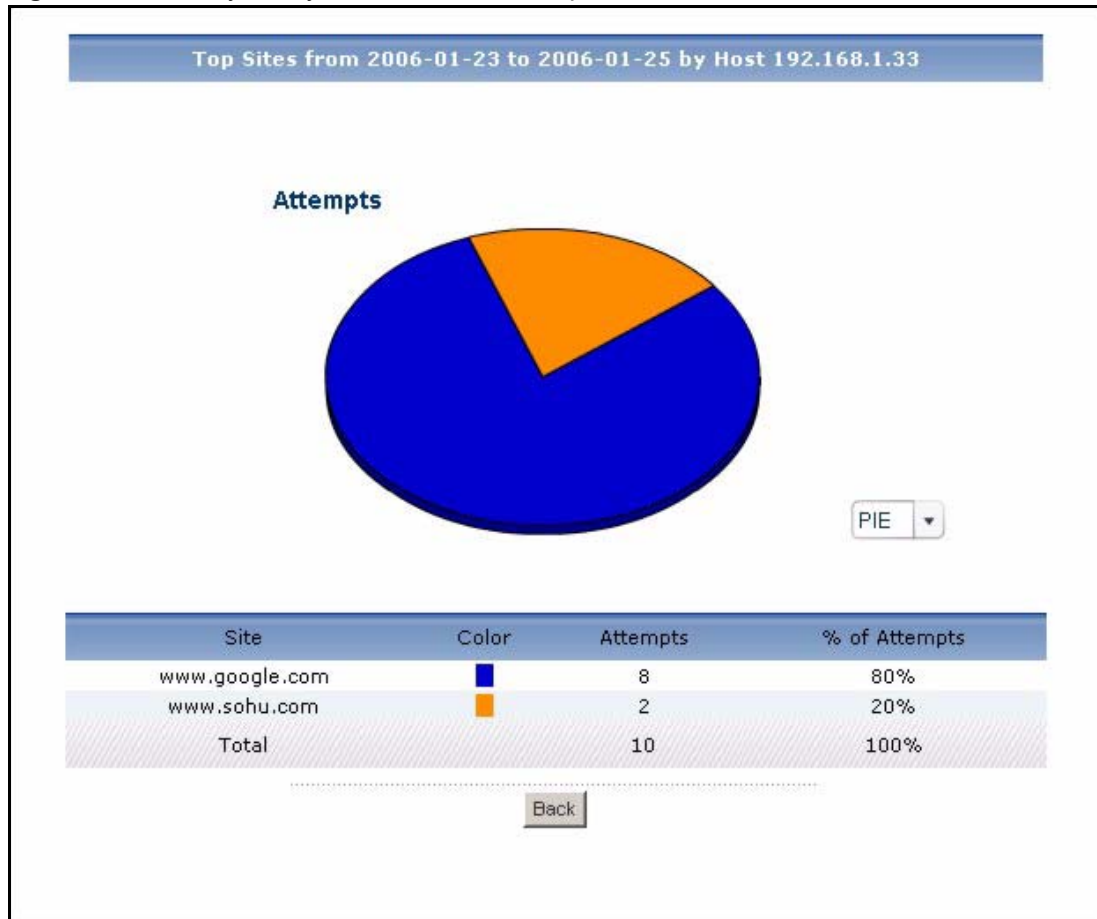
Table 82 Security Policy > WEB Allowed > Top Hosts

LABEL	DESCRIPTION
Settings	<p>Use this field or Last ... Days to specify what historical information is included in the report. Click Settings. The Report Display Settings screen appears.</p>  <p>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.</p> <p>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.</p>
graph	<p>The graph displays the information in the table visually.</p> <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	<p>This field displays the top sources of forwarded 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.</p> <p>Each source is identified by its IP address. Click on a source to look at the top destinations of forwarded web traffic for the selected source. The Top Forwarded Web Hosts Drill-Down report appears.</p>
Color	<p>This field displays what color represents each source in the graph.</p>
Attempts	<p>This field displays how much traffic (in megabytes) the device handled for each source.</p>
% of Attempts	<p>This field displays what percentage of all attempts to access allowed web sites was made from each sources.</p>
Total	<p>This entry displays the totals for the sources above.</p>

7.2.6 Top Allowed Web Hosts Drill-Down

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

Click on a specific source in **Security Policy > WEB Allowed > Top Hosts** to open this screen.

Figure 88 Security Policy > WEB Allowed > Top Hosts > Drill-Down

Each field is described in the following table.

Table 83 Security Policy > WEB Allowed > 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.
graph	The graph displays the information in the table visually. <ul style="list-style-type: none"> • Select PIE chart or BAR chart in the drop-down list box. 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. The yellow conversation box identifies the slice or bar. • 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 forwarded 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.

Table 83 Security Policy > WEB Allowed > Top Hosts > Drill-Down

LABEL	DESCRIPTION
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.

CHAPTER 8

Authentication

Use these screens to look at who successfully logged into the ZyXEL device (for management or monitoring purposes) or who tried to log in but failed.

8.1 Successful Login Screen

Use this screen to look at who successfully logged into the ZyXEL device (for management or monitoring purposes). See [section 2.4 on page 28](#) 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 **Event > Device Login > Successful Login** to open the **Successful Login** screen.

Figure 89 Event > Device Login > Successful Login

Successful Login from 2006-01-19 to 2006-01-25		
		Last <input type="text" value="0"/> Days Settings
Time	Login User	Login Type
2006-01-24 09:13:19	admin	SMT
2006-01-24 09:13:15	admin	SMT
2006-01-24 09:11:46	admin	SMT
2006-01-24 09:10:47	admin	SMT
Total Count:4 Total Page:1 First 1 Last <input type="text"/> Go		

Each field is described in the following table.

Table 84 Event > Device Login > Successful Login

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	Select how many more days of information, ending with current information today, you want to look at. Select 0 if you only want to look at today's information.

Table 84 Event > Device Login > Successful Login

LABEL	DESCRIPTION
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 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.
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.s
Go	Enter the page number you want to see, and click Go .

8.2 Failed Login Screen

Use this screen to look at who tried to log in into the ZyXEL device (for management or monitoring purposes) but failed. See [section 2.4 on page 28](#) 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 **Event > Device Login > Failed Login** to open the **Failed Login** screen.

Figure 90 Event > Device Login > Failed Login

The screenshot shows a web interface for a 'Failed Login' report. At the top, it says 'Failed Login from 2006-01-19 to 2006-01-25'. Below this is a search filter 'Last 0 Days' and a 'Settings' link. The main part of the screen is a table with three columns: 'Time', 'Login User', and 'Login Type'. The table contains four rows of data, all showing failed login attempts by 'admin' on '2006-01-24'. At the bottom, there is a summary 'Total Count:4 Total Page:1' and navigation links 'First 1 Last' followed by a 'Go' button.

Failed Login from 2006-01-19 to 2006-01-25		
		Last <input type="text" value="0"/> Days Settings
Time	Login User	Login Type
2006-01-24 09:13:19	admin	SMT
2006-01-24 09:13:15	admin	SMT
2006-01-24 09:11:46	admin	SMT
2006-01-24 09:10:47	admin	SMT
Total Count:4 Total Page:1 First 1 Last <input type="text"/> Go		

Each field is described in the following table.

