Vantage Report

User's Guide

Version 3.0
10/2006
Edition 1

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

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

Related 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. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

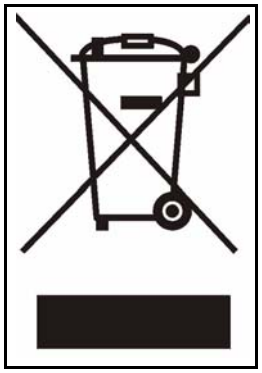
- The version number on the title page is the version of Vantage Report that is documented in this User's Guide.
- Enter means for you to type one or more characters and press the carriage return. Select or Choose means for you to use one of the predefined choices.
- The choices of a menu item are in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

Icons Used in Figures

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

Computer	Server	Networking Device
		

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction 29

Introducing Vantage Report 31
The Vantage Report Server 33
The Web Configurator 37

Monitor and Traffic 63

Monitor 65
Traffic 73
VPN 139

Network Attack and Security Policy 183

Network Attack 185
Security Policy 243

Event, Log Viewer and Schedule Report 285

Event 287
Log Viewer 295
Schedule Report 299

System and Troubleshooting 315

System 317
Troubleshooting 335

Appendices and Index 337

Table of Contents

About This User's Guide **3**

Document Conventions **4**

Contents Overview **7**

Table of Contents **9**

List of Figures **17**

List of Tables **23**

Part I: Introduction **29**

Chapter 1
Introducing Vantage Report **31**

1.1 Introduction 31
1.2 Versions 31

Chapter 2
The Vantage Report Server **33**

2.1 Starting and Stopping the Vantage Report Server 33
2.2 E-Mail in the Vantage Report Server 34
2.3 Time in the Vantage Report Server 34
2.4 ZyXEL Device Configuration and Source Data 35

Chapter 3
The Web Configurator **37**

3.1 Web Configurator Requirements 37
3.2 Web Configurator Access 37
3.3 Title Bar 40
3.4 Device Window 40
3.5 Function Window 43
3.6 Report Window 52
3.6.1 Device Information Screen 52
3.6.2 Monitors and Statistical Reports 52
3.6.3 View Logs 56
3.7 Dashboard 57
3.8 Dashboard 59

Part II: Monitor and Traffic 63

Chapter 4
Monitor 65

4.1 Bandwidth Monitor 65
4.2 Service Monitor 66
4.3 Attack Monitor 68
4.4 Intrusion Monitor 68
4.5 Anti-Virus Monitor 69
4.6 Anti-Spam Monitor 70

Chapter 5
Traffic 73

5.1 Bandwidth 73
5.1.1 Bandwidth Summary 73
5.1.2 Bandwidth Summary Drill-Down 75
5.1.3 Bandwidth Top Protocols 77
5.1.4 Bandwidth Top Protocols Drill-Down 79
5.1.5 Top Bandwidth Hosts 81
5.1.6 Top Bandwidth Hosts Drill-Down 84
5.1.7 Top Bandwidth Users 85
5.1.8 Top Bandwidth Users Drill-Down 88
5.1.9 Top Bandwidth Destinations 89
5.1.10 Top Bandwidth Destinations Drill-Down 92
5.2 Web Traffic 93
5.2.1 Top Web Sites 93
5.2.2 Top Web Sites Drill-Down 96
5.2.3 Top Web Hosts 97
5.2.4 Top Web Hosts Drill-Down 99
5.2.5 Top Web Users 101
5.2.6 Top Web Users Drill-Down 103
5.3 FTP Traffic 104
5.3.1 Top FTP Sites 104
5.3.2 Top FTP Sites Drill-Down 107
5.3.3 Top FTP Hosts 108
5.3.4 Top FTP Hosts Drill-Down 110
5.3.5 Top FTP Users 111
5.3.6 Top FTP Users Drill-Down 113
5.4 Mail Traffic 115
5.4.1 Top Mail Sites 115
5.4.2 Top Mail Sites Drill-Down 118
5.4.3 Top Mail Hosts 119
5.4.4 Top Mail Hosts Drill-Down 121

5.4.5 Top Mail Users 122
5.4.6 Top Mail Users Drill-Down 124
5.5 Other Traffic 126
5.5.1 Platform Selection 126
5.5.2 Service Settings 126
5.5.3 Top Destinations of Other Traffic 127
5.5.4 Top Destinations of Other Traffic Drill-Down 129
5.5.5 Top Sources of Other Traffic 131
5.5.6 Top Sources of Other Traffic Drill-Down 133
5.5.7 Top Other Traffic Users 134
5.5.8 Top Users of Other Traffic Drill-Down 136

Chapter 6
VPN 139

6.1 VPN Site-to-Site 139
6.1.1 VPN Link Status 139
6.1.2 VPN Traffic Monitor 140
6.1.3 Top VPN Peer Gateways 141
6.1.4 Top VPN Peer Gateways Drill-Down 143
6.1.5 Top VPN Sites 145
6.1.6 Top VPN Sites Drill-Down 147
6.1.7 Top VPN Tunnels 148
6.1.8 Top VPN Tunnels Drill-Down 151
6.1.9 Top VPN Protocols 152
6.1.10 Top VPN Protocols Drill-Down 154
6.1.11 Top VPN Hosts 156
6.1.12 Top VPN Hosts Drill-Down 159
6.1.13 Top VPN Users 160
6.1.14 Top VPN Users Drill-Down 163
6.1.15 Top VPN Destinations 164
6.1.16 Top VPN Destinations Drill-Down 167
6.2 VPN Remote Access 168
6.2.1 VPN Total Users and Traffic 168
6.2.2 VPN User Status 169
6.2.3 Top VPN Protocols 170
6.2.4 Top VPN Protocols Drill-Down 173
6.2.5 Top VPN Destinations 174
6.2.6 Top VPN Destinations Drill-Down 177
6.3 Xauth 178
6.3.1 VPN Successful Login 178
6.3.2 VPN Failed Login 180

Part III: Network Attack and Security Policy 183

Chapter 7
Network Attack 185

7.1 Attack 185
7.1.1 Attack Summary 185
7.1.2 Attack Summary Drill-Down 187
7.1.3 Top Attacks 189
7.1.4 Top Attacks Drill-Down 191
7.1.5 Top Attack Sources 193
7.1.6 Top Attack Sources Drill-Down 195
7.1.7 Attack Types 197
7.1.8 Attack Types Drill-Down 198
7.2 Intrusion 200
7.2.1 Intrusion Summary 200
7.2.2 Intrusion Summary Drill-Down 201
7.2.3 Top Intrusion Signatures 203
7.2.4 Top Intrusion Signatures Drill-Down 205
7.2.5 Top Intrusion Sources 206
7.2.6 Top Intrusion Sources Drill-Down 208
7.2.7 Top Intrusion Destinations 210
7.2.8 Top Intrusion Destinations Drill-Down 212
7.2.9 Intrusion Severities 213
7.2.10 Intrusion Severities Drill-Down 215
7.3 AntiVirus 217
7.3.1 Virus Summary 217
7.3.2 Virus Summary Drill-Down 218
7.3.3 Top Viruses 220
7.3.4 Top Viruses Drill-Down 222
7.3.5 Top Virus Sources 224
7.3.6 Top Virus Sources Drill-Down 226
7.3.7 Top Virus Destinations 228
7.3.8 Top Virus Destinations Drill-Down 230
7.4 AntiSpam 232
7.4.1 Spam Summary 232
7.4.2 Spam Summary Drill-Down 234
7.4.3 Top Spam Senders 236
7.4.4 Top Spam Sources 238
7.4.5 Spam Scores 240

Chapter 8
Security Policy 243

8.1 Firewall Access Control 243

8.1.1 Top Users Blocked 243
8.1.2 Top Packets Blocked 245
8.2 Application Access Control 247
8.2.1 Top Applications Blocked 247
8.2.2 Top Users Blocked 249
8.2.3 Top Applications Allowed 251
8.3 Blocked Web Accesses 253
8.3.1 Web Block Summary 254
8.3.2 Web Block Summary Drill-Down 255
8.3.3 Top Blocked Web Sites 257
8.3.4 Top Blocked Web Sites Drill-Down 259
8.3.5 Top Blocked Web Hosts 260
8.3.6 Top Blocked Web Hosts Drill-Down 262
8.3.7 Top Blocked Web Users 263
8.3.8 Top Blocked Web Users Drill-Down 265
8.3.9 Blocked Web Categories 267
8.3.10 Blocked Web Categories Drill-Down 268
8.4 Allowed Web Accesses 270
8.4.1 Web Allowed Summary 270
8.4.2 Web Allowed Summary Drill-Down 271
8.4.3 Top Allowed Web Sites 273
8.4.4 Top Allowed Web Sites Drill-Down 275
8.4.5 Top Allowed Web Hosts 277
8.4.6 Top Allowed Web Hosts Drill-Down 279
8.4.7 Top Allowed Web Users 280
8.4.8 Top Allowed Web Users Drill-Down 282

Part IV: Event, Log Viewer and Schedule Report 285

Chapter 9
Event 287

9.1 Successful Logins 287
9.2 Failed Logins 288
9.3 Top Sessions Per Host 290
9.4 Top Sessions Per User 292

Chapter 10
Log Viewer 295

10.1 Log Viewer 295

Chapter 11
Schedule Report 299

11.1 Scheduled Report Summary Screen 299
11.2 Customize Daily Report Screen 301
11.3 Customize Weekly Report Screen 304
11.4 Customize Overtime Report Screen 307
11.5 Template List 310
11.6 Template Add/Edit 311

Part V: System and Troubleshooting 315

Chapter 12
System 317

12.1 General Configuration Screen 317
12.1.1 Configuring for Hostname Reverse 318
12.2 Server Configuration Screen 322
12.3 User Management Screens 323
12.3.1 User Management Summary Screen 323
12.3.2 Add/Edit User Account Screen 324
12.4 Data Maintenance Screens 325
12.4.1 Data Backup and Data Restore Screen 325
12.4.2 Device List Export and Device List Import Screen 326
12.5 Upgrade Screen 327
12.6 Registration Screens 327
12.6.1 Registration Summary Screen 328
12.6.2 Registration Screen 329
12.7 Log Receiver Screens 330
12.7.1 Log Receiver By Day Screen 330
12.7.2 Log Receiver By Day > By Device Screen 331
12.7.3 Log Receiver By Day > By Device > By Category Screen 332
12.7.4 Log Receiver By Device Screen 332
12.7.5 Log Receiver By Device > By Category Screen 333
12.8 About Screen 334

Chapter 13
Troubleshooting 335

Part VI: Appendices and Index 337

Appendix A Product Specifications 339

Appendix B Setting up Your Computer's IP Address 345

Appendix C ZyNOS Log Descriptions 351

13.1 Syslog Logs 372

Appendix D ZyWALL 1050 Log Descriptions 375

Appendix E Open Software Announcements 417

Appendix F Legal Information 447

Appendix G Customer Support 449

Index 453

List of Figures

Figure 1 Typical Vantage Report Application 31
Figure 2 Web Configurator Login Screen 38
Figure 3 Web Configurator Main Screen 39
Figure 4 Device Window 41
Figure 5 Add/Edit Device and Add/Edit Folder Screens 42
Figure 6 Device Window Right-Click Menu 43
Figure 7 Function Window 44
Figure 8 Function Window Right-Click Menu 52
Figure 9 Device Information Screen 52
Figure 10 Report Window: Monitor and Statistical Report Examples 53
Figure 11 Typical Monitor Layout 53
Figure 12 Report Window Right-Click Menu 54
Figure 13 Typical Statistical Report Layout 55
Figure 14 Report Window Right-Click Menu 56
Figure 15 View Logs 57
Figure 16 Dashboard Initial View 58
Figure 17 Dashboard Configure 58
Figure 18 Dashboard Select Device and Monitor or Summary 59
Figure 19 Dashboard Configured 60
Figure 20 Monitor > Bandwidth 65
Figure 21 Monitor > Service 67
Figure 22 Monitor > Attack 68
Figure 23 Monitor > Intrusion 69
Figure 24 Monitor > AntiVirus 70
Figure 25 Monitor > AntiSpam 71
Figure 26 Traffic > Bandwidth > Summary 73
Figure 27 Traffic > Bandwidth > Summary > Drill-Down 76
Figure 28 Traffic > Bandwidth > Top Protocols 77
Figure 29 Traffic > Bandwidth > Top Protocol > Drill-Down 80
Figure 30 Traffic > Bandwidth > Top Hosts 82
Figure 31 Traffic > Bandwidth > Top Hosts > Drill-Down 84
Figure 32 Traffic > Bandwidth > Top Users 86
Figure 33 Traffic > Bandwidth > Top Users > Drill-Down 88
Figure 34 Traffic > Bandwidth > Top Destinations 90
Figure 35 Traffic > Bandwidth > Top Destinations > Drill-Down 92
Figure 36 Traffic > WEB > Top Sites 94
Figure 37 Traffic > WEB > Top Sites > Drill-Down 96
Figure 38 Traffic > WEB > Top Hosts 98

Figure 39 Traffic > WEB > Top Hosts > Drill-Down 100
Figure 40 Traffic > WEB > Top Users 101
Figure 41 Traffic > WEB > Top Users > Drill-Down 103
Figure 42 Traffic > FTP > Top Sites 105
Figure 43 Traffic > FTP > Top Sites > Drill-Down 107
Figure 44 Traffic > FTP > Top Hosts 108
Figure 45 Traffic > FTP > Top Hosts > Drill-Down 110
Figure 46 Traffic > FTP > Top Users 112
Figure 47 Traffic > FTP > Top Users > Drill-Down 114
Figure 48 Traffic > MAIL > Top Sites 116
Figure 49 Traffic > MAIL > Top Sites > Drill-Down 118
Figure 50 Traffic > MAIL > Top Hosts 119
Figure 51 Traffic > MAIL > Top Hosts > Drill-Down 121
Figure 52 Traffic > MAIL > Top Users 123
Figure 53 Traffic > MAIL > Top Users > Drill-Down 125
Figure 54 Traffic > Customization > Customization (Platform Selection) 126
Figure 55 Traffic > Customization > Customization (Service Settings) 127
Figure 56 Traffic > Customization > Top Destinations 128
Figure 57 Traffic > Customization > Top Destinations > Drill-Down 130
Figure 58 Traffic > Customization > Top Sources 131
Figure 59 Traffic > Customization > Top Sources > Drill-Down 133
Figure 60 Traffic > Customization > Top Users 134
Figure 61 Traffic > Customization > Top Users > Drill-Down 136
Figure 62 VPN > Site-to-Site > Link Status 139
Figure 63 VPN > Site-to-Site > Traffic Monitor 140
Figure 64 VPN > Site-to-Site > Top Peer Gateways 142
Figure 65 VPN > Site-to-Site > Top Peer Gateways > Drill-Down 144
Figure 66 VPN > Site-to-Site > Top Sites 145
Figure 67 VPN > Site-to-Site > Top Sites > Drill-Down 147
Figure 68 VPN > Site-to-Site > Top Tunnels 149
Figure 69 VPN > Site-to-Site > Top Tunnels > Drill-Down 151
Figure 70 VPN > Site-to-Site > Top Protocols 152
Figure 71 VPN > Site-to-Site > Top Protocols > Drill-Down 155
Figure 72 VPN > Site-to-Site > Top Hosts 156
Figure 73 VPN > Site-to-Site > Top Hosts > Drill-Down 159
Figure 74 VPN > Site-to-Site > Top Users 161
Figure 75 VPN > Site-to-Site > Top Users > Drill-Down 163
Figure 76 VPN > Site-to-Site > Top Destinations 165
Figure 77 VPN > Site-to-Site > Top Destinations > Drill-Down 167
Figure 78 VPN > Remote Access > Total Users And Traffic 169
Figure 79 VPN > Remote Access > User Status 170
Figure 80 VPN > Remote Access > Top Protocols 171
Figure 81 VPN > Remote Access > Top Protocols > Drill-Down 173

Figure 82 VPN > Remote Access > Top Destinations 175
Figure 83 VPN > Remote Access > Top Destinations > Drill-Down 177
Figure 84 VPN > Xauth> Successful Login 179
Figure 85 VPN > Xauth> Failed Login 180
Figure 86 Network Attack > Attack > Summary 186
Figure 87 Network Attack > Attack > Summary > Drill-Down 188
Figure 88 Network Attack > Attack > Top Attacks 190
Figure 89 Network Attack > Attack > Top Attacks > Drill-Down 192
Figure 90 Network Attack > Attack > Top Sources 194
Figure 91 Network Attack > Attack > Top Sources > Drill-Down 196
Figure 92 Network Attack > Attack > By Type 197
Figure 93 Network Attack > Attack > By Type > Drill-Down 199
Figure 94 Network Attack > Intrusion > Summary 200
Figure 95 Network Attack > Intrusion > Summary > Drill-Down 202
Figure 96 Network Attack > Intrusion > Top Intrusions 203
Figure 97 Network Attack > Intrusion > Top Intrusions > Drill-Down 205
Figure 98 Network Attack > Intrusion > Top Sources 207
Figure 99 Network Attack > Intrusion > Top Sources > Drill-Down 209
Figure 100 Intrusion > Top Destinations 210
Figure 101 Network Attack > Intrusion > Top Destinations > Drill-Down 212
Figure 102 Network Attack > Intrusion > By Severity 214
Figure 103 Network Attack > Intrusion > By Severity > Drill-Down 216
Figure 104 Network Attack > AntiVirus > Summary 217
Figure 105 Network Attack > AntiVirus > Summary > Drill-Down 219
Figure 106 Network Attack > AntiVirus > Top Viruses 221
Figure 107 Network Attack > AntiVirus > Top Viruses > Drill-Down 223
Figure 108 Network Attack > AntiVirus > Top Sources 225
Figure 109 Network Attack > AntiVirus > Top Sources > Drill-Down 227
Figure 110 Network Attack > AntiVirus > Top Destinations 229
Figure 111 Network Attack > AntiVirus > Top Destinations > Drill-Down 231
Figure 112 Network Attack > AntiSpam > Summary 233
Figure 113 Network Attack > AntiSpam > Summary > Drill-Down 235
Figure 114 Network Attack > AntiSpam > Top Senders 237
Figure 115 Network Attack > AntiSpam > Top Sources 239
Figure 116 Network Attack > AntiSpam > By Score 241
Figure 117 Security Policy > Firewall Access Control > Top Users Blocked 244
Figure 118 Security Policy > Firewall Access Control > Top Packets Blocked 246
Figure 119 Security Policy > Application Access Control > Top Applications Blocked 248
Figure 120 Security Policy > Application Access Control > Top Users Blocked 250
Figure 121 Security Policy > Application Access Control > Top Applications Allowed 252
Figure 122 Security Policy > WEB Blocked > Summary 254
Figure 123 Security Policy > WEB Blocked > Summary > Drill-Down 256
Figure 124 Security Policy > WEB Blocked > Top Sites 257

Figure 125 Security Policy > WEB Blocked > Top Sites > Drill-Down 259
Figure 126 Security Policy > WEB Blocked > Top Hosts 260
Figure 127 Security Policy > WEB Blocked > Top Hosts > Drill-Down 262
Figure 128 Security Policy > WEB Blocked > Top Users 264
Figure 129 Security Policy > WEB Blocked > Top Users > Drill-Down 266
Figure 130 Security Policy > WEB Blocked > By Category 267
Figure 131 Security Policy > WEB Blocked > By Category > Drill-Down 269
Figure 132 Security Policy > WEB Allowed > Summary 270
Figure 133 Security Policy > WEB Allowed > Summary > Drill-Down 272
Figure 134 Security Policy > WEB Allowed > Top Sites 274
Figure 135 Security Policy > WEB Allowed > Top Sites > Drill-Down 276
Figure 136 Security Policy > WEB Allowed > Top Hosts 277
Figure 137 Security Policy > WEB Allowed > Top Hosts > Drill-Down 279
Figure 138 Security Policy > WEB Allowed > Top Users 281
Figure 139 Security Policy > WEB Allowed > Top Users > Drill-Down 283
Figure 140 Event > Login > Successful Login 287
Figure 141 Event > Login > Failed Login 289
Figure 142 Event > Session Per Host > Top Hosts 290
Figure 143 Event > Session Per Host > Top Users 292
Figure 144 Log Viewer > All Logs 296
Figure 145 Schedule Report > Summary 300
Figure 146 Schedule Report > Summary > Add (Daily Report)) 302
Figure 147 Schedule Report > Summary > Add (Weekly Report) 305
Figure 148 Schedule Report > Summary > Add (Overtime Report) 308
Figure 149 Schedule Report > Template 311
Figure 150 Schedule Report > Template > Add 312
Figure 151 System > General Configuration 318
Figure 152 Windows XP: Start Menu 319
Figure 153 Windows XP: Control Panel 320
Figure 154 Windows XP: Control Panel: Network Connections: Properties 320
Figure 155 Windows XP: Local Area Connection Properties 321
Figure 156 Windows XP: Advanced TCP/IP Settings: WINS 321
Figure 157 System > Server Configuration 322
Figure 158 System > User Management 323
Figure 159 Add/Edit User Account Screen 324
Figure 160 System > Data Maintenance > Configuration 325
Figure 161 System > Data Maintenance > Device List 326
Figure 162 System > Upgrade 327
Figure 163 System > Registration 328
Figure 164 Registration Screen 329
Figure 165 System > Log Receiver By Day(Summary) 331
Figure 166 System > Log Receiver By Day(Summary) > By Device 331
Figure 167 System > Log Receiver By Day(Summary) > By Device > By Category 332

Figure 168 System > Log Receiver By Device) 333
Figure 169 System > Log Receiver By Device > By Category 334
Figure 170 System > About 334
Figure 171 Windows XP: Start Menu 346
Figure 172 Windows XP: Control Panel 346
Figure 173 Windows XP: Control Panel: Network Connections: Properties 347
Figure 174 Windows XP: Local Area Connection Properties 347
Figure 175 Windows XP: Advanced TCP/IP Settings 348
Figure 176 Windows XP: Internet Protocol (TCP/IP) Properties 349

List of Tables

Table 1 Differences Between Basic Version and Full Version 32
Table 2 Processing Times by Menu Item 34
Table 3 ZyNOS-based ZyXEL Device Configuration Requirements by Menu Item 35
Table 4 ZyWALL 1050 Configuration Requirements by Menu Item 36
Table 5 Title Bar 40
Table 6 Device Window 41
Table 7 Add/Edit Device and Add/Edit Folder Screen Fields 43
Table 8 Function Window 44
Table 9 Function differences for Basic and Full Versions 51
Table 10 Device Information Screen Fields 52
Table 11 Typical Monitor Features 54
Table 12 Typical Statistical Report Features 55
Table 13 View Logs 57
Table 14 Dashboard 61
Table 15 Monitor > Bandwidth 65
Table 16 Monitor > Service 67
Table 17 Monitor > Attack 68
Table 18 Monitor > Intrusion 69
Table 19 Monitor > AntiVirus 70
Table 20 Monitor > AntiSpam 71
Table 21 Traffic > Bandwidth > Summary 74
Table 22 Traffic > Bandwidth > Summary > Drill-Down 76
Table 23 Traffic > Bandwidth > Top Protocols 78
Table 24 Traffic > Bandwidth > Top Protocol > Drill-Down 80
Table 25 Traffic > Bandwidth > Top Hosts 82
Table 26 Traffic > Bandwidth > Top Hosts > Drill-Down 85
Table 27 Traffic > Bandwidth > Top Users 86
Table 28 Traffic > Bandwidth > Top Users > Drill-Down 88
Table 29 Traffic > Bandwidth > Top Destinations 90
Table 30 Traffic > Bandwidth > Top Destinations > Drill-Down 93
Table 31 Traffic > WEB > Top Sites 94
Table 32 Traffic > WEB > Top Sites > Drill-Down 96
Table 33 Traffic > WEB > Top Hosts 98
Table 34 Traffic > WEB > Top Hosts > Drill-Down 100
Table 35 Traffic > WEB > Top Users 102
Table 36 Traffic > WEB > Top Users > Drill-Down 104
Table 37 Traffic > FTP > Top Sites 105
Table 38 Traffic > FTP > Top Sites > Drill-Down 107

Table 39 Traffic > FTP > Top Hosts 109
Table 40 Traffic > FTP > Top Hosts > Drill-Down 111
Table 41 Traffic > FTP > Top Users 112
Table 42 Traffic > FTP > Top Hosts > Drill-Down 114
Table 43 Traffic > MAIL > Top Sites 116
Table 44 Traffic > MAIL > Top Sites > Drill-Down 118
Table 45 Traffic > MAIL > Top Hosts 120
Table 46 Traffic > MAIL > Top Hosts > Drill-Down 122
Table 47 Traffic > MAIL > Top Users 123
Table 48 Traffic > MAIL > Top Users > Drill-Down 125
Table 49 Service > Customization > Customization (Service Settings) 127
Table 50 Traffic > Customization > Top Destinations 128
Table 51 Traffic > Customization > Top Destinations > Drill-Down 130
Table 52 Traffic > Customization > Top Sources 131
Table 53 Traffic > Customization > Top Sources > Drill-Down 133
Table 54 Traffic > Customization > Top Users 135
Table 55 Traffic > Customization > Top Users > Drill-Down 137
Table 56 VPN > Site-to-Site > Link Status 140
Table 57 VPN > Site-to-Site > Traffic Monitor 141
Table 58 VPN > Site-to-Site > Top Peer Gateways 142
Table 59 VPN > Site-to-Site > Top Peer Gateways > Drill-Down 144
Table 60 VPN > Site-to-Site > Top Sites 146
Table 61 VPN > Site-to-Site > Top Sites > Drill-Down 148
Table 62 VPN > Site-to-Site > Top Tunnels 149
Table 63 VPN > Site-to-Site > Top Tunnels > Drill-Down 151
Table 64 VPN > Site-to-Site > Top Protocols 153
Table 65 VPN > Site-to-Site > Top Protocols > Drill-Down 155
Table 66 VPN > Site-to-Site > Top Hosts 157
Table 67 VPN > Site-to-Site > Top Hosts > Drill-Down 159
Table 68 VPN > Site-to-Site > Top Users 161
Table 69 VPN > Site-to-Site > Top Users > Drill-Down 164
Table 70 VPN > Site-to-Site > Top Destinations 165
Table 71 VPN > Site-to-Site > Top Destinations > Drill-Down 168
Table 72 VPN > Remote Access > Total Users And Traffic 169
Table 73 VPN > Remote Access > User Status 170
Table 74 VPN > Remote Access > Top Protocols 171
Table 75 VPN > Remote Access > Top Protocols > Drill-Down 173
Table 76 VPN > Remote Access > Top Destinations 175
Table 77 VPN > Remote Access > Top Destinations > Drill-Down 177
Table 78 VPN > Xauth> Successful Login 179
Table 79 VPN > Xauth> Failed Login 180
Table 80 Network Attack > Attack > Summary 186
Table 81 Network Attack > Attack > Summary > Drill-Down 188

Table 82 Network Attack > Attack > Top Attacks 190
Table 83 Network Attack > Attack > Top Attacks > Drill-Down 192
Table 84 Network Attack > Attack > Top Sources 194
Table 85 Network Attack > Attack > Top Sources > Drill-Down 196
Table 86 Network Attack > Attack > By Type 198
Table 87 Network Attack > Attack > By Type > Drill-Down 199
Table 88 Network Attack > Intrusion > Summary 201
Table 89 Network Attack > Intrusion > Summary > Drill-Down 202
Table 90 Network Attack > Intrusion > Top Intrusions 204
Table 91 Network Attack > Intrusion > Top Intrusions > Drill-Down 205
Table 92 Network Attack > Intrusion > Top Sources 207
Table 93 Network Attack > Intrusion > Top Sources > Drill-Down 209
Table 94 Intrusion > Top Destinations 211
Table 95 Network Attack > Intrusion > Top Destinations > Drill-Down 212
Table 96 Network Attack > Intrusion > By Severity 214
Table 97 Network Attack > Intrusion > By Severity > Drill-Down 216
Table 98 Network Attack > AntiVirus > Summary 218
Table 99 Network Attack > AntiVirus > Summary > Drill-Down 219
Table 100 Network Attack > AntiVirus > Top Viruses 221
Table 101 Network Attack > AntiVirus > Top Viruses > Drill-Down 223
Table 102 Network Attack > AntiVirus > Top Sources 225
Table 103 Network Attack > AntiVirus > Top Sources > Drill-Down 227
Table 104 Network Attack > AntiVirus > Top Destinations 229
Table 105 Network Attack > AntiVirus > Top Destinations > Drill-Down 231
Table 106 Network Attack > AntiSpam > Summary 233
Table 107 Network Attack > AntiSpam > Summary > Drill-Down 235
Table 108 Network Attack > AntiSpam > Top Senders 237
Table 109 Network Attack > AntiSpam > Top Sources 239
Table 110 Network Attack > AntiSpam > By Score 241
Table 111 Security Policy > Firewall Access Control > Top Users Blocked 244
Table 112 Security Policy > Firewall Access Control > Top Packets Blocked 246
Table 113 Security Policy > Application Access Control > Top Applications Blocked 248
Table 114 Security Policy > Application Access Control > Top Applications Blocked 250
Table 115 Security Policy > Application Access Control > Top Applications Allowed 252
Table 116 Security Policy > WEB Blocked > Summary 254
Table 117 Security Policy > WEB Blocked > Summary > Drill-Down 256
Table 118 Security Policy > WEB Blocked > Top Sites 258
Table 119 Security Policy > WEB Blocked > Top Sites > Drill-Down 259
Table 120 Security Policy > WEB Blocked > Top Hosts 261
Table 121 Security Policy > WEB Blocked > Top Hosts > Drill-Down 262
Table 122 Security Policy > WEB Blocked > Top Users 264
Table 123 Security Policy > WEB Blocked > Top Users > Drill-Down 266
Table 124 Security Policy > WEB Blocked > By Category 268

Table 125 Security Policy > WEB Blocked > By Category > Drill-Down 269
Table 126 Security Policy > WEB Allowed > Summary 271
Table 127 Security Policy > WEB Allowed > Summary > Drill-Down 272
Table 128 Security Policy > WEB Allowed > Top Sites 274
Table 129 Security Policy > WEB Allowed > Top Sites > Drill-Down 276
Table 130 Security Policy > WEB Allowed > Top Hosts 278
Table 131 Security Policy > WEB Allowed > Top Hosts > Drill-Down 279
Table 132 Security Policy > WEB Allowed > Top Users 281
Table 133 Security Policy > WEB Allowed > Top Users > Drill-Down 283
Table 134 Event > Login > Successful Login 288
Table 135 Event > Device Login > Failed Login 289
Table 136 Event > Session Per Host > Top Hosts 291
Table 137 Event > Session Per Host > Top Users 293
Table 138 Log Viewer > All Logs 296
Table 139 Schedule Report > Summary 300
Table 140 Schedule Report > Summary > Add (Daily Report) 303
Table 141 Schedule Report > Summary > Add (Weekly Report) 306
Table 142 Schedule Report > Summary > Add (Overtime Report) 309
Table 143 Schedule Report > Template 311
Table 144 Schedule Report > Template > Add 312
Table 145 System > General Configuration 318
Table 146 System > Server Configuration 322
Table 147 System > User Management 323
Table 148 Add/Edit User Account Screen 324
Table 149 System > Data Maintenance > Configuration 326
Table 150 System > Data Maintenance > Device List 326
Table 151 System > Upgrade 327
Table 152 Information for Using an Existing MyZyXEL.com Account 328
Table 153 Information for Upgrading the Version or Number of Devices 328
Table 154 System > Registration 328
Table 155 Registration Screen 330
Table 156 System > Log Receiver By Day(Summary) 331
Table 157 System > Log Receiver By Day(Summary) > By Device 331
Table 158 System > Log Receiver By Day(Summary) > By Device > By Category 332
Table 159 System > Log Receiver By Device 333
Table 160 System > Log Receiver By Device > By Category 334
Table 161 Troubleshooting 335
Table 162 Web Configurator Specifications 339
Table 163 System Notifications Specifications 339
Table 164 Feature Specifications 339
Table 165 Key Features 339
Table 166 VRPT 3.0 Device and Feature Support 340
Table 167 System Maintenance Logs 351

Table 168 System Error Logs 353
Table 169 Access Control Logs 353
Table 170 TCP Reset Logs 354
Table 171 Packet Filter Logs 355
Table 172 ICMP Logs 355
Table 173 CDR Logs 355
Table 174 PPP Logs 356
Table 175 UPnP Logs 356
Table 176 Content Filtering Logs 356
Table 177 Attack Logs 357
Table 178 Remote Management Logs 358
Table 179 Wireless Logs 359
Table 180 IPSec Logs 359
Table 181 IKE Logs 360
Table 182 PKI Logs 363
Table 183 802.1X Logs 365
Table 184 ACL Setting Notes 366
Table 185 ICMP Notes 366
Table 186 IDP Logs 368
Table 187 AV Logs 368
Table 188 AS Logs 370
Table 189 AS Directions for Multiple WAN Devices 371
Table 190 AS Directions for Single WAN Devices 371
Table 191 Syslog Logs 372
Table 192 RFC-2408 ISAKMP Payload Types 373
Table 193 Content Filter Logs 375
Table 194 Forward Web Site Logs 375
Table 195 Blocked Web Site Logs 375
Table 196 User Logs 377
Table 197 myZyXEL.com Logs 378
Table 198 IDP Logs 382
Table 199 Application Patrol Logs 385
Table 200 IKE Logs 387
Table 201 IPSec Logs 391
Table 202 Firewall Logs 392
Table 203 Sessions Limit Logs 393
Table 204 Policy Route Logs 393
Table 205 Built-in Services Logs 394
Table 206 System Logs 397
Table 207 Connectivity Check Logs 401
Table 208 Device HA Logs 403
Table 209 Routing Protocol Logs 405
Table 210 NAT Logs 407

Table 211 PKI Logs 408
Table 212 Interface Logs 411
Table 213 Account Logs 414
Table 214 Port Grouping Logs 414
Table 215 Force Authentication Logs 414
Table 216 File Manager Logs 415

PART I
Introduction

Introducing Vantage Report (31)
The Vantage Report Server (33)
The Web Configurator (37)

1

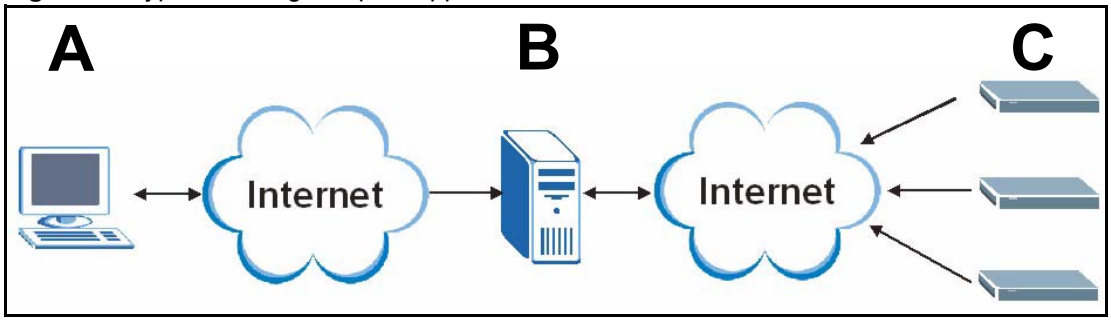
Introducing Vantage Report

Please see the Quick Start Guide for Vantage Report setup requirements, installation, and access. This chapter introduces Vantage Report. See Appendix A on page 339 for a list of key features.

1.1 Introduction

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

Figure 1 Typical Vantage Report Application



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

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

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

1.2 Versions

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

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

The following table shows some of the differences between the basic and full version.

Table 1 Differences Between Basic Version and Full Version

FEATURE	BASIC	FULL
Number of supported devices	1	up to 100
Supported formats for scheduled reports	PDF	PDF, HTML
Drill-down reports	1 layer	2 layers
Reverse DNS lookup	no	yes
Reverse Hostname lookup	no	yes
Web usage by category	no	yes
AntiVirus	no	yes
AntiSpam	no	yes
Dashboard	no	yes
Number of scheduled reports	20	20 per device
Customizable scheduled report templates	no	yes
Schedule Report Format	PDF	PDF, HTML
Reports for the ZyWALL 1050	no	yes

There is also a free trial of the full version. The trial version is the same as the full version except that it only supports one device. You can get the trial version by registering Vantage Report. See Section 12.6 on page 327 for more information

2

The Vantage Report Server

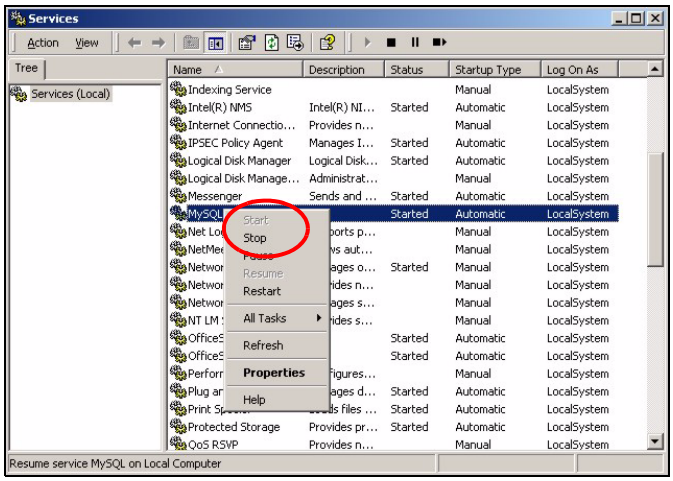
This chapter explains several characteristics of the Vantage Report server.

2.1 Starting and Stopping the Vantage Report Server

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

Before the Vantage Report server can send e-mail to anyone, you have to configure the SMTP mail server. See Section 12.2 on page 322 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 12.3 on page 323). 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 11 on page 299 for more information.
- **system notifications** - When certain system parameters cross a threshold (minimum or maximum) value, the Vantage Report server sends e-mail to the Vantage Report administrator (the e-mail address associated with the **root** account). Some of these messages are warnings; in some situations, however, the Vantage Report server starts or stops receive logs. See Appendix A on page 339 for a list of parameters and threshold values. One of the threshold values can be configured. See Section 12.1 on page 317.
- **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 37 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 12.2 on page 322 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

Table 2 Processing Times by Menu Item

MENU ITEM	TIME (MIN)
Traffic, Network Attack, Security Policy, Authentication	5
Log Viewer > All Logs	5

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 ZyNOS-based ZyXEL Device Configuration Requirements 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	traffic statistics	--	--
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 > Firewall Access Control	log entries	Access Control	--
Security Policy > Application Access Control	N/A	N/A	N/A
Security Policy > WEB Blocked	log entries	Blocked Web Sites	--
Security Policy > WEB Allowed	log entries	Forward Web Sites	--
Event > Login	log entries	System Maintenance	--
Event > Session Per Host	log entries	Access Control	--
Log Viewer > All 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.

Table 4 ZyWALL 1050 Configuration Requirements by Menu Item

MENU ITEM(S)	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Monitor > Bandwidth	traffic statistics	--	--
Monitor > Service	traffic statistics	--	--
Monitor > Attack	log entries	IDP	--
Monitor > Intrusion	log entries	IDP	IDP > Signature
Monitor > AntiVirus	N/A	N/A	N/A
Monitor > AntiSpam	N/A	N/A	N/A
Traffic	traffic statistics log entries	-- User	--
VPN	log entries	IPSec, User	--
Network Attack > Attack	log entries	IDP	--
Network Attack > Intrusion	log entries	IDP	IDP > Signature
Network Attack > AntiVirus	N/A	N/A	N/A
Network Attack > AntiSpam	N/A	N/A	N/A
Security Policy > Firewall Access Control	log entries	Firewall	--
Security Policy > Application Access Control	log entries	Application Patrol	--
Security Policy > WEB Blocked	log entries	Blocked web sites	--
Security Policy > WEB Allowed	log entries	Forward web sites	--
Event > Login	log entries	User	--
Event > Session Per Host	log entries	Sessions Limit, User	--
Log Viewer > All 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.