Table 85 Event > Device Login > Failed Login

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	Select how many more days of information, ending with current information today, you want to look at. Select 0 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 used to try unsuccessfully to log into the 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.s
Go	Enter the page number you want to see, and click Go .

CHAPTER 9

Log Viewer

Use these screens to look at all log entries or critical log entries for the selected ZyXEL device.

9.1 Regular Log Viewer

Regular log entries are all the log entries that the selected device records. See [section 2.3 on page 27](#) for more information about update frequencies for regular log entries and critical log entries. See [section 2.4 on page 28](#) for more information about the source data used by the report.

Vantage Report consolidates regular log entries. See [Appendix B on page 216](#) for Vantage Report's internal log consolidation frequency.

Click **Log Viewer** > **All Logs** to look at regular log entries. The screen is shown below.

Figure 91 Log Viewer > All Logs

The screenshot shows the 'Select All Logs' interface. It includes search filters for Day (2005-12-03), Start Time (00:00), End Time (24:00), Start Date, End Date, Category (Traffic Log), and Advanced Search (checked). Below these are fields for Source IP, Destination IP, Keyword, Services ([Custom Service]), Protocol (All), and Port. Search and Reset buttons are present. A table of log entries follows, with columns for Time, Source:Port, Destination:Port, Category, and Message. The table contains 11 entries for Traffic Log on 2005-12-03. A pagination bar at the bottom shows 'Total Count:122294 Total Page:12230' and navigation links.

Time	Source:Port	Destination:Port	Category	Message
2005-12-03 00:00:00	192.168.70.97	61.219.38.89	Traffic Log	Traffic Log
2005-12-03 00:00:00	192.168.70.90	192.168.70.250	Traffic Log	Traffic Log
2005-12-03 00:00:01	192.168.70.48:51188	192.168.70.250:53	Traffic Log	Traffic Log
2005-12-03 00:00:01	192.168.70.48:51188	172.23.5.2:53	Traffic Log	Traffic Log
2005-12-03 00:00:01	192.168.70.80	192.168.70.250	Traffic Log	Traffic Log
2005-12-03 00:00:01	192.168.70.103	192.168.70.250	Traffic Log	Traffic Log
2005-12-03 00:00:01	192.168.70.59	192.168.70.250	Traffic Log	Traffic Log
2005-12-03 00:00:01	192.168.70.50	192.168.70.250	Traffic Log	Traffic Log
2005-12-03 00:00:02	192.168.70.104	192.168.70.250	Traffic Log	Traffic Log
2005-12-03 00:00:02	192.168.101.33	192.168.101.250	Traffic Log	Traffic Log

The fields in the first three rows (and **Search** and **Reset**) appear when you open the report. The fields in the next three rows (above **Search** and **Reset**) appear if you do not select **All Categories** in the **Category** field and if you 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 86 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.
Start Time	Enter the time of the earliest log entries you want to see, if you select Day .
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 from more than one day.
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 can also click the Calendar icon to specify the date.

Table 86 Log Viewer > All Logs

LABEL	DESCRIPTION
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 . You can also click the Calendar icon to specify the date.
Category	This field depends on the model of the selected ZyXEL device. Select what type of log entries you want to see. You can also select All Categories .
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.
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.
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.
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.
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.s
Go	Enter the page number you want to see, and click Go .

9.2 Critical Log Viewer

Critical log entries are a subset of regular log entries. They are updated more frequently because they are important and may require immediate attention. For example, critical log entries include some messages in system maintenance, system errors, firewall access, TCP reset, attack, PPP, IDP, anti-virus, and anti-spam. See [section 2.3 on page 27](#) for more information about update frequencies for regular log entries and critical log entries. See [section 2.4 on page 28](#) for more information about the source data used by the report.

Click **Log Viewer > Critical Logs** to look at critical log entries. The screen is shown below. Unlike the **Regular Log Viewer**, the **Critical Log Viewer** does not have **Service**, **Protocol**, or **Port** fields because these fields are usually used for traffic logs, which are not critical.

Figure 92 Log Viewer > Critical Logs

Select Critical Logs

Day:

Start Time: :
 End Time: :

Days

Start Date:
 End Date:

Category: Advanced Search

Source IP: Destination IP:

Keyword:

Time	Source:Port	Destination:Port	Category	Message
2006-01-24 18:14:20	192.168.1.34:110	172.25.21.28:3474	Anti Virus	POP3 Virus infected - ID:3338,Trojan-Proxy.Win32.Agent.gx,01547.tf!
2006-01-24 18:14:20	172.25.21.28:3472	192.168.1.34:25	Anti Virus	SMTP Virus infected - ID:3338,Trojan-Proxy.Win32.Agent.gx,01547.tf!
2006-01-24 18:14:20	172.25.21.28:1862	192.168.1.34:1122	Anti Virus	FTPDATA Virus infected - ID:2242,Backdoor.Win32.Agent.f,00000.tf<013>!
2006-01-24 18:14:20	192.168.1.34:80	172.25.21.28:3469	Anti Virus	HTTP Virus infected - ID:2242,Backdoor.Win32.Agent.f,/00000.tf!
2006-01-24 18:10:52	192.168.1.34:110	172.25.21.28:3474	Anti Virus	POP3 Virus infected - ID:3338,Trojan-Proxy.Win32.Agent.gx,01547.tf!
2006-01-24 18:10:52	172.25.21.28:3472	192.168.1.34:25	Anti Virus	SMTP Virus infected - ID:3338,Trojan-Proxy.Win32.Agent.gx,01547.tf!
2006-01-24 18:10:52	172.25.21.28:1862	192.168.1.34:1122	Anti Virus	FTPDATA Virus infected - ID:2242,Backdoor.Win32.Agent.f,00000.tf<013>!
2006-01-24 18:10:52	192.168.1.34:80	172.25.21.28:3469	Anti Virus	HTTP Virus infected - ID:2242,Backdoor.Win32.Agent.f,/00000.tf!
2006-01-24 17:02:03	192.168.1.34:110	172.25.21.28:3474	Anti Virus	POP3 Virus infected - ID:3338,Trojan-Proxy.Win32.Agent.gx,01547.tf!
2006-01-24 17:02:03	172.25.21.28:3472	192.168.1.34:25	Anti Virus	SMTP Virus infected - ID:3338,Trojan-Proxy.Win32.Agent.gx,01547.tf!

Total Count:48 Total Page:5 [First](#) [1](#) [2](#) [3](#) [4](#) [5](#) [Last](#)

The fields in the first three rows (and **Search** and **Reset**) appear when you open the report. The fields in the next three rows (above **Search** and **Reset**) appear if you do not select **All Categories** in the **Category** field and if you 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 87 Log Viewer > Critical Logs

LABEL	DESCRIPTION
Day	Select this if you want to look at log entries from one day or part of one day.
Start Time	Enter the time of the earliest log entries you want to see, if you select Day .
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 from more than one day.
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 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 . You can also click the Calendar icon to specify the date.
Category	This field depends on the model of the selected ZyXEL device. Select what type of log entries you want to see. You can also select All Categories .
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.
Destination IP	Enter the destination IP address in the event that generated the log entry.
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.
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.
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.
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.s
Go	Enter the page number you want to see, and click Go .