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

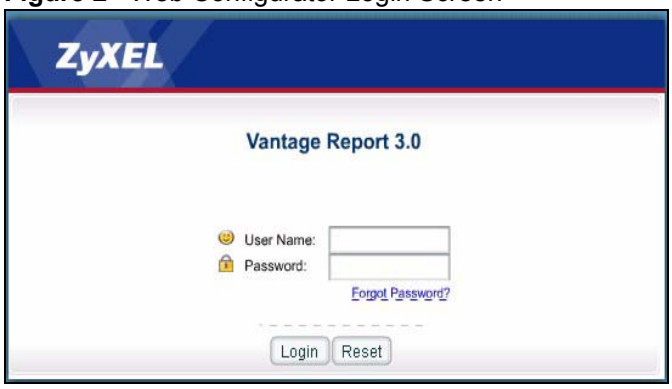
To access the web configurator, follow these steps:

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



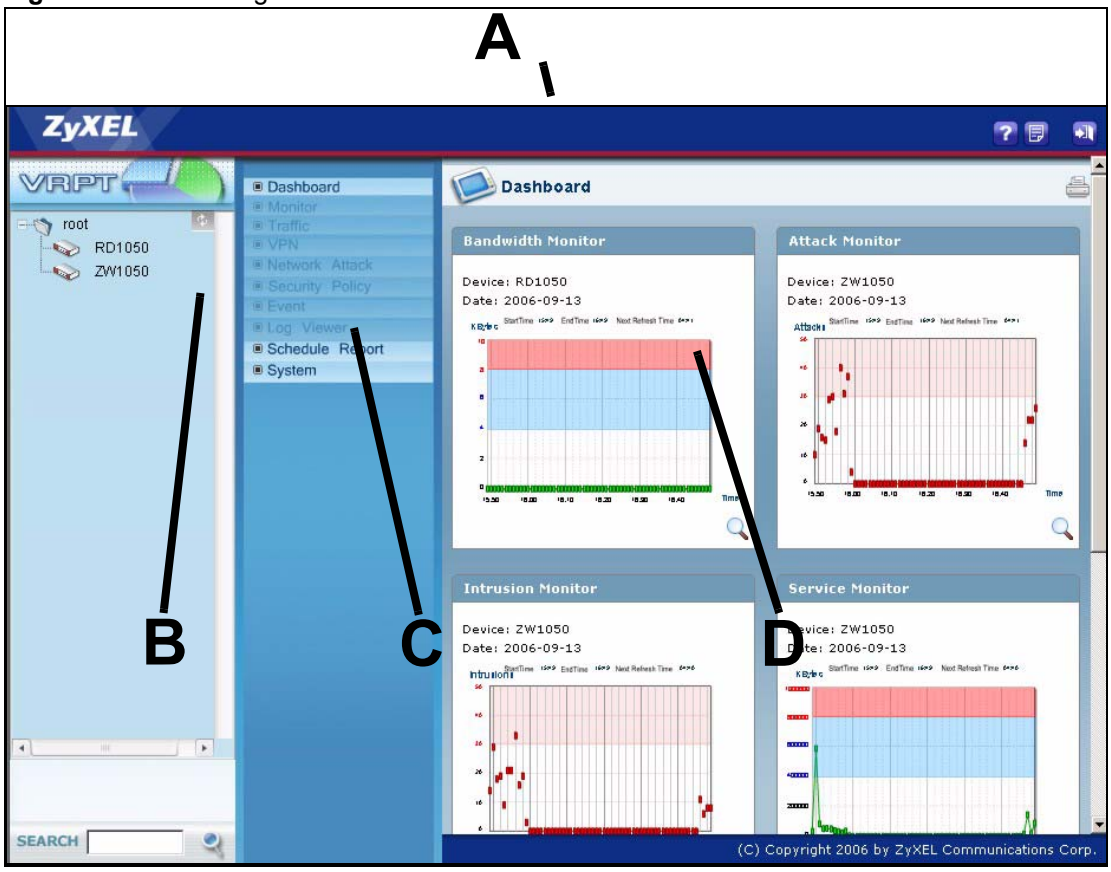
If you forget your password, enter your user name, and click **Forget Password?**. Vantage Report sends your password to the e-mail address (if any) for your **User Name**. See Section 2.2 on page 34 for more information about e-mail in Vantage Report and Section 12.3 on page 323 for more information about SMTP configuration.

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

See Section 12.3 on page 323 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).

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 5 Title Bar

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

3.4 Device Window

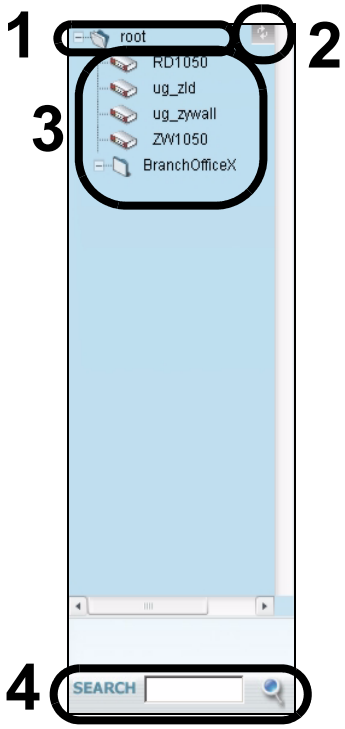
Use the device window to select which device(s) you want to include in a report, add devices to Vantage Report, and remove devices from Vantage Report.

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 6 Device Window

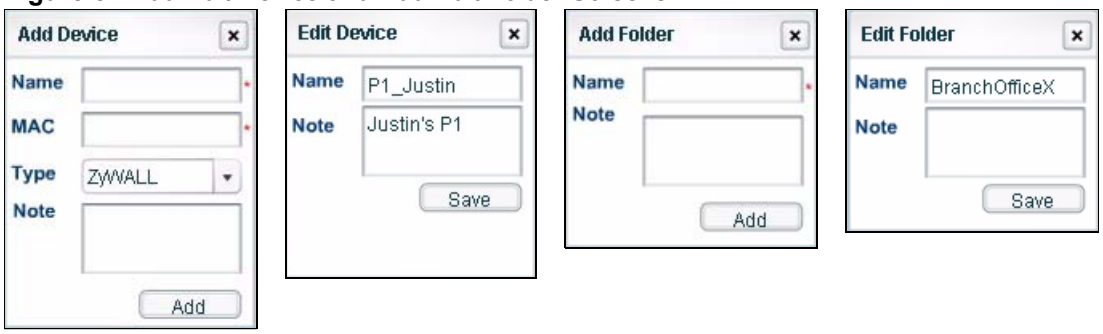
SECTION	DESCRIPTION
1	**To add a device to Vantage Report,** • right click on root, and select **Add Device**. The **Add Device** screen appears in the device window. (See Figure 5.) **To add a folder to Vantage Report,** • right click on root, and select **Add Folder**. The **Add Folder** screen appears in the device window. (See Figure 5.)
2	**To update the device window,** • click the **Refresh** button.

Table 6 Device Window

SECTION	DESCRIPTION
3	**To move a device in the device window tree** • right-click on the device, and select **Cut it**. Then right-click the destination folder and select **Paste to**. **To select which device is included in a report** • click on the device. **To look at the basic information about a device,** • click on the device. The **Device Information** screen appears in the report window. (See Figure 5.) **To edit the basic information about a device,** • right-click on the device, and select **Edit Device**. The **Edit Device** screen appears in the device window. (See Figure 5.) **To edit the basic information about a folder,** • right-click on the folder, and select **Edit Folder**. The **Edit Folder** screen appears in the device window. (See Figure 5.) **To remove a device from Vantage Report,** • right-click on the device, and select **Delete Device**. Vantage Report confirms you want to delete it before doing so. **To remove a folder from Vantage Report,** • right-click on the folder, and select **Delete Folder**. Vantage Report confirms you want to delete it before doing so.
4	**To search for a device,** • type any part of the name, MAC address, or note 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 (see Section 3.6.1 on page 52). 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 on page 42.

Figure 5 Add/Edit Device and Add/Edit Folder Screens



Each field is explained in the following table.

Table 7 Add/Edit Device and Add/Edit Folder Screen Fields

LABEL	DESCRIPTION
Name	Enter the name of the device or folder you want to add to Vantage Report. The device name can consist of alphanumeric characters, underscores(_), periods(.), or dashes(-), and it must be 1-28 characters long. This name is used to refer to the device (or folder) in Vantage Report, and it has to be different than other device (or folder) names in Vantage Report. You can use the system name of a device as the name for that device.
MAC	This field is not available in the **Edit Device** screen. Enter the LAN MAC address of the device you want to add. For the ZyWALL 1050, use the first (lowest) LAN MAC address. Once you add the device, you cannot change the MAC address anymore.
Type	This field is not available in the **Edit Device** screen. Select the model type of the device you want to add. Choices are: **ZyWALL**, **Prestige**, **IDP 10**, and **ZyWALL 1050**. Not all reports (and fields in reports) are available with all models. See Table 166 on page 340 for a list of which items Vantage Report supports with various firmware versions of various devices.
Note	Enter any additional notes you want to make for the device or folder here.
Add	This field is available in the **Add Device** screen. Click this to add the device to Vantage Report. It takes time before Vantage Report displays information received from this device.
Save	This field is available in the **Edit Device** screen. Click this to save your changes to Vantage Report.

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

Figure 6 Device Window Right-Click Menu

Click **About Macromedia Flash Player 8...** to get information about the current version of Flash.

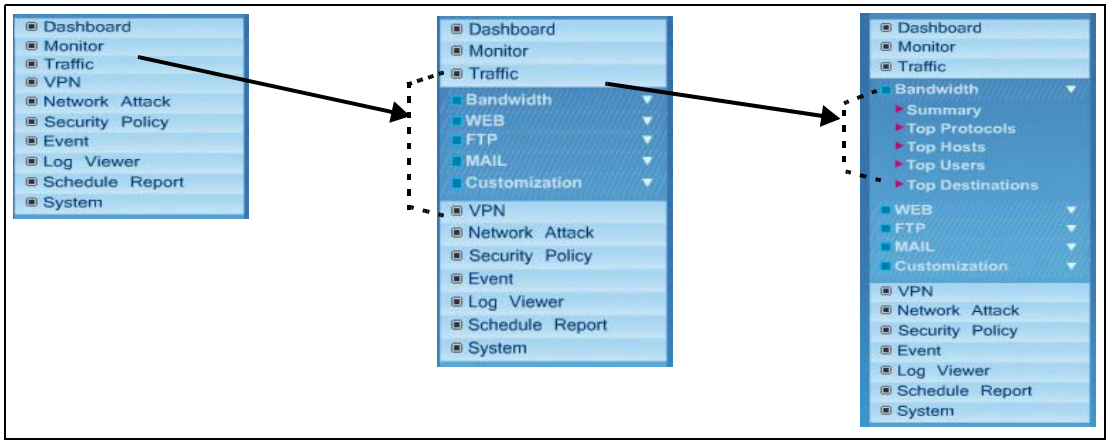
3.5 Function Window

Use the function window to select which monitor, statistical report, or screen you want to open.

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



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 8 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.

Not every report (or fields in a report) is available with every model of device and firmware version. See Table 166 on page 340 for a list of which items Vantage Report supports with various firmware versions of various devices.

Table 8 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
Dashboard		The dashboard gives a quick top level summary of activity across devices. The dashboard is available with the full version of Vantage Report.
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.

Table 8 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
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.
	Top Users	Use this report to look at the top users generating traffic through the selected device. You can also use this report to look at the top services used by any top bandwidth user.
	Top Destinations	Use this report to look at the top destinations of traffic in the selected device. You can also use this report to look at the services that were used the most to access the top destination IP addresses.
WEB	Top Sites	Use this report to look at the top destinations of web traffic. You can also use this report to look at the top sources of web traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of web traffic. You can also use this report to look at the top destinations of web traffic for any top source.
	Top Users	Use this report to look at the top sources of web traffic by user. You can also use this report to look at the top destinations of web traffic for any top user.
FTP	Top Sites	Use this report to look at the top destinations of FTP traffic. You can also use this report to look at the top sources of FTP traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of FTP traffic. You can also use this report to look at the top destinations of FTP traffic for any top source.
	Top Users	Use this report to look at the top sources of FTP traffic by user. You can also use this report to look at the top destinations of FTP traffic for any top user.
MAIL	Top Sites	Use this report to look at the top destinations of mail traffic. You can also use this report to look at the top sources of mail traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of mail traffic. You can also use this report to look at the top destinations of mail traffic for any top source.
	Top Users	Use this report to look at the top sources of mail traffic by user. You can also use this report to look at the top destinations of mail traffic for any top user.

Table 8 Function Window

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

Table 8 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
Xauth	Successful Login	Use this report to monitor the total number of users that have successfully logged in to use one of the device's VPN tunnels.
	Failed Login	Use this report to monitor the total number of users that have made unsuccessful attempts to log in to use one of the device's VPN tunnels.
Network 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 Attacks	Use this report to look at the top kinds of DoS attacks by number of attacks. You can also use this report to look at the top categories of DoS attacks for any top source.
	Top Sources	Use this report to look at the top sources of DoS attacks by number of attacks. You can also use this report to look at the top categories of DoS attacks for any top source.
	By 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.
	By Type	Use this report to look at the top categories of DoS attacks by number of attacks. You can also use this report to look at the top sources of DoS attacks for any top category.
Intrusion		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 8 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. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
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.
Firewall Access Control	Top Users Blocked	Use this report to look at the users from which the device blocked the most traffic.
	Top Packets Blocked	Use this report to look at the firewall rule that blocked the most packets.
Application Access Control	Top Applications Blocked	Use this report to look at the applications for which the device blocked the most connections.
	Top Users Blocked	Use this report to look at the users for which the device blocked the most connections.
	Top Applications Allowed	Use this report to look at the applications for which the device allowed the most connections.

Table 8 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
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.
	Top Users	Use this report to look at the users for which the device blocked the most web site access attempts. You can also look at the top destinations for any user for which the device blocked the most web site access attempts.
	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.
	Top Users	Use this report to look at the top users for which the device forwarded web traffic. You can also use this report to look at the top destinations for any top source of forwarded web traffic.
Event		
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.
Session Per Host		A device can limit a user's maximum number of NAT sessions. Use these screens to see who has exceeded the maximum number of NAT sessions the most often.
	Top Hosts	Use this screen to see which hosts have most frequently gone over the maximum number of NAT sessions per host.
	Top Users	Use this screen to see which users have most frequently gone over the maximum number of NAT sessions per host.
Log Viewer		Use these screens to look at log entries for the selected ZyXEL device.
All Logs		Use these log viewer screens to look at all the log entries for the selected ZyXEL device.
Schedule Report		
Summary		Use these screens to set up and maintain daily, weekly, and overtime (one-time) reports that Vantage Report sends by e-mail.

Table 8 Function Window

LEVEL 1/2	LEVEL 3	FUNCTION
Template		Use these screens to add and edit report templates.
System		The **root** account can use all of the following screens. Other users can use the **About** screen and some features in **User Management**.
General Configuration		Use this screen to maintain global reporting settings, such as how many days of logs to keep and default chart type.
Server Configuration		Use this screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports.
User Management		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	You can use this screen to backup or restore the settings in the **General Configuration**, **Server Configuration**, and **User Management** screens. (The format is XML.)
	Device List	You can use this screen to export the current device window to an XML file, or you can add devices stored in XML format to Vantage Report.
Upgrade		Use this screen to install new releases of Vantage Report. Do not use this screen to upgrade to the full version.
Registration		Use this screen to get the trial version, upgrade to the full version, or increase the number of devices Vantage Report supports.
Log Receiver	By Day(Summary)	Use this screen to look at the total number of logs that Vantage Report received by day. You can also use this screen to look at the total number of logs that Vantage Report received from each device on a particular day. You can also use this screen to look at the number of logs in each category that Vantage Report received from an individual device on a particular day.
	By Device	Use this screen to look at the number of logs in each category that Vantage Report received from an individual device over a selected range of days. You can also use this screen to look at the number of logs in each category that Vantage Report received from an individual device over a selected range of days.
About		Use this screen to get the current release and copyright for Vantage Report.

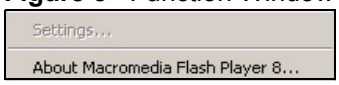
The following table lists the differences in the functions for the basic and full versions.

Table 9 Function differences for Basic and Full Versions

FEATURE	BASIC	FULL	NOTES
Bandwidth Report by Direction	ALL	Incoming Outgoing ALL LAN-WAN LAN-DMZ LAN-LAN WAN-WAN WAN-DMZ WAN-LAN DMZ-WAN DMZ-DMZ DMZ-LAN	
Traffic > Bandwidth	Yes	Yes	Bandwidth monitor is available for basic version.
Traffic > WEB	Yes	Yes	
Traffic > FTP	Yes	Yes	
Traffic > MAIL	Yes	Yes	
Traffic > Customization	Yes	Yes	
VPN > Site to Site > Top Peer Gateways	Yes	Yes	
VPN > Site to Site > Top Hosts	Yes	Yes	
VPN others	No	Yes	
Network Attack >Attack	Yes	Yes	
Network Attack > Intrusion (Report for IDP10)	Yes	Yes	Available for 2.00(XA0) and later.
Network Attack > Intrusion (Report for ZyWALL series and the ZyWALL 1050)	No	Yes	Available for 4.00 and later if ZyWALL series. Available for 1.01 and later for the ZyWALL 1050.
Network Attack >AntiVirus	No	Yes	Available for 4.00 and later.
Network Attack >AntiSpam	No	Yes	Available for 4.00 and later.
Security Policy >Firewall Access Control	No	Yes	
Security Policy > Application Access Control	No	Yes	
Security Policy > WEB Blocked > By Category	No	Yes	
Security Policy > WEB Blocked Others	Yes	Yes	
Security Policy > WEB Allowed Report	Yes	Yes	
Event > Login	Yes	Yes	
Event > Session Per Host	No	Yes	

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 8...** 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.

3.6.1 Device Information Screen

When you first click on a device in the device window, the information you configured for the device display in the report window. See Section 3.4 on page 40 for how to add and edit device information.

Figure 9 Device Information Screen

Each field is explained in the following table.

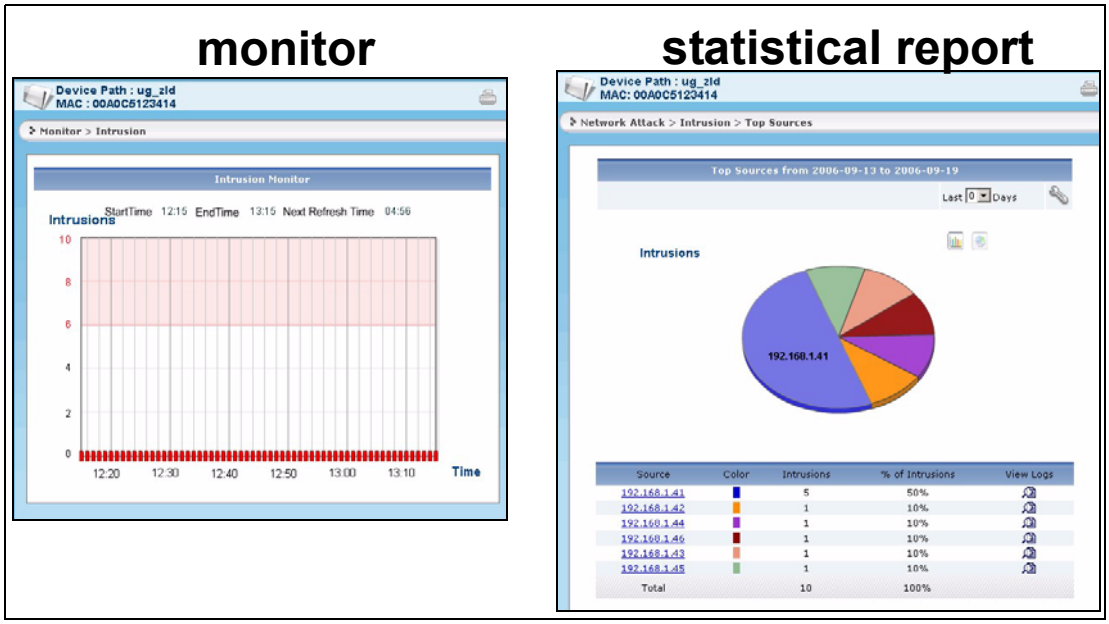
Table 10 Device Information Screen Fields

LABEL	DESCRIPTION
Device Path	You can create multiple layers of folders for devices. This field displays the name used to refer to the device in Vantage Report and the folders that the device is in. For example, if the device path is “folder1/folder2/myZW5”, “folder1” is in the root folder, “folder2” is in folder1 and “myZW5” is the name of the device and it is in folder2.
Device MAC	This is the LAN MAC address of the device. For the ZyWALL 1050, this is the first (lowest) LAN MAC address.
Device Type	This is the model type of the device. It can be **ZyWALL**, **Prestige**, **IDP 10**, and **ZyWALL 1050**. Not all reports (and fields in reports) are available with all models. See Table 166 on page 340 for a list of which items Vantage Report supports with various firmware versions of various devices.
Device Note	This is any additional notes you added for the device.

3.6.2 Monitors and Statistical Reports

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 10.

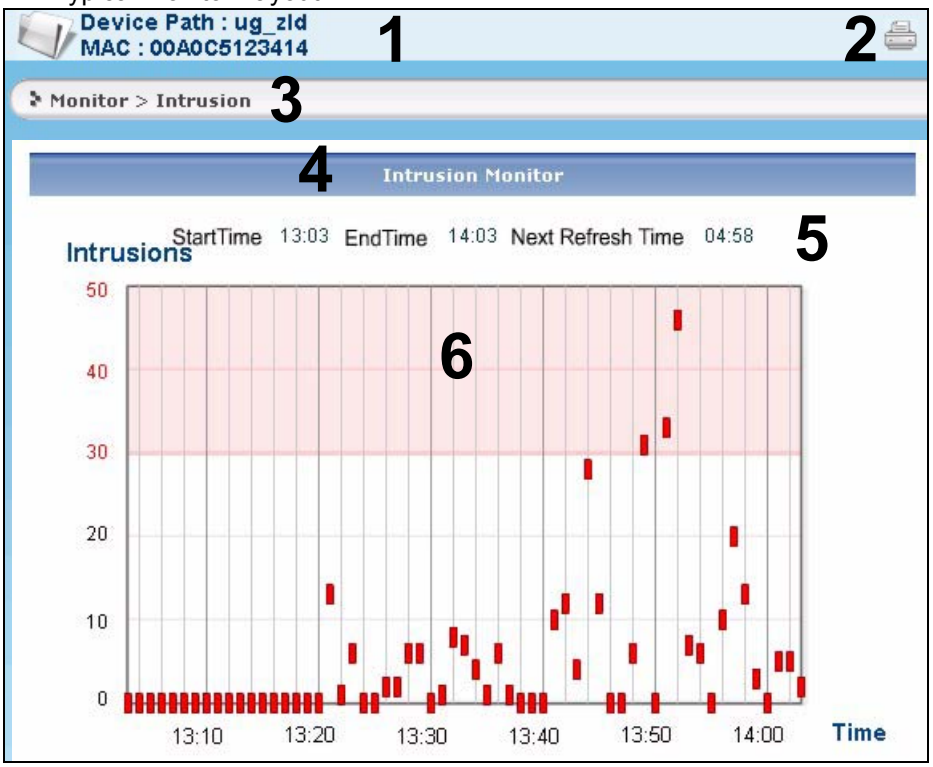
Figure 10 Report Window: Monitor and Statistical Report Examples



3.6.2.1 Monitor Layout

A typical monitor is shown in Figure 4.

Figure 11 Typical Monitor Layout



Each numbered section above is described in the following table.

Table 11 Typical Monitor Features

SECTION	DESCRIPTION
1	**Device Name**, **MAC**: These fields are the same ones you entered when you added the device. (See Section 3.4 on page 40.)
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 34.
6	The graph shows how the status changes over time. The X-axis (horizontal) is time. See Section 2.3 on page 34 for more information about clock time in Vantage Report. The Y-axis (vertical) depends on the type of monitor you select. In Figure 11, the Y-axis is the number of attacks the device has detected during one-minute intervals. See Section 2.4 on page 35 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.

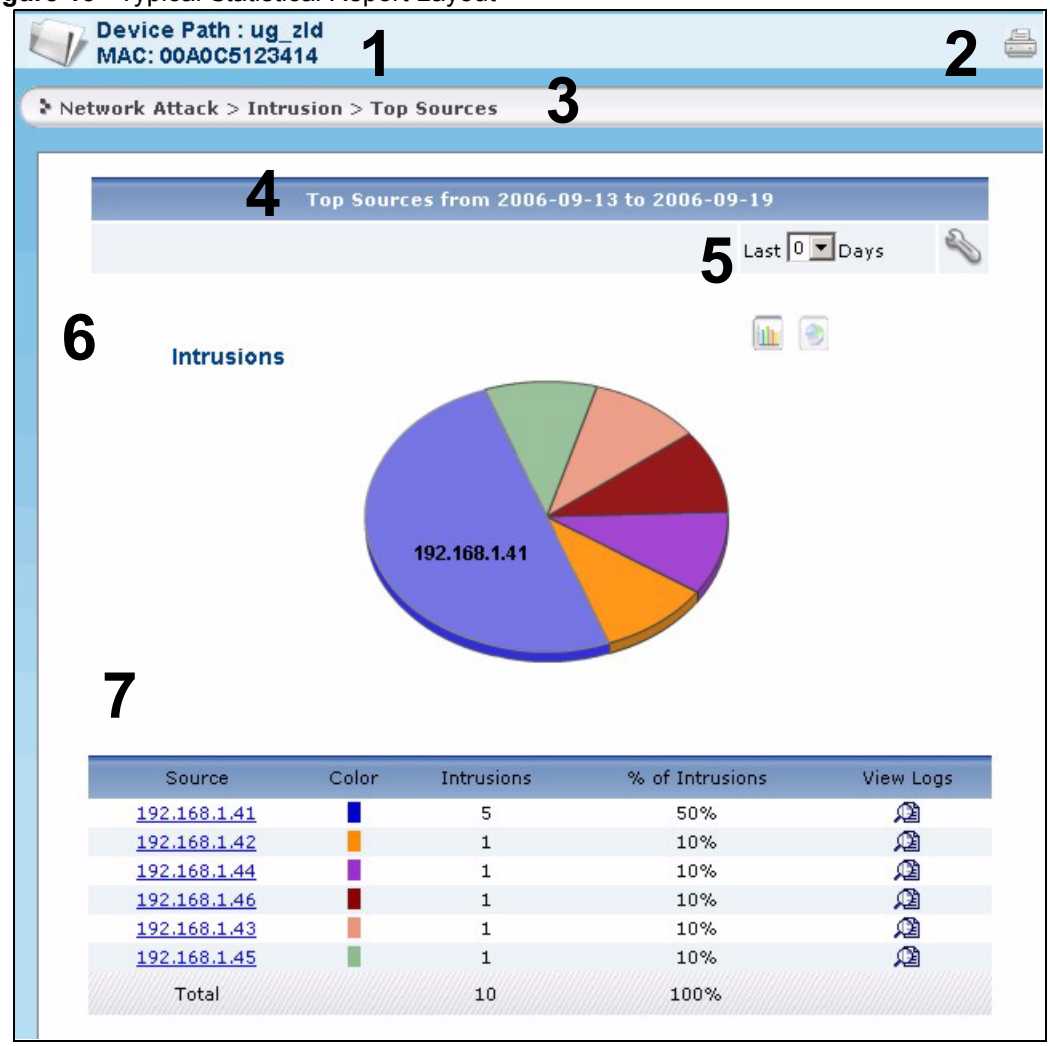
Figure 12 Report Window Right-Click Menu

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 8...** to get information about the current version of Flash.

3.6.2.2 Statistical Report Layout

A typical statistical report is shown in Figure 13.

Figure 13 Typical Statistical Report Layout



Each numbered section above is described in the following table.

Table 12 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 42.)
2	**Print** icon: Click this icon to **print** the current screen.
3	This field shows the menu items you selected to open this statistical report.
4	This field displays the title of the statistical report. The title includes the date(s) you specified in section 5.

Table 12 Typical Statistical Report Features

SECTION	DESCRIPTION
5	**Last Days**, **Settings**: Use one of these fields to specify what historical information is included in the report. • Select how many days, ending (and including) today, in the **Last 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 12.1 on page 317. 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. These fields are not available in drill-down reports because these reports use the same historical information as the main report. See Section 2.3 on page 34 for more information about time in these screens.
6	The graph displays the specified report visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. See Section 12.1 on page 317. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little. See Section 2.4 on page 35 for more information about the source data used by the statistical report.
7	In the table, • Click on a link to drill down into the report. The current report is replaced by a detailed report for the selected record. The detailed report uses the same historical information you select in #5. • If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with IP addresses (for example, “www.yahoo.com/ 200.100.20.10”). See Section 12.1 on page 317. • Some reports provide extra information (for example, number of traffic events) in the table. See each report for more information. • Click a view logs icon to display the logs related to the individual record. See See Section 2.4 on page 35 for more information about the source data used by the statistical report.

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

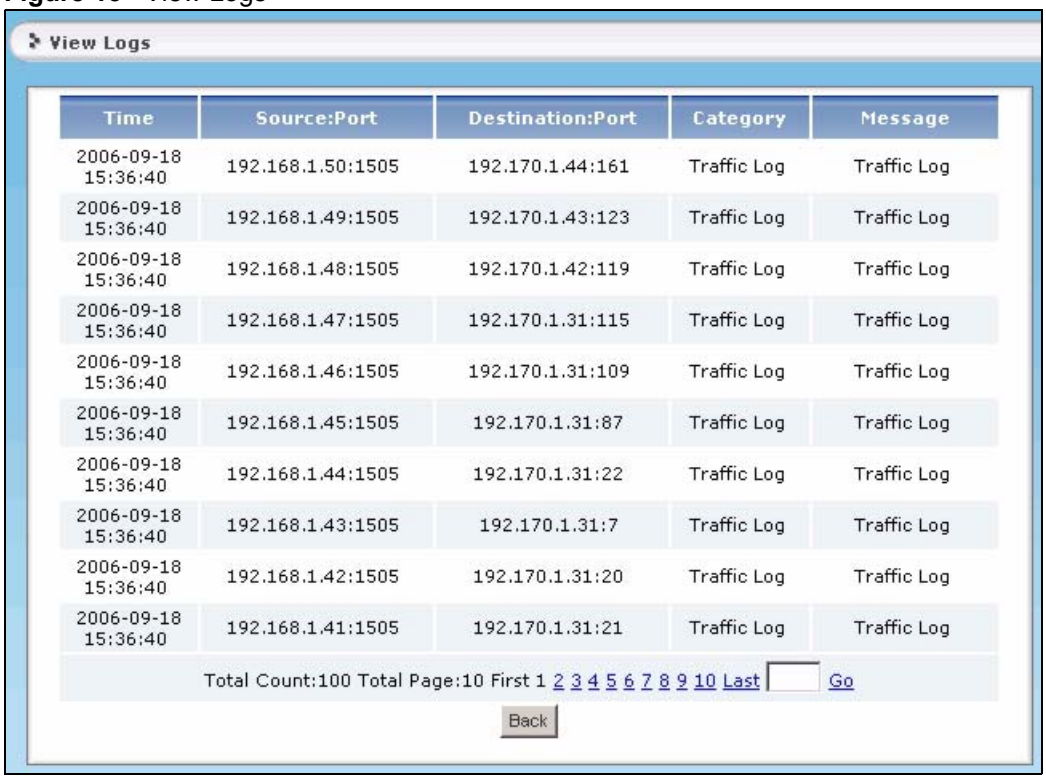
Figure 14 Report Window Right-Click Menu

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 8...** to get information about the current version of Flash.

3.6.3 View Logs

The **View Logs** screen displays the logs related to an individual record in a statistical report. See Appendix C on page 351 and Appendix D on page 375 for information on the logs.

Figure 15 View Logs



Each field is described in the following table.

Table 13 View Logs

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

3.7 Dashboard

The dashboard gives a quick top level summary of activity across devices. You get to pre-configure a list of reports or monitors you want Vantage Report to display first when you log in. The dashboard is available with the full version of Vantage Report.

The dashboard looks like this before you configure it.

Figure 16 Dashboard Initial View

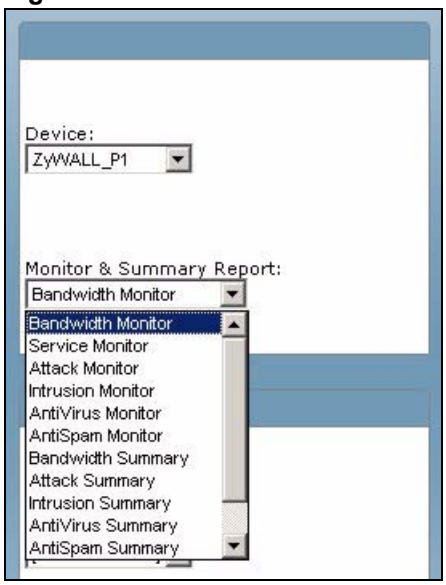
The following screen appears after you click the “here” link.

Figure 17 Dashboard Configure

Select devices and then the monitor or summary to display for each. You can select the same device in more that one section of the dashboard.

Not every ZyXEL device supports every report. Only select a monitor or summary that the device supports.

Figure 18 Dashboard Select Device and Monitor or Summary

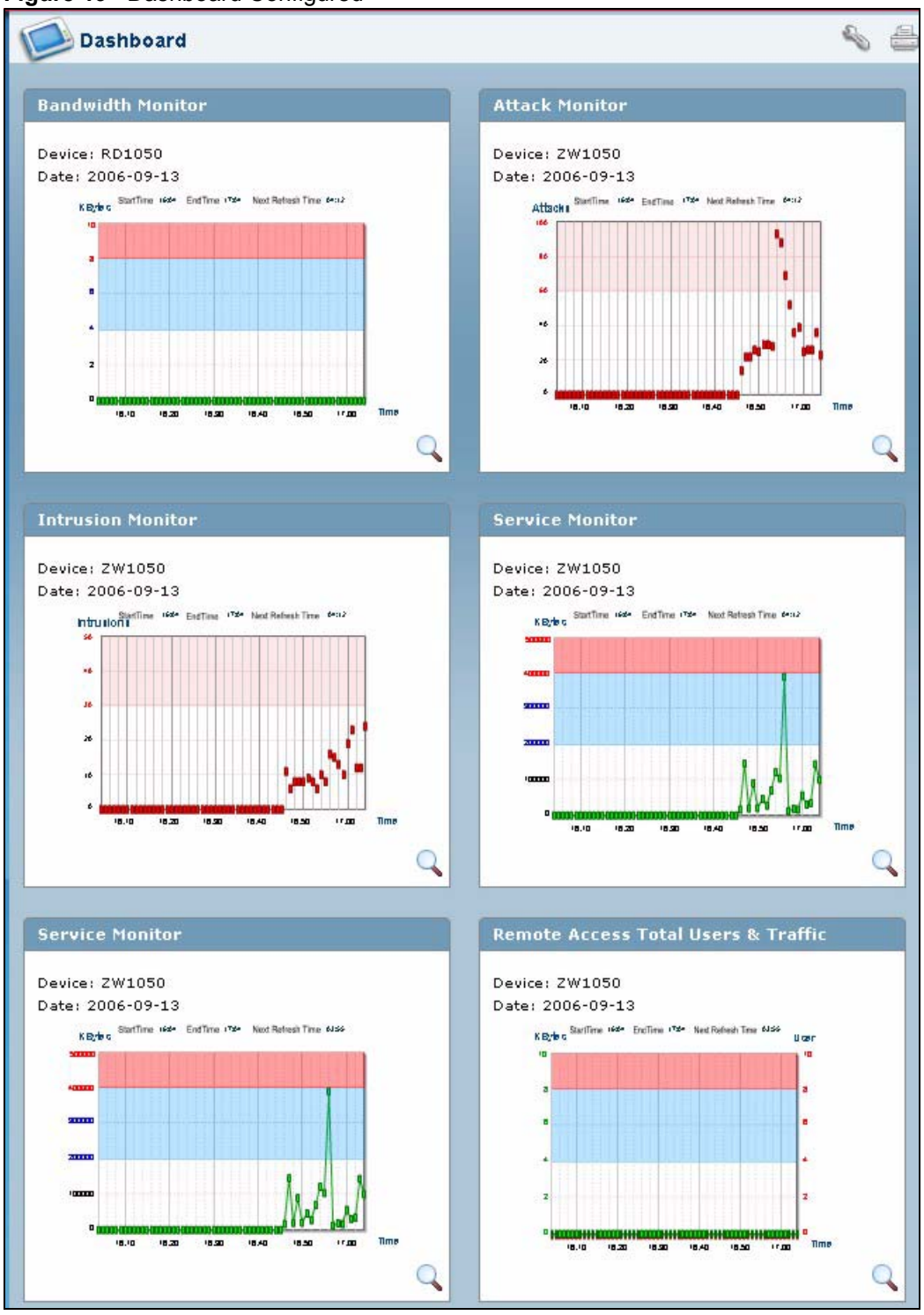


3.8 Dashboard

The dashboard looks as follows when you finish configuring it.

Click a report or monitor for more details on any of your pre-selected devices and reports. The dashboard is available with the full version of Vantage Report.

Figure 19 Dashboard Configured



The following table describes the dashboard icons. See the other sections in this user's guide for details on the monitors and summaries.

Table 14 Dashboard

ICON	DESCRIPTION
	The setting icon returns you to the dashboard configuration screen.
	The print icon prints the dashboard screen.
	The view detail icon zooms in on the monitor or summary to show you the details.

PART II
Monitor and Traffic

Monitor (65)
Traffic (73)
VPN (139)

4

Monitor

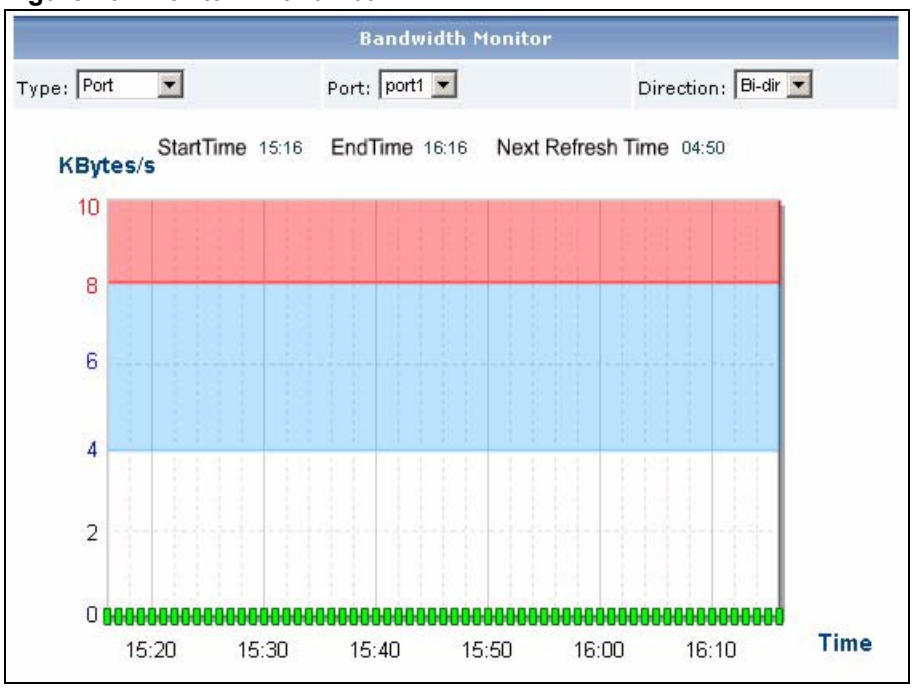
Use monitors to check the status of ZyXEL devices. See Section 2.3 on page 34 for a related discussion about time.