CHAPTER 10

Schedule Report

Use these screens to set up and maintain daily, weekly, and one-time reports that Vantage Report sends by e-mail. See [section 2.2 on page 26](#) for more information about e-mail in Vantage Report.

10.1 Scheduled Report Summary Screen

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See [section 11.2 on page 203](#) for more information.

Note: 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 11.1 on page 202](#) for more information.

Note: 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.

Click **Schedule Reports > Schedule Reports** to open the **Scheduled Reports** summary screen.

Figure 93 Schedule Reports > Schedule Reports

Add Additional Scheduled Reports					
<input type="button" value="Add"/>	Add Daily Report				
<input type="button" value="Add"/>	Add Weekly Report				
<input type="button" value="Add"/>	Add Overtime Report				
Summary of Scheduled Reports					
Index	Task No.	To E-mail Address	E-mail Subject	Report Time	Task Type
<input type="checkbox"/>	1	email@zyxel.com.tw	bandwidth	Every day 00:22:21	Daily Report
<input type="checkbox"/>	2	email2@zyxel.com.tw	top sites	Every Sun 00:43:18	Weekly Report
<input type="checkbox"/>	3	email3@zyxel.com.tw	attacks	2006-02-11 00:37:07	Overtime Report
Total Count:3 Total Page:1 First 1 Last <input type="text" value=""/> Go					
<input type="button" value="Delete"/>					

Each field is described in the following table.

Table 88 Schedule Reports > Schedule Reports

LABEL	DESCRIPTION
Add (Daily Report)	Click this to generate and send one or more statistical reports daily. Each report comes from the previous day's information. The Customize Scheduled Report screen appears.
Add (Weekly Report)	Click this to generate and send one or more statistical reports weekly. Each report comes from the previous week's information. The Customize Scheduled Report screen appears.
Add (Overtime Report)	Click this to generate and send one or more statistical reports once, using information from a specified number of days. The Customize Scheduled Report screen appears.
Summary of Scheduled Reports	
Index	Click this, and click Delete to delete the scheduled report.
Task No.	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 punctuation marks at the end.
E-mail Subject	This field displays the subject line in the e-mail message Vantage Report sends.
Report Time	This field displays how often and when Vantage Report starts generating the scheduled report. It might take over an hour to finish a scheduled report, if there are a lot of reports and a lot of log entries and traffic statistics. For overtime reports, the date is the day after the last day in the report. You cannot change the start time.
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.s
Go	Enter the page number you want to see, and click Go .

10.2 Customize Daily Report Screen

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See [section 11.2 on page 203](#) for more information.

Note: Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report only saves one day of information (today's information), daily reports have no information in them. See [section 11.1 on page 202](#) for more information.

Note: 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** field for more information.

To access this screen, click **Add (Daily Report)** in the **Schedule Reports > Schedule Reports** screen.

Figure 94 Schedule Reports > Schedule Reports > Add (Daily Report)

Customize Daily Report

Destination E-mail Address (Comma Separated): *

E-mail Subject: *

E-mail Body: *

E-mail Attached Files

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler

Report Type: PDF only

Include All Data in a Single Report (only for PDF)

Report List

<input type="checkbox"/> Bandwidth Summary	<input type="checkbox"/> Attack Summary	<input checked="" type="checkbox"/> AntiVirus Top Sources
<input type="checkbox"/> Bandwidth Top Hosts	<input type="checkbox"/> Attack Top Sources	<input checked="" type="checkbox"/> AntiVirus Top Destinations
<input type="checkbox"/> Bandwidth Top Protocols	<input type="checkbox"/> Attack By Category	<input checked="" type="checkbox"/> AntiSpam Summary
<input type="checkbox"/> WEB Top Sites	<input checked="" type="checkbox"/> Intrusion Summary	<input checked="" type="checkbox"/> AntiSpam Top Senders
<input type="checkbox"/> WEB Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Intrusions	<input checked="" type="checkbox"/> AntiSpam Top Sources
<input type="checkbox"/> FTP Top Sites	<input checked="" type="checkbox"/> Intrusion Top Sources	<input checked="" type="checkbox"/> AntiSpam By Score
<input type="checkbox"/> FTP Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Destinations	<input type="checkbox"/> WEB Blocked Summary
<input type="checkbox"/> MAIL Top Sites	<input checked="" type="checkbox"/> Intrusion By Severity	<input type="checkbox"/> WEB Blocked Top Sites
<input type="checkbox"/> MAIL Top Hosts	<input checked="" type="checkbox"/> AntiVirus Summary	<input type="checkbox"/> WEB Blocked Top Hosts
<input checked="" type="checkbox"/> Customization Top Destinations		<input checked="" type="checkbox"/> WEB Blocked By Category
<input type="checkbox"/> Customization Top Sources		<input type="checkbox"/> WEB Allowed Summary
<input type="checkbox"/> VPN Top Peer Gateways	<input checked="" type="checkbox"/> AntiVirus Top Viruses	<input type="checkbox"/> WEB Allowed Top Sites
<input type="checkbox"/> VPN Top Hosts		<input type="checkbox"/> WEB Allowed Top Hosts

If you are using the standard version of Vantage Report, some reports are not available, so these reports are disabled in this screen. Each field is described in the following table.

Table 89 Schedule Reports > Schedule Reports > Add (Daily Report)

LABEL	DESCRIPTION
Destination E-mail Address	Enter the e-mail address(es) to which Vantage Report sends the selected report(s). 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.
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\schedule</code> in the Vantage Report installation directory.
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.
Report Type	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 for if you selected PDF format. Select this if you want to combine all the selected report(s) into one file.
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.
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.

10.3 Customize Weekly Report Screen

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See [section 11.2 on page 203](#) for more information.

Note: 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 11.1 on page 202](#) for more information.

Note: 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** field for more information.

Figure 95 Schedule Reports > Schedule Reports > Add (Weekly Report)

Customize Weekly Report

Destination E-mail Address (Comma Separated): *

E-mail Subject: *

E-mail Body: *

E-mail Attached Files

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler

Report Type: PDF only

Include All Data in a Single Report (only for PDF)

Day to Submit: ▼

Report List

<input type="checkbox"/> Bandwidth Summary	<input type="checkbox"/> Attack Summary	<input checked="" type="checkbox"/> AntiVirus Top Sources
<input type="checkbox"/> Bandwidth Top Hosts	<input type="checkbox"/> Attack Top Sources	<input checked="" type="checkbox"/> AntiVirus Top Destinations
<input type="checkbox"/> Bandwidth Top Protocols	<input type="checkbox"/> Attack By Category	<input checked="" type="checkbox"/> AntiSpam Summary
<input type="checkbox"/> WEB Top Sites	<input checked="" type="checkbox"/> Intrusion Summary	<input checked="" type="checkbox"/> AntiSpam Top Senders
<input type="checkbox"/> WEB Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Intrusions	<input checked="" type="checkbox"/> AntiSpam Top Sources
<input type="checkbox"/> FTP Top Sites	<input checked="" type="checkbox"/> Intrusion Top Sources	<input checked="" type="checkbox"/> AntiSpam By Score
<input type="checkbox"/> FTP Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Destinations	<input type="checkbox"/> WEB Blocked Summary
<input type="checkbox"/> MAIL Top Sites	<input checked="" type="checkbox"/> Intrusion By Severity	<input type="checkbox"/> WEB Blocked Top Sites
<input type="checkbox"/> MAIL Top Hosts	<input checked="" type="checkbox"/> AntiVirus Summary	<input type="checkbox"/> WEB Blocked Top Hosts
<input checked="" type="checkbox"/> Customization Top Destinations		<input checked="" type="checkbox"/> WEB Blocked By Category
<input type="checkbox"/> Customization Top Sources		<input type="checkbox"/> WEB Allowed Summary
<input type="checkbox"/> VPN Top Peer Gateways	<input checked="" type="checkbox"/> AntiVirus Top Viruses	<input type="checkbox"/> WEB Allowed Top Sites
<input type="checkbox"/> VPN Top Hosts		<input type="checkbox"/> WEB Allowed Top Hosts

If you are using the standard version of Vantage Report, some reports are not available, so

these reports are disabled in this screen. Each field is described in the following table.