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 20 Monitor > Bandwidth



Each field is described in the following table.

Table 15 Monitor > Bandwidth

LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Type	Select **Port** to view bandwidth usage by physical interface. Select **Interface** to view bandwidth usage by logical interface. This field is not available with all models.

Table 15 Monitor > Bandwidth

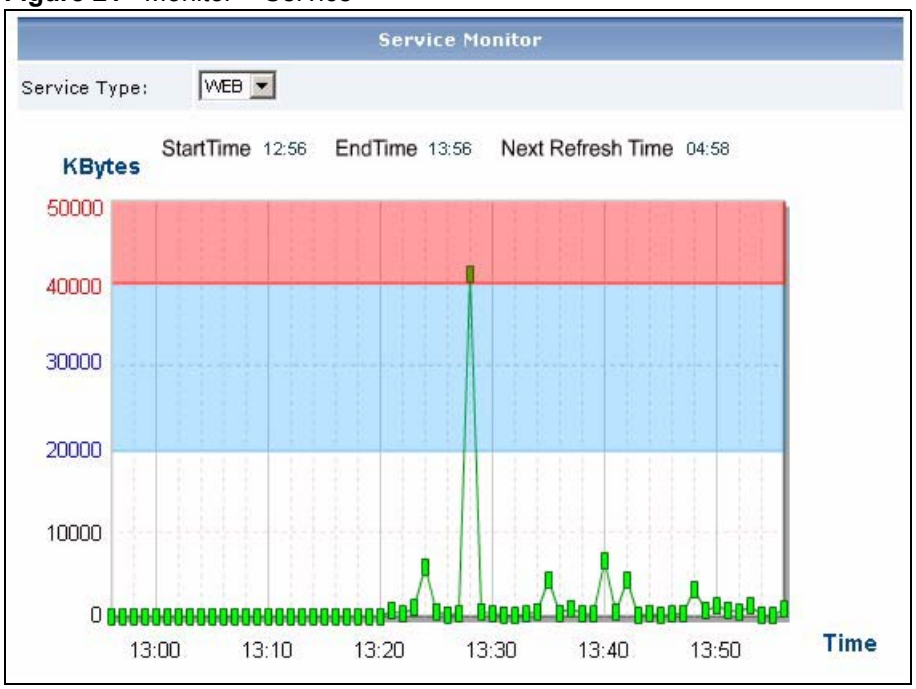
LABEL	DESCRIPTION
Port	This field displays when you select **Port** in the **Type** field. Select the physical interface for which you want to view bandwidth usage. This field is not available with all models.
Interface	This field displays when you select **Interface** in the **Type** field. Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select for which direction of traffic, you want to view bandwidth usage. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device This field is not available with all models.
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 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**.

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 21 Monitor > Service



Each field is described in the following table.

Table 16 Monitor > Service

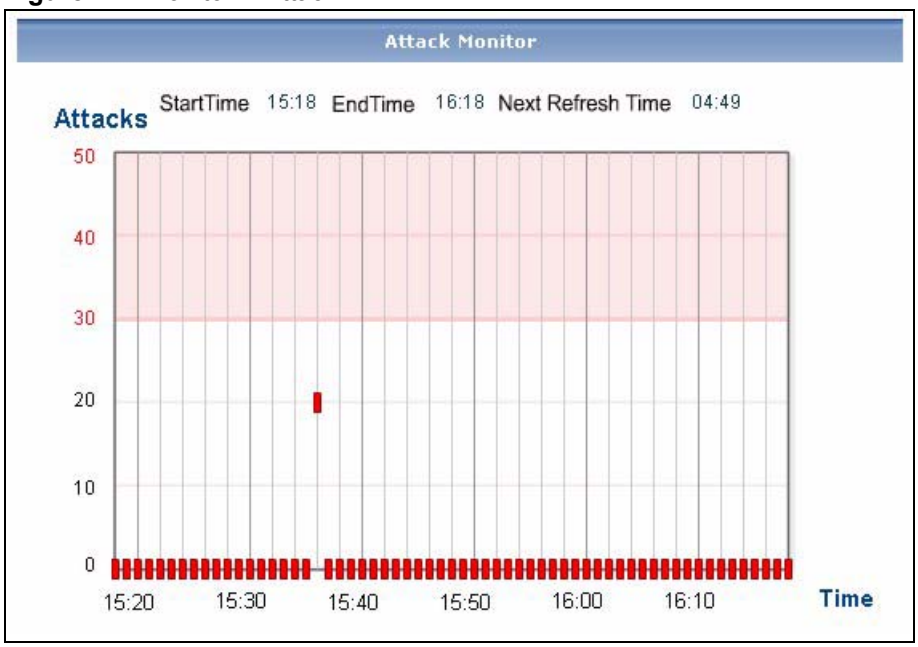
LABEL	DESCRIPTION
title	This field displays the title of the monitor. It does not include the service you select in the **Service Type** field.
Service Type	Select the service whose traffic you want to look at. Choices are: **WEB** - Look at the amount of traffic generated by HTTP/HTTPS services. **FTP** - 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**.

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 22 Monitor > Attack



Each field is described in the following table.

Table 17 Monitor > Attack

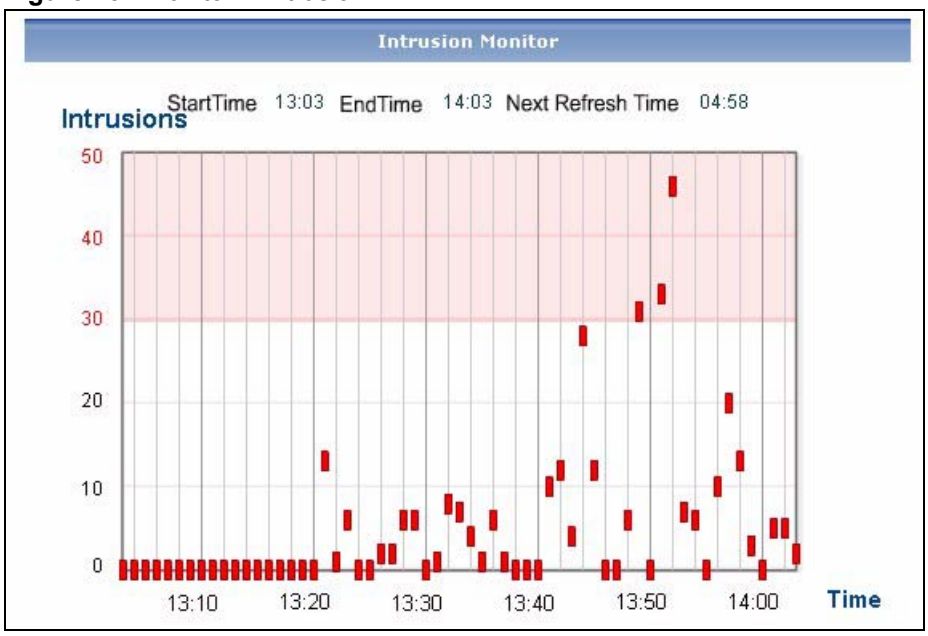
LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next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

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 23 Monitor > Intrusion



Each field is described in the following table.

Table 18 Monitor > Intrusion

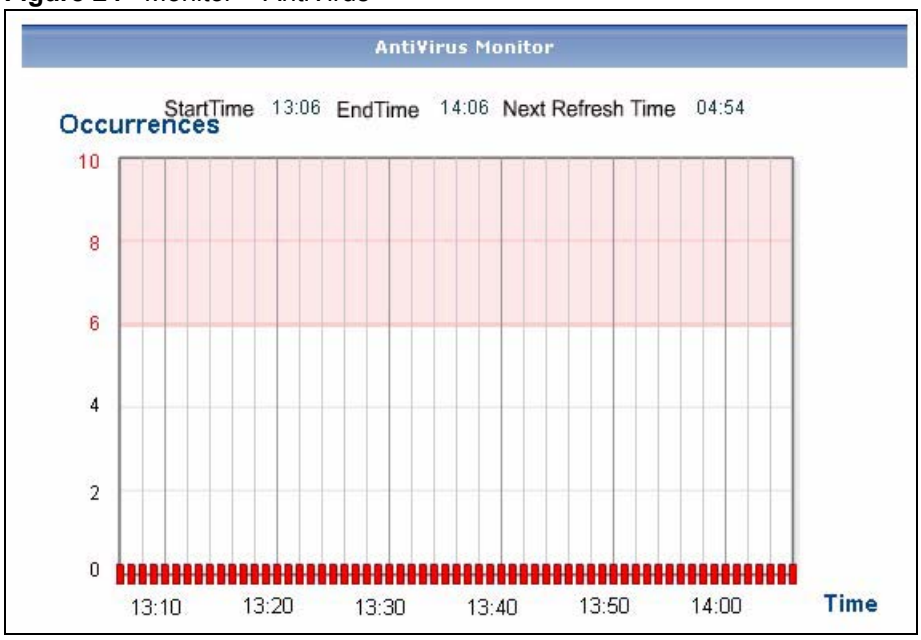
LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next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

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 24 Monitor > AntiVirus



Each field is described in the following table.

Table 19 Monitor > AntiVirus

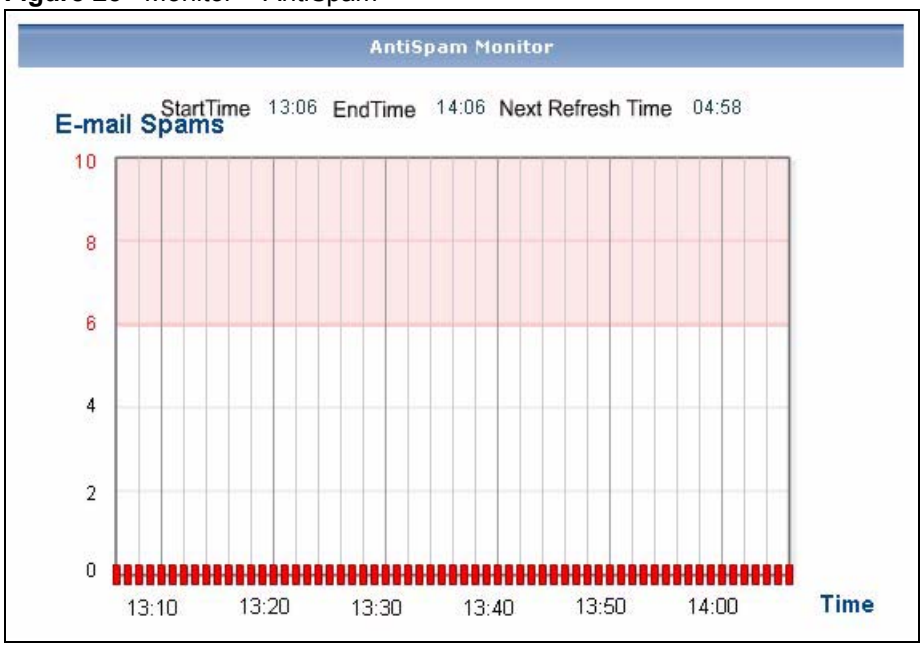
LABEL	DESCRIPTION
title	This field displays the title of the monitor.
Start Time	This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph.
End Time	This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph.
Next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

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 25 Monitor > AntiSpam



Each field is described in the following table.

Table 20 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**.

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

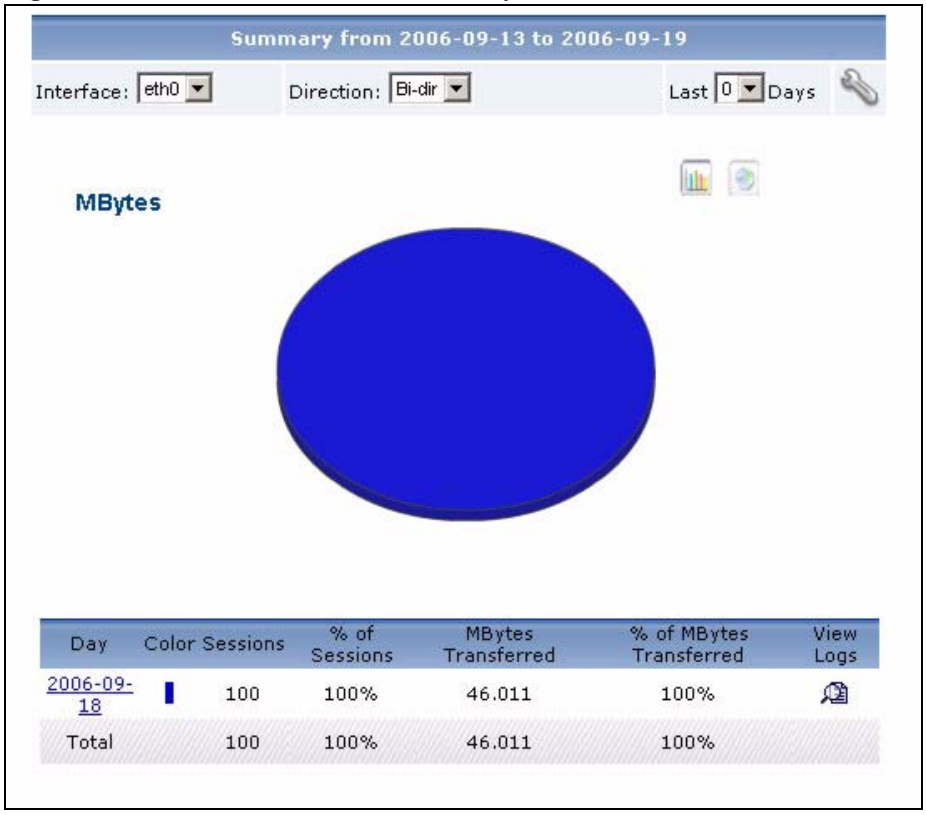
Use these reports to look at how much traffic was handled by ZyXEL devices, who used the most bandwidth in a ZyXEL device, and which protocols were used. You can also look at traffic in various directions.

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 26 Traffic > Bandwidth > Summary



Each field is described in the following table.

Table 21 Traffic > Bandwidth > Summary

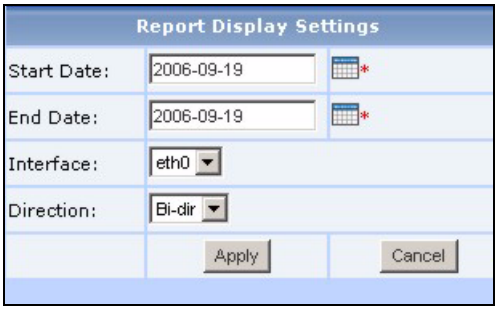
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device For models where no **Interface** field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. **All** - all traffic, regardless of direction **INBOUND** - all traffic routed from the WAN **OUTBOUND** - all traffic routed to the WAN
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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.
Settings	Use these fields or **Last ... Days** to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. These fields reset to their default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 21 Traffic > Bandwidth > Summary

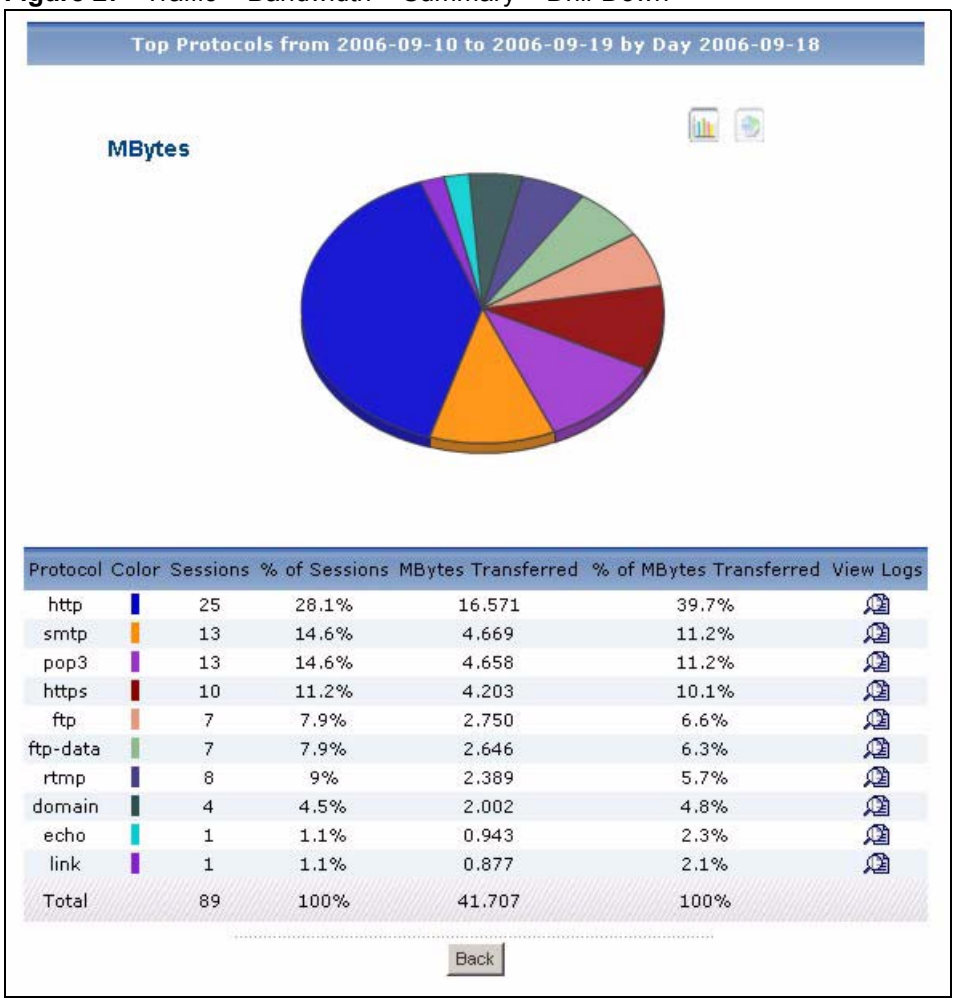
LABEL	DESCRIPTION
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top services by amount of traffic in the selected time interval. The **Bandwidth Summary Drill-Down** report appears.
Color	This field displays what color represents each record (time interval) in the graph.
Sessions	This field displays the number of traffic events in each interval.
% of Sessions	This field displays what percentage each record's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled in each time interval.
% of MBytes Transferred	This field displays what percentage each record's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the records above.

5.1.2 Bandwidth Summary Drill-Down

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

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

Figure 27 Traffic > Bandwidth > Summary > Drill-Down



Each field is described in the following table.

Table 22 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	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services in the selected time interval, sorted by the amount of traffic attributed to each one. These services may be different than the ones you manage in the **Service Settings** screen.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service in the selected time interval.
% of Sessions	This field displays what percentage each service's number of traffic events makes out of the time interval's total number of traffic events.

Table 22 Traffic > Bandwidth > Summary > Drill-Down

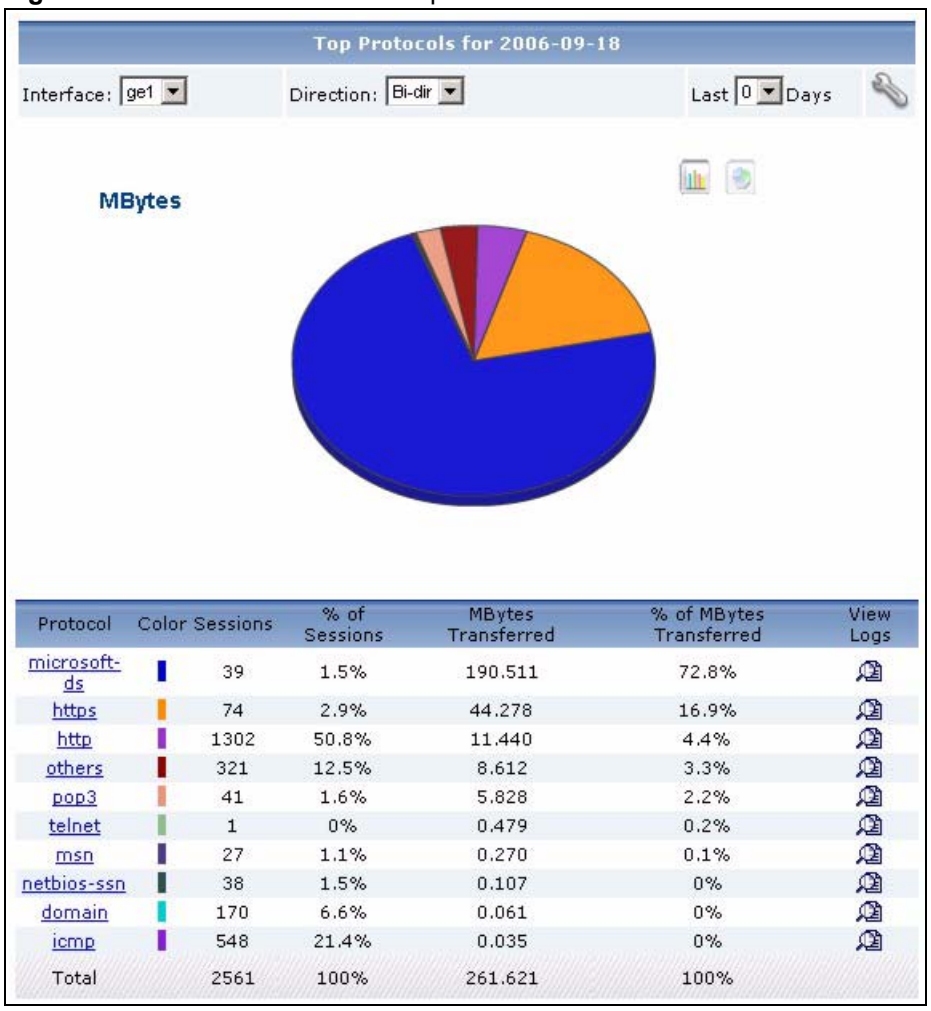
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each service in the selected time interval.
% of MBytes Transferred	This field displays what percentage of the time interval's total traffic belonged to each service.
View Logs	Click this icon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

5.1.3 Bandwidth Top Protocols

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

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

Figure 28 Traffic > Bandwidth > Top Protocols



Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
microsoft-ds		39	1.5%	190.511	72.8%	
https		74	2.9%	44.278	16.9%	
http		1302	50.8%	11.440	4.4%	
others		321	12.5%	8.612	3.3%	
pop3		41	1.6%	5.828	2.2%	
telnet		1	0%	0.479	0.2%	
msn		27	1.1%	0.270	0.1%	
netbios-ssn		38	1.5%	0.107	0%	
domain		170	6.6%	0.061	0%	
icmp		548	21.4%	0.035	0%	
Total		2561	100%	261.621	100%	

Each field is described in the following table.

Table 23 Traffic > Bandwidth > Top Protocols

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.
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device For models where no **Interface** field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. **All** - all traffic, regardless of direction **INBOUND** - all traffic routed from the WAN **OUTBOUND** - all traffic routed to the WAN
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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.
Settings	Use these fields or **Last ... Days** to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  The **Interface** and **Direction** fields are the same as in the main screen. Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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 23 Traffic > Bandwidth > Top Protocols

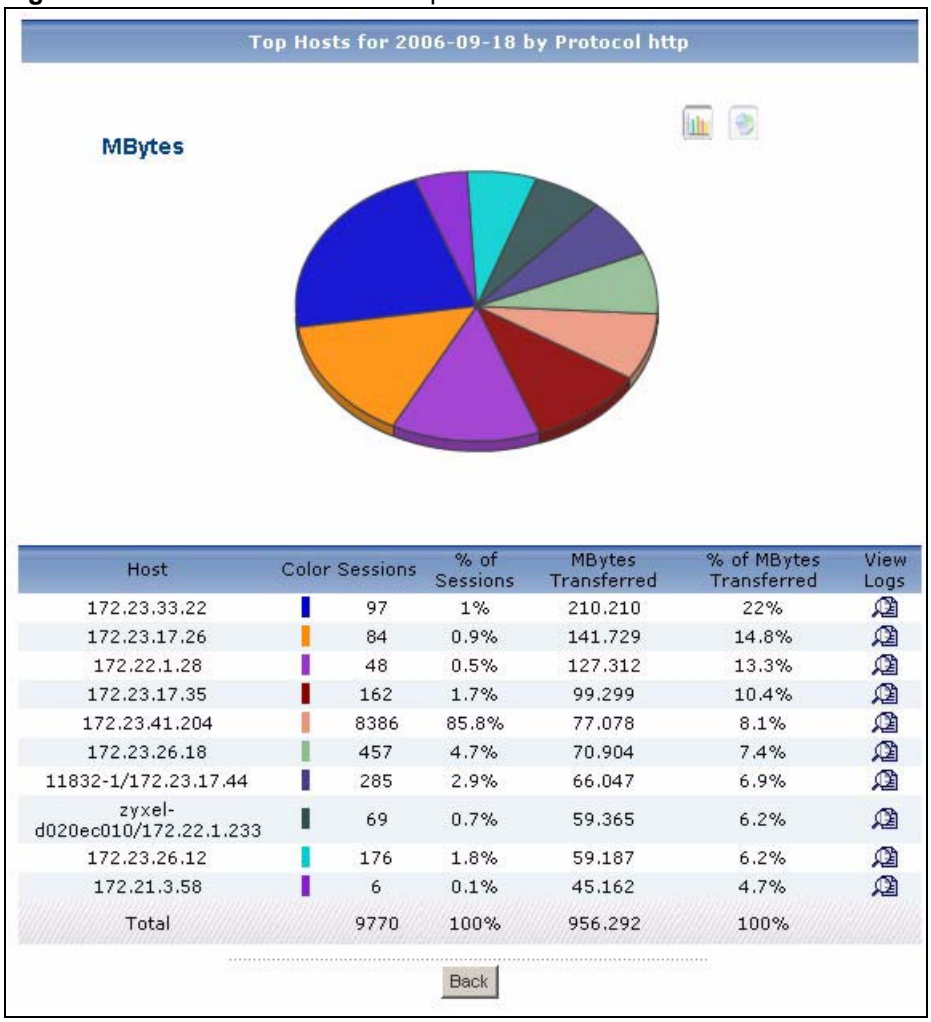
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services generating traffic through the selected device, sorted by the amount of traffic for each one. If the number of services is less than the maximum number of records displayed in this table, every service is displayed. These services may be different than the ones you manage in the **Service Settings** screen. Click on a service to look at the top sources of traffic for the selected service. The **Bandwidth Top Protocols Drill-Down** report appears.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service.
% of Sessions	This field displays what percentage each service's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each service generated through the selected device.
% of MBytes Transferred	This field displays what percentage each record's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above.

5.1.4 Bandwidth Top Protocols Drill-Down

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

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

Figure 29 Traffic > Bandwidth > Top Protocol > Drill-Down



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.23.33.22		97	1%	210.210	22%	
172.23.17.26		84	0.9%	141.729	14.8%	
172.22.1.28		48	0.5%	127.312	13.3%	
172.23.17.35		162	1.7%	99.299	10.4%	
172.23.41.204		8386	85.8%	77.078	8.1%	
172.23.26.18		457	4.7%	70.904	7.4%	
11832-1/172.23.17.44		285	2.9%	66.047	6.9%	
zyxel-d020ec010/172.22.1.233		69	0.7%	59.365	6.2%	
172.23.26.12		176	1.8%	59.187	6.2%	
172.21.3.58		6	0.1%	45.162	4.7%	
Total		9770	100%	956.292	100%	

Each field is described in the following table.

Table 24 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of traffic for the selected service, sorted by the amount of traffic generated by each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events each source generated using the selected service.

Table 24 Traffic > Bandwidth > Top Protocol > Drill-Down

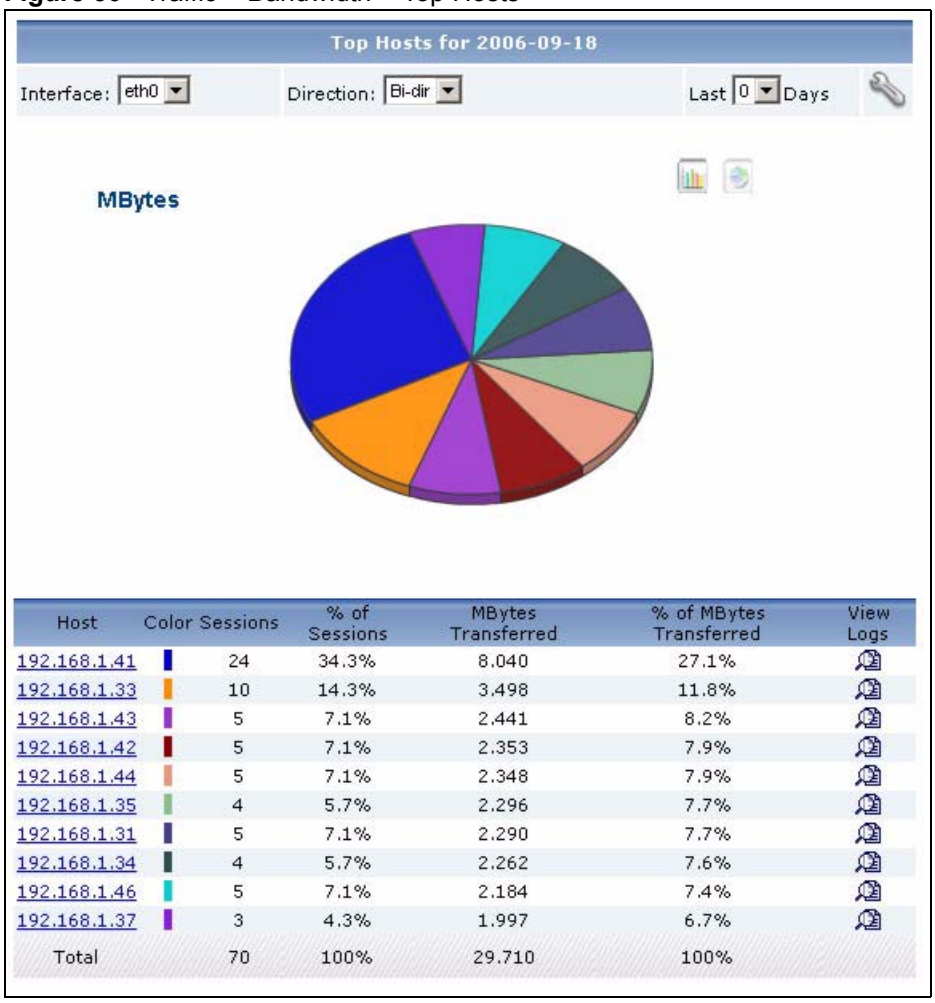
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage of the selected service's total number of traffic events came from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) each source generated using the selected service.
% of MBytes Transferred	This field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

5.1.5 Top Bandwidth Hosts

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

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

Figure 30 Traffic > Bandwidth > Top Hosts



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.41		24	34.3%	8.040	27.1%	
192.168.1.33		10	14.3%	3.498	11.8%	
192.168.1.43		5	7.1%	2.441	8.2%	
192.168.1.42		5	7.1%	2.353	7.9%	
192.168.1.44		5	7.1%	2.348	7.9%	
192.168.1.35		4	5.7%	2.296	7.7%	
192.168.1.31		5	7.1%	2.290	7.7%	
192.168.1.34		4	5.7%	2.262	7.6%	
192.168.1.46		5	7.1%	2.184	7.4%	
192.168.1.37		3	4.3%	1.997	6.7%	
Total		70	100%	29.710	100%	

Each field is described in the following table.

Table 25 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.
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device For models where no **Interface** field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. **All** - all traffic, regardless of direction **INBOUND** - all traffic routed from the WAN **OUTBOUND** - all traffic routed to the WAN

Table 25 Traffic > Bandwidth > Top Hosts

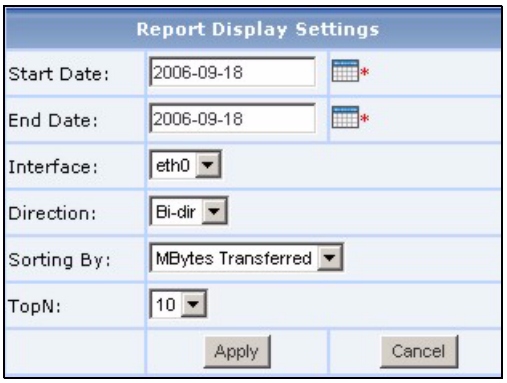
LABEL	DESCRIPTION
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can 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.
Settings	Use these fields or **Last ... Days** to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top services by amount of traffic for the selected source. The **Bandwidth Top Hosts Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.

Table 25 Traffic > Bandwidth > Top Hosts

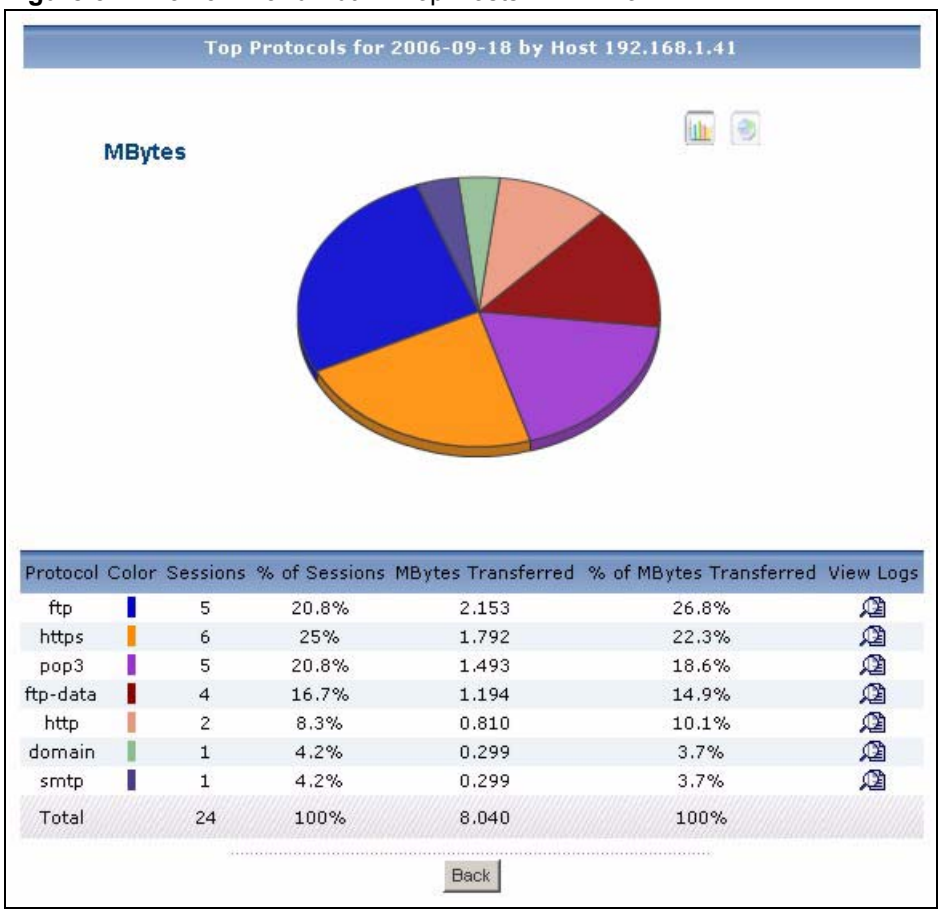
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each source generated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

5.1.6 Top Bandwidth Hosts Drill-Down

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

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

Figure 31 Traffic > Bandwidth > Top Hosts > Drill-Down



Each field is described in the following table.

Table 26 Traffic > Bandwidth > Top Hosts > Drill-Down

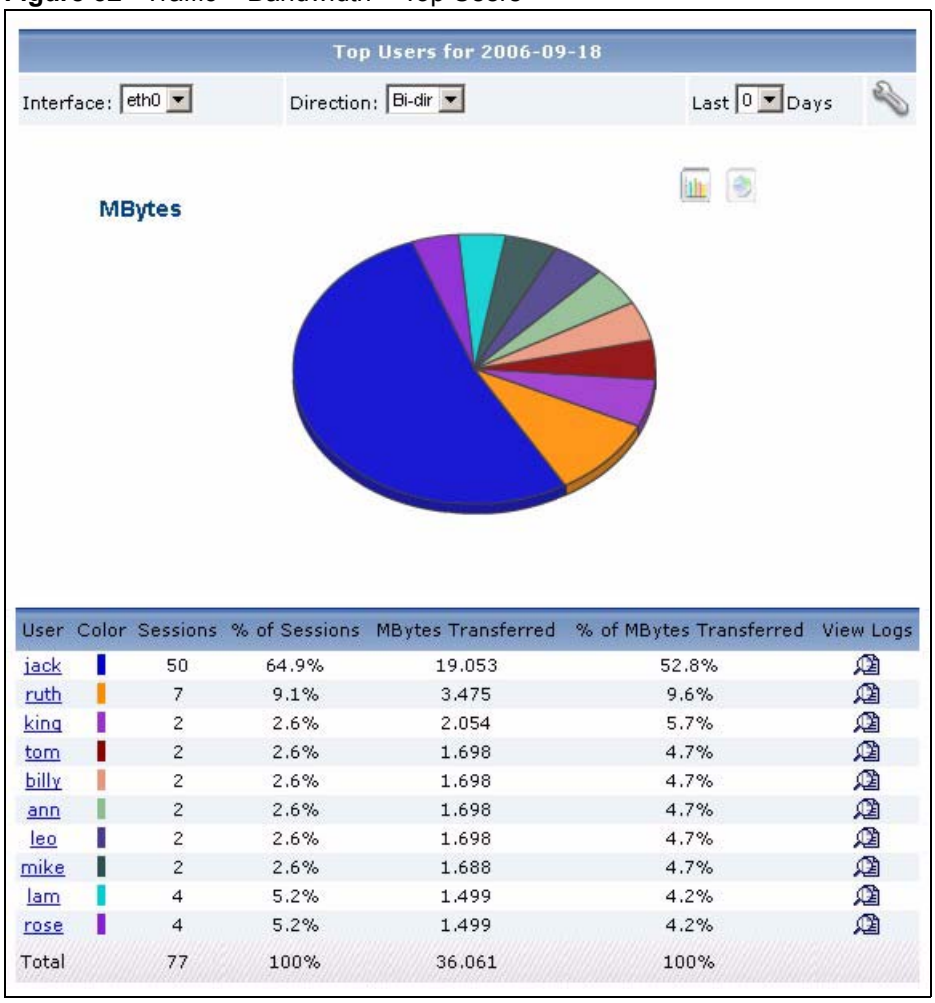
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services used by the selected source, sorted by the amount of traffic attributed to each one. These services may be different than the ones you manage in the **Service Settings** screen.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events the selected source generated using each service.
% of Sessions	This field displays what percentage of the selected source's total number of traffic events belong to each service.
MBytes Transferred	This field displays how much traffic (in megabytes) the selected source generated using each service.
% of MBytes Transferred	This field displays what percentage of the selected source's total traffic belongs to each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. If the number of services used by the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.1.7 Top Bandwidth Users

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

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

Figure 32 Traffic > Bandwidth > Top Users



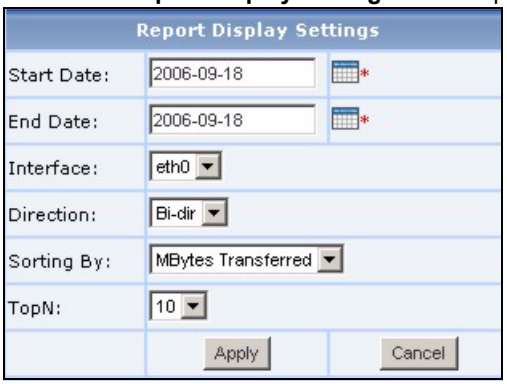
User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
jack		50	64.9%	19.053	52.8%	
ruth		7	9.1%	3.475	9.6%	
king		2	2.6%	2.054	5.7%	
tom		2	2.6%	1.698	4.7%	
billy		2	2.6%	1.698	4.7%	
ann		2	2.6%	1.698	4.7%	
leo		2	2.6%	1.698	4.7%	
mike		2	2.6%	1.688	4.7%	
lam		4	5.2%	1.499	4.2%	
rose		4	5.2%	1.499	4.2%	
Total		77	100%	36.061	100%	

Each field is described in the following table.