Table 90 Schedule Reports > Schedule Reports > Add (Weekly Report)

LABEL	DESCRIPTION
Destination E-mail Address	Enter the e-mail address(es) to which Vantage Report sends the selected report(s). 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.
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.
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.
Report Type	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 for if you selected PDF format. Select this if you want to combine all the selected report(s) into one file.
Day to Submit	Select the day of the week to generate and send the selected report(s).
Function Window	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.
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.

10.4 Customize Overtime Report Screen

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See [section 11.2 on page 203](#) for more information.

Note: Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves six days of information, overtime reports only consist of information from these six days, not necessarily the whole specified date range. See [section 11.1 on page 202](#) for more information.

Note: 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** field for more information.

Figure 96 Schedule Reports > Schedule Reports > Add (Overtime Report)

Customize Overtime Report

Destination E-mail Address (Comma Separated): *

E-mail Subject: *

E-mail Body: *

E-mail Attached Files

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler

Report Type: PDF only

Include All Data in a Single Report (only for PDF)

Start Date: * End Date: *

Report List

<input type="checkbox"/> Bandwidth Summary	<input type="checkbox"/> Attack Summary	<input checked="" type="checkbox"/> AntiVirus Top Sources
<input type="checkbox"/> Bandwidth Top Hosts	<input type="checkbox"/> Attack Top Sources	<input checked="" type="checkbox"/> AntiVirus Top Destinations
<input type="checkbox"/> Bandwidth Top Protocols	<input type="checkbox"/> Attack By Category	<input checked="" type="checkbox"/> AntiSpam Summary
<input type="checkbox"/> WEB Top Sites	<input checked="" type="checkbox"/> Intrusion Summary	<input checked="" type="checkbox"/> AntiSpam Top Senders
<input type="checkbox"/> WEB Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Intrusions	<input checked="" type="checkbox"/> AntiSpam Top Sources
<input type="checkbox"/> FTP Top Sites	<input checked="" type="checkbox"/> Intrusion Top Sources	<input checked="" type="checkbox"/> AntiSpam By Score
<input type="checkbox"/> FTP Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Destinations	<input type="checkbox"/> WEB Blocked Summary
<input type="checkbox"/> MAIL Top Sites	<input checked="" type="checkbox"/> Intrusion By Severity	<input type="checkbox"/> WEB Blocked Top Sites
<input type="checkbox"/> MAIL Top Hosts	<input checked="" type="checkbox"/> AntiVirus Summary	<input type="checkbox"/> WEB Blocked Top Hosts
<input checked="" type="checkbox"/> Customization Top Destinations		<input checked="" type="checkbox"/> WEB Blocked By Category
<input type="checkbox"/> Customization Top Sources		<input type="checkbox"/> WEB Allowed Summary
<input type="checkbox"/> VPN Top Peer Gateways	<input checked="" type="checkbox"/> AntiVirus Top Viruses	<input type="checkbox"/> WEB Allowed Top Sites
<input type="checkbox"/> VPN Top Hosts		<input type="checkbox"/> WEB Allowed Top Hosts

If you are using the standard version of Vantage Report, some reports are not available, so these reports are disabled in this screen. Each field is described in the following table.

Table 91 Schedule Reports > Schedule Reports > Add (Overtime Report)

LABEL	DESCRIPTION
Destination E-mail Address	Enter the e-mail address(es) to which Vantage Report sends the selected report(s). 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.
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.
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.
Report Type	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 for if you selected PDF format. Select this if you want to combine all the selected report(s) into one file.
Start Date	Select the day to start collecting information for the selected report(s). Vantage Report starts collecting information at the beginning of this day.
End Date	Select the day to stop collecting information for the selected report(s). Vantage Report stops collecting information at the end of this day.
Function Window	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.
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.

CHAPTER 11

System

The `root` account 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 users who can access Vantage Report
- Backup the current configuration and restore a different configuration
- Export the current device window 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 professional version, or increase the number of devices Vantage Report supports.
- 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

11.1 General Configuration Screen

Note: Only the `root` account 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 > General Configuration** to open the **General Configuration** screen.

Figure 97 System > General Configuration

Each field is described in the following table.

Table 92 System > General Configuration

LABEL	DESCRIPTION
Critical Log	Select Enable if you want Vantage Report to start updating the critical log. Select Disable if you want Vantage Report to stop updating the critical log. This has no effect on existing critical log entries or on the Select Critical Logs screen.
Stored Log Days	Enter the number of days that Vantage Report should keep logs and traffic information. Vantage Report automatically deletes logs and traffic information that are older than this. You cannot generate statistical reports or look at logs for information older than this. This affects scheduled reports too because they can only use whatever information is stored in Vantage Report. If you want scheduled reports to have a complete set of information, you should set this field accordingly. Deleted information is saved in comma-separated files on the Vantage Report server. These files have CSV extensions and are saved in <Vantage Report installation directory>\data\backup\db.
Default Chart Type	Select the default chart type 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.
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 <code>root</code> 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.

11.2 Server Configuration Screen

Note: Only the `root` account can open this screen.

Use the **Server Configuration** screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports. See [section 2.2 on page 26](#) for more information. Click **System > Server Configuration** to open the **Server Configuration** screen.

Figure 98 System > Server Configuration

Each field is described in the following table.

Table 93 System > Server Configuration

LABEL	DESCRIPTION
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.
User Name	Enter the user name for the Vantage Report account. If the user name is not required, leave this field blank.
Password	Enter the password for the Vantage Report account. If the password is not required, leave this field blank.
Sender E-mail	Enter the complete e-mail address for the Vantage Report account.
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.
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.

11.3 User Maintenance Screens

The `root` account can use these screens to view, add, edit, or remove Vantage Report 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.

11.3.1 User Maintenance Summary Screen

Click **System > User Maintenance** to open the **User Maintenance** summary screen.

Figure 99 System > User Maintenance

Index	User Name	E-mail	Description	Status
<input checked="" type="checkbox"/>	root		VRPT administrator	on line
<input type="checkbox"/>	tom	tom@anycompany.com.tw		off line

Total Count:2 Total Page:1 [First](#) [1](#) [Last](#) [Go](#)

Other (non-**root**) users can only see their account in this screen. Each field is described in the following table.

Table 94 System > User Maintenance

LABEL	DESCRIPTION
Index	This field is only available for the root account. Select the check box next to a user account, and click Delete to remove the account. You cannot delete the root account.
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.
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
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.

11.3.2 Add/Edit User Account Screen

To access this screen, click **System > User Maintenance**, and click a user name to edit it or click the **Add** button to create a new account.

Figure 100 Add/Edit User Account Screen

Each field is described in the following table.

Table 95 Add/Edit User Account Screen

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 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 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 (<code>root</code> only) and forgotten passwords.
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.

11.4 Data Maintenance Screens

Note: Only the `root` account can open these screens.

Use the data maintenance screens to backup the current configuration, restore a different configuration, export the device window, or import a different device window.

11.4.1 Data Backup and Data Restore Screen

Note: Only the `root` account can open this screen.

You can use this screen to backup or restore the settings in the **General Configuration**, **Server Configuration**, and **User Maintenance** screens. The backup format is XML. You cannot backup or restore the logs, traffic information, or other settings. To access this screen, click **System > Data Maintenance > Configuration Backup & Restore**.

Figure 101 System > Data Maintenance > Configuration Backup & Restore

The screenshot shows a web interface for configuration backup and restore. It features two main panels. The top panel, titled 'Data Backup', includes a label 'Destination: To Your Computer' and a 'Backup' button. The bottom panel, titled 'Data Restore', includes a label 'Source: From Your Computer', a 'File Name:' label with an input field, a 'Browse...' button, and 'Restore' and 'Reset' buttons.

Each field is described in the following table.

Table 96 System > Data Maintenance > Configuration Backup & Restore

LABEL	DESCRIPTION
Backup	Click this to look at or save the current settings in the General Configuration , Server Configuration , and User Maintenance 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.

11.4.2 Device List Export and Device List Import Screen

Note: Only the `root` account can open this screen.

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. To access this screen, click **System > Data Maintenance > Device List Import & Export**.

Figure 102 System > Data Maintenance > Device List Import & Export

The screenshot shows two main sections. The top section, 'Device List Export', has a dropdown menu set to 'To Your Computer' and an 'Export' button. The bottom section, 'Device List Import', has a dropdown menu set to 'From Your Computer'. Below this is a 'File Name:' label followed by a text input field and a 'Browse...' button. At the bottom of the import section are 'Import' and 'Reset' buttons.

Each field is described in the following table.

Table 97 System > Data Maintenance > Device List Import & Export

LABEL	DESCRIPTION
Export	Click this to look at or save the current device window 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 window + devices in XML file) is more than your license allows.
Reset	Click this to clear the fields in this screen.

11.5 Upgrade Screen

Note: Only the `root` account 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 professional version. To access this screen, click **System > Upgrade**.

Figure 103 System > Upgrade



Each field is described in the following table.

Table 98 System > 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.

11.6 Registration Screens

Note: Only the `root` account can open these screens.

Use these screens to

- get the trial version of Vantage Report (if you have not installed it before);
- upgrade to the professional version of Vantage Report; or
- increase the number of devices in Vantage Report.

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.

If you want to use an existing myZyXEL.com account, you need your ...
<ul style="list-style-type: none"> • myZyXEL.com user name • myZyXEL.com password
If you want to upgrade to the professional version or increase the number of devices, you need your ...
<ul style="list-style-type: none"> • license key (iCard for the upgrade or increase)

11.6.1 Registration Summary Screen

To access this screen, click **System > Registration**.

Figure 104 System > Registration

Registration	
VRPT 2.3 Professional Version	
Account on myZyXEL.com:	brentfolbrecht
Authentication Code(AC):	0579C2B3102BF8A21D8B9CF7FF6357C3D777
Supported Maximum Nodes:	25
License Allowed Nodes:	5
Used Nodes:	1
<input type="button" value="Refresh"/> <input type="button" value="Upgrade"/>	

The fields in this screen depend on what version (standard or professional) 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 99 System > Registration

LABEL	DESCRIPTION
	The first field displays the current release and current version.
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.
Trial Rest Days	This field displays if you have the trial version. This field displays the number of remaining days you can use the trial version. When this time is over, Vantage Report reverts to the standard version.
Supported Maximum Nodes	This field appears if you have the professional 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 Nodes .
License Allowed Nodes	This field appears if you have the professional version. It displays the number of devices you can add in Vantage Report based on your current license(s).
Used Nodes	This field appears if you have the professional version. It displays the number of devices you currently have added in Vantage Report.
Refresh	Click this to update the information in this screen.
Trial	This field appears if you have the standard 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 professional 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.

11.6.2 Registration 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 > Registration**.

Figure 105 Registration Screen

The screenshot shows a web form titled "Registration". It contains the following elements:

- License Key:** A text input field with a red asterisk to its right.
- Account Type:** Two radio buttons: "New myZyXEL.com account" (selected) and "Existing myZyXEL.com account".
- Instruction:** "(Type username and password from 6 to 20 characters.)"
- User Name:** A text input field with a red asterisk to its right.
- Password:** A text input field with a red asterisk to its right.
- Confirm Password:** A text input field with a red asterisk to its right.
- E-mail Address:** A text input field with a red asterisk to its right.
- Country:** A dropdown menu showing "Afghanistan" with a red asterisk to its right.
- Buttons:** "Upgrade" and "Cancel" buttons at the bottom.

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 100 Registration Screen

LABEL	DESCRIPTION
License Key	This field appears if you are upgrading to the professional version or increasing the number of devices. Enter the license key on the iCard.
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 or underscores(_) long. If you are using an existing myZyXEL.com account, enter the user name for that account.

Table 100 Registration 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 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 professional version, or increase the number of devices in Vantage Report.
Cancel	Click this to return to the Registration summary screen without registering.

11.7 About Screen

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

Figure 106 System > About

Version:	2.3
Date:	2005-09-11
Copyright:	Copyright (c) 2005 ZyXEL Communications Corporation. (All rights reserved)

APPENDIX A

Troubleshooting

PROBLEM	CORRECTIVE ACTION
<p>There is no information in any report for my device.</p>	<p>If you just added the device, wait. See Table 2 on page 27 for the amount of time it takes for information to appear in each report.</p> <p>Look for the device's MAC address in <code>vrpt\log\LogRecord.log</code> 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.</p> <ul style="list-style-type: none"> • 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 2.4. <p>Check the amount of available disk space on the Vantage Report server. If it is less than the value in Appendix B on page 216, the Vantage Report server stops receiving log entries.</p> <p>Make sure your ZyXEL devices support Vantage Report. Check the release notes for the current firmware version.</p> <p>Check the connections between the ZyXEL devices and Vantage Report server.</p> <p>If the problem continues, contact your local vendor.</p>
<p>There is information in some reports, but there is no information in others.</p>	<p>Make sure your ZyXEL devices support these reports. Check the release notes for the current firmware version.</p> <p>Make sure you have configured the ZyXEL devices correctly. See section 2.4.</p> <p>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.</p> <p>If the problem continues, contact your local vendor.</p>

APPENDIX B

Product Specifications

All values are accurate at the time of writing.