Table 27 Traffic > Bandwidth > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Interface	Select the logical interface for which you want to view bandwidth usage.
Direction	Select which kind of traffic, by direction, you want to look at. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device
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 27 Traffic > Bandwidth > Top Users

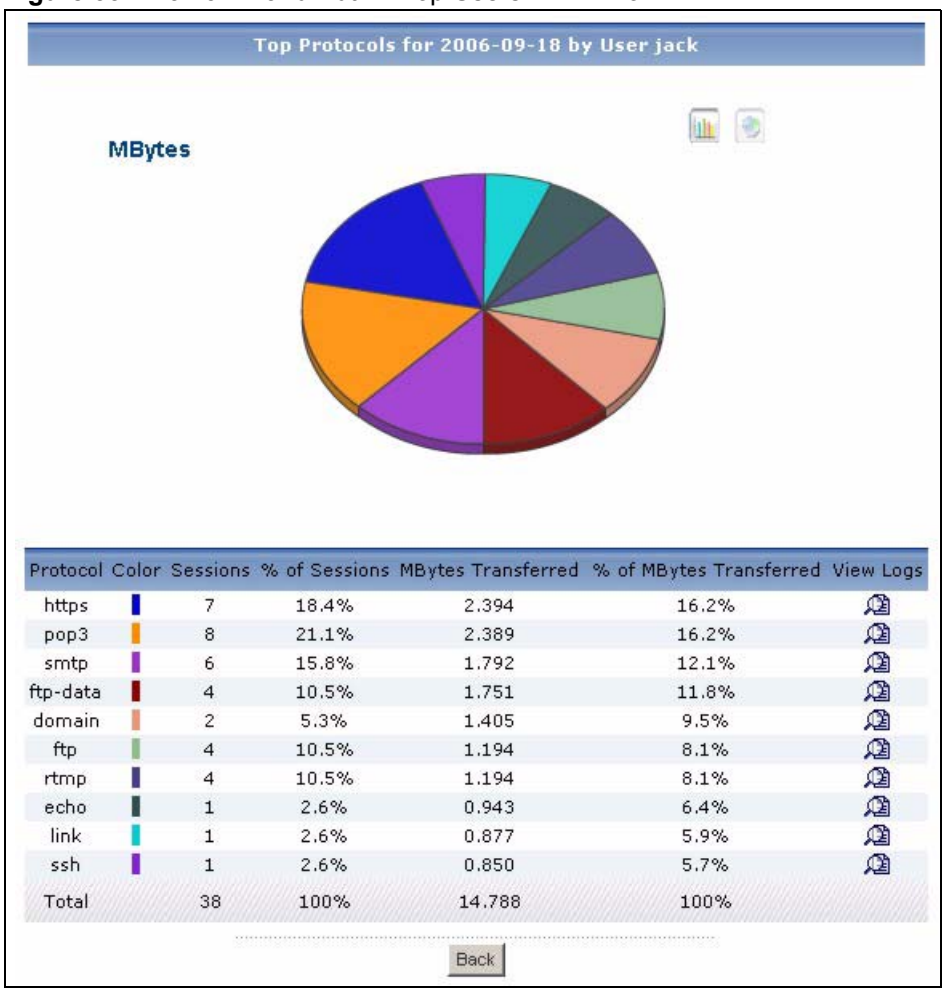
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users with the most traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click a user name to look at the top services by amount of traffic for the selected user. The **Bandwidth Top Users Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each user generated through the selected device.
% of MBytes Transferred	This field displays what percentage each user's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

5.1.8 Top Bandwidth Users Drill-Down

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

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

Figure 33 Traffic > Bandwidth > Top Users > Drill-Down



Each field is described in the following table.

Table 28 Traffic > Bandwidth > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. I
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services used by the selected user, sorted by the amount of traffic attributed to each one. These services may be different than the ones you manage in the **Service Settings** screen.
Color	This field displays what color represents each service in the graph.

Table 28 Traffic > Bandwidth > Top Users > Drill-Down

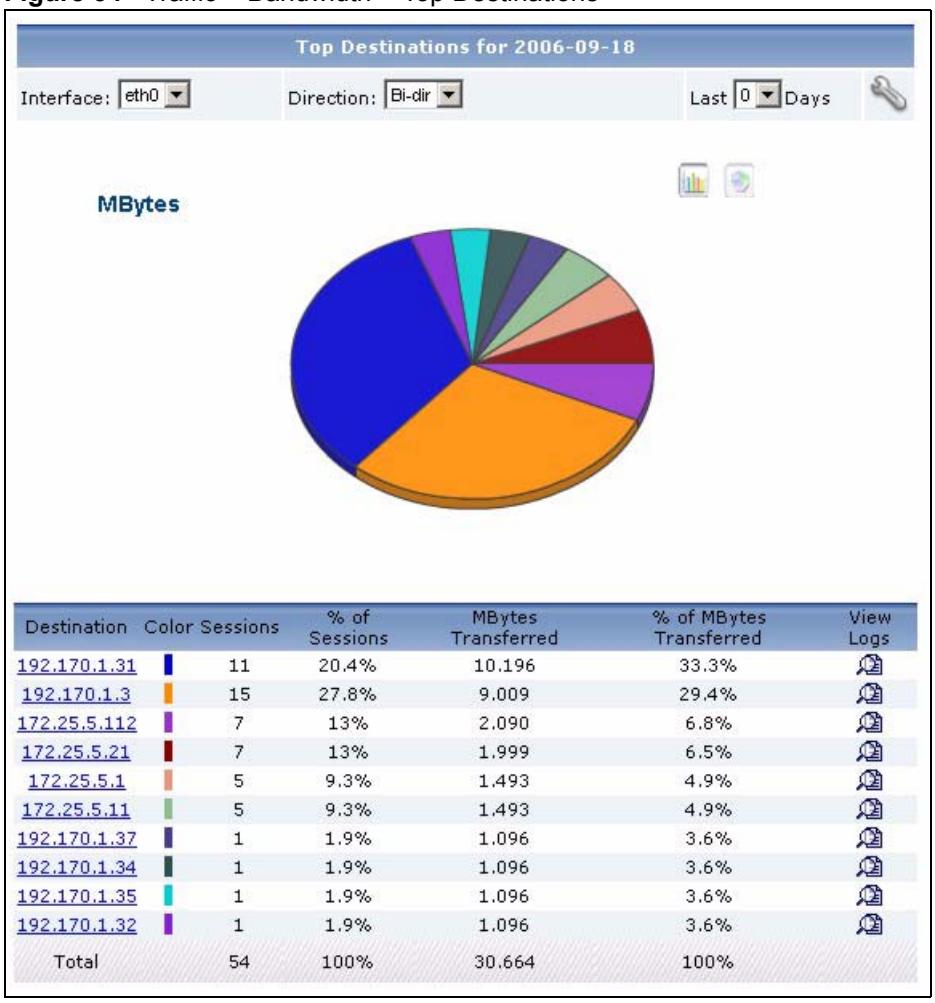
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events the selected user generated using each service.
% of Sessions	This field displays what percentage of the selected user's total number of traffic events was generated using each service.
MBytes Transferred	This field displays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

5.1.9 Top Bandwidth Destinations

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

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

Figure 34 Traffic > Bandwidth > Top Destinations



Destination	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.31		11	20.4%	10.196	33.3%	
192.170.1.3		15	27.8%	9.009	29.4%	
172.25.5.112		7	13%	2.090	6.8%	
172.25.5.21		7	13%	1.999	6.5%	
172.25.5.1		5	9.3%	1.493	4.9%	
172.25.5.11		5	9.3%	1.493	4.9%	
192.170.1.37		1	1.9%	1.096	3.6%	
192.170.1.34		1	1.9%	1.096	3.6%	
192.170.1.35		1	1.9%	1.096	3.6%	
192.170.1.32		1	1.9%	1.096	3.6%	
Total		54	100%	30.664	100%	

Each field is described in the following table.

Table 29 Traffic > Bandwidth > 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.
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device For models where no **Interface** field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. **All** - all traffic, regardless of direction **INBOUND** - all traffic routed from the WAN **OUTBOUND** - all traffic routed to the WAN

Table 29 Traffic > Bandwidth > Top Destinations

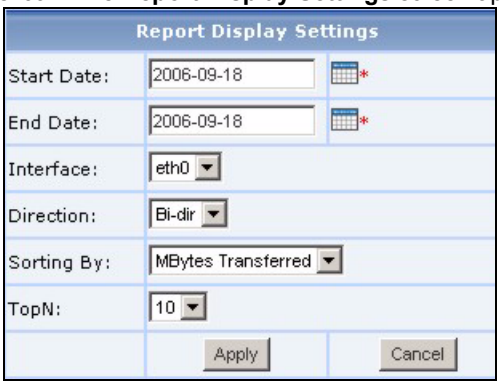
LABEL	DESCRIPTION
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the destinations to which the selected device sent the most traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a destination to look at the top sources of web traffic for the selected destination. The **Top Destinations Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.

Table 29 Traffic > Bandwidth > Top Destinations

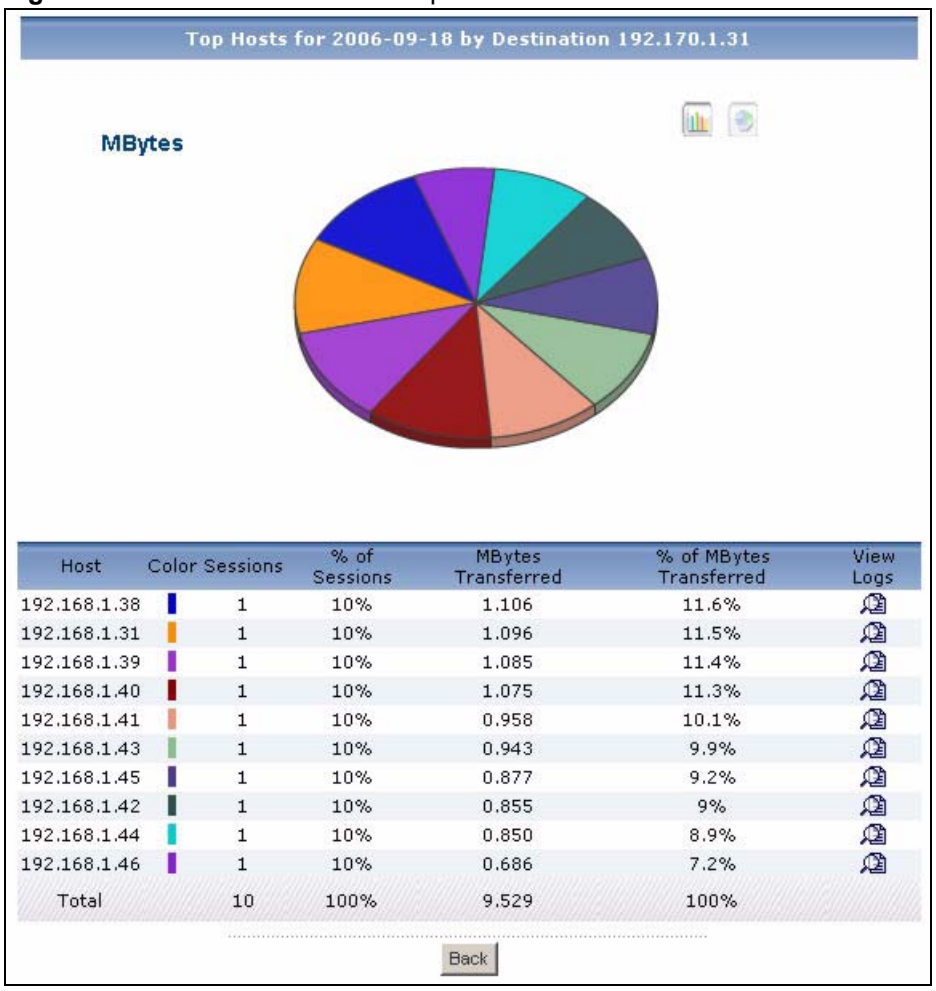
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the selected device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

5.1.10 Top Bandwidth Destinations Drill-Down

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

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

Figure 35 Traffic > Bandwidth > Top Destinations > Drill-Down



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.38		1	10%	1.106	11.6%	
192.168.1.31		1	10%	1.096	11.5%	
192.168.1.39		1	10%	1.085	11.4%	
192.168.1.40		1	10%	1.075	11.3%	
192.168.1.41		1	10%	0.958	10.1%	
192.168.1.43		1	10%	0.943	9.9%	
192.168.1.45		1	10%	0.877	9.2%	
192.168.1.42		1	10%	0.855	9%	
192.168.1.44		1	10%	0.850	8.9%	
192.168.1.46		1	10%	0.686	7.2%	
Total		10	100%	9.529	100%	

Each field is described in the following table.

Table 30 Traffic > Bandwidth > 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources that sent traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events was sent from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) there was for the selected destination from each source.
% of MBytes Transferred	This field displays what percentage of a destination's traffic came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the services above. If the number of services used by the selected user is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.2 Web Traffic

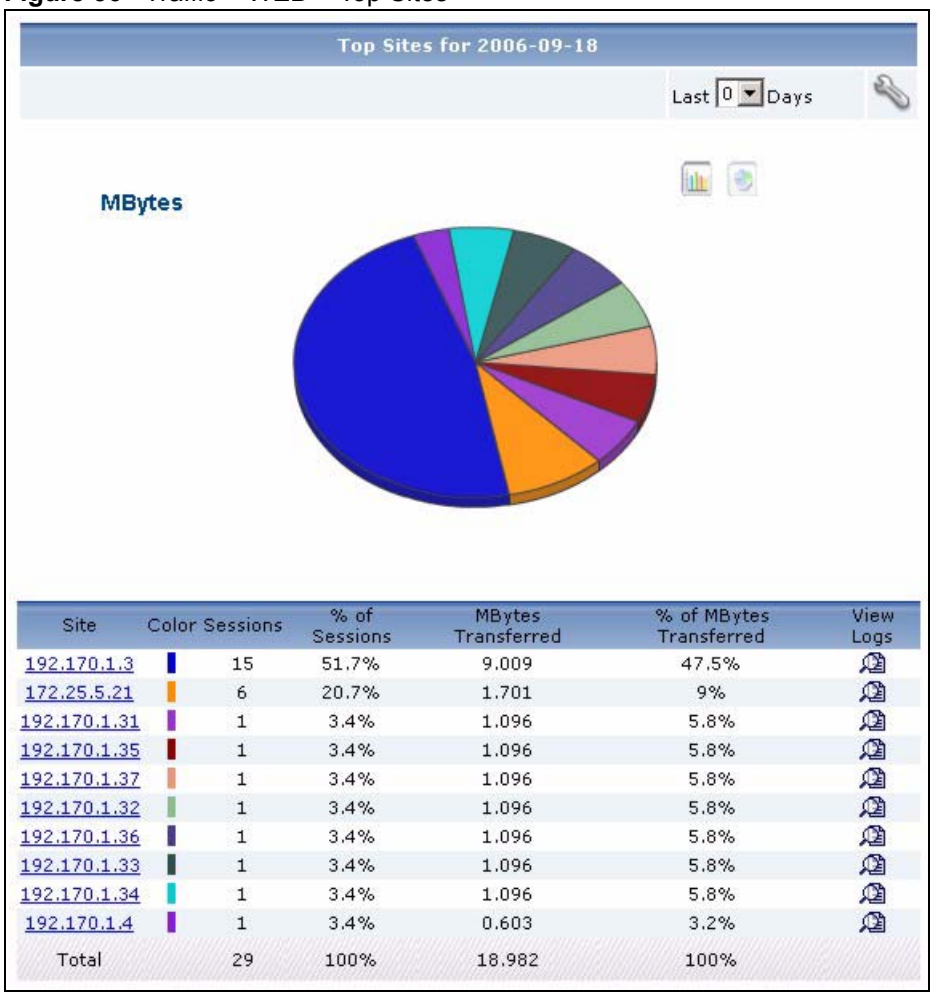
Use this report to look at the top destinations and sources of web traffic.

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 36 Traffic > WEB > Top Sites



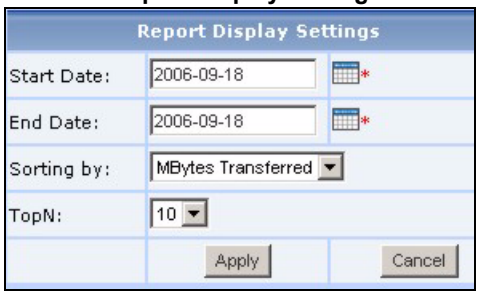
Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.3		15	51.7%	9.009	47.5%	
172.25.5.21		6	20.7%	1.701	9%	
192.170.1.31		1	3.4%	1.096	5.8%	
192.170.1.35		1	3.4%	1.096	5.8%	
192.170.1.37		1	3.4%	1.096	5.8%	
192.170.1.32		1	3.4%	1.096	5.8%	
192.170.1.36		1	3.4%	1.096	5.8%	
192.170.1.33		1	3.4%	1.096	5.8%	
192.170.1.34		1	3.4%	1.096	5.8%	
192.170.1.4		1	3.4%	0.603	3.2%	
Total		29	100%	18.982	100%	

Each field is described in the following table.

Table 31 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 31 Traffic > WEB > Top Sites

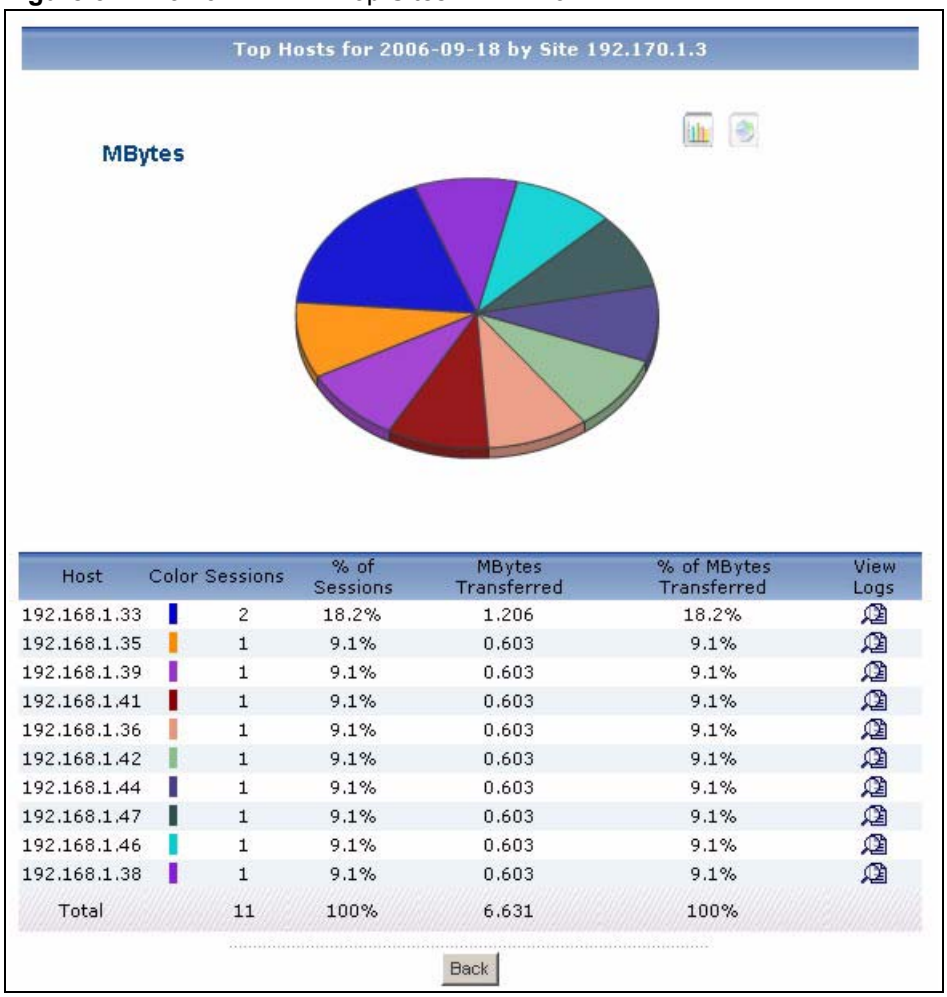
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a destination to look at the top sources of web traffic for the selected destination. The **Top Web Sites Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of the traffic went to each destination out of the total amount of traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.2.2 Top Web Sites Drill-Down

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

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

Figure 37 Traffic > WEB > Top Sites > Drill-Down



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33		2	18.2%	1.206	18.2%	
192.168.1.35		1	9.1%	0.603	9.1%	
192.168.1.39		1	9.1%	0.603	9.1%	
192.168.1.41		1	9.1%	0.603	9.1%	
192.168.1.36		1	9.1%	0.603	9.1%	
192.168.1.42		1	9.1%	0.603	9.1%	
192.168.1.44		1	9.1%	0.603	9.1%	
192.168.1.47		1	9.1%	0.603	9.1%	
192.168.1.46		1	9.1%	0.603	9.1%	
192.168.1.38		1	9.1%	0.603	9.1%	
Total		11	100%	6.631	100%	

Each field is described in the following table.

Table 32 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.

Table 32 Traffic > WEB > Top Sites > Drill-Down

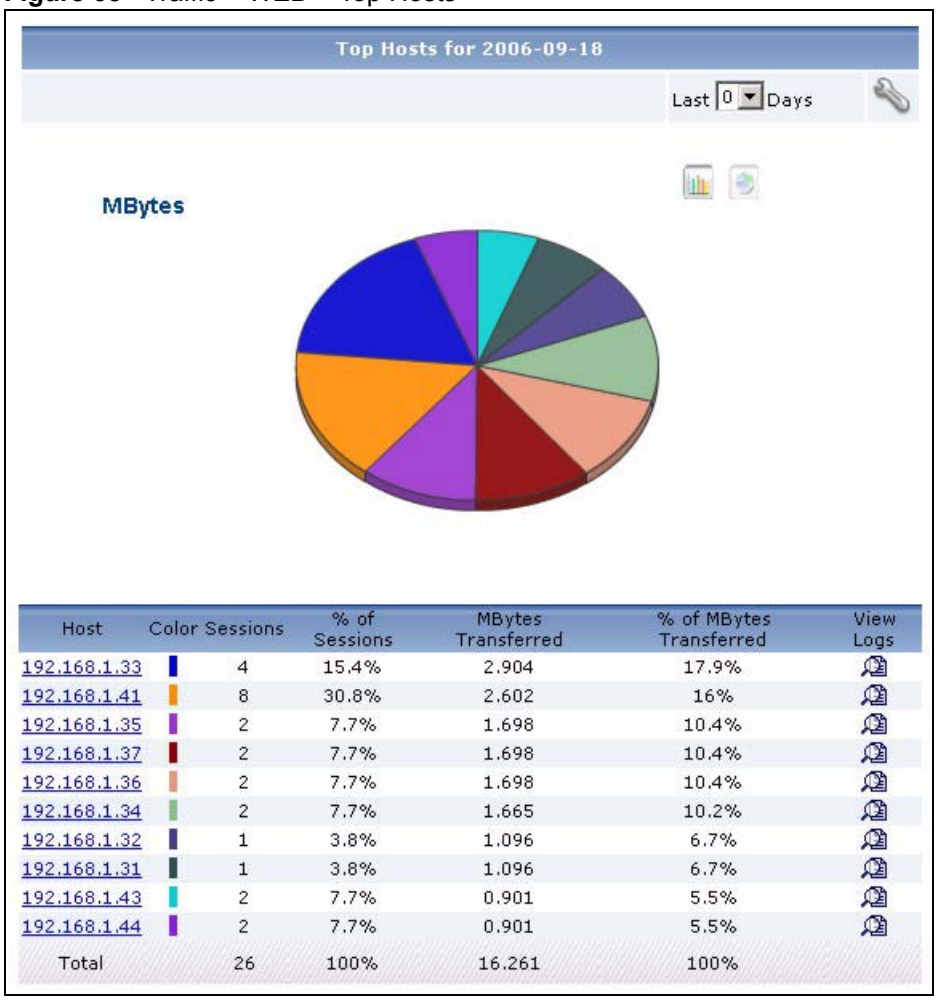
LABEL	DESCRIPTION
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events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

5.2.3 Top Web Hosts

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

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

Figure 38 Traffic > WEB > Top Hosts



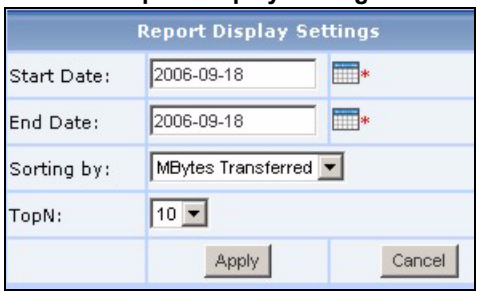
Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33		4	15.4%	2.904	17.9%	
192.168.1.41		8	30.8%	2.602	16%	
192.168.1.35		2	7.7%	1.698	10.4%	
192.168.1.37		2	7.7%	1.698	10.4%	
192.168.1.36		2	7.7%	1.698	10.4%	
192.168.1.34		2	7.7%	1.665	10.2%	
192.168.1.32		1	3.8%	1.096	6.7%	
192.168.1.31		1	3.8%	1.096	6.7%	
192.168.1.43		2	7.7%	0.901	5.5%	
192.168.1.44		2	7.7%	0.901	5.5%	
Total		26	100%	16.261	100%	

Each field is described in the following table.

Table 33 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	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 > WEB > Top Hosts

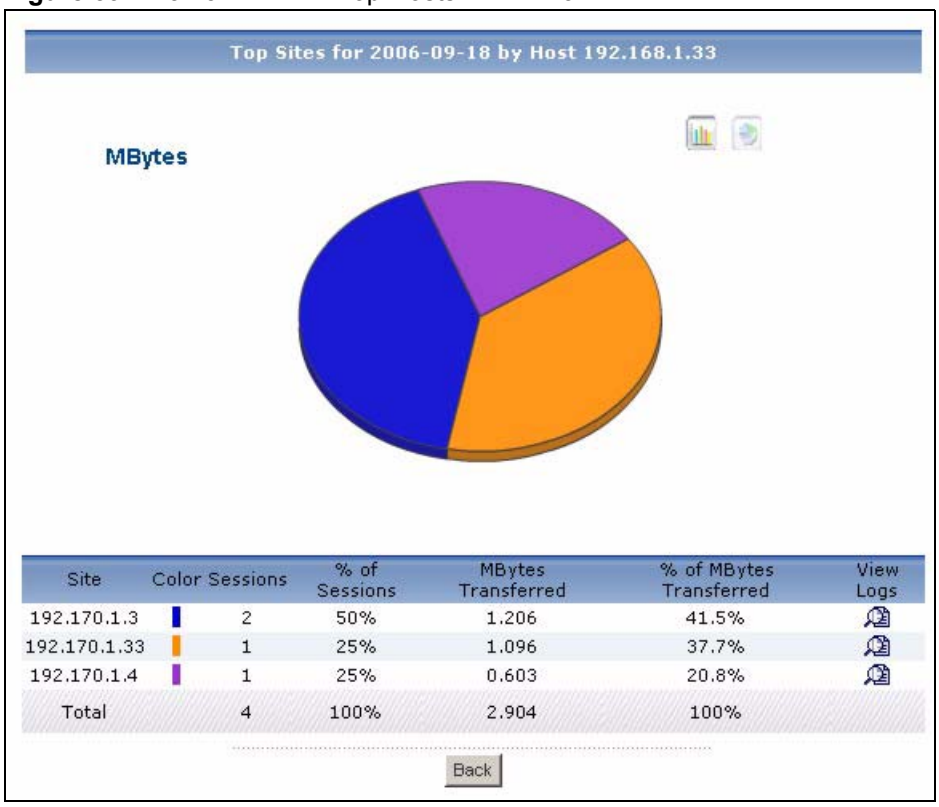
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of web traffic for the selected source. The **Top Web Hosts Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of web traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of web traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.2.4 Top Web Hosts Drill-Down

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

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

Figure 39 Traffic > WEB > Top Hosts > Drill-Down



Each field is described in the following table.

Table 34 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic from the selected source, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected source to each destination.
% of Sessions	This field displays what percentage of the selected source’s total number of traffic events was sent to each destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from the selected source to each destination.

Table 34 Traffic > WEB > Top Hosts > Drill-Down

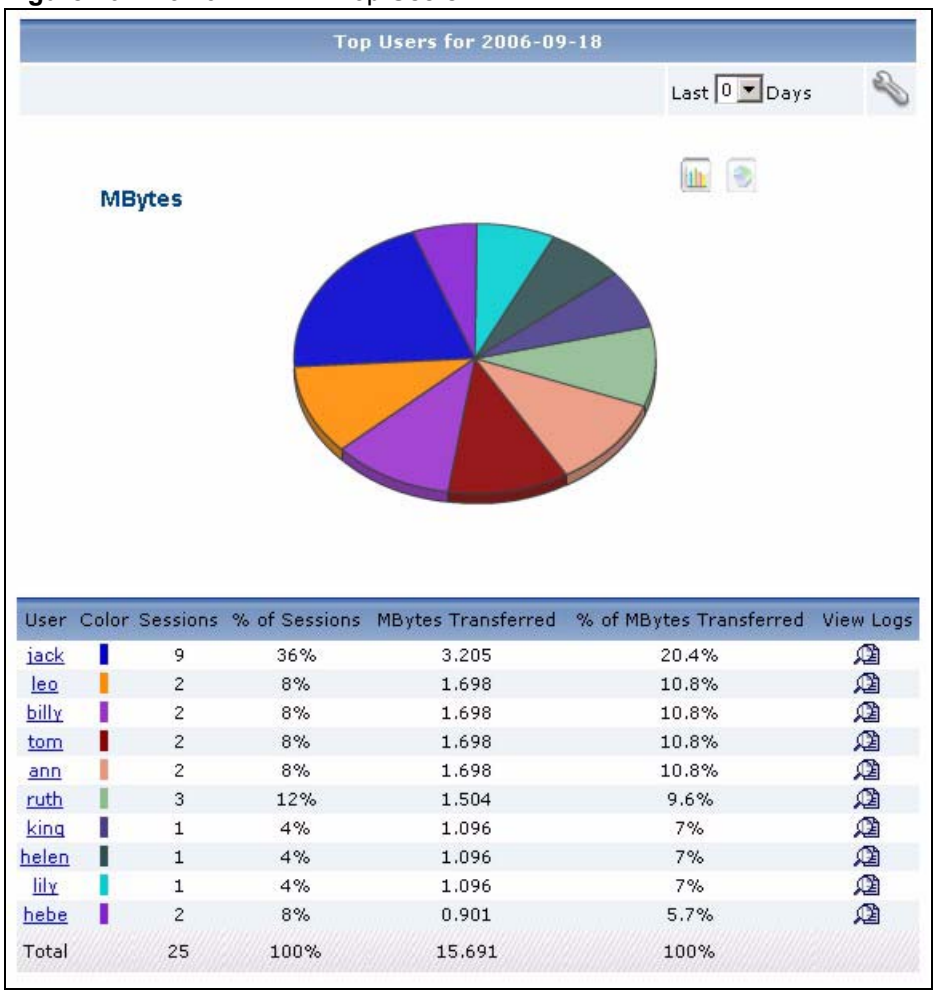
LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage of the selected source's traffic was sent to each destination.
Total	This entry displays the totals for the destinations above. If the number of destinations of web traffic from the selected source is greater than the maximum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

5.2.5 Top Web Users

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

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

Figure 40 Traffic > WEB > Top Users



User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
jack		9	36%	3.205	20.4%	
leo		2	8%	1.698	10.8%	
billy		2	8%	1.698	10.8%	
tom		2	8%	1.698	10.8%	
ann		2	8%	1.698	10.8%	
ruth		3	12%	1.504	9.6%	
king		1	4%	1.096	7%	
helen		1	4%	1.096	7%	
lily		1	4%	1.096	7%	
hebe		2	8%	0.901	5.7%	
Total		25	100%	15.691	100%	

Each field is described in the following table.

Table 35 Traffic > WEB > Top Users

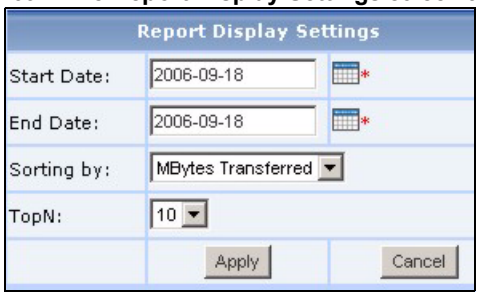
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that send the most web traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source. The **Top Web Users Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 35 Traffic > WEB > Top Users

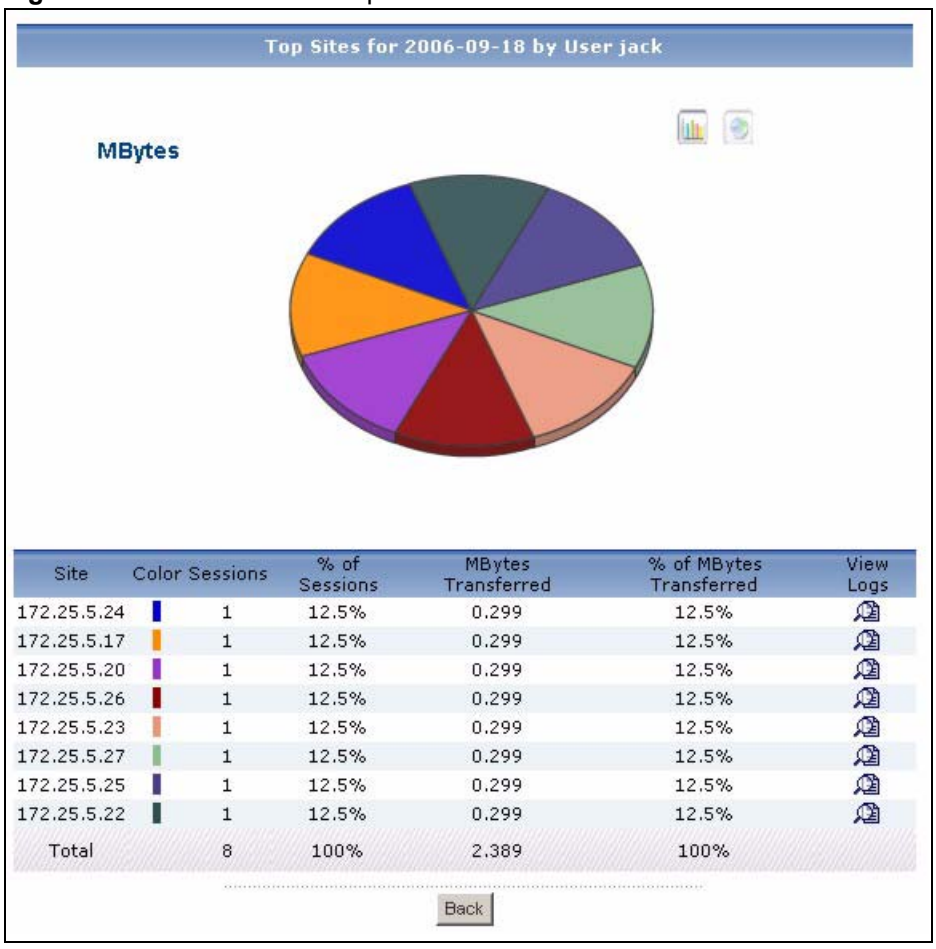
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click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

5.2.6 Top Web Users Drill-Down

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

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

Figure 41 Traffic > WEB > Top Users > Drill-Down



Each field is described in the following table.

Table 36 Traffic > WEB > Top Users > Drill-Down

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

5.3 FTP Traffic

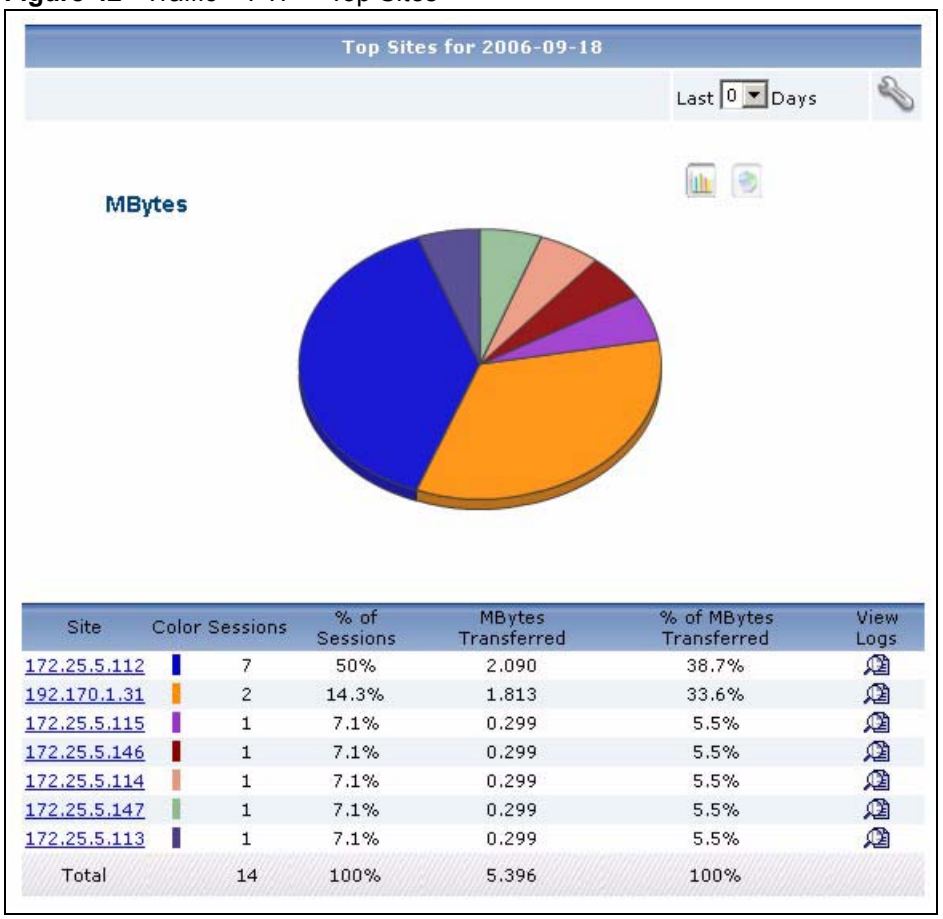
Use this report to look at the top destinations and sources of FTP traffic.

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 42 Traffic > FTP > Top Sites



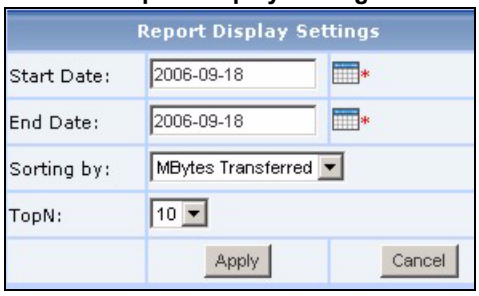
Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.112		7	50%	2.090	38.7%	
192.170.1.31		2	14.3%	1.813	33.6%	
172.25.5.115		1	7.1%	0.299	5.5%	
172.25.5.146		1	7.1%	0.299	5.5%	
172.25.5.114		1	7.1%	0.299	5.5%	
172.25.5.147		1	7.1%	0.299	5.5%	
172.25.5.113		1	7.1%	0.299	5.5%	
Total		14	100%	5.396	100%	

Each field is described in the following table.