See [Table 2 on page 27](#) for specifications about the time it takes the Vantage Report server to process information from ZyXEL devices.

Table 101 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

Table 102 System Notifications Specifications

FEATURE	SPECIFICATION
Maximum number of records in any table in the database	15,000,000
Warning: Maximum number of records in any table in the database	10,000,000
Minimum amount of free disk space required to run Vantage Report	600 MB
Warning: Minimum amount of free disk space required to run Vantage Report	per Low Free Disk Mark

Table 103 Feature Specifications

FEATURE	SPECIFICATION
Maximum Number of Entries in the Table at the Bottom of Each Statistical Report	10
Log Consolidation Frequency	4 minutes

Appendix C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/ME/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

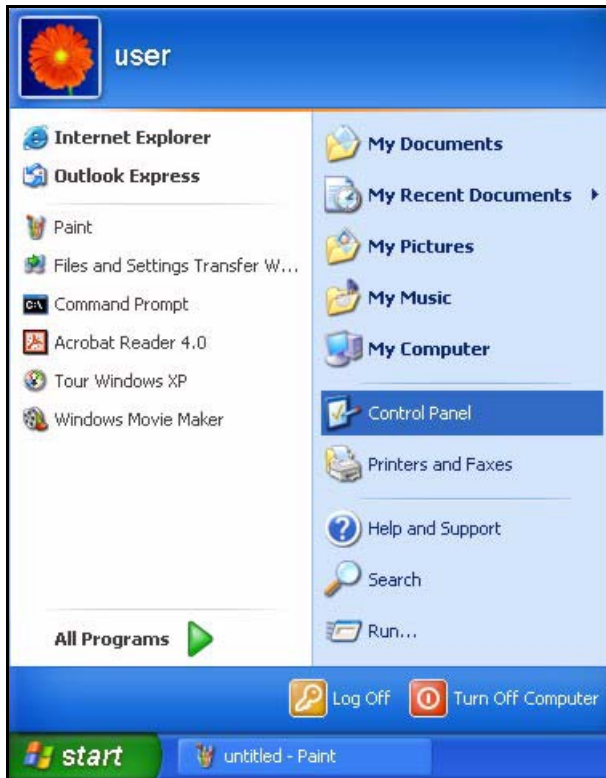
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 2000/NT/XP

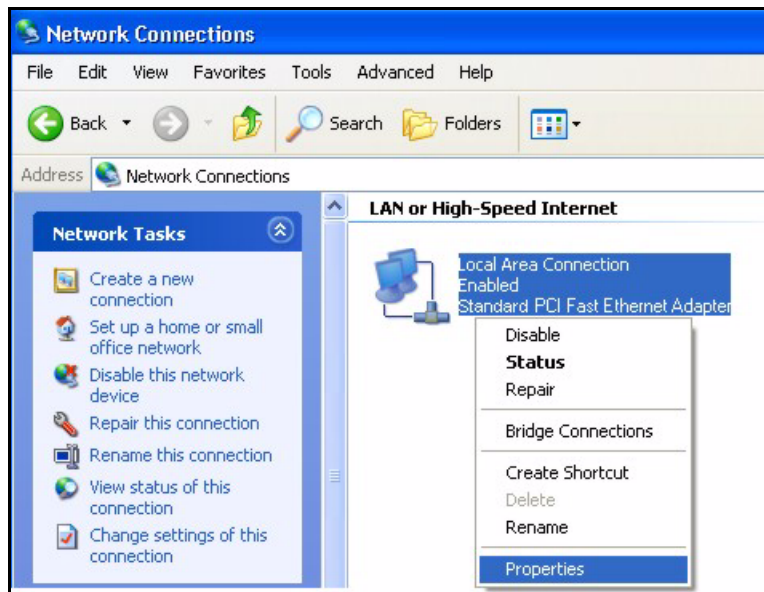
- 1 For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.