Table 37 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 37 Traffic > FTP > Top Sites

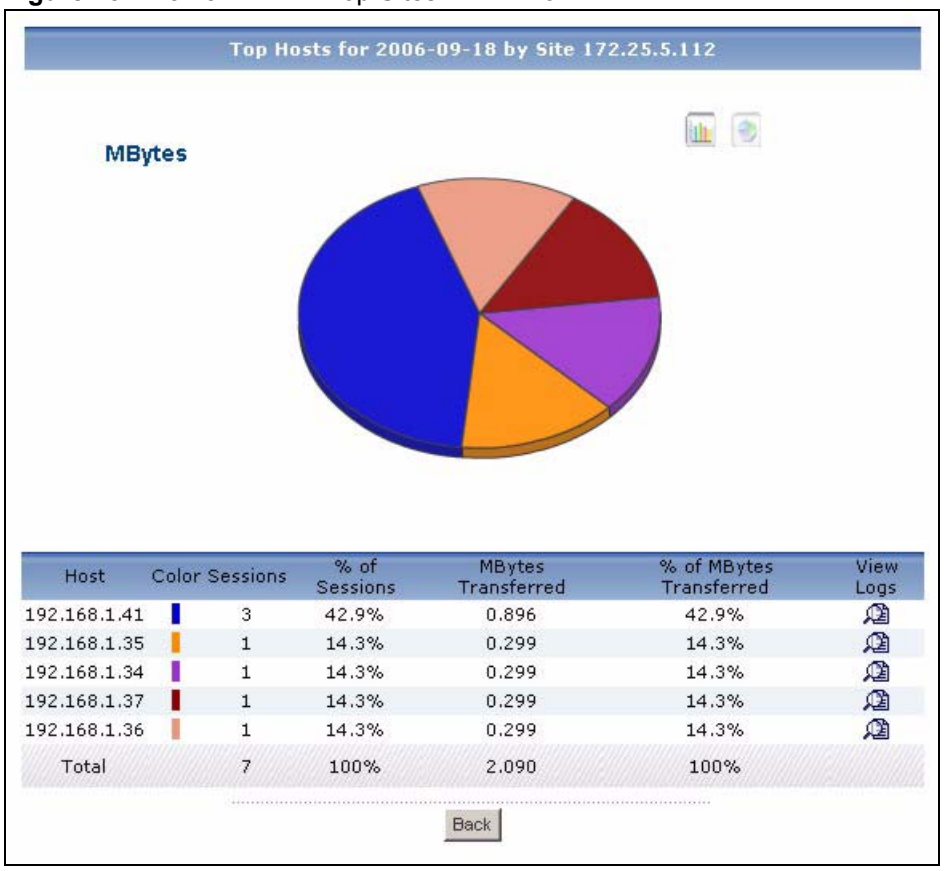
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a destination to look at the top sources of FTP traffic for the selected destination. The **Top FTP Sites Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination’s traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.3.2 Top FTP Sites Drill-Down

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

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

Figure 43 Traffic > FTP > Top Sites > Drill-Down



Each field is described in the following table.

Table 38 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of FTP traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.

Table 38 Traffic > FTP > Top Sites > Drill-Down

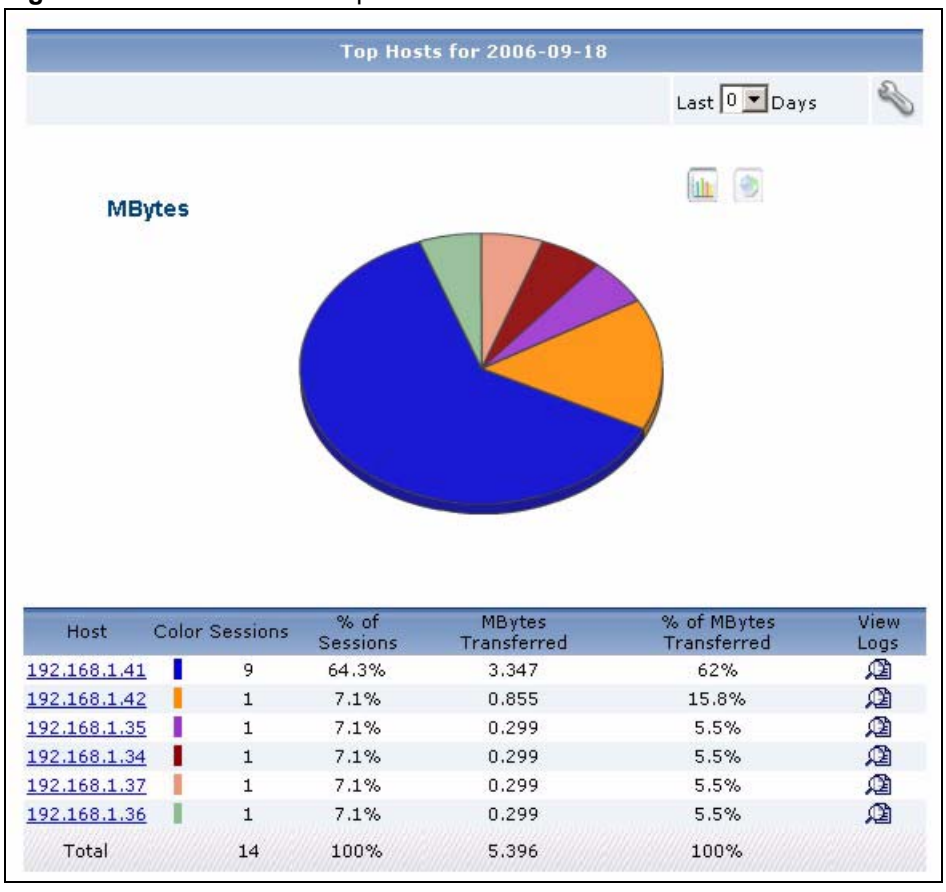
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events came from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) was generated from each source to the selected destination.
% of MBytes Transferred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

5.3.3 Top FTP Hosts

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

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

Figure 44 Traffic > FTP > Top Hosts



Each field is described in the following table.

Table 39 Traffic > FTP > Top Hosts

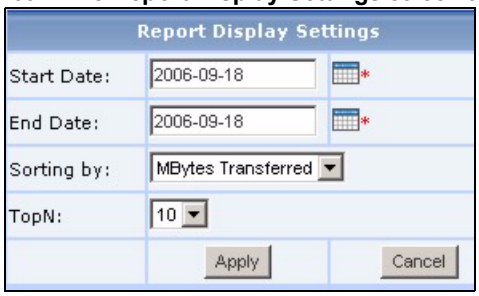
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of FTP traffic for the selected source. The **Top FTP Hosts Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 39 Traffic > FTP > Top Hosts

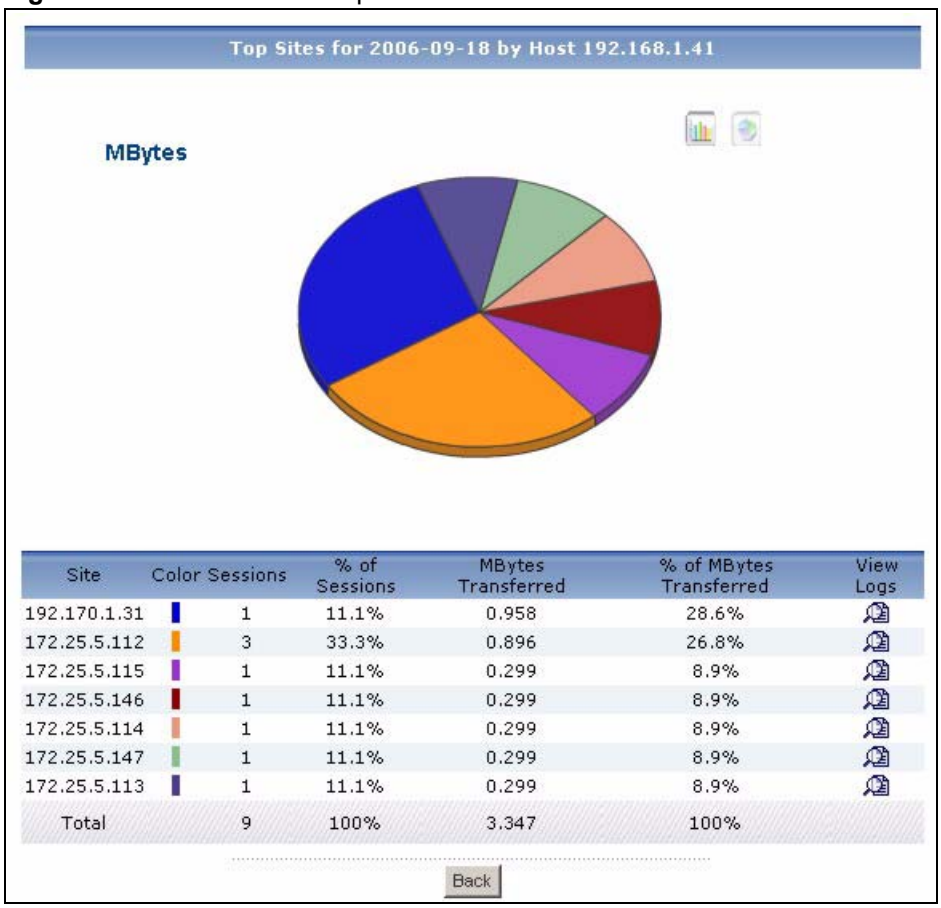
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs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

5.3.4 Top FTP Hosts Drill-Down

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

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

Figure 45 Traffic > FTP > Top Hosts > Drill-Down



Each field is described in the following table.

Table 40 Traffic > FTP > Top Hosts > Drill-Down

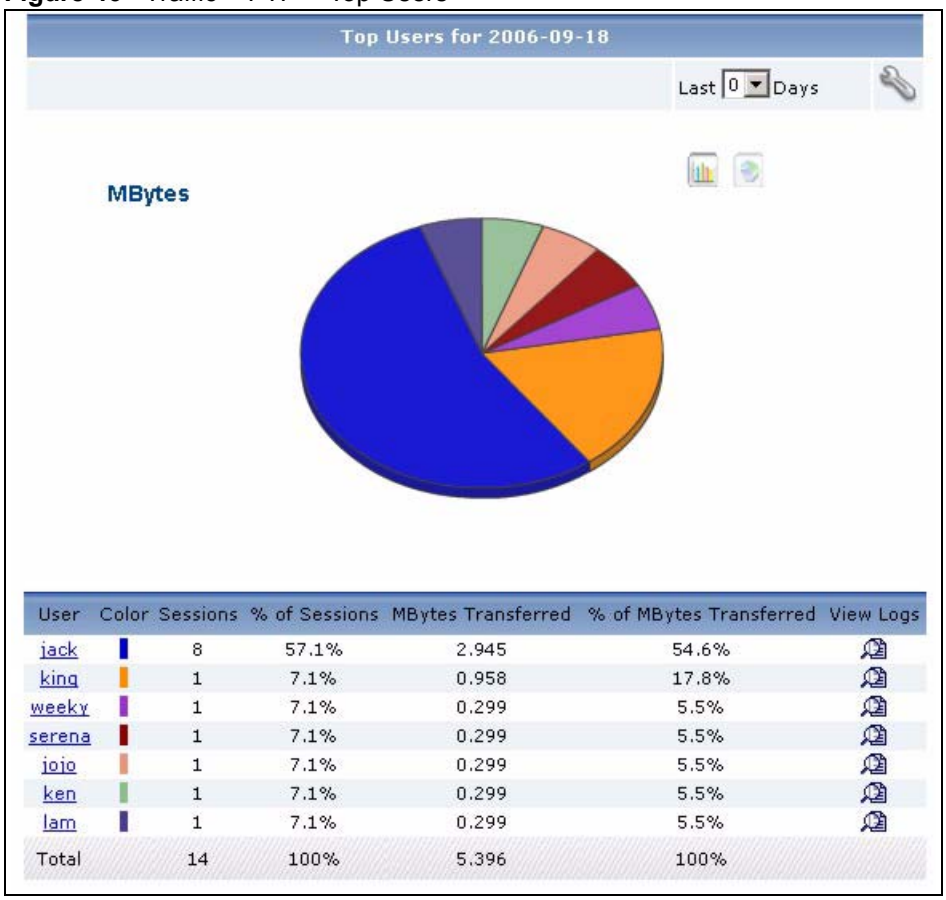
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default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

5.3.5 Top FTP Users

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

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

Figure 46 Traffic > FTP > Top Users



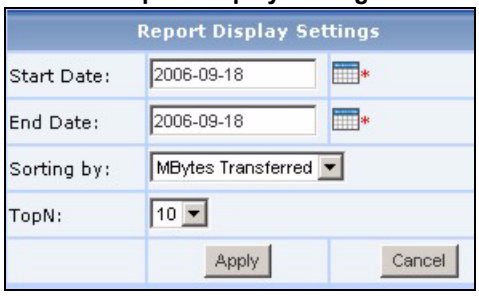
User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
jack		8	57.1%	2.945	54.6%	
king		1	7.1%	0.958	17.8%	
weeky		1	7.1%	0.299	5.5%	
serena		1	7.1%	0.299	5.5%	
jojo		1	7.1%	0.299	5.5%	
ken		1	7.1%	0.299	5.5%	
lam		1	7.1%	0.299	5.5%	
Total		14	100%	5.396	100%	

Each field is described in the following table.

Table 41 Traffic > FTP > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 41 Traffic > FTP > Top Users

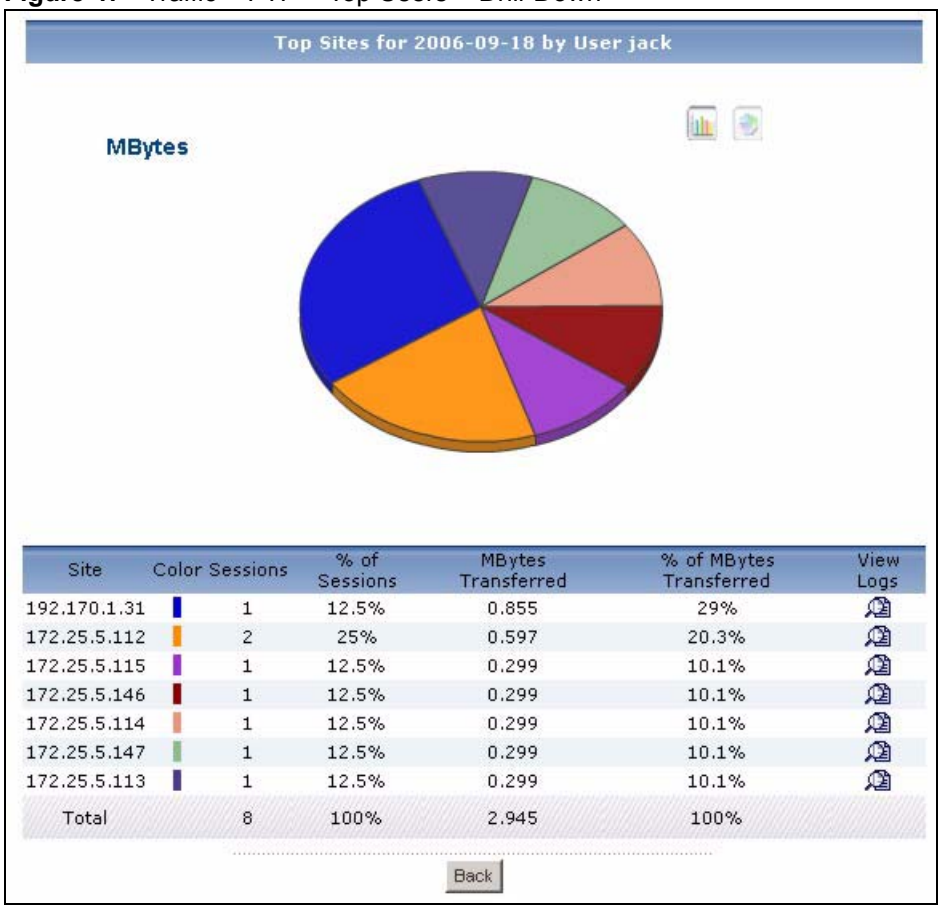
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that sent the most FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click a user name to look at the top destinations of FTP traffic for the selected user. The **Top FTP Users Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.3.6 Top FTP Users Drill-Down

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

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

Figure 47 Traffic > FTP > Top Users > Drill-Down



Each field is described in the following table.

Table 42 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of FTP traffic from the selected user, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected user to each destination.
% of Sessions	This field displays what percentage of the selected user’s total number of traffic events went to each destination.

Table 42 Traffic > FTP > Top Hosts > Drill-Down

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

5.4 Mail Traffic

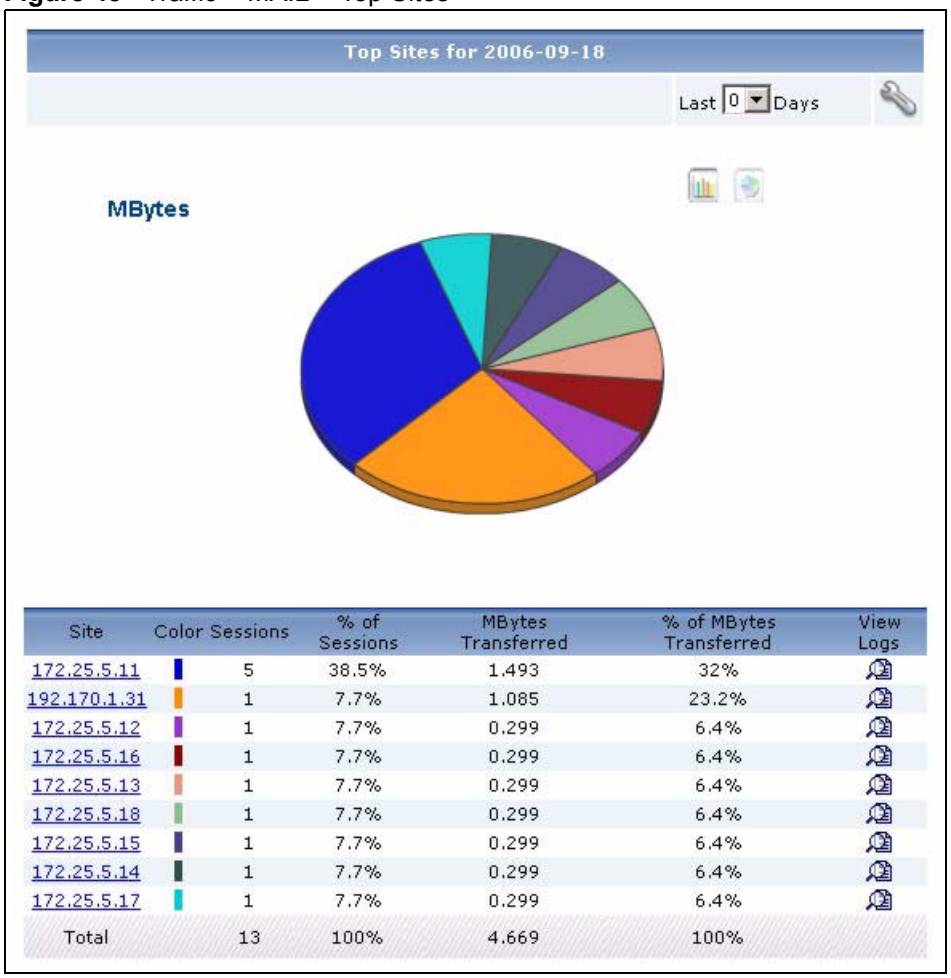
Use this report to look at the top destinations and sources of mail traffic.

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 48 Traffic > MAIL > Top Sites



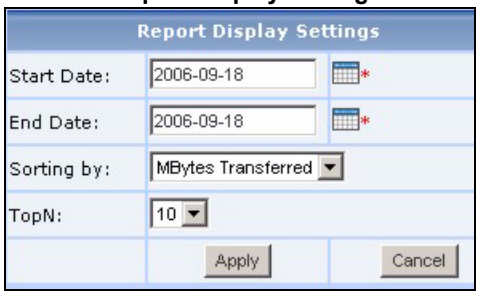
Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.11		5	38.5%	1.493	32%	
192.170.1.31		1	7.7%	1.085	23.2%	
172.25.5.12		1	7.7%	0.299	6.4%	
172.25.5.16		1	7.7%	0.299	6.4%	
172.25.5.13		1	7.7%	0.299	6.4%	
172.25.5.18		1	7.7%	0.299	6.4%	
172.25.5.15		1	7.7%	0.299	6.4%	
172.25.5.14		1	7.7%	0.299	6.4%	
172.25.5.17		1	7.7%	0.299	6.4%	
Total		13	100%	4.669	100%	

Each field is described in the following table.

Table 43 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 43 Traffic > MAIL > Top Sites

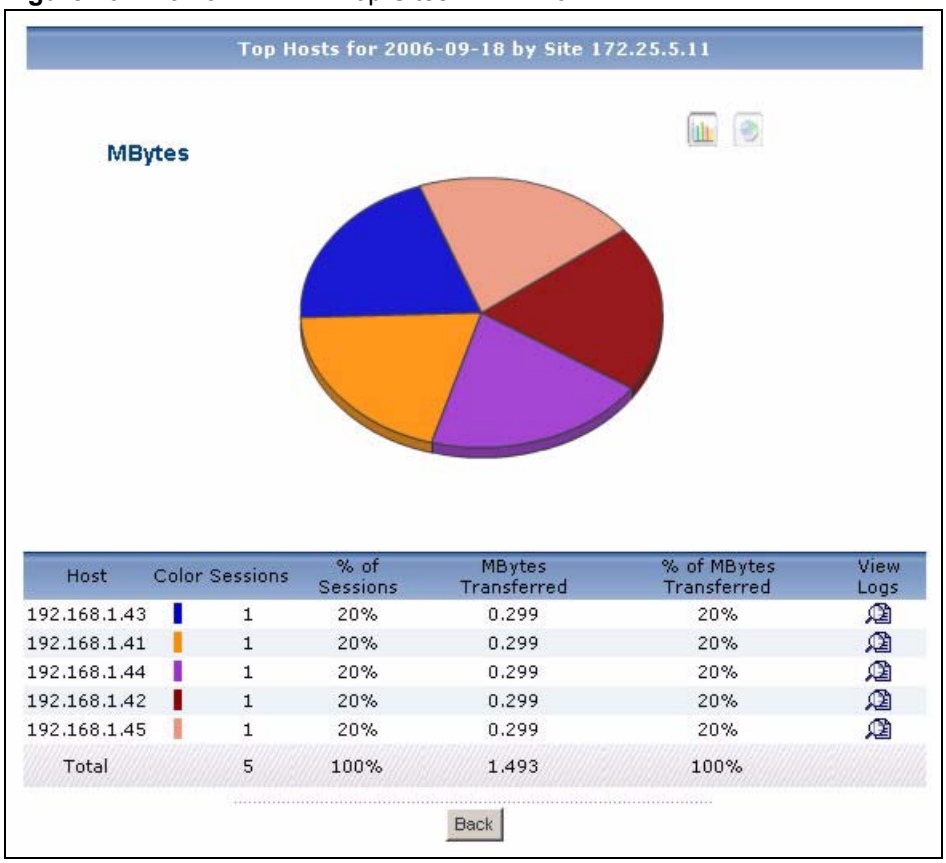
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a destination to look at the top sources of mail traffic for the selected destination. The **Top Mail Sites Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination’s traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.4.2 Top Mail Sites Drill-Down

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

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

Figure 49 Traffic > MAIL > Top Sites > Drill-Down



Each field is described in the following table.

Table 44 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of mail traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.

Table 44 Traffic > MAIL > Top Sites > Drill-Down

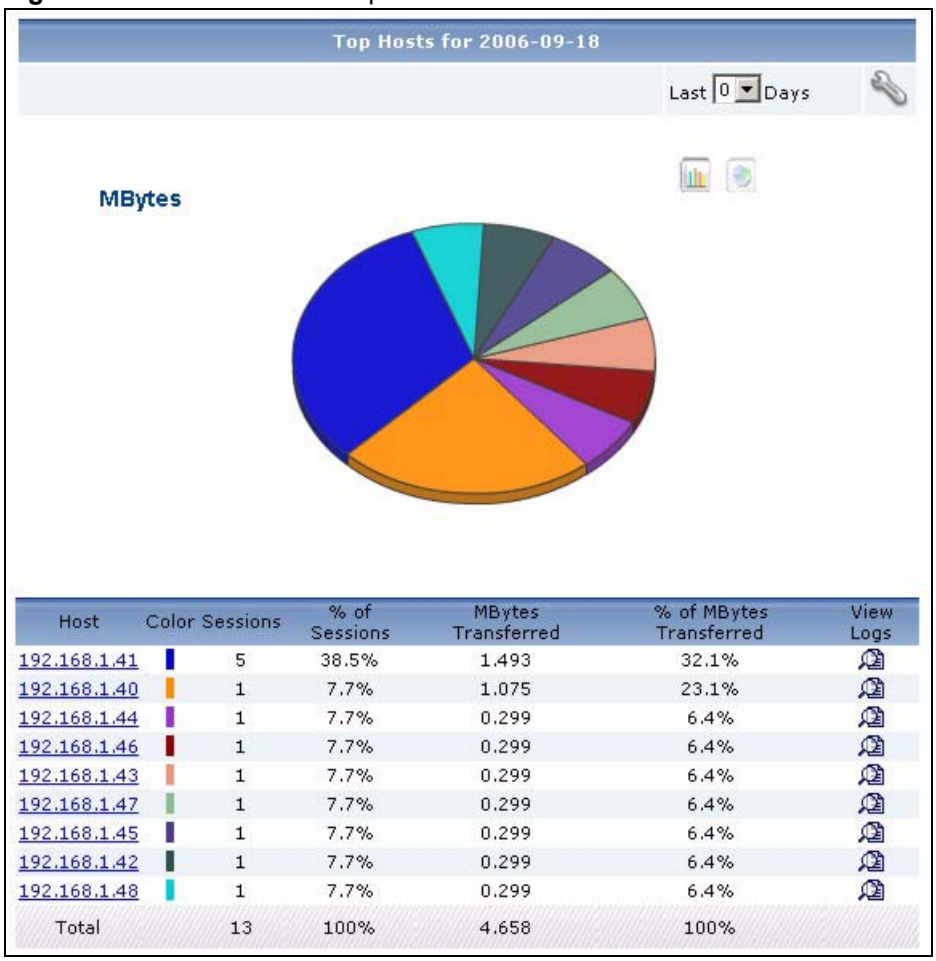
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage of the selected destination's total number of traffic events came from each source.
MBytes Transferred	This field displays how much traffic (in megabytes) came from each source to the selected destination.
% of MBytes Transferred	This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

5.4.3 Top Mail Hosts

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

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

Figure 50 Traffic > MAIL > Top Hosts



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.41		5	38.5%	1.493	32.1%	
192.168.1.40		1	7.7%	1.075	23.1%	
192.168.1.44		1	7.7%	0.299	6.4%	
192.168.1.46		1	7.7%	0.299	6.4%	
192.168.1.43		1	7.7%	0.299	6.4%	
192.168.1.47		1	7.7%	0.299	6.4%	
192.168.1.45		1	7.7%	0.299	6.4%	
192.168.1.42		1	7.7%	0.299	6.4%	
192.168.1.48		1	7.7%	0.299	6.4%	
Total		13	100%	4.658	100%	

Each field is described in the following table.

Table 45 Traffic > MAIL > Top Hosts

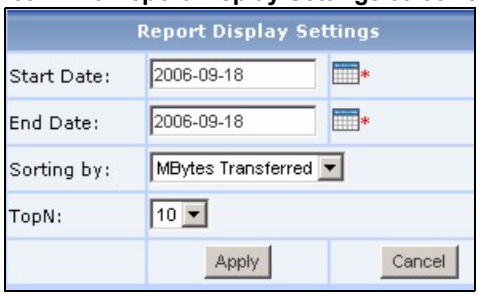
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of mail traffic for the selected source. The **Top Mail Hosts Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 45 Traffic > MAIL > Top Hosts

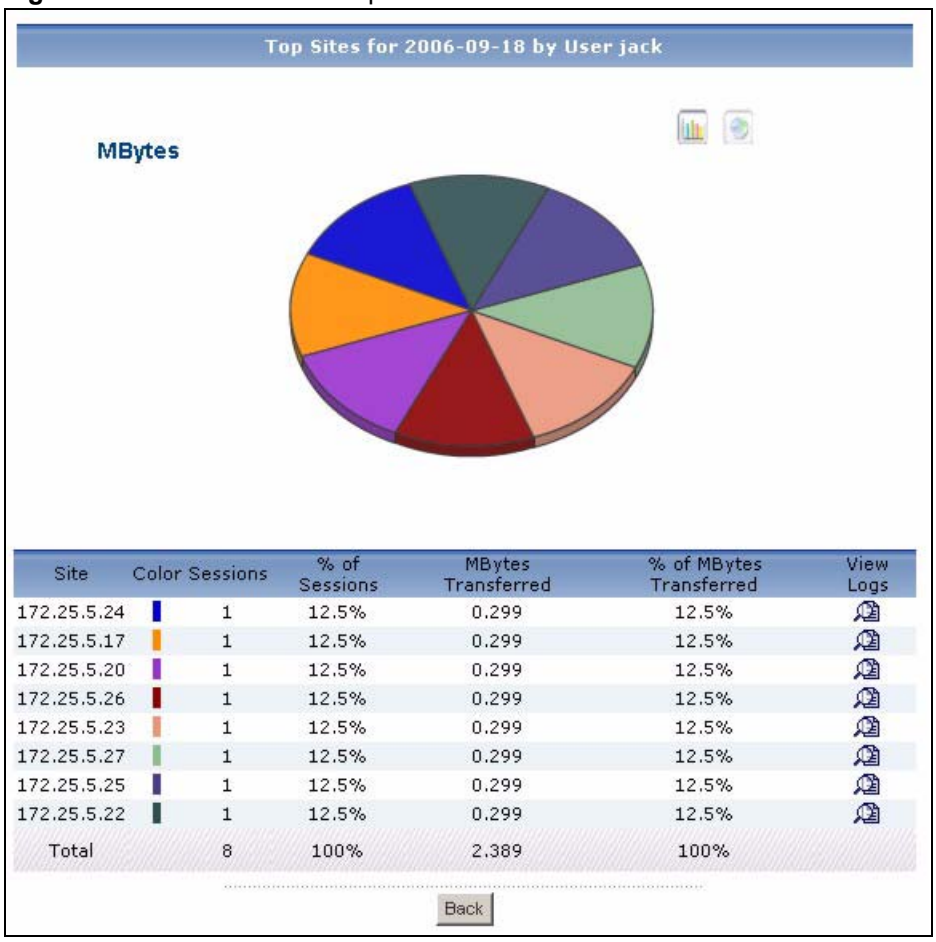
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs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

5.4.4 Top Mail Hosts Drill-Down

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

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

Figure 51 Traffic > MAIL > Top Hosts > Drill-Down



Each field is described in the following table.

Table 46 Traffic > MAIL > Top Hosts > Drill-Down

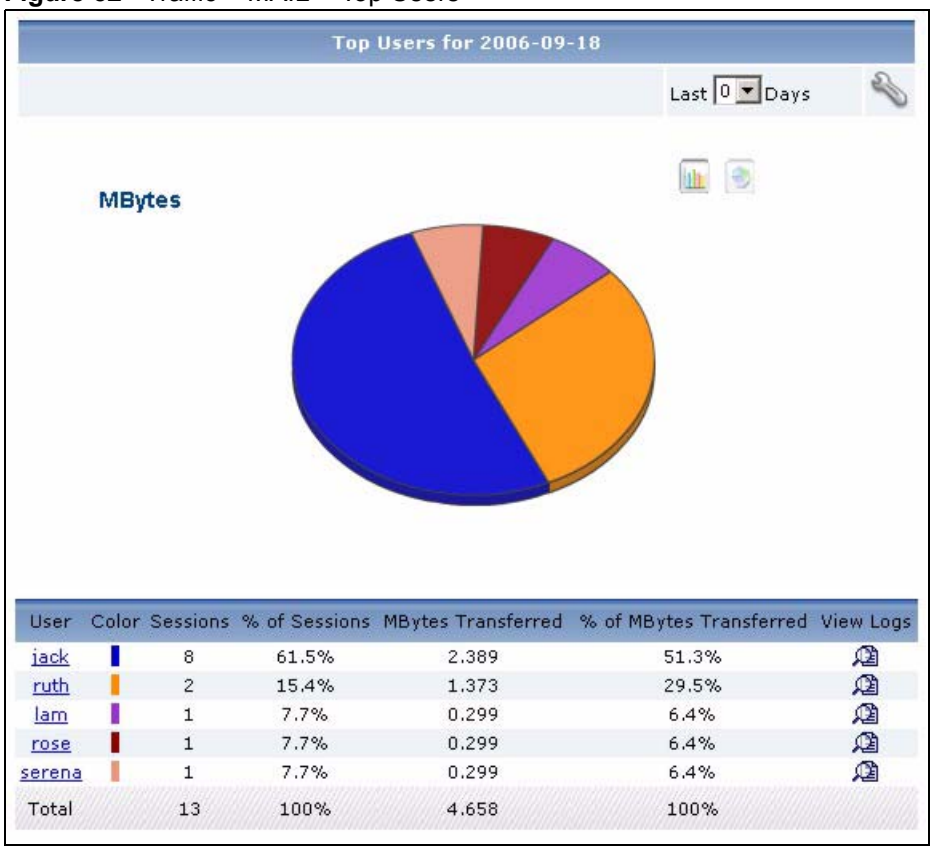
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default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

5.4.5 Top Mail Users

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

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

Figure 52 Traffic > MAIL > Top Users



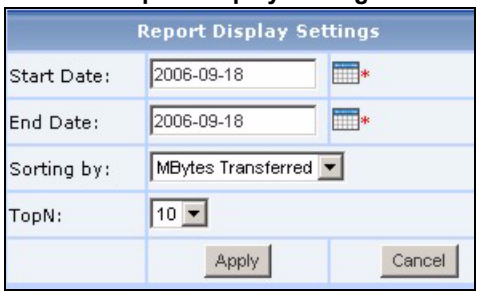
User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
jack		8	61.5%	2.389	51.3%	
ruth		2	15.4%	1.373	29.5%	
lam		1	7.7%	0.299	6.4%	
rose		1	7.7%	0.299	6.4%	
serena		1	7.7%	0.299	6.4%	
Total		13	100%	4.658	100%	

Each field is described in the following table.

Table 47 Traffic > MAIL > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 47 Traffic > MAIL > Top Users

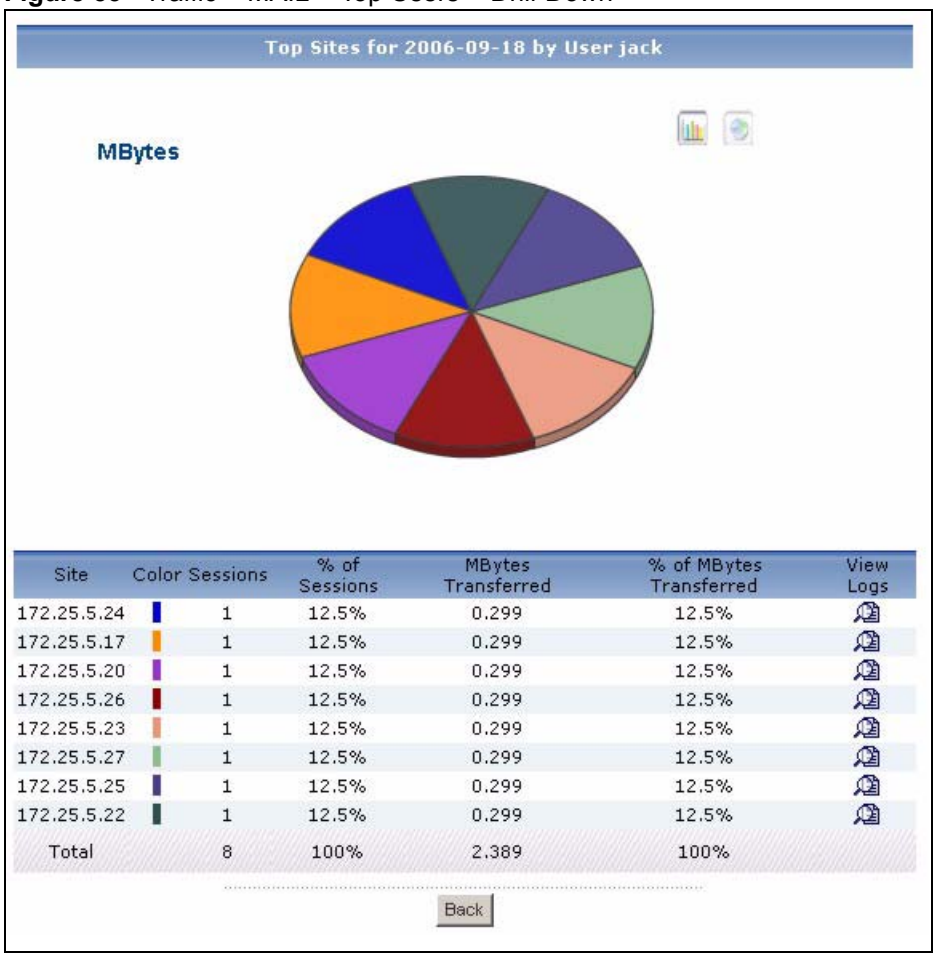
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that send the most mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of mail traffic for the selected source. The **Top Mail Users Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.4.6 Top Mail Users Drill-Down

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

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

Figure 53 Traffic > MAIL > Top Users > Drill-Down



Each field is described in the following table.

Table 48 Traffic > MAIL > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of mail traffic from the selected user, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected user to each destination.
% of Sessions	This field displays what percentage of the selected user’s total number of traffic events went to each destination.

Table 48 Traffic > MAIL > Top Users > Drill-Down

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

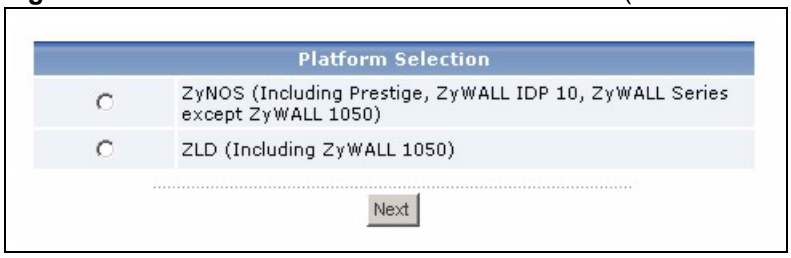
5.5 Other Traffic

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

5.5.1 Platform Selection

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

Figure 54 Traffic > Customization > Customization (Platform Selection)



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

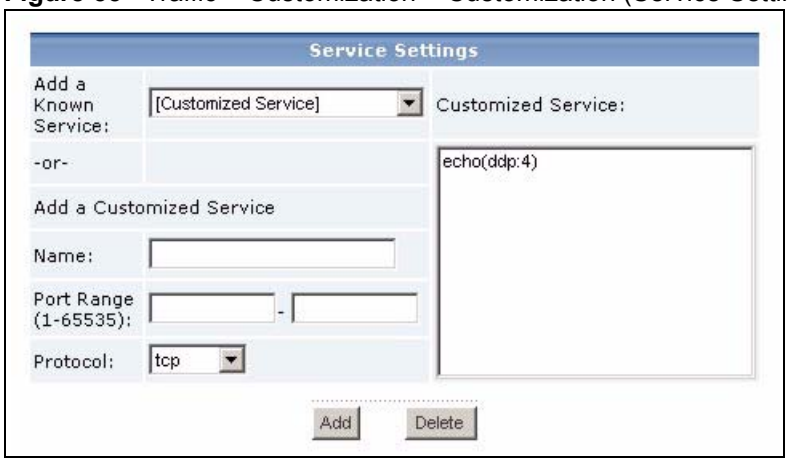
Then click **Next**.

5.5.2 Service Settings

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

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

Figure 55 Traffic > Customization > Customization (Service Settings)



Each field is described in the following table.

Table 49 Service > Customization > Customization (Service Settings)

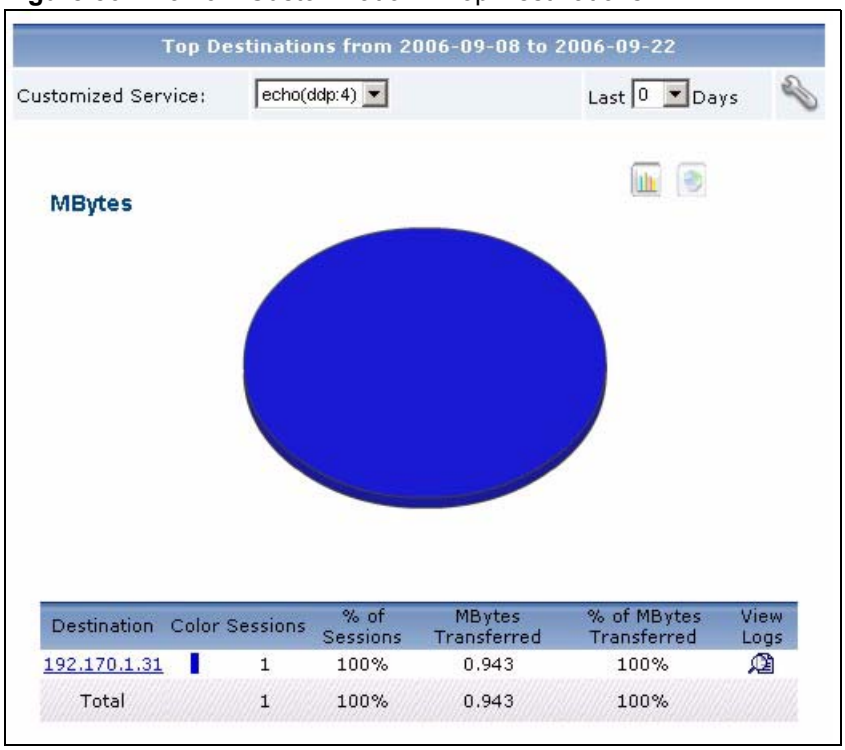
LABEL	DESCRIPTION
Add a Known Service	Use this drop-down box to add a service to the **Customized Service** drop-down box. • Select a pre-defined service from the drop-down list box, and click the **Add** button; or • Select **[Customized Service]**, fill in the **Add a Customized Service** section,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

5.5.3 Top Destinations of Other Traffic

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

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

Figure 56 Traffic > Customization > Top Destinations

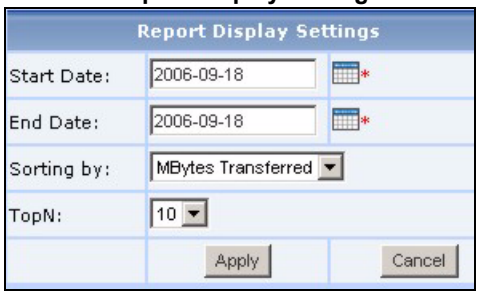


Each field is described in the following table.

Table 50 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 50 Traffic > Customization > Top Destinations

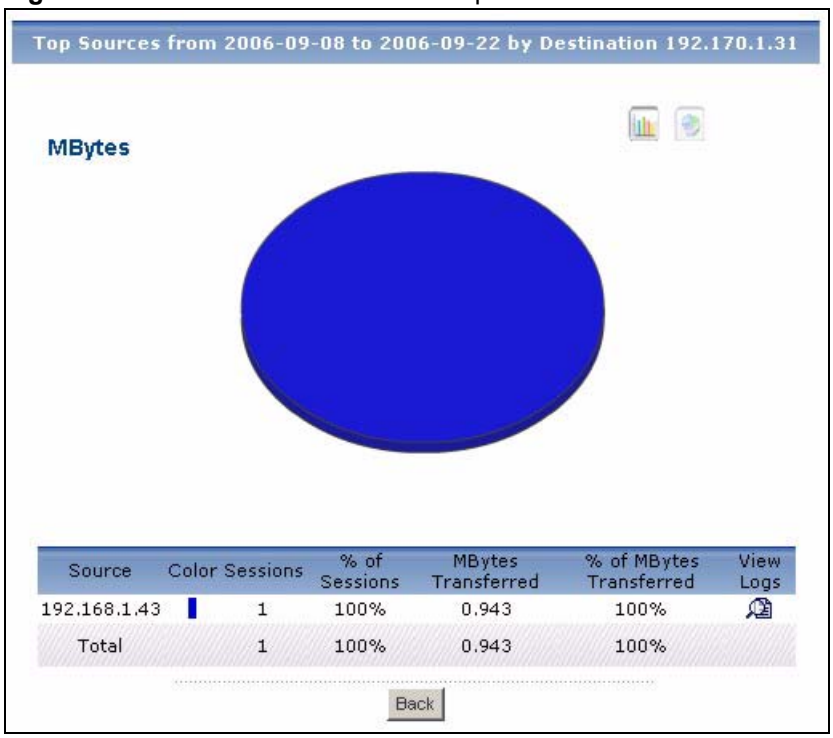
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the top sources of the selected service's traffic for the selected destination. The **Top Destinations for Other Services Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

5.5.4 Top Destinations of Other Traffic Drill-Down

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

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

Figure 57 Traffic > Customization > Top Destinations > Drill-Down



Each field is described in the following table.

Table 51 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected service's traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events for the selected destination.
MBytes Transferred	This field displays how much traffic (in megabytes) was sent from each source to the selected destination.
% of MBytes Transferred	This field displays what percentage of the selected destination's traffic came from each source.

Table 51 Traffic > Customization > Top Destinations > Drill-Down

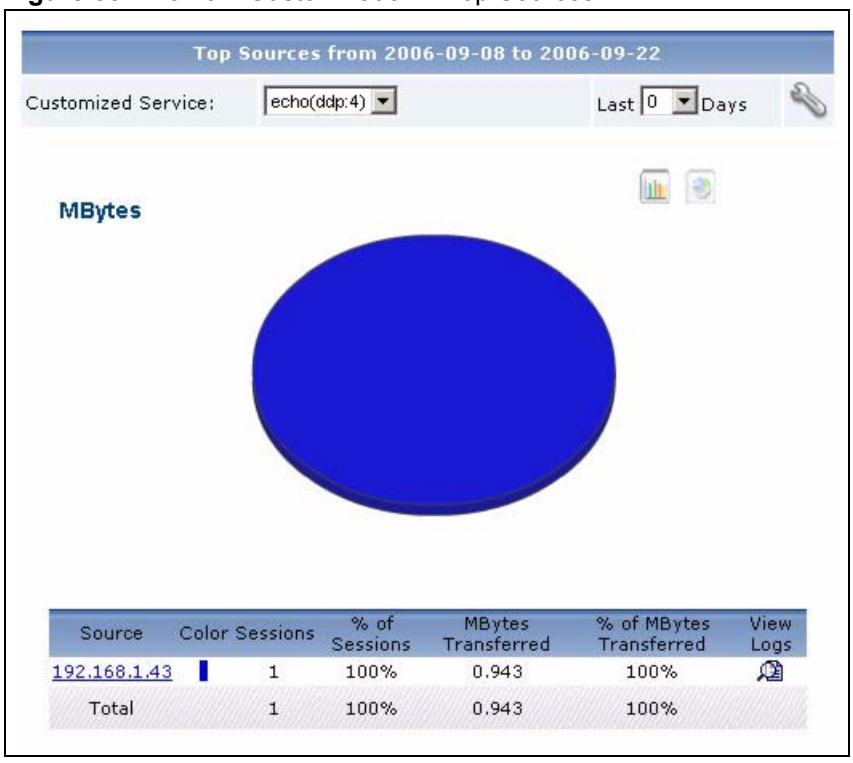
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

5.5.5 Top Sources of Other Traffic

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

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

Figure 58 Traffic > Customization > Top Sources



Each field is described in the following table.

Table 52 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.

Table 52 Traffic > Customization > Top Sources

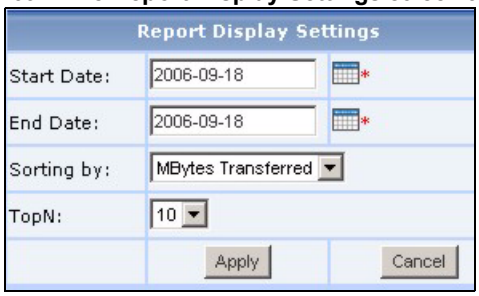
LABEL	DESCRIPTION
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of the selected service's traffic for the selected source. The **Top Sources for Other Services Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 52 Traffic > Customization > Top Sources

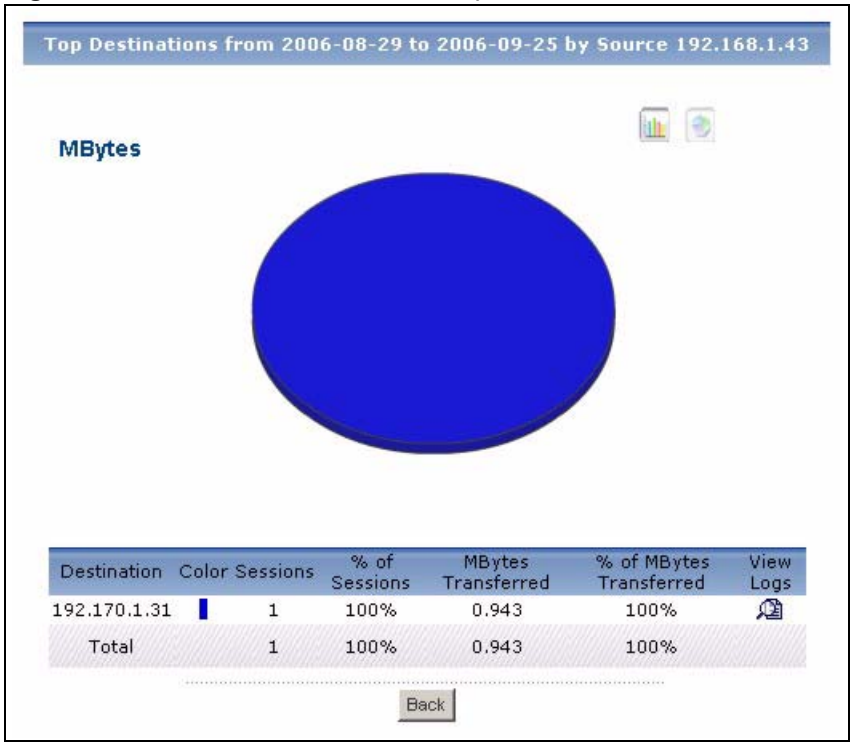
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs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

5.5.6 Top Sources of Other Traffic Drill-Down

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

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

Figure 59 Traffic > Customization > Top Sources > Drill-Down



Each field is described in the following table.

Table 53 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	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 53 Traffic > Customization > Top Sources > Drill-Down

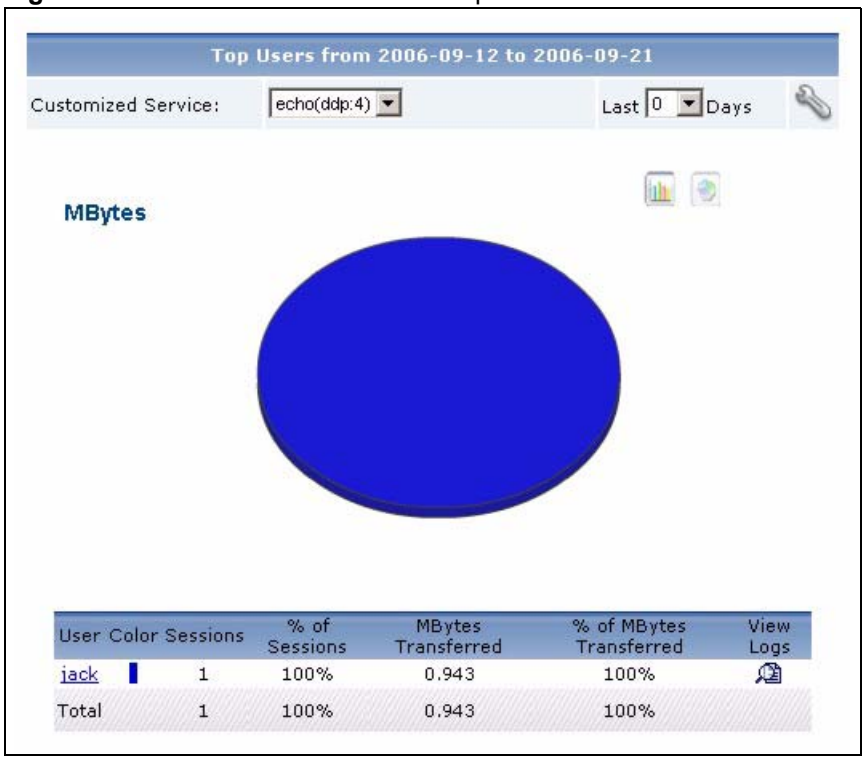
LABEL	DESCRIPTION
Destination	This field displays the top destinations of the selected service's traffic from the selected source, sorted by the amount of traffic attributed to each one. Each destination is identified by its IP address.
Color	This field displays what color represents each destination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

5.5.7 Top Other Traffic Users

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

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

Figure 60 Traffic > Customization > Top Users



Each field is described in the following table.

Table 54 Traffic > Customization > Top Users

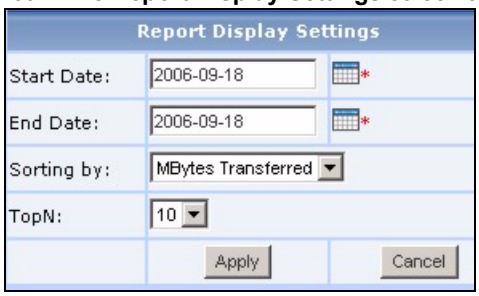
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Customized Service	Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that sent the most of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of the selected service's traffic for the selected source. The **Top Users for Other Services Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.

Table 54 Traffic > Customization > Top Users

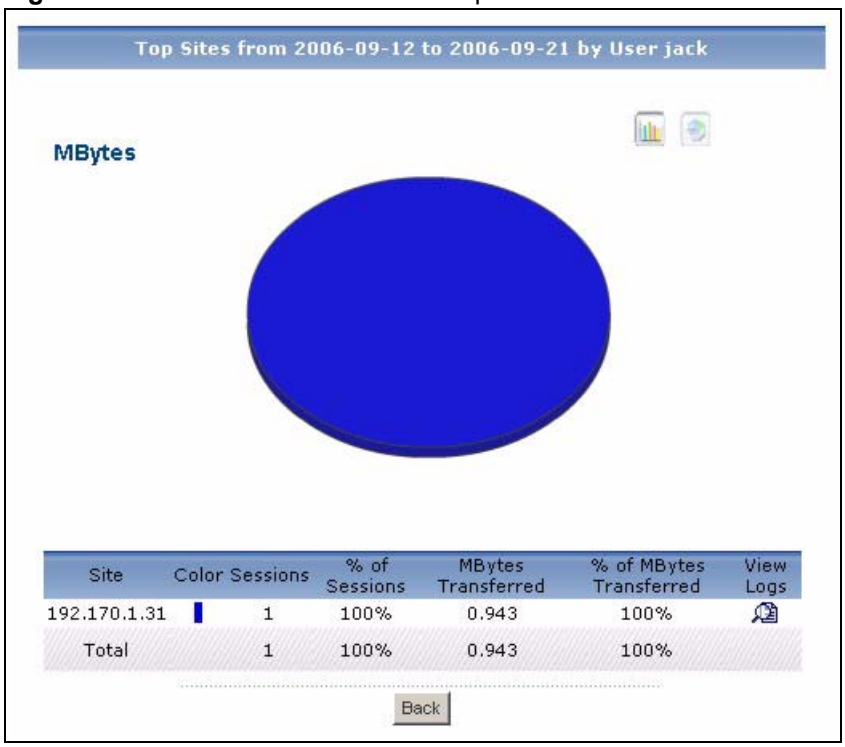
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events for the time range of the report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes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

5.5.8 Top Users of Other Traffic Drill-Down

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

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

Figure 61 Traffic > Customization > Top Users > Drill-Down



Each field is described in the following table.

Table 55 Traffic > Customization > Top Users > Drill-Down

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

6 VPN

6.1 VPN Site-to-Site

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

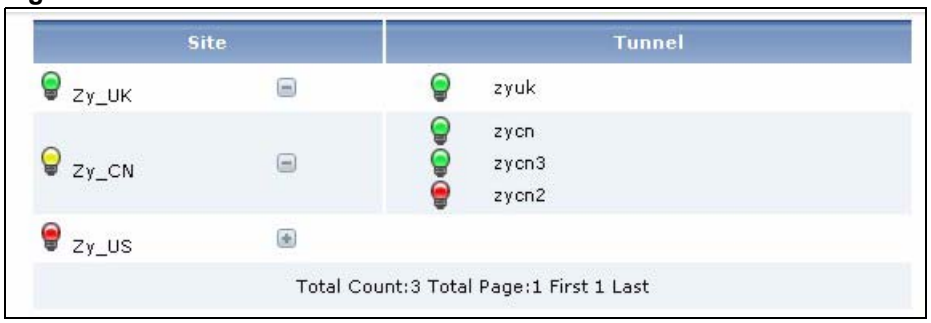
To look at VPN usage reports, each ZyXEL device must record forwarded IPSec VPN traffic in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to Logs > Log Settings, and make sure IPSec is enabled.

6.1.1 VPN Link Status

Use this report to see which of the device's VPN tunnels are connected.

Click **VPN > Site-to-Site > Link Status** to open this screen.

Figure 62 VPN > Site-to-Site > Link Status



Each field is described in the following table.

Table 56 VPN > Site-to-Site > Link Status

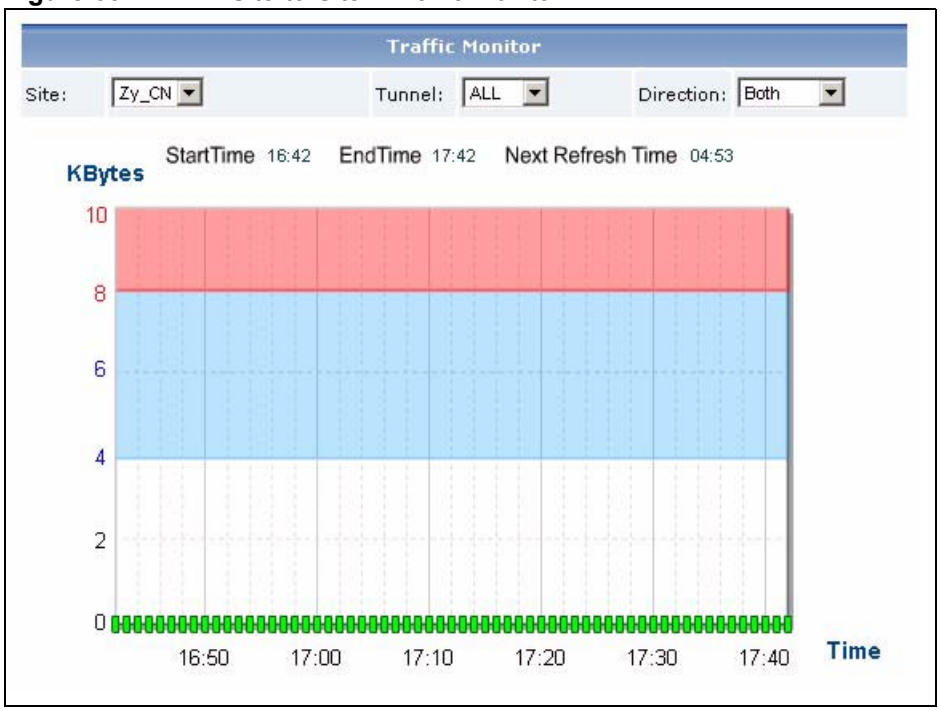
LABEL	DESCRIPTION
Site	This column displays the names of peer IPSec routers. Each IPSec router is identified by the name of the phase 1 IKE SA (also known as the gateway policy). A site's status icon is green when all of the configured VPN tunnels between the device and the peer IPSec router are connected. A site's status icon is yellow when some of the configured VPN tunnels between the device and the peer IPSec router are connected. A site's status icon is red when none of the configured VPN tunnels between the device and the peer IPSec router are connected.
Tunnel	This column displays the names of the device's VPN tunnels. A tunnel's status icon is green when the VPN tunnel is connected. A tunnel's status icon is red when the VPN tunnel is not connected.
Total	This entry displays the total number of sites on each page of the report.

6.1.2 VPN Traffic Monitor

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

Click **VPN > Site-to-Site > Traffic Monitor** to open this screen.

Figure 63 VPN > Site-to-Site > Traffic Monitor



Each field is described in the following table.

Table 57 VPN > Site-to-Site > Traffic Monitor

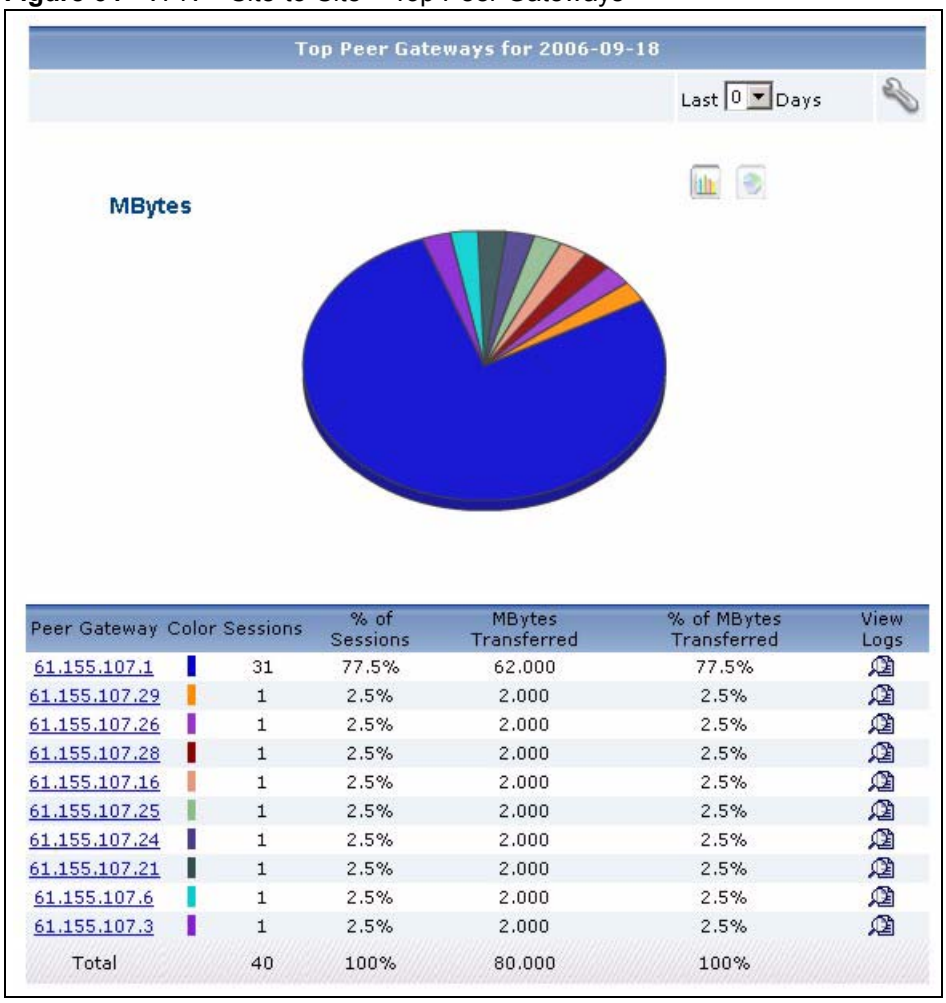
LABEL	DESCRIPTION
Site	Select a peer IPSec router.
Tunnel	Select a VPN tunnel. Select **All** to display the total traffic for the device's VPN tunnels with the selected site.
Direction	Select for which direction of traffic, you want to view bandwidth usage. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.
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 is handled by the device each minute X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the **Start Time** and **End Time**.

6.1.3 Top VPN Peer Gateways

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

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

Figure 64 VPN > Site-to-Site > Top Peer Gateways



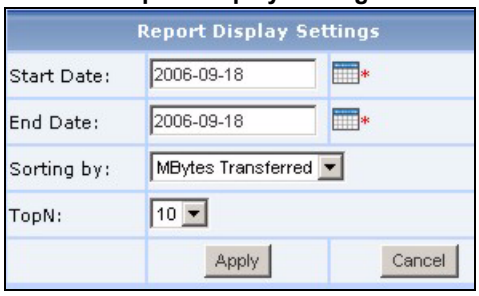
Peer Gateway	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
61.155.107.1		31	77.5%	62.000	77.5%	
61.155.107.29		1	2.5%	2.000	2.5%	
61.155.107.26		1	2.5%	2.000	2.5%	
61.155.107.28		1	2.5%	2.000	2.5%	
61.155.107.16		1	2.5%	2.000	2.5%	
61.155.107.25		1	2.5%	2.000	2.5%	
61.155.107.24		1	2.5%	2.000	2.5%	
61.155.107.21		1	2.5%	2.000	2.5%	
61.155.107.6		1	2.5%	2.000	2.5%	
61.155.107.3		1	2.5%	2.000	2.5%	
Total		40	100%	80.000	100%	

Each field is described in the following table.

Table 58 VPN > Site-to-Site > 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 58 VPN > Site-to-Site > Top Peer Gateways

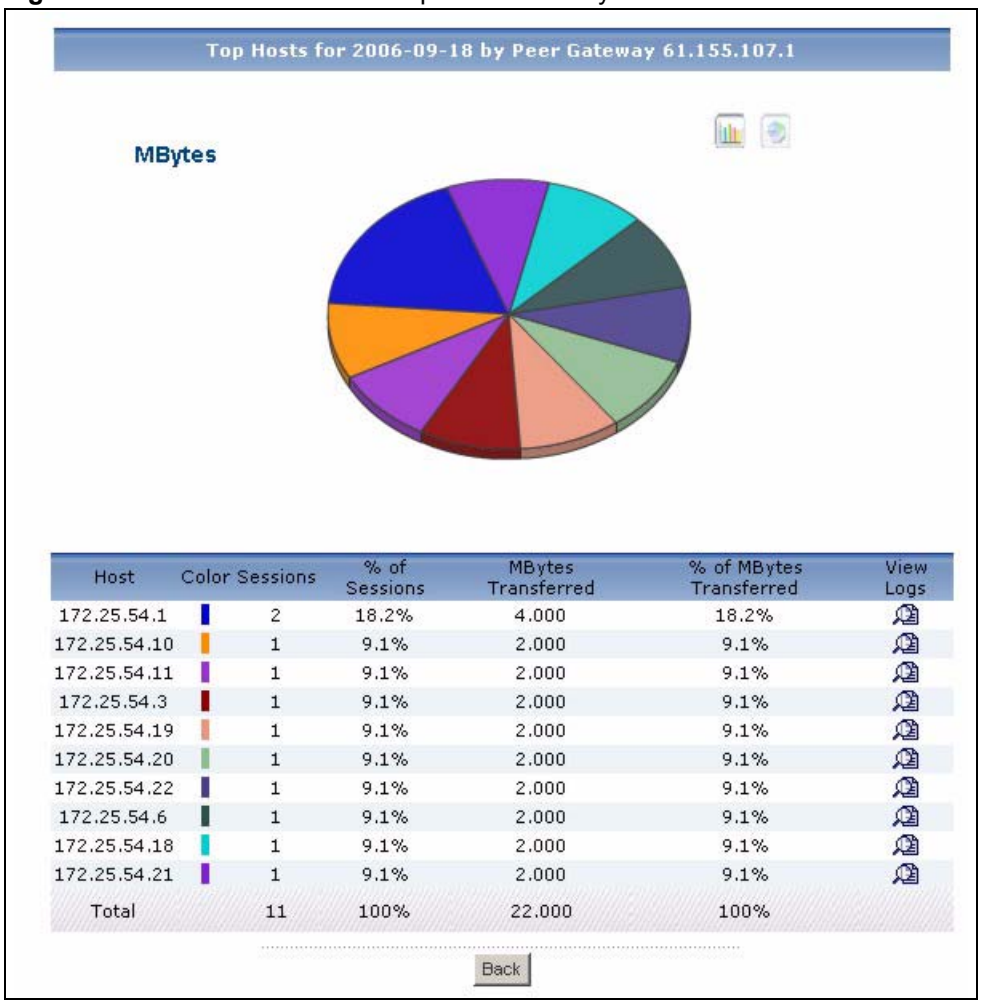
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Peer Gateway	This field displays the top destinations of VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by the IP address of the remote gateway. Click on a destination to look at the top sources of VPN traffic for the selected destination. The **Top VPN Peer Gateways Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.4 Top VPN Peer Gateways Drill-Down

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

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

Figure 65 VPN > Site-to-Site > Top Peer Gateways > Drill-Down



Each field is described in the following table.

Table 59 VPN > Site-to-Site > 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of VPN traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.

Table 59 VPN > Site-to-Site > Top Peer Gateways > Drill-Down

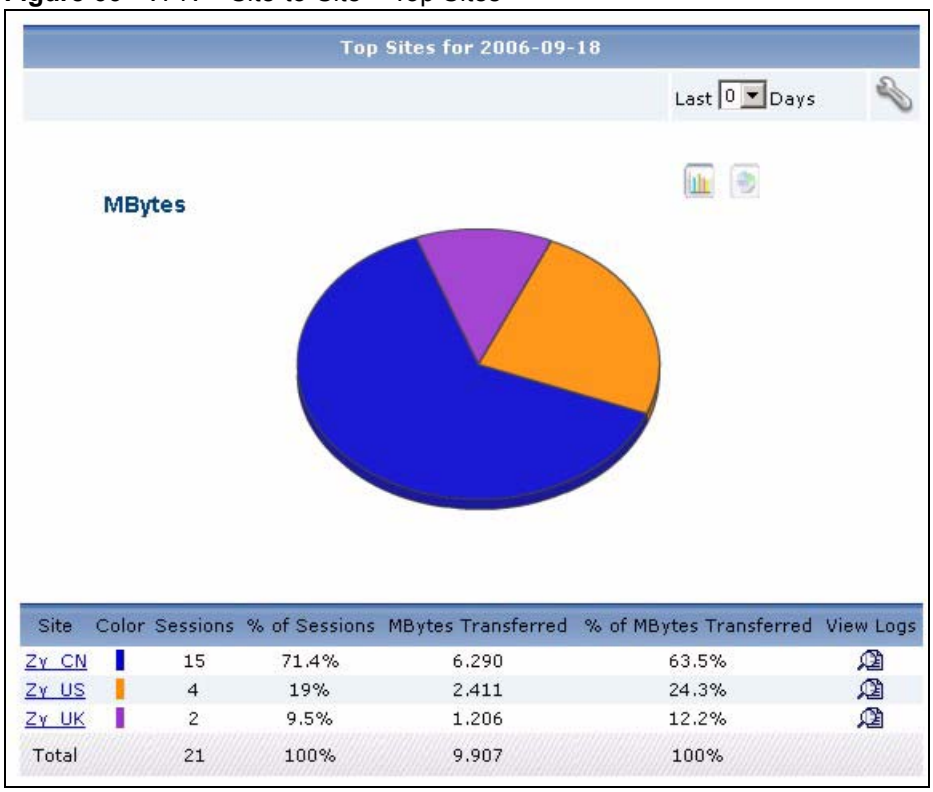
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events for the selected destination.
MBytes Transferred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

6.1.5 Top VPN Sites

Use this report to look at the peer IPSec routers with the most VPN traffic.

Click **VPN > Site-to-Site > Top Sites** to open this screen.

Figure 66 VPN > Site-to-Site > Top Sites



Each field is described in the following table.

Table 60 VPN > Site-to-Site > Top Sites

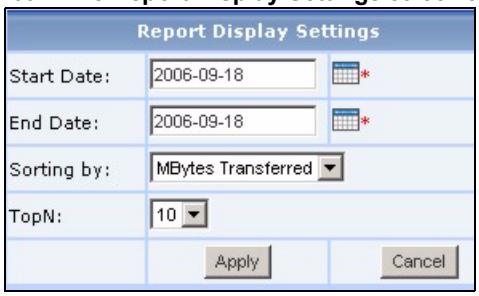
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the peer IPSec routers with the most VPN traffic, sorted by the amount of traffic for each one. If the number of peer IPSec routers is less than the maximum number of records displayed in this table, every peer IPSec router is displayed. Each peer IPSec router is identified by the name of the phase 1 IKE SA (also known as the gateway policy). Click on a name to look at the top sources of VPN traffic for the selected site. The **Top VPN Sites Drill-Down** report appears.
Color	This field displays what color represents each site in the graph.
Sessions	This field displays the number of traffic events for each site.
% of Sessions	This field displays what percentage each site's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 60 VPN > Site-to-Site > Top Sites

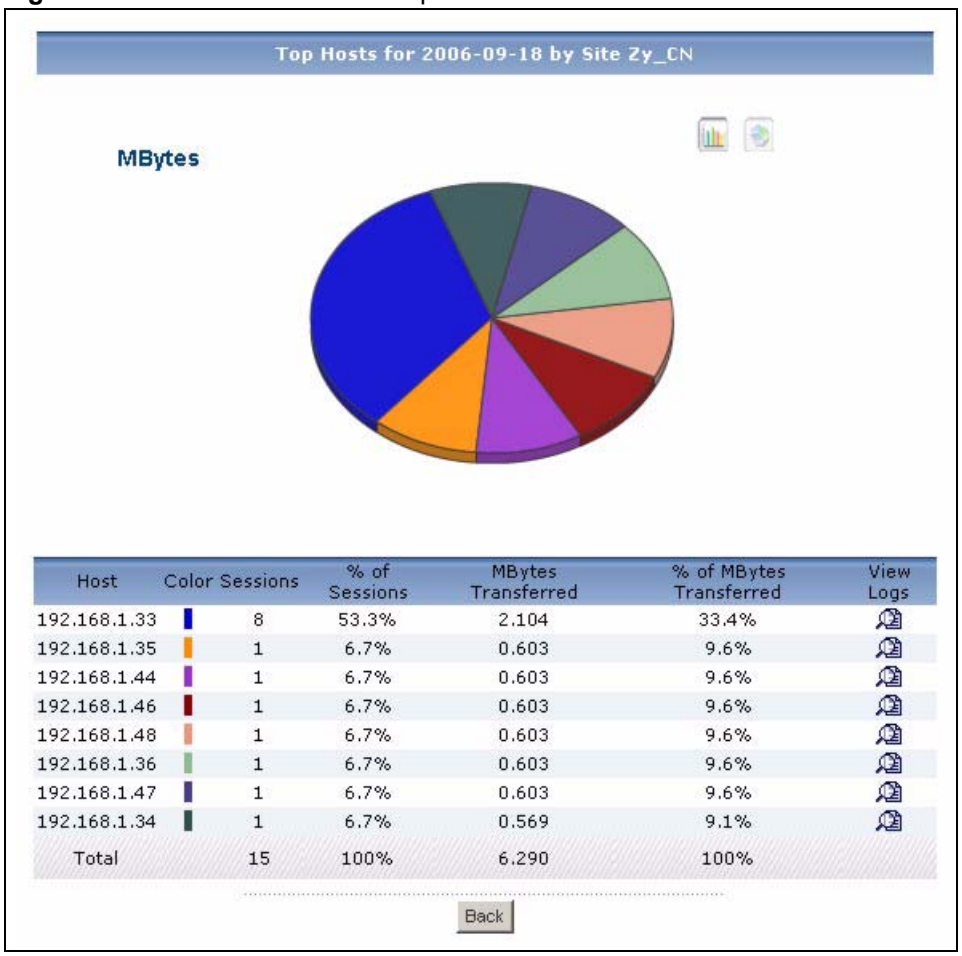
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each site.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each site.
View Logs	Click this icon to see the logs that go with the record.
Total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

6.1.6 Top VPN Sites Drill-Down

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

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

Figure 67 VPN > Site-to-Site > Top Sites > Drill-Down



Each field is described in the following table.

Table 61 VPN > Site-to-Site > Top Sites > Drill-Down

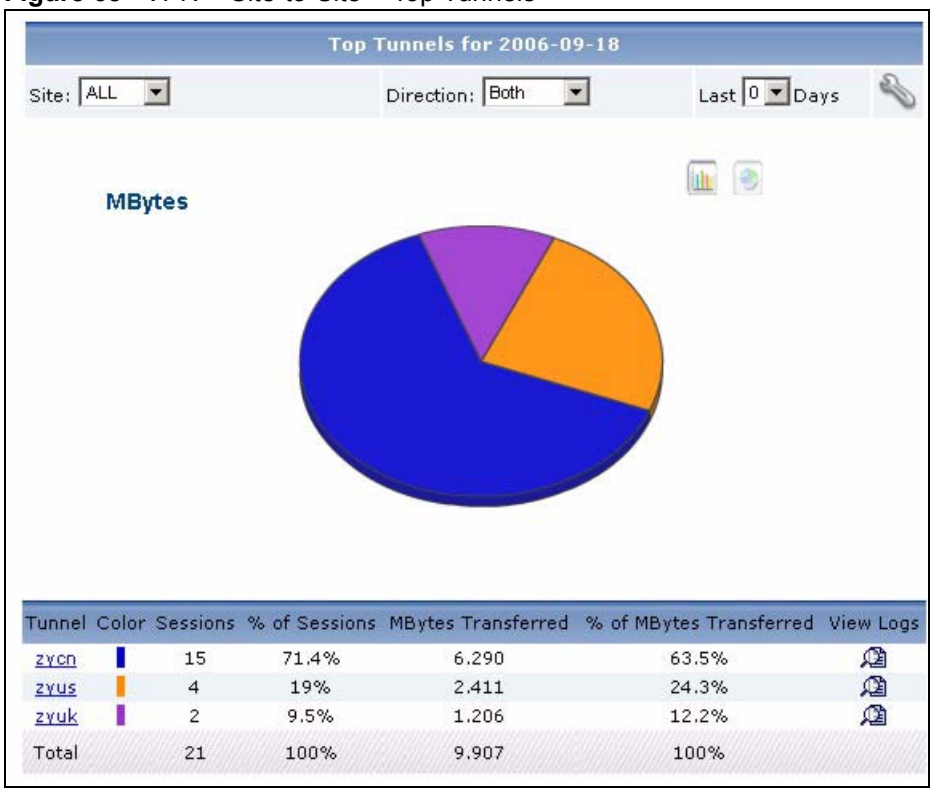
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default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

6.1.7 Top VPN Tunnels

Use this report to look at the VPN tunnels with the most VPN traffic.

Click **VPN > Site-to-Site > Top Tunnels** to open this screen.