Figure 107 Windows XP: Start Menu

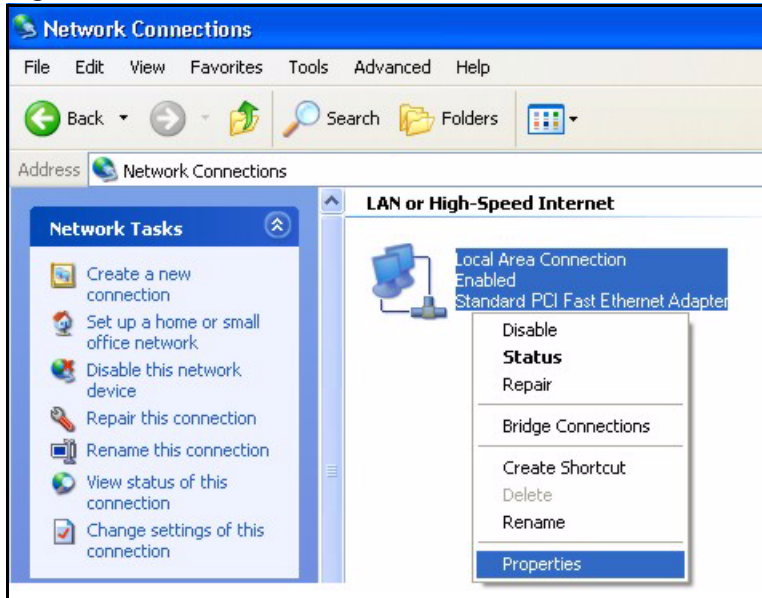


2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

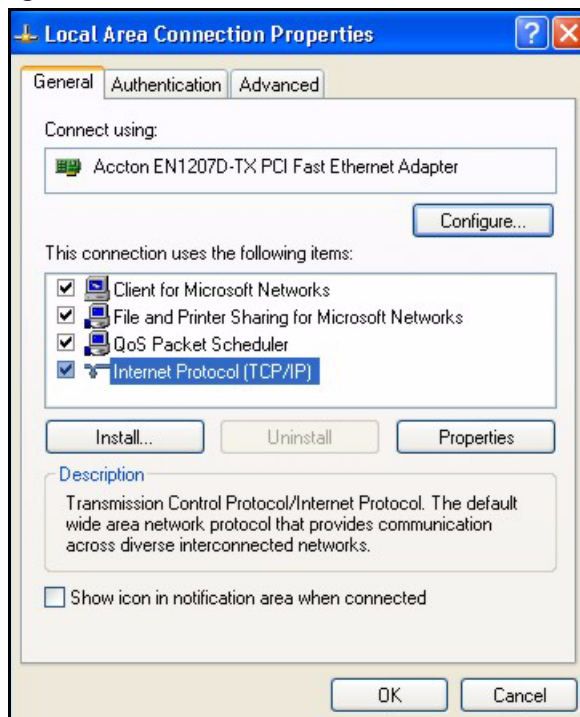
Figure 108 Windows XP: Control Panel



3 Right-click **Local Area Connection** and then click **Properties**.

Figure 109 Windows XP: Control Panel: Network Connections: Properties

- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

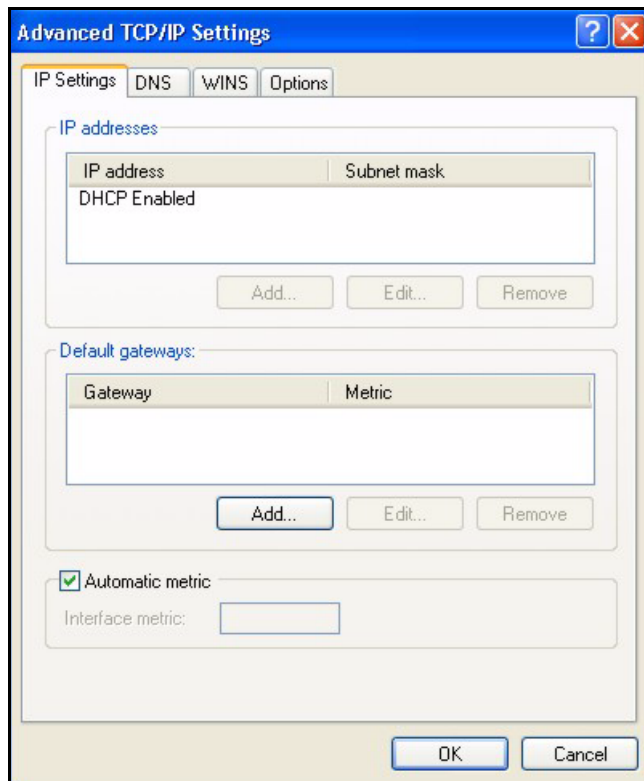
Figure 110 Windows XP: Local Area Connection Properties

- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 111 Windows XP: Advanced TCP/IP Settings



- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

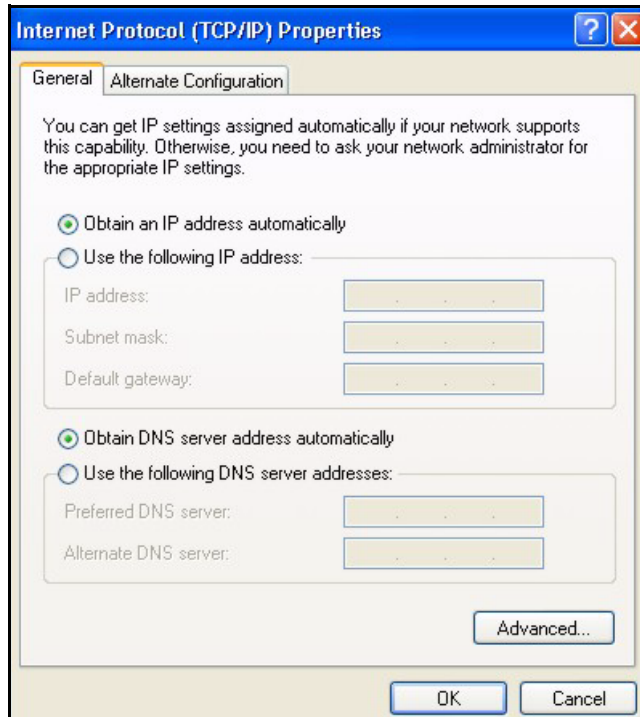
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 112 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

1 Click **Start, All Programs, Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Appendix D

Log Descriptions

This appendix provides descriptions of example device log messages. Log messages vary by device

Table 104 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.
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.

Table 104 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
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.

Table 105 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.

Table 106 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>, <ruled>	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.
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.

Table 107 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. Default timeout values: ICMP idle timeout (s): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP idle (established) timeout (s): 3600
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 108 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.

Table 109 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. For type and code details, see Table 121 .
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. For type and code details, see Table 121 .

Table 109 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
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 110 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 111 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 112 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 113 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 ZyWALL cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The ZyWALL 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.

Table 114 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. For type and code details, see Table 121 .
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. For type and code details, see Table 121 .
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. For type and code details, see Table 121 .
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 121 .
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. For type and code details, see Table 121 .
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. For type and code details, see Table 121 .
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 121 .

Table 115 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" CLI 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.

Table 116 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.
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.

Table 116 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
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.

Table 116 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
XAUTH fail! Username: <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.
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.

Table 116 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
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.

Table 117 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.
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.

Table 117 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
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 118 for the corresponding descriptions of the codes.

Table 118 Certificate Path Verification Failure Reason 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).
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.

Table 118 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 119 802.1X 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.
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 120 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.
(L to L/ZW)	LAN to LAN/ ZyWALL	ACL set for packets traveling from the LAN to the LAN or the ZyWALL.
(W to W/ZW)	WAN to WAN/ ZyWALL	ACL set for packets traveling from the WAN to the WAN or the ZyWALL.
(D to D/ZW)	DMZ to DMZ/ ZyWALL	ACL set for packets traveling from the DMZ to the DM or the ZyWALL.

Table 121 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

Table 121 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
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 122 Syslog Logs

LOG MESSAGE	DESCRIPTION
<pre><Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>"</pre>	<p>"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 various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.</p>

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 123 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

Table 123 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Appendix E

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 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.

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 Hibemate 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 2.3 incorporate source code covered under the GPL, LGPL, Sun Microsystems, Inc. Binary Code License, Quarz 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 2.3”

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.

Index

A

Add Device screen [34](#)
 additional ZyXEL device configuration [28](#)
 anti-spam
 monitors [49](#)
 source data [28](#)
 statistical reports [147](#)
 ZyXEL device configuration [28](#)
 anti-virus
 monitors [48](#)
 source data [28](#)
 statistical reports [133](#)
 ZyXEL device configuration [28](#)
 attacks
 monitors [46](#)
 source data [28](#)
 statistical reports [102](#)
 ZyXEL device configuration [28](#)
 authentication
 failed login [185](#)
 source data [28](#)
 successful login [184](#)
 ZyXEL device configuration [28](#)
 authentication code [210](#)

B

bandwidth
 source data [28](#)
 ZyXEL device configuration [28](#)
 bandwidth. See device traffic.

C

clock time [27](#)
 configuration
 backup [207](#)
 e-mail [203](#)
 general [202](#)
 restore [207](#)
 screens [202](#)
 SMTP mail server [203](#)
 users [204](#)

Contact Information [4](#)
 Contacting Customer Support [4](#)
 copyright [2](#)
 critical log entries [190](#)
 enable/disable [203](#)
 critical log viewer
 processing time [27](#)
 source data [28](#)
 ZyXEL device configuration [28](#)
 Customer Support [4](#)
 customized service field
 where configured [92](#)
 where used [94, 98](#)
 customized service traffic. See other service traffic.

D

data backup [207](#)
 data restore [207](#)
 Denmark, Contact Information [4](#)
 Device Information screen [34](#)
 device list
 export [207](#)
 import [207](#)
 device traffic
 direction in statistical reports [53, 57, 61](#)
 events [54, 56, 58, 59, 61, 63](#)
 monitors [44](#)
 statistical reports [52](#)
 device window [32](#)
 export [207](#)
 import [207](#)
 refresh [33](#)
 right-click [35](#)
 DNS reverse. See reverse DNS.
 drill-down [23, 43](#)

E

Edit Device screen [34](#)
 e-mail [26](#)
 forget password [27](#)
 low free disk mark [203](#)
 scheduled reports [27](#)

SMTP settings [26](#), [203](#)
system notification [27](#)
test SMTP mail server [27](#), [204](#)

F

failed login [185](#)
 source data [28](#)
 ZyXEL device configuration [28](#)
Finland, Contact Information [4](#)
forget password [27](#), [31](#)
France, Contact Information [4](#)
FTP
 monitors [46](#)
FTP traffic
 events [72](#), [73](#), [75](#), [77](#)
 statistical reports [70](#)
function window [32](#), [35](#)
 list of screens [36](#)
 right-click [39](#)

G

Germany, Contact Information [4](#)

H

help icon [32](#)
HTTP/HTTPS. See web traffic.