Figure 68 VPN > Site-to-Site > Top Tunnels

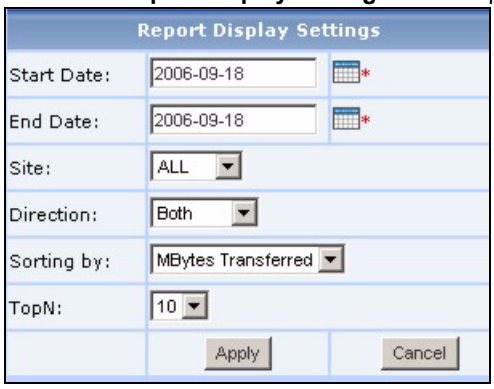


Each field is described in the following table.

Table 62 VPN > Site-to-Site > Top Tunnels

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.
Site	Select a peer IPSec router. Select **All** to display the device's VPN tunnels with the most traffic, regardless of which peer IPSec router they use.
Direction	Select for which direction of traffic, you want to view bandwidth usage. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.
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 VPN > Site-to-Site > Top Tunnels

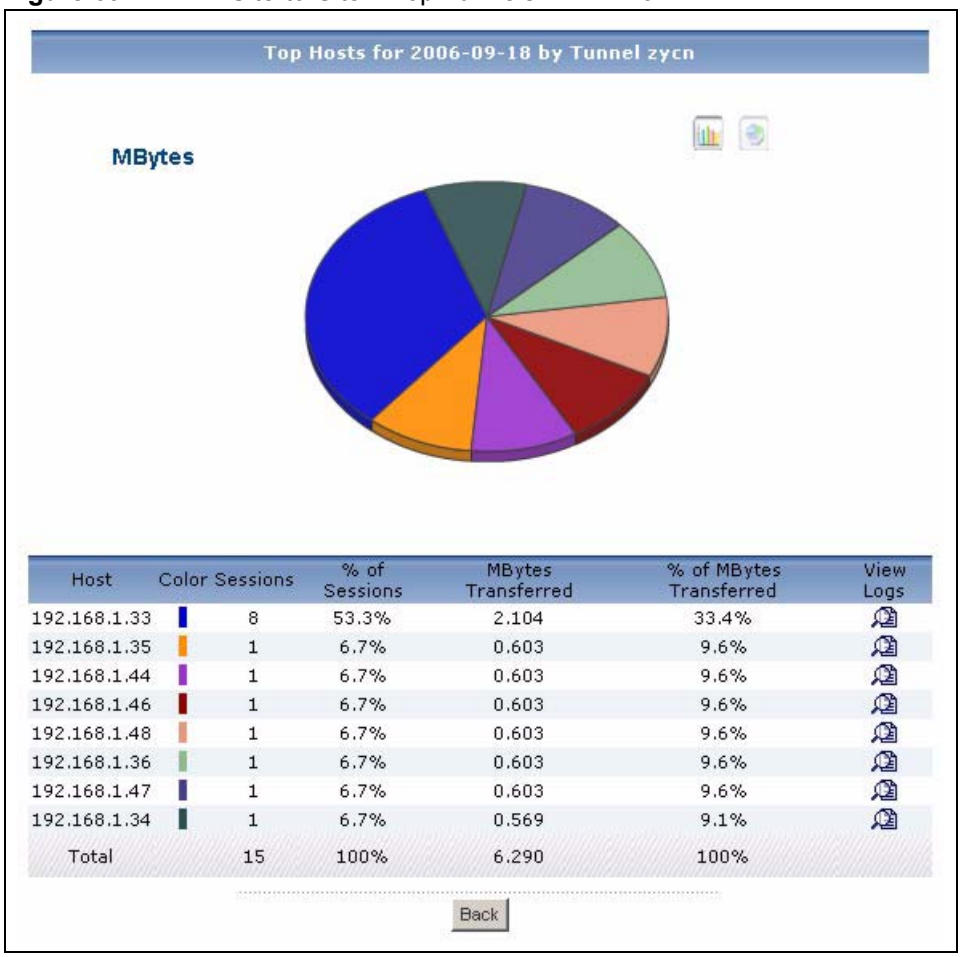
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Site** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Tunnel	This field displays the phase 2 IPSec tunnels with the most VPN traffic, sorted by the amount of traffic for each one. If the number of tunnels is less than the maximum number of records displayed in this table, every tunnel is displayed. Each tunnel is identified by the name of the phase 2 IPSec SA (also known as the network policy). Click on a name to look at the top sources of VPN traffic for the selected tunnel. The **Top VPN Tunnels Drill-Down** report appears.
Color	This field displays what color represents each tunnel in the graph.
Sessions	This field displays the number of traffic events for each tunnel.
% of Sessions	This field displays what percentage each tunnel's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each tunnel.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each tunnel.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.8 Top VPN Tunnels Drill-Down

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

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

Figure 69 VPN > Site-to-Site > Top Tunnels > Drill-Down



Each field is described in the following table.

Table 63 VPN > Site-to-Site > Top Tunnels > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of VPN traffic for the selected VPN tunnel, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.

Table 63 VPN > Site-to-Site > Top Tunnels > Drill-Down

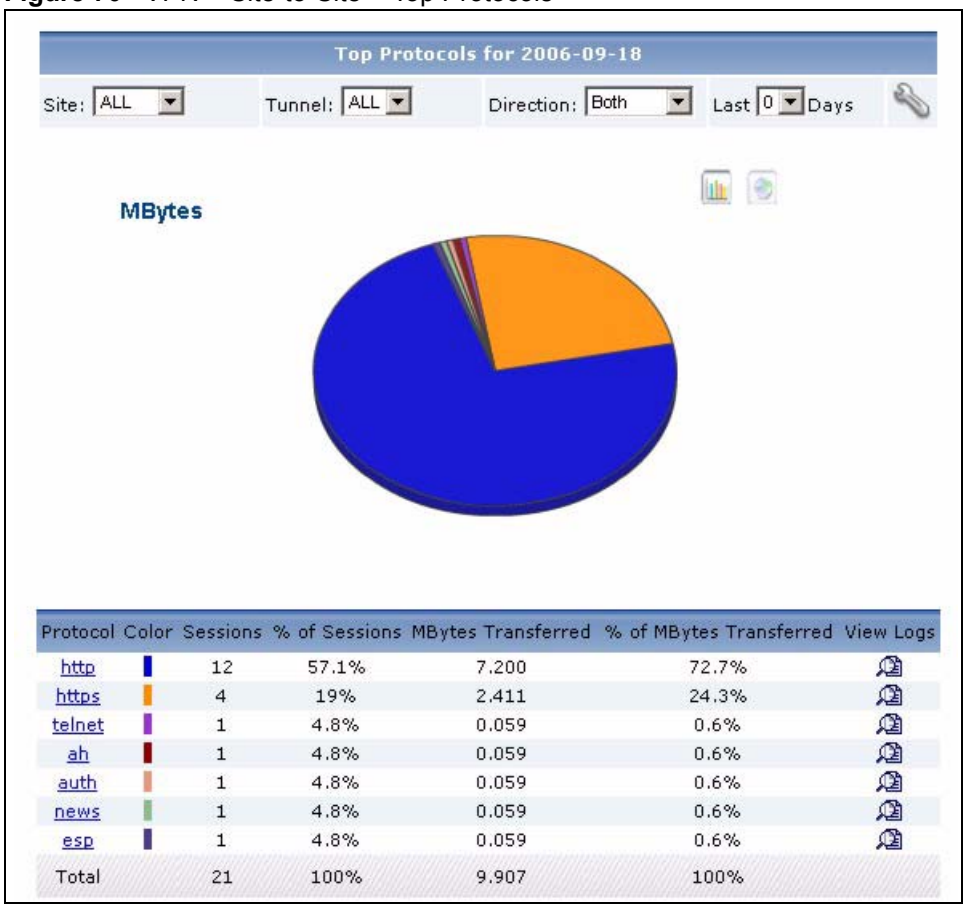
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events from each host to the selected VPN tunnel.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected VPN tunnel.
MBytes Transferred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

6.1.9 Top VPN Protocols

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

Click **VPN > Site-to-Site > Top Protocols** to open this screen.

Figure 70 VPN > Site-to-Site > Top Protocols



Each field is described in the following table.

Table 64 VPN > Site-to-Site > Top Protocols

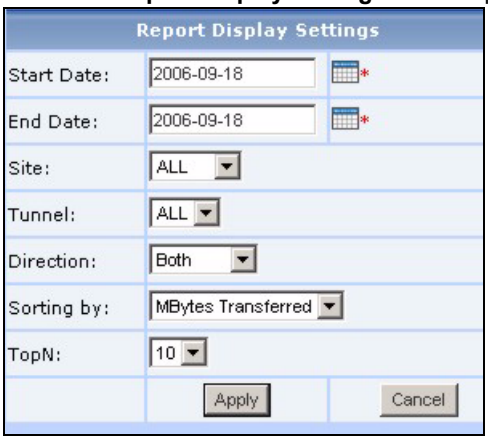
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Site	Select a peer IPSec router. Select **All** to display the device's VPN tunnels with the most traffic, regardless of which peer IPSec router they use.
Tunnel	Select a VPN tunnel. Select **All** to display the total traffic for the device's VPN tunnels with the selected site (or all sites).
Direction	Select for which direction of traffic, you want to view bandwidth usage. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.
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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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 64 VPN > Site-to-Site > Top Protocols

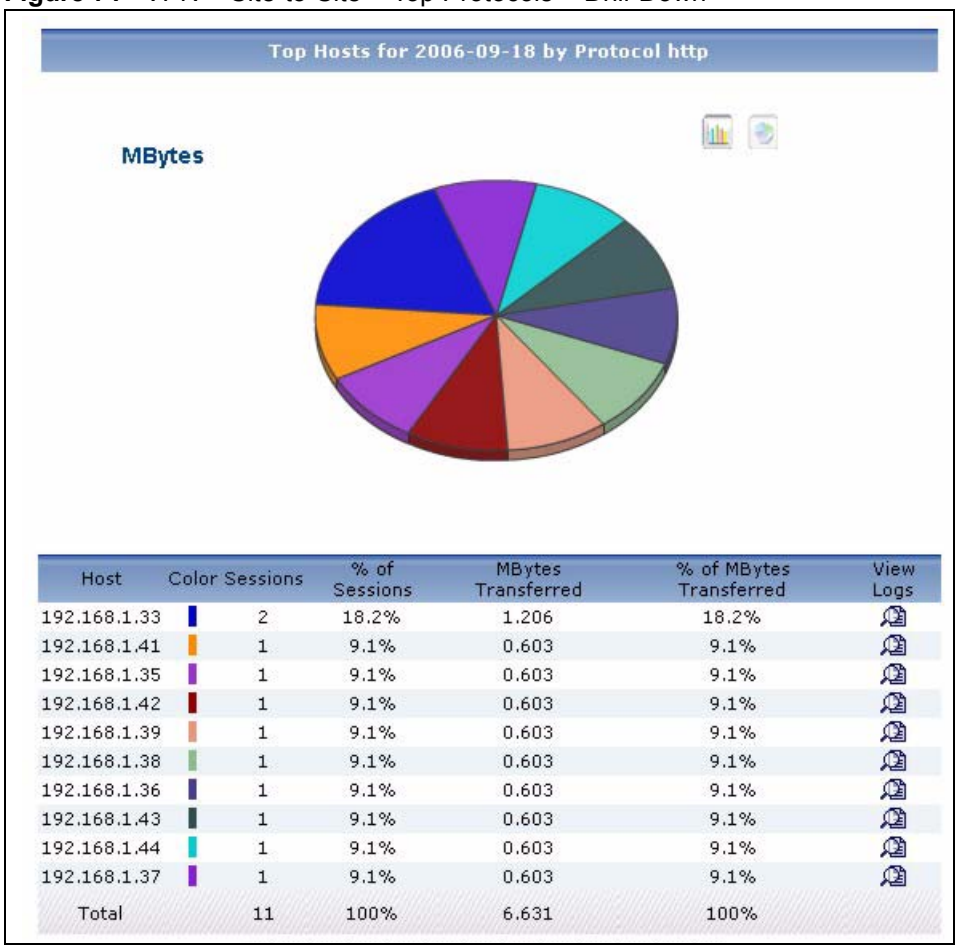
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most used by VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through VPN. The **Top VPN Protocols Drill-Down** report appears.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the protocols above.

6.1.10 Top VPN Protocols Drill-Down

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

Click on a specific service in **VPN > Site-to-Site > Top Protocols** to open this screen.

Figure 71 VPN > Site-to-Site > Top Protocols > Drill-Down



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33		2	18.2%	1.206	18.2%	
192.168.1.41		1	9.1%	0.603	9.1%	
192.168.1.35		1	9.1%	0.603	9.1%	
192.168.1.42		1	9.1%	0.603	9.1%	
192.168.1.39		1	9.1%	0.603	9.1%	
192.168.1.38		1	9.1%	0.603	9.1%	
192.168.1.36		1	9.1%	0.603	9.1%	
192.168.1.43		1	9.1%	0.603	9.1%	
192.168.1.44		1	9.1%	0.603	9.1%	
192.168.1.37		1	9.1%	0.603	9.1%	
Total		11	100%	6.631	100%	

Each field is described in the following table.

Table 65 VPN > Site-to-Site > Top Protocols > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of VPN traffic using the selected service, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected VPN traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) went through VPN for each host.

Table 65 VPN > Site-to-Site > Top Protocols > Drill-Down

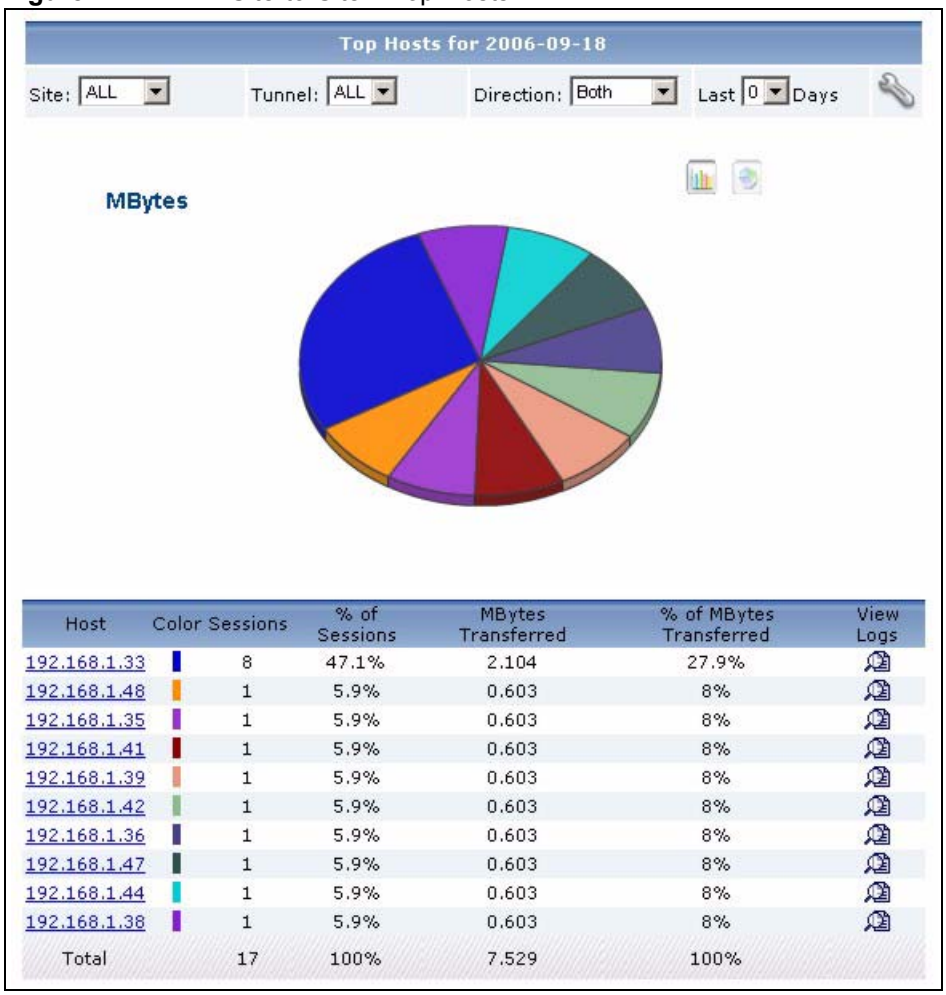
LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage of the selected VPN traffic was for each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above. If the number of hosts of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

6.1.11 Top VPN Hosts

Use this report to look at the top senders or receivers of VPN traffic.

Click **VPN > Site-to-Site > Top Hosts** to open this screen.

Figure 72 VPN > Site-to-Site > Top Hosts



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33		8	47.1%	2.104	27.9%	
192.168.1.48		1	5.9%	0.603	8%	
192.168.1.35		1	5.9%	0.603	8%	
192.168.1.41		1	5.9%	0.603	8%	
192.168.1.39		1	5.9%	0.603	8%	
192.168.1.42		1	5.9%	0.603	8%	
192.168.1.36		1	5.9%	0.603	8%	
192.168.1.47		1	5.9%	0.603	8%	
192.168.1.44		1	5.9%	0.603	8%	
192.168.1.38		1	5.9%	0.603	8%	
Total		17	100%	7.529	100%	

Each field is described in the following table.

Table 66 VPN > Site-to-Site > 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.
Site	Select a peer IPSec router. Select **All** to display the device's VPN tunnels with the most traffic, regardless of which peer IPSec router they use. This field is not available with all models.
Tunnel	Select a VPN tunnel. Select **All** to display the total traffic for the device's VPN tunnels with the selected site (or all sites). This field is not available with all models.
Direction	Select for which direction of traffic, you want to view bandwidth usage. This field is not available with all models. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.
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 66 VPN > Site-to-Site > Top Hosts

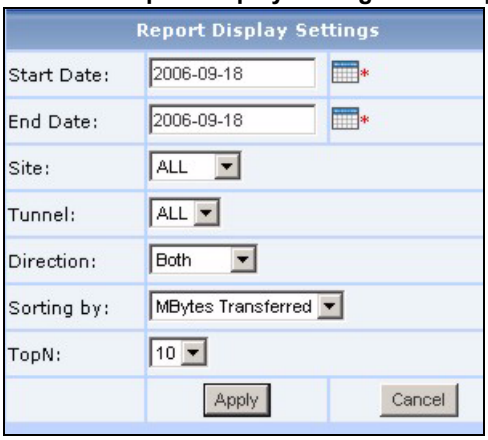
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of hosts is less than the maximum number of records displayed in this table, every host is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a host to look at the top destinations of VPN traffic for the selected host. The **Top VPN Hosts Drill-Down** report appears.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each host.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each host.

Table 66 VPN > Site-to-Site > Top Hosts

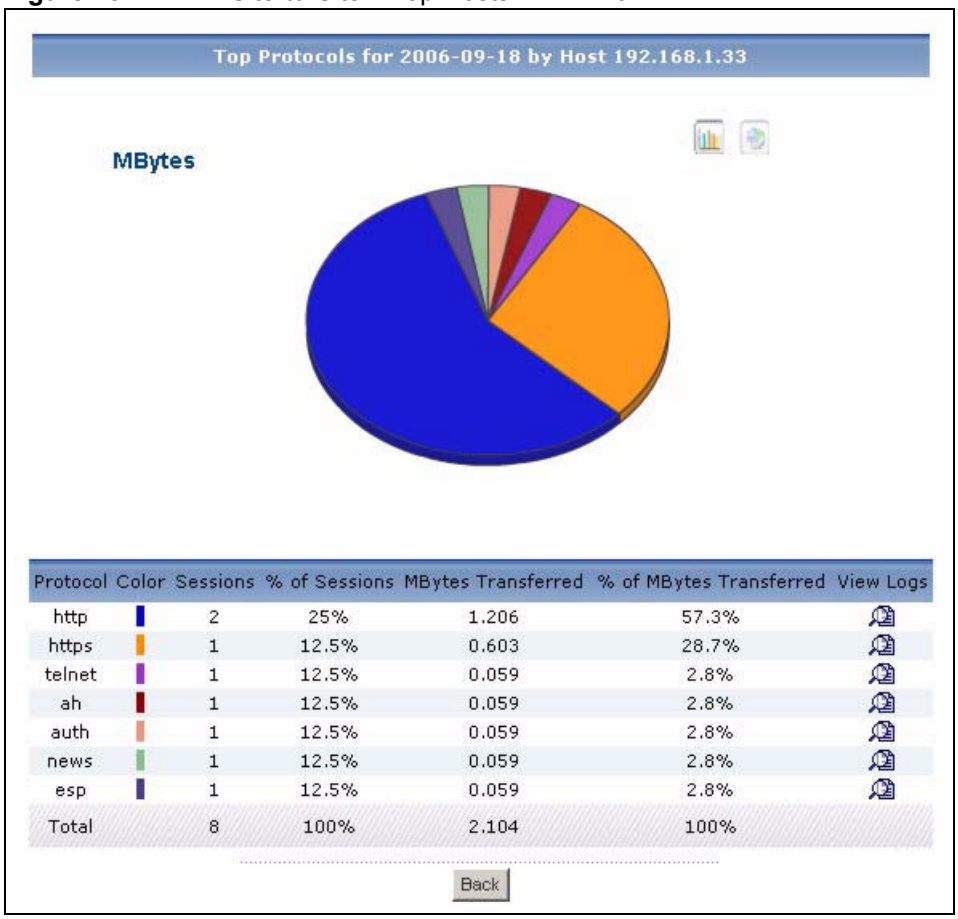
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above.

6.1.12 Top VPN Hosts Drill-Down

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

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

Figure 73 VPN > Site-to-Site > Top Hosts > Drill-Down



Each field is described in the following table.

Table 67 VPN > Site-to-Site > 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 67 VPN > Site-to-Site > Top Hosts > Drill-Down

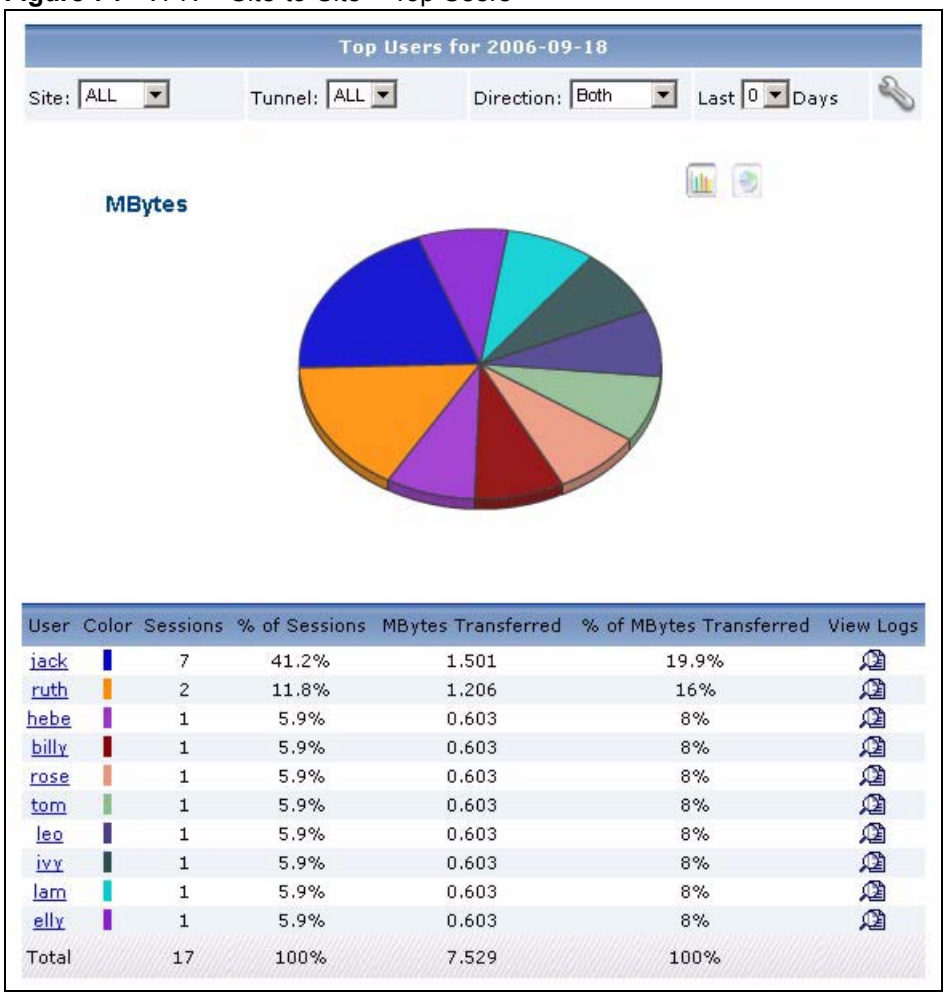
LABEL	DESCRIPTION
Protocol	This field displays the top services of VPN traffic from the selected host, sorted by the amount of traffic attributed to each one. Each service is identified by its IP address.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events of each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected VPN traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the VPN tunnels for each protocol.
% of MBytes Transferred	This field displays what percentage of the selected VPN traffic belonged to each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the protocols above. If the number of protocols of the selected VPN traffic 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.

6.1.13 Top VPN Users

Use this report to look at the users that send or receive the most VPN traffic.

Click **VPN > Site-to-Site > Top Users** to open this screen.

Figure 74 VPN > Site-to-Site > Top Users



User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
jack		7	41.2%	1.501	19.9%	
ruth		2	11.8%	1.206	16%	
hebe		1	5.9%	0.603	8%	
billy		1	5.9%	0.603	8%	
rose		1	5.9%	0.603	8%	
tom		1	5.9%	0.603	8%	
leo		1	5.9%	0.603	8%	
ivy		1	5.9%	0.603	8%	
lam		1	5.9%	0.603	8%	
elly		1	5.9%	0.603	8%	
Total		17	100%	7.529	100%	

Each field is described in the following table.

Table 68 VPN > Site-to-Site > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Site	Select a peer IPSec router. Select **All** to display the device's VPN tunnels with the most traffic, regardless of which peer IPSec router they use.
Tunnel	Select a VPN tunnel. Select **All** to display the total traffic for the device's VPN tunnels with the selected site (or all sites).
Direction	Select for which direction of traffic, you want to view bandwidth usage. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.

Table 68 VPN > Site-to-Site > Top Users

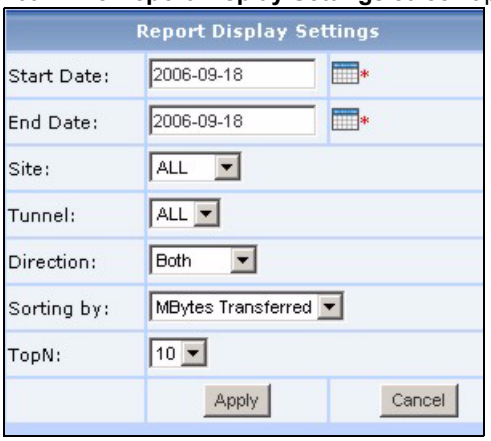
LABEL	DESCRIPTION
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top senders or receivers of VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user to look at the top destinations of VPN traffic for the selected user. The **Top VPN Users Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.

Table 68 VPN > Site-to-Site > Top Users

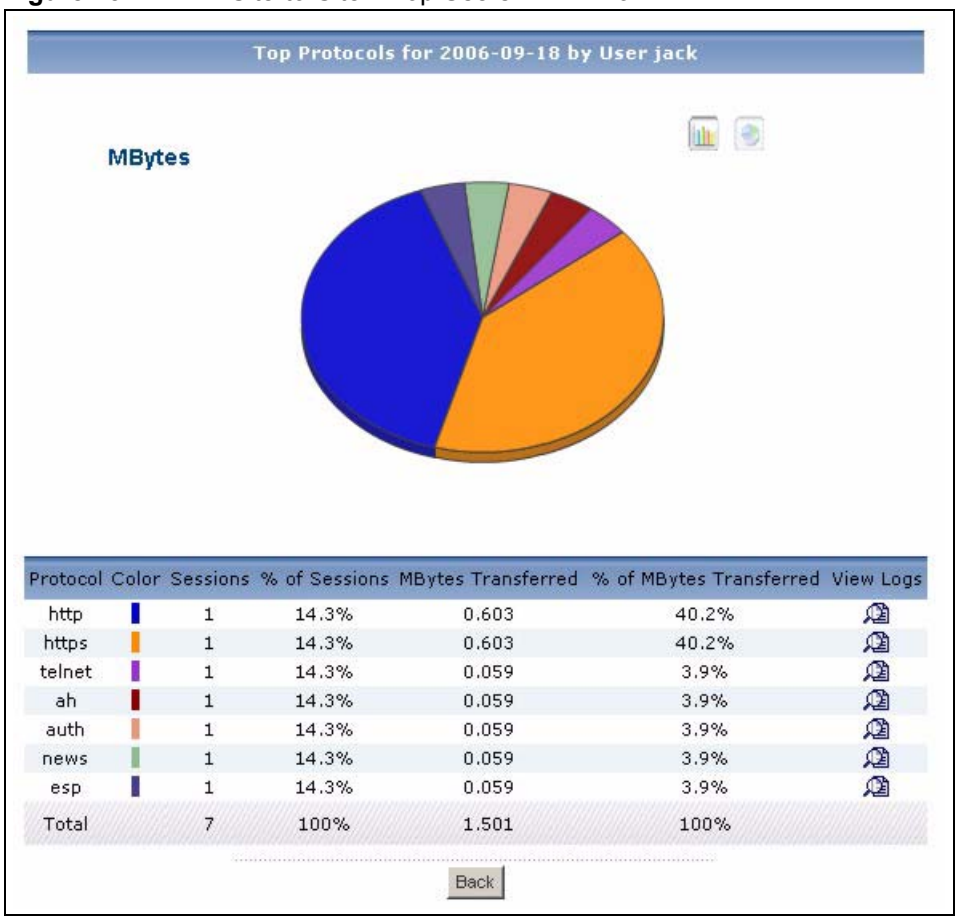
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for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

6.1.14 Top VPN Users Drill-Down

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

Click on a specific source in **VPN > Site-to-Site > Top Users** to open this screen.

Figure 75 VPN > Site-to-Site > Top Users > Drill-Down



Each field is described in the following table.

Table 69 VPN > Site-to-Site > Top Users > Drill-Down

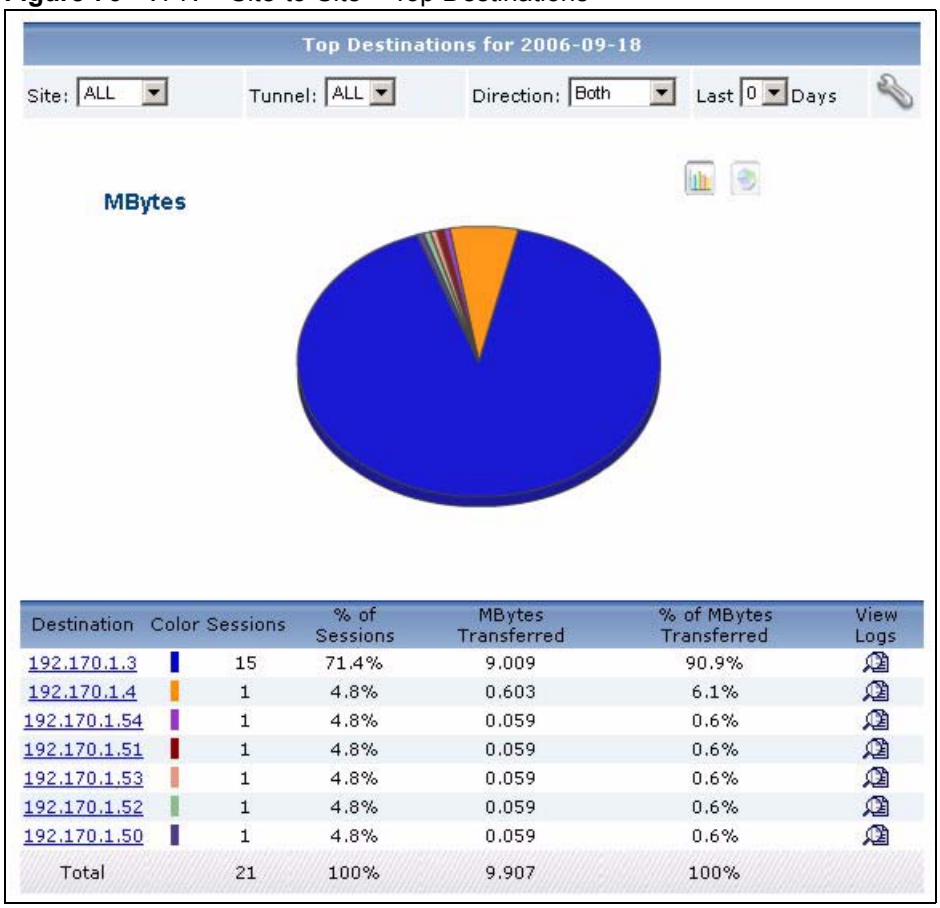
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services of VPN traffic from the selected user, sorted by the amount of traffic attributed to each one. Each service is identified by its IP address.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events of each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected VPN traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the VPN tunnels for each protocol.
% of MBytes Transferred	This field displays what percentage of the selected VPN traffic belonged to each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the protocols above. If the number of protocols of the selected VPN traffic 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.

6.1.15 Top VPN Destinations

Use this report to look at the destinations with the most VPN traffic.

Click **VPN > Site-to-Site > Top Destinations** to open this screen.

Figure 76 VPN > Site-to-Site > Top Destinations



Each field is described in the following table.

Table 70 VPN > Site-to-Site > 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.
Site	Select a peer IPSec router. Select **All** to display the device's VPN tunnels with the most traffic, regardless of which peer IPSec router they use.
Tunnel	Select a VPN tunnel. Select **All** to display the total traffic for the device's VPN tunnels with the selected site (or all sites).
Direction	Select for which direction of traffic, you want to view bandwidth usage. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.

Table 70 VPN > Site-to-Site > Top Destinations

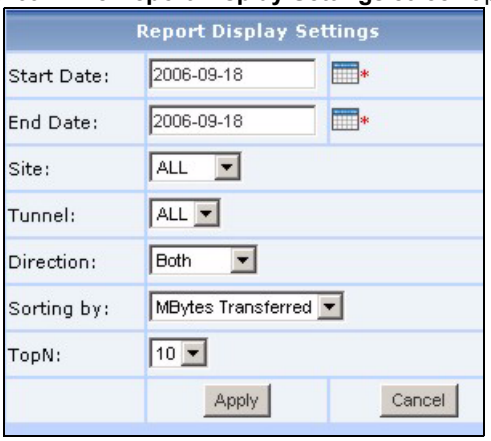
LABEL	DESCRIPTION
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. This field returns to zero, so you can 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the IP addresses to which the selected device sent the most VPN traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the top destinations of VPN traffic for the selected destination. The **Top VPN Destinations Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.

Table 70 VPN > Site-to-Site > Top Destinations

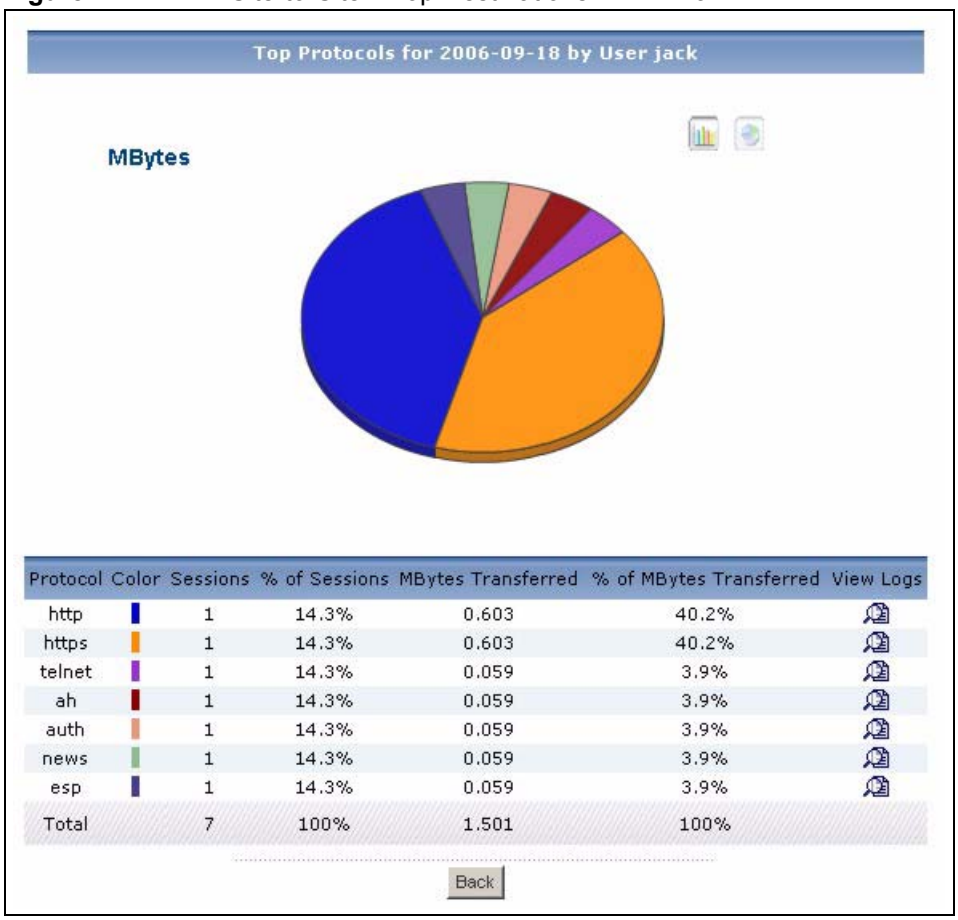
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled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

6.1.16 Top VPN Destinations Drill-Down

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

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

Figure 77 VPN > Site-to-Site > Top Destinations > Drill-Down



Each field is described in the following table.

Table 71 VPN > Site-to-Site > 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services of VPN traffic from the selected destination, sorted by the amount of traffic attributed to each one. Each service is identified by its IP address.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events of each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected VPN traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the VPN tunnels for each protocol.
% of MBytes Transferred	This field displays what percentage of the selected VPN traffic belonged to each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the protocols above. If the number of protocols of the selected VPN traffic 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 VPN Remote Access

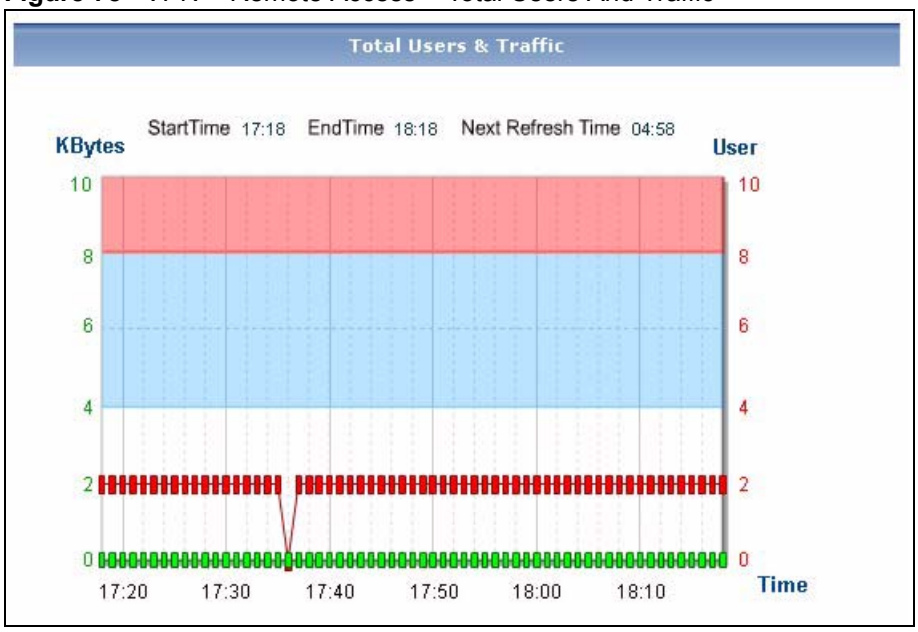
VPN tunnels with the remote gateway set as any are called dynamic tunnels (only the remote device can initiate a dynamic VPN tunnel). Devices can use xauth to authenticate remote users (by username and password) when they try to initiate a dynamic VPN tunnel. The VPN remote access screens display statistics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

6.2.1 VPN Total Users and Traffic

Use this report to monitor the total number of remote access users connected to the device and the amount of traffic the device handled for the dynamic VPN tunnels.