I

iCard [209](#)
idle timeout [32](#)
intrusions
 monitors [47](#)
 source data [28](#)
 statistical reports [113](#)
 ZyXEL device configuration [28](#)
IPSec VPN traffic. See VPN traffic.

L

license key [209](#)
list of screens [36](#)
log entries [22](#)
 critical. See regular log entries.
 how used [28](#)
 regular. See regular log entries.
log settings requirements [28](#)
log viewer
 critical log entries. See critical log viewer.
 regular log entries. See regular log viewer.
Login screen [30](#)
logout icon [32](#)
low free disk mark [203](#)

M

MAC [34](#)
mail traffic
 events [79](#), [80](#), [82](#), [84](#)
 monitors [46](#)
 statistical reports [77](#)
main screen [31](#)
 parts of [32](#)
monitors [22](#)
 anti-spam [49](#)
 anti-virus [48](#)
 attacks [46](#)
 device traffic [44](#)
 end time [41](#)
 FTP [46](#)
 graph [41](#)
 intrusions [47](#)
 mail traffic [46](#)
 next refresh time [41](#)
 printing [41](#)
 processing time [27](#)
 right-click [41](#)
 service traffic [45](#)
 source data [28](#)
 start time [41](#)
 typical layout [40](#)
 VPN traffic [46](#)
 web traffic [46](#)
 ZyXEL device configuration [28](#)
myZyXEL.com [209](#)

N

North America Contact Information [4](#)
 Norway, Contact Information [4](#)
 number of devices
 currently allowed [210](#)
 currently used [210](#)
 increase allowed [209](#)
 maximum allowed [210](#)

O

other service traffic
 configure customized service field [92](#)
 events [95](#), [96](#), [98](#), [100](#)
 statistical reports [93](#)

P

password
 default value [31](#)
 POP3/SMTP traffic. See mail traffic.
 port number [26](#)
 printing
 monitors [41](#)
 statistical reports [42](#)
 processing time [27](#)
 Product Model [4](#)
 professional version [23](#)

Q

Quick Start Guide [22](#)

R

registration [23](#)
 authentication code [210](#)
 iCard [209](#)
 license key [209](#)
 myZyXEL.com [209](#)
 regular log entries [188](#)
 regular log viewer
 processing time [27](#)

source data [28](#)
 ZyXEL device configuration [28](#)

Regular Mail [4](#)
 related documentation [20](#)
 report window [32](#), [40](#)
 typical layouts [40](#)
 reverse DNS [23](#), [43](#), [203](#)

S

scheduled reports [23](#), [27](#), [203](#)
 daily [195](#)
 generation time [195](#)
 one-time [199](#)
 overtime [199](#)
 requirements [194](#)
 store log days and [194](#)
 summary [194](#)
 weekly [197](#)
 security timeout [32](#)
 service traffic
 monitors [45](#)
 SMTP mail server [26](#)
 test [27](#), [204](#)
 software release
 upgrade [208](#)
 source data [28](#)
 how used in screens [28](#)
 log entries [28](#)
 traffic statistics [28](#)
 Spain, Contact Information [5](#)
 spam. See anti-spam.
 standard version [23](#)
 statistical reports [22](#)
 anti-spam [147](#)
 anti-virus [133](#)
 attacks [102](#)
 dates [43](#)
 default chart type [43](#), [203](#)
 device traffic [52](#)
 end date [43](#)
 FTP traffic [70](#)
 graph [43](#)
 graph type [43](#)
 intrusions [113](#)
 last X days [43](#)
 mail traffic [77](#)
 other service traffic [93](#)
 printing [42](#)
 processing time [27](#)
 right-click [43](#)
 settings [43](#)
 start date [43](#)

- table [43](#)
- title [43](#)
- typical layout [42](#)
- VPN traffic [84](#)
- web block [158](#)
- web forward [158](#)
- web traffic [63](#)
- yellow conversation box [43](#)
- store log days
 - effects of [43](#)
 - scheduled reports and [194](#), [203](#)
 - setting [203](#)
- store log days and [203](#)
- successful login [184](#)
 - source data [28](#)
 - ZyXEL device configuration [28](#)
- Support E-mail [4](#)
- Sweden, Contact Information [5](#)
- syntax conventions [20](#)
- system notification [27](#)
 - low free disk mark setting [203](#)

T

- Telephone [4](#)
- time [27](#)
 - clock time [27](#)
 - processing time [27](#)
- title bar [32](#)
- traffic statistics
 - how used [28](#)
 - in typical application [22](#)
- trial version [24](#)
- typical application [22](#)

U

- upgrade
 - software release [208](#)
 - versions [209](#)
- user name
 - default value [31](#)
- users
 - add [205](#)
 - change password [205](#)
 - edit [205](#)
 - list [205](#)
 - on line vs off line [205](#)
 - password [205](#)
 - screens [204](#)

V

- Vantage Report
 - license key [209](#)
 - typical application [22](#)
 - users. See users.
- Vantage Report server [22](#), [26](#)
 - as service [23](#), [26](#)
 - clock time in [27](#)
 - configuration. See configuration.
 - e-mail in [26](#)
 - port number [26](#)
 - processing time [27](#)
 - source data [28](#)
 - starting [26](#)
 - stopping [26](#)
 - time in [27](#)
- Vantage Report users. See users.
- versions [23](#)
 - differences [24](#)
 - professional [23](#), [209](#)
 - standard [23](#)
 - trial [24](#), [209](#), [210](#)
 - upgrade [209](#)
- virus. See anti-virus.
- VPN traffic
 - events [86](#), [87](#), [90](#), [91](#)
 - monitors [46](#)
 - source data [28](#)
 - statistical reports [84](#)
 - ZyXEL device configuration [28](#)

W

- Warranty Information [4](#)
- web block
 - source data [28](#)
 - statistical reports [158](#)
 - ZyXEL device configuration [28](#)
- web configurator [30](#)
 - default password [31](#)
 - default user name [31](#)
 - in typical application [22](#)
 - minimum requirements [30](#)
 - starting [30](#)
 - timeout [32](#)
 - URL [30](#)
- web forward
 - source data [28](#)
 - statistical reports [158](#)
 - ZyXEL device configuration [28](#)
- Web Site [4](#)
- web traffic

events [65](#), [66](#), [68](#), [70](#)
monitors [46](#)
statistical reports [63](#)
Worldwide Contact Information [4](#)

Z

ZyXEL device
add [33](#), [34](#), [207](#)
configuration [28](#)
device type setting [34](#)
edit basic information [33](#)
import [207](#)
in typical application [22](#)
MAC setting [34](#)
remove [33](#)
search for [33](#)
select [33](#)
source data. See source data.
view basic information [33](#)