Click **VPN > Remote Access > Total Users And Traffic** to open this screen.

Figure 78 VPN > Remote Access > Total Users And Traffic



Each field is described in the following table.

Table 72 VPN > Remote Access > Total Users And Traffic

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 amount of traffic or number of users handled by the device each minute. Green represents the amount of traffic and red represents the number of users. If you allow dynamic VPN tunnels without using xauth, you can see the amount of traffic, but the users are not counted. X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the **Start Time** and **End Time**.

6.2.2 VPN User Status

Use this report to see which of the device's remote access users are connected.

Click **VPN > Remote Access > User Status** to open this screen.

Figure 79 VPN > Remote Access > User Status

Each field is described in the following table.

Table 73 VPN > Remote Access > User Status

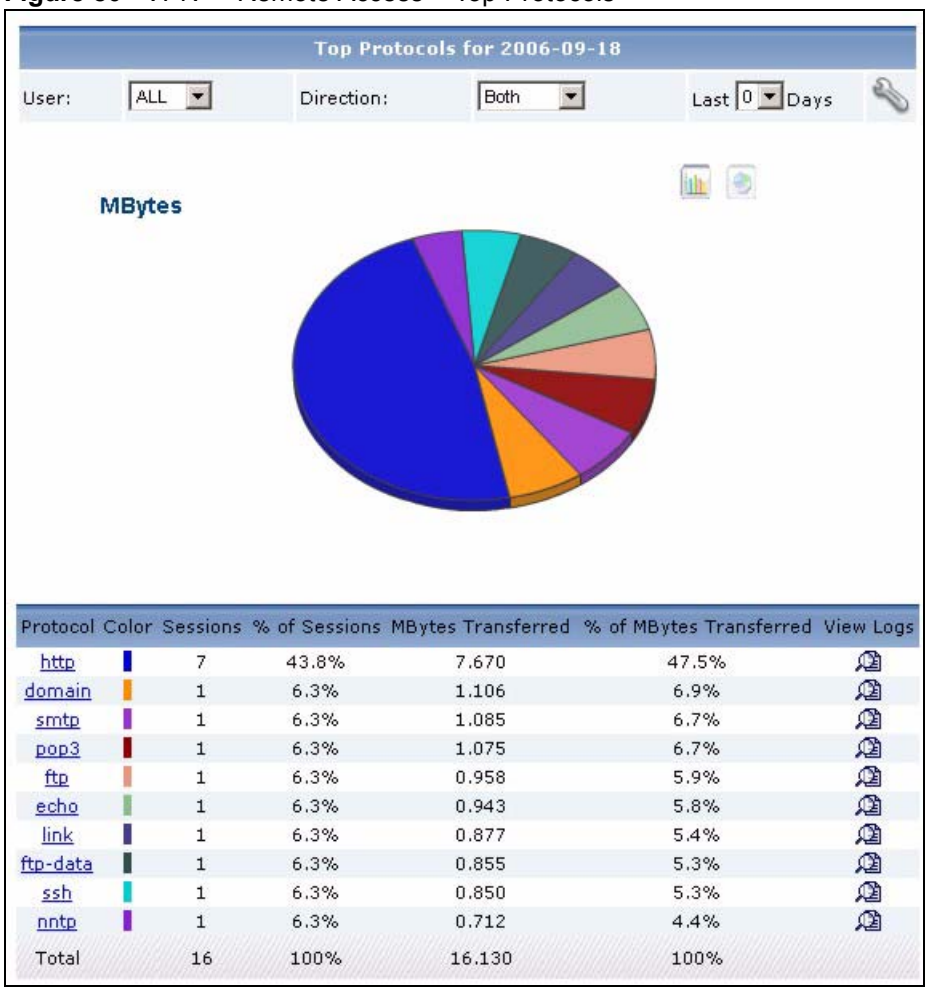
LABEL	DESCRIPTION
User Status	Select **Online** to display the list of users that are using a remote access connection to the device. Select **Offline** to display the list of users that are not currently using a remote access connection to the device. Select **All** to display the all of the configured remote access users for the device, regardless of whether or not they are connected.
User Name	This field displays the top remote access senders or receivers of VPN traffic in the selected device. Click the title of this column to sort the list of users in alphabetical or reverse-alphabetical order. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Time	This column displays when the remote access user last logged in. The current length (duration) of the login displays if the remote access user is still logged in. The log out time displays if the remote access user has already logged out. Click the title of this column to sort the list of users in chronological or reverse-chronological order.
Total	This entry displays the total number of sites on each page of the report.

6.2.3 Top VPN Protocols

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

Click **VPN > Remote Access > Top Protocols** to open this screen.

Figure 80 VPN > Remote Access > Top Protocols



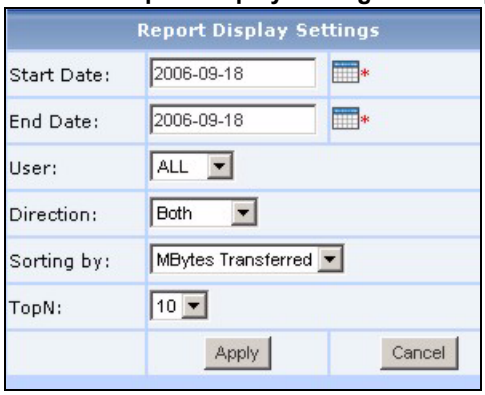
Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
http		7	43.8%	7.670	47.5%	
domain		1	6.3%	1.106	6.9%	
smtp		1	6.3%	1.085	6.7%	
pop3		1	6.3%	1.075	6.7%	
ftp		1	6.3%	0.958	5.9%	
echo		1	6.3%	0.943	5.8%	
link		1	6.3%	0.877	5.4%	
ftp-data		1	6.3%	0.855	5.3%	
ssh		1	6.3%	0.850	5.3%	
nntp		1	6.3%	0.712	4.4%	
Total		16	100%	16.130	100%	

Each field is described in the following table.

Table 74 VPN > Remote Access > Top Protocols

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.
User	Select a remote access user. Select **All** to display the protocols with the most traffic sent through the remote access VPN tunnels.
Direction	Select for which direction of traffic, you want to view statistics. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.
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 VPN > Remote Access > Top Protocols

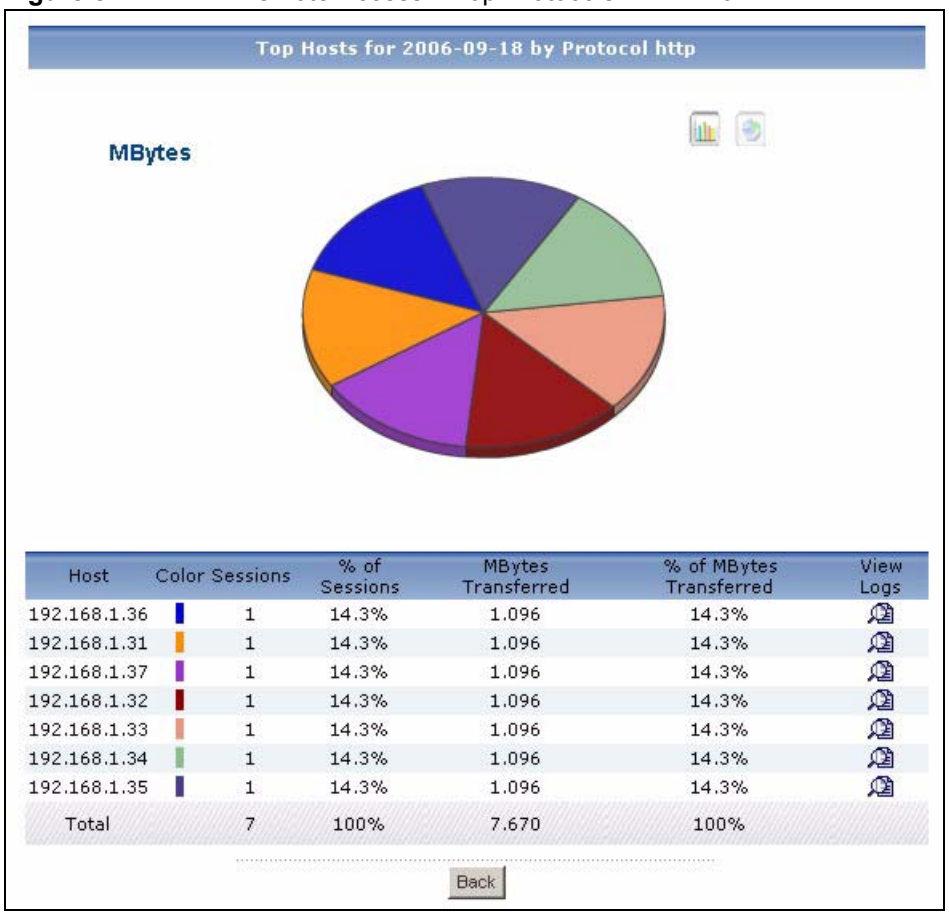
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most used by remote access VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through VPN. The **Top VPN Protocols Drill-Down** report appears.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

6.2.4 Top VPN Protocols Drill-Down

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

Click on a specific service in **VPN > Remote Access > Top Protocols** to open this screen.

Figure 81 VPN > Remote Access > Top Protocols > Drill-Down



Each field is described in the following table.

Table 75 VPN > Remote Access > Top Protocols > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of VPN traffic using the selected service, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.

Table 75 VPN > Remote Access > Top Protocols > Drill-Down

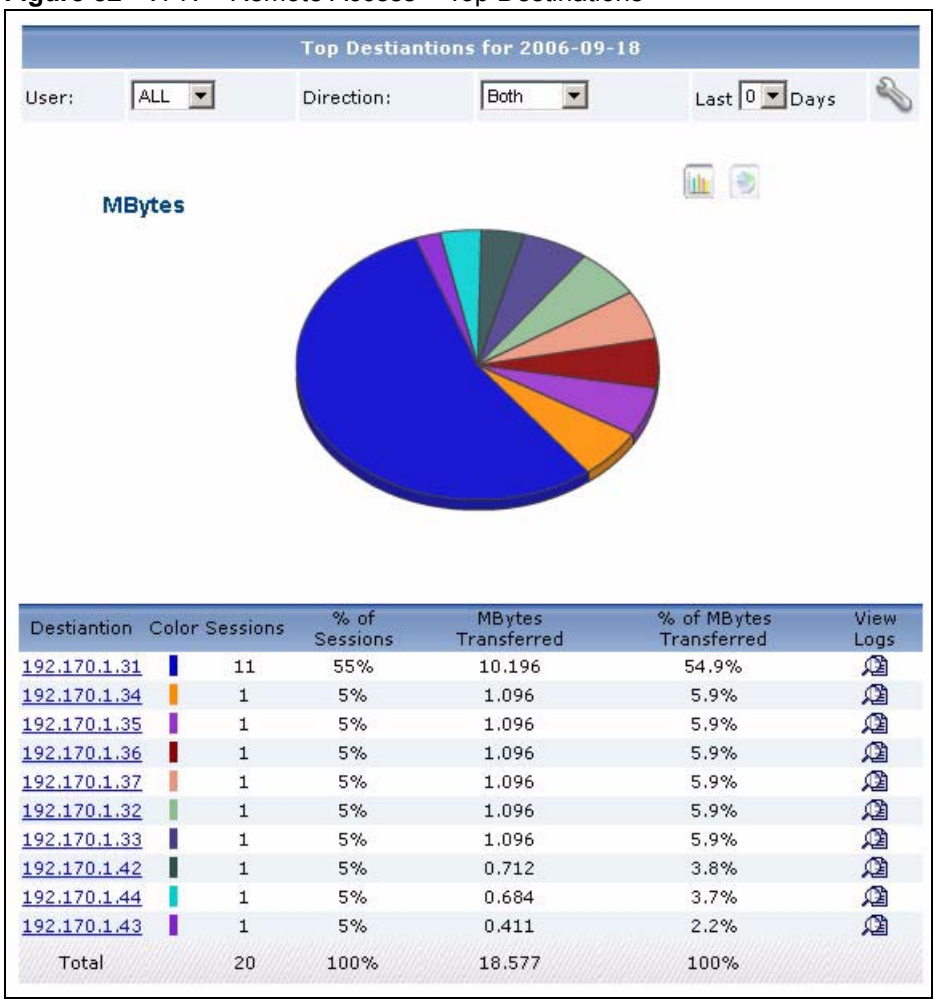
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected VPN traffic.
MBytes Transferred	This field displays how much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

6.2.5 Top VPN Destinations

Use this report to look at the destinations with the most remote access VPN traffic.

Click **VPN > Remote Access > Top Destinations** to open this screen.

Figure 82 VPN > Remote Access > Top Destinations



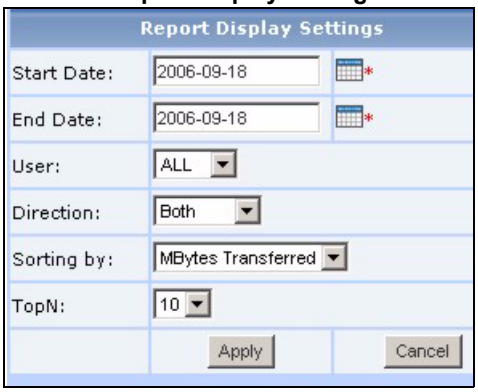
Destiantion	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.31		11	55%	10.196	54.9%	
192.170.1.34		1	5%	1.096	5.9%	
192.170.1.35		1	5%	1.096	5.9%	
192.170.1.36		1	5%	1.096	5.9%	
192.170.1.37		1	5%	1.096	5.9%	
192.170.1.32		1	5%	1.096	5.9%	
192.170.1.33		1	5%	1.096	5.9%	
192.170.1.42		1	5%	0.712	3.8%	
192.170.1.44		1	5%	0.684	3.7%	
192.170.1.43		1	5%	0.411	2.2%	
Total		20	100%	18.577	100%	

Each field is described in the following table.

Table 76 VPN > Remote Access > 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.
User	Select a remote access user. Select **All** to display the destinations with the most traffic sent through the remote access VPN tunnels.
Direction	Select for which direction of traffic, you want to view statistics. **Both** - all traffic sent or received through the VPN tunnels. **Incoming** - all traffic the device received through the VPN tunnels. **Outgoing** - all traffic sent through the VPN tunnels.
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 76 VPN > Remote Access > Top Destinations

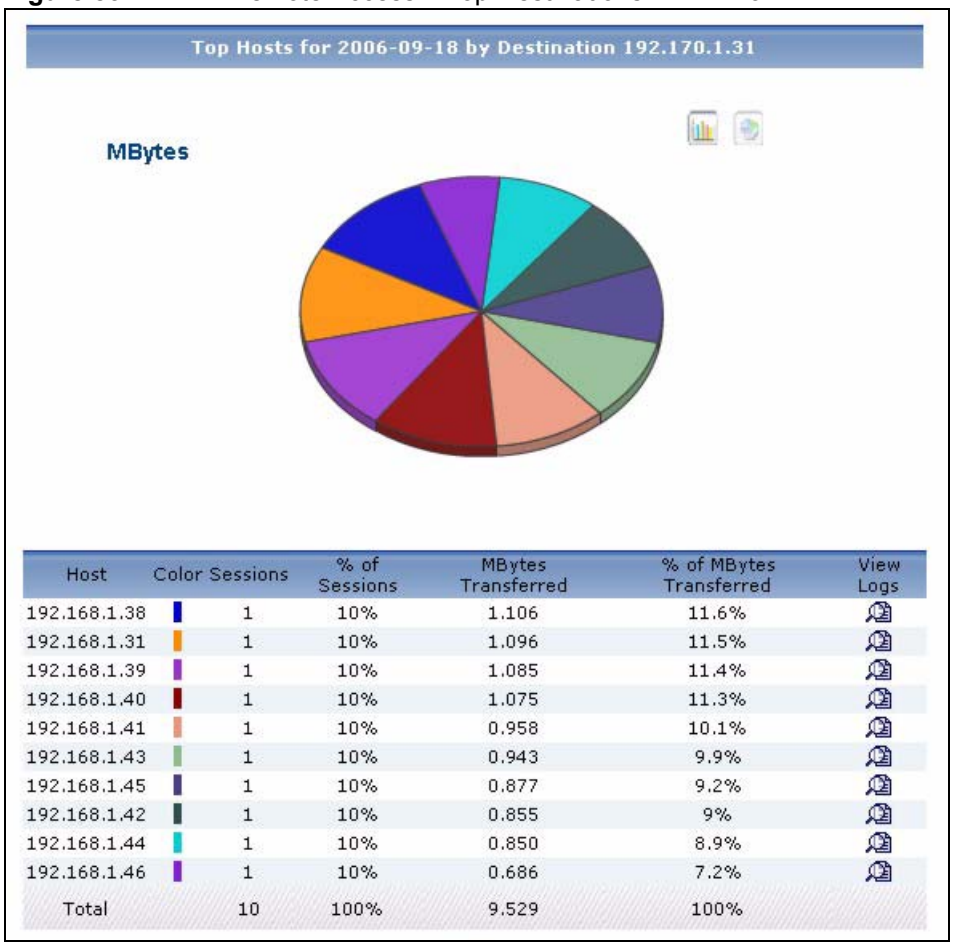
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the IP addresses to which the selected device sent the most remote access VPN traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the top destinations of VPN traffic for the selected destination. The **Top VPN Destinations Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of VPN traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.2.6 Top VPN Destinations Drill-Down

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

Click on a specific destination in **VPN > Remote Access > Top Destinations** to open this screen.

Figure 83 VPN > Remote Access > Top Destinations > Drill-Down



Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.38		1	10%	1.106	11.6%	
192.168.1.31		1	10%	1.096	11.5%	
192.168.1.39		1	10%	1.085	11.4%	
192.168.1.40		1	10%	1.075	11.3%	
192.168.1.41		1	10%	0.958	10.1%	
192.168.1.43		1	10%	0.943	9.9%	
192.168.1.45		1	10%	0.877	9.2%	
192.168.1.42		1	10%	0.855	9%	
192.168.1.44		1	10%	0.850	8.9%	
192.168.1.46		1	10%	0.686	7.2%	
Total		10	100%	9.529	100%	

Each field is described in the following table.

Table 77 VPN > Remote Access > 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 77 VPN > Remote Access > Top Destinations > Drill-Down

LABEL	DESCRIPTION
Host	This field displays the top sources that sent remote access VPN traffic to the selected destination, sorted by the amount of traffic attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events of each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for the selected VPN traffic.
MBytes Transferred	This field displays how much traffic (in megabytes) was handled through the VPN tunnels for each host.
% of MBytes Transferred	This field displays what percentage of the selected VPN traffic belonged to each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the hosts above. If the number of hosts of the selected remote access VPN traffic 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 Xauth

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

6.3.1 VPN Successful Login

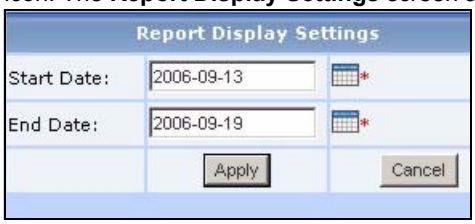
Use this report to monitor the total number of users that have successfully logged in to use one of the device's VPN tunnels.

Click **VPN > Xauth > Successful Login** to open this screen.

Figure 84 VPN > Xauth> Successful Login

Each field is described in the following table.

Table 78 VPN > Xauth> Successful Login

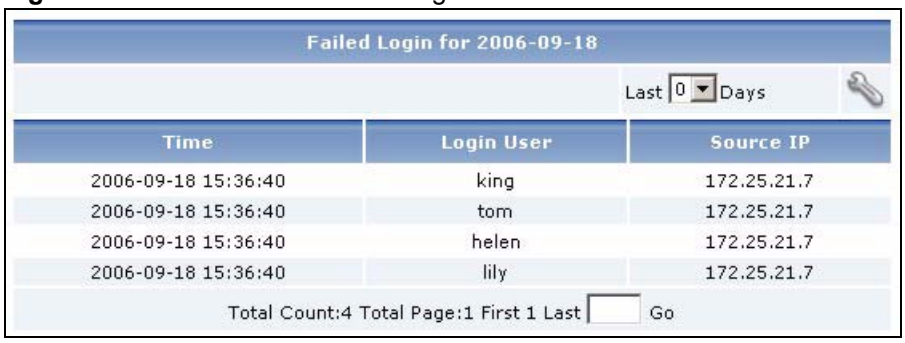
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
Time	This column displays when the user last logged in. The entries are sorted in chronological order.
Login User	This field displays the user name of a user that logged into one of the device's VPN tunnels. Each user is identified by user name.
Source IP	This is the IP address from which the user logged into one of the device's VPN tunnels.
Total	This entry displays the total number of users on the current page of the report. If you want to see a different page of the report, type the number of the page in the field.

6.3.2 VPN Failed Login

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

Click **VPN > Xauth> Failed Login** to open this screen.

Figure 85 VPN > Xauth> Failed Login



Each field is described in the following table.

Table 79 VPN > Xauth> Failed Login

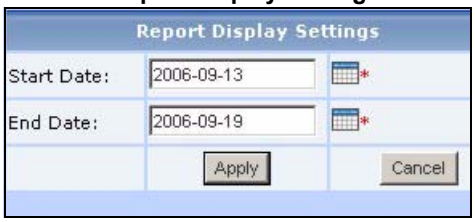
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
Time	This column displays when the user last failed to log in. The entries are sorted in chronological order.
Login User	This field displays the user name of a user that failed to log into one of the device's VPN tunnels. Each user is identified by user name.

Table 79 VPN > Xauth> Failed Login

LABEL	DESCRIPTION
Source IP	This is the IP address from which the user attempted to log into one of the device's VPN tunnels.
Total	This entry displays the total number of users on the current page of the report. If you want to see a different page of the report, type the number of the page in the field.

PART III
Network Attack and Security Policy

Network Attack (185)
Security Policy (243)

7

Network Attack

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

7.1 Attack

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

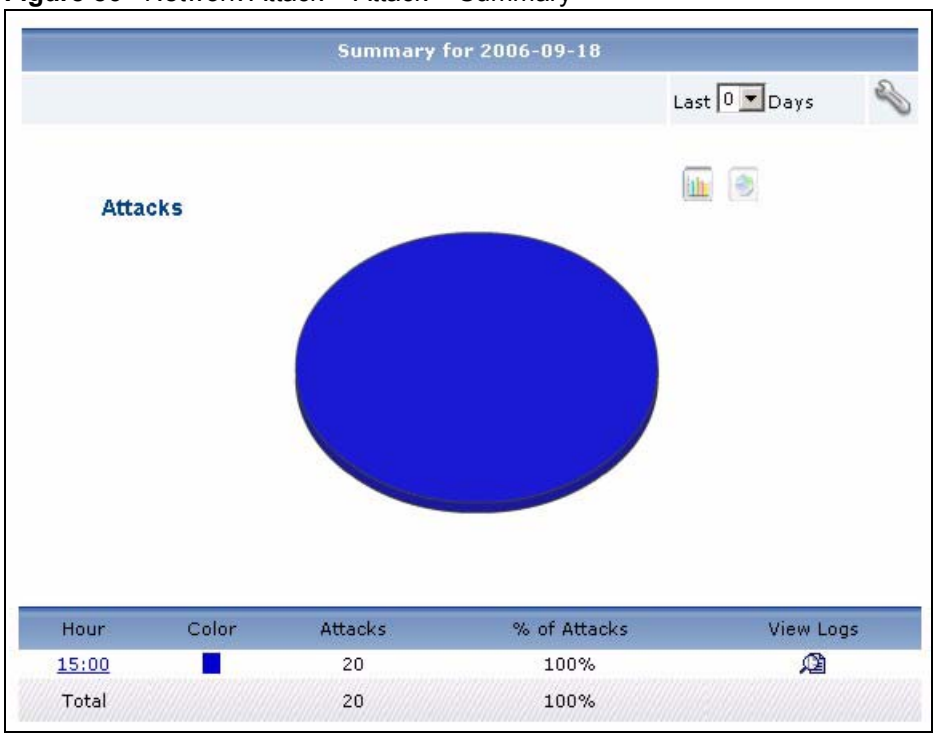
7.1.1 Attack Summary

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

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 86 Network Attack > Attack > Summary



Each field is described in the following table.

Table 80 Network Attack > Attack > Summary

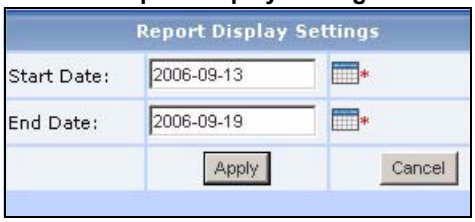
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.

Table 80 Network Attack > Attack > Summary

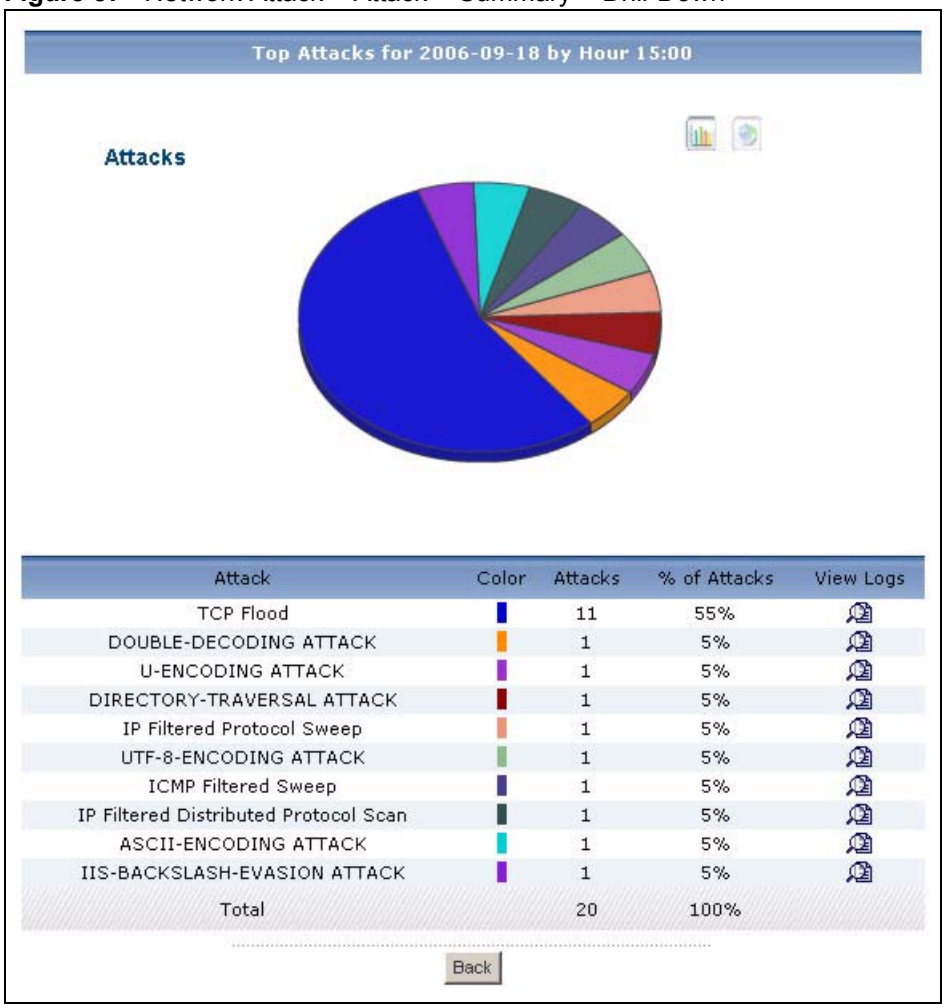
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top categories of attacks in the selected time interval. The **Attack Summary Drill-Down** report appears.
Color	This field displays what color represents each time interval in the graph.
Attacks	This field displays the number of DoS attacks in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.1.2 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 87 Network Attack > Attack > Summary > Drill-Down



Each field is described in the following table.

Table 81 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks in the selected time interval, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks by each category occurred in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks in the selected time interval comes from each category.
View Logs	Click this icon to see the logs that go with the record.

Table 81 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.

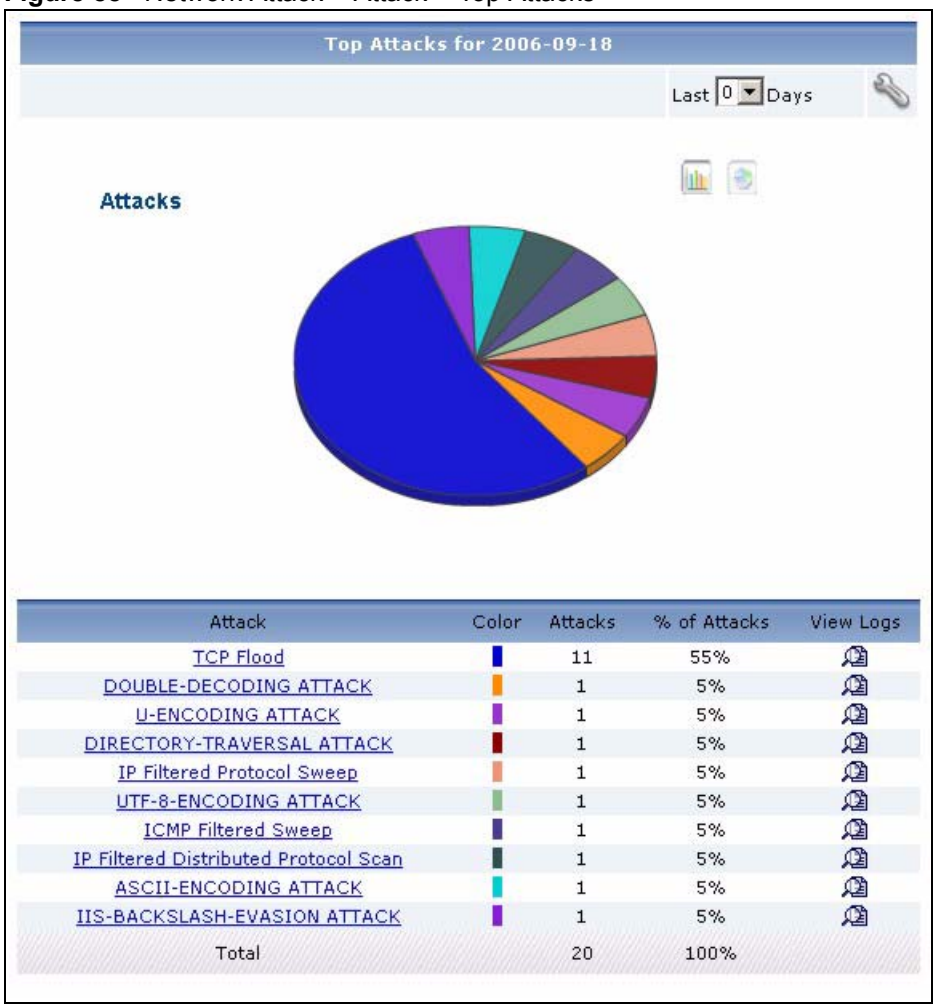
7.1.3 Top Attacks

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

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 Attacks** to open this screen.

Figure 88 Network Attack > Attack > Top Attacks

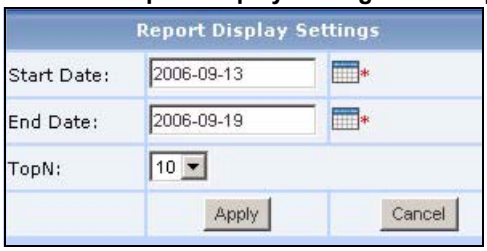


Each field is described in the following table.

Table 82 Network Attack > Attack > Top Attacks

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 Network Attack > Attack > Top Attacks

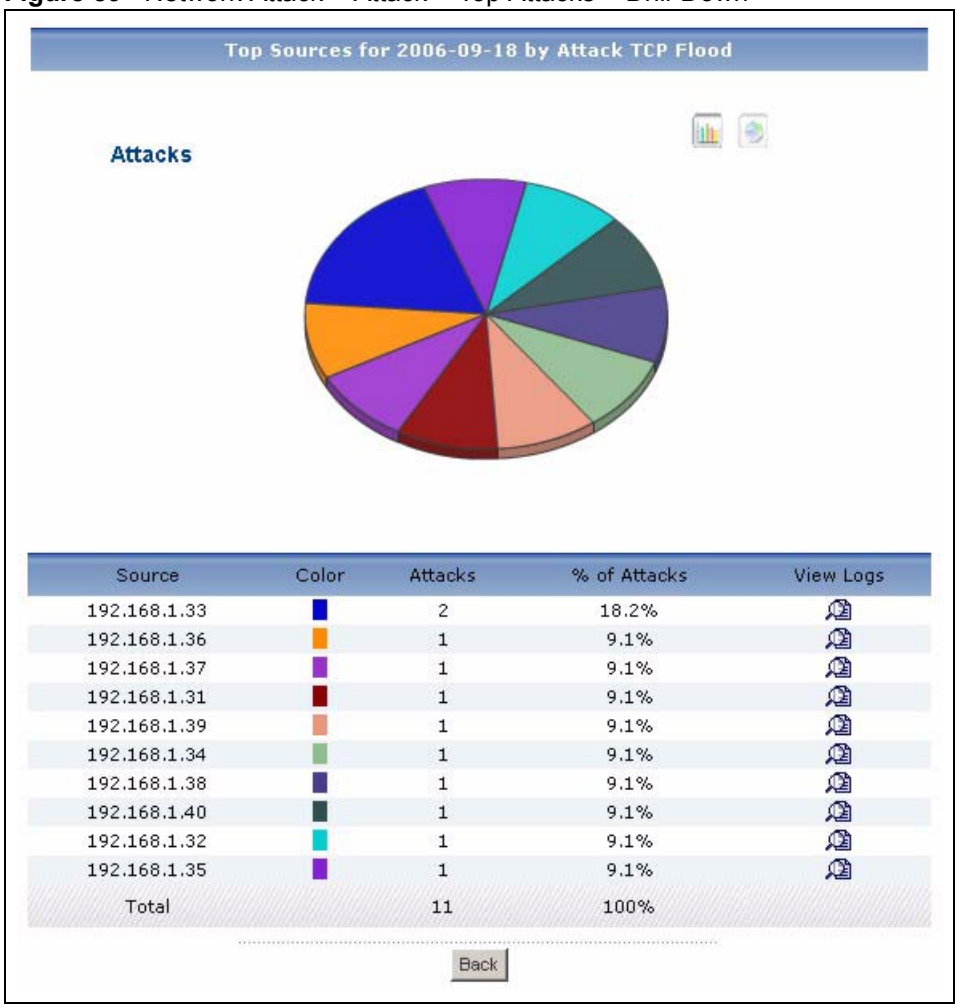
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks in the selected time interval, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks from each category occurred in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks in the selected time interval comes from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above. If the number of categories in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.

7.1.4 Top Attacks Drill-Down

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

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

Figure 89 Network Attack > Attack > Top Attacks > Drill-Down



Each field is described in the following table.

Table 83 Network Attack > Attack > Top Attacks > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected category of DoS attacks.
Color	This field displays what color represents each source in the graph.
Attacks	This field displays the number of DoS attacks in the selected category that came from each source.
% of Attacks	This field displays what percentage of all DoS attacks in the selected category came from each source.
View Logs	Click this icon to see the logs that go with the record.

Table 83 Network Attack > Attack > Top Attacks > Drill-Down

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

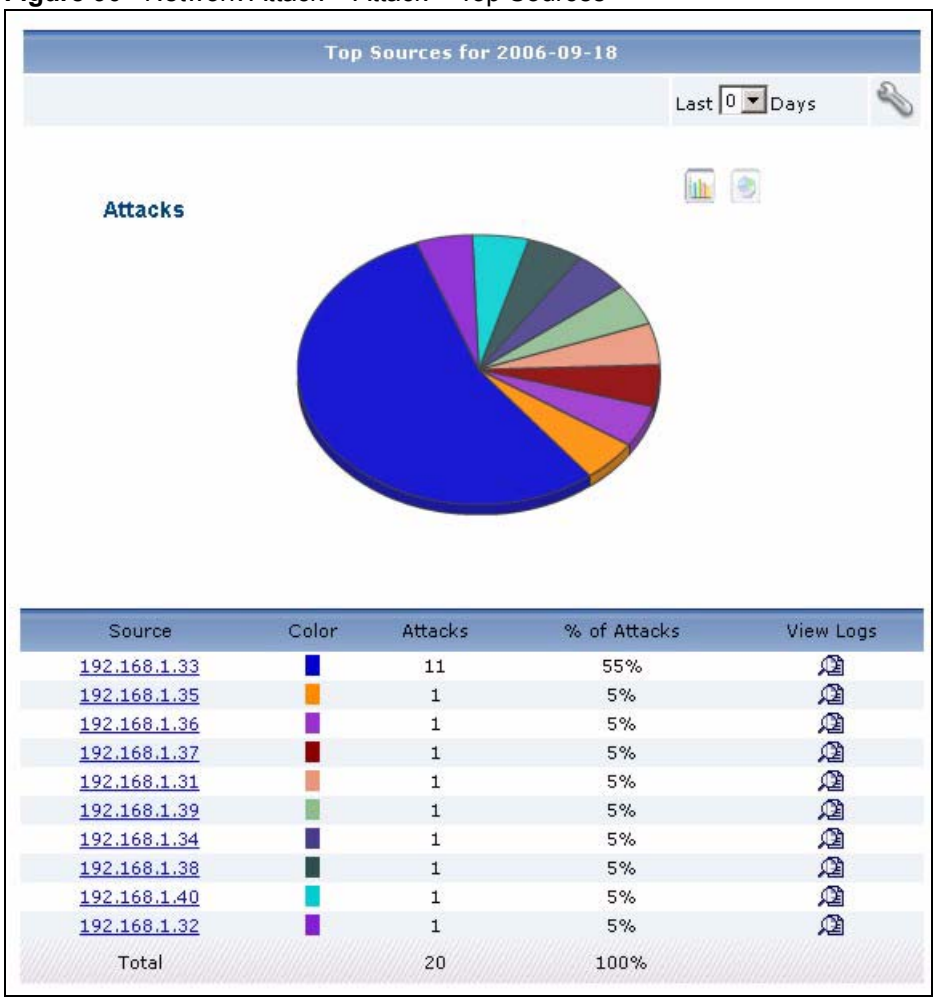
7.1.5 Top Attack Sources

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

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 90 Network Attack > Attack > Top Sources



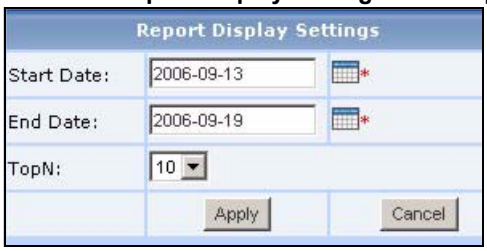
Source	Color	Attacks	% of Attacks	View Logs
192.168.1.33		11	55%	
192.168.1.35		1	5%	
192.168.1.36		1	5%	
192.168.1.37		1	5%	
192.168.1.31		1	5%	
192.168.1.39		1	5%	
192.168.1.34		1	5%	
192.168.1.38		1	5%	
192.168.1.40		1	5%	
192.168.1.32		1	5%	
Total		20	100%	

Each field is described in the following table.

Table 84 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	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 84 Network Attack > Attack > Top Sources

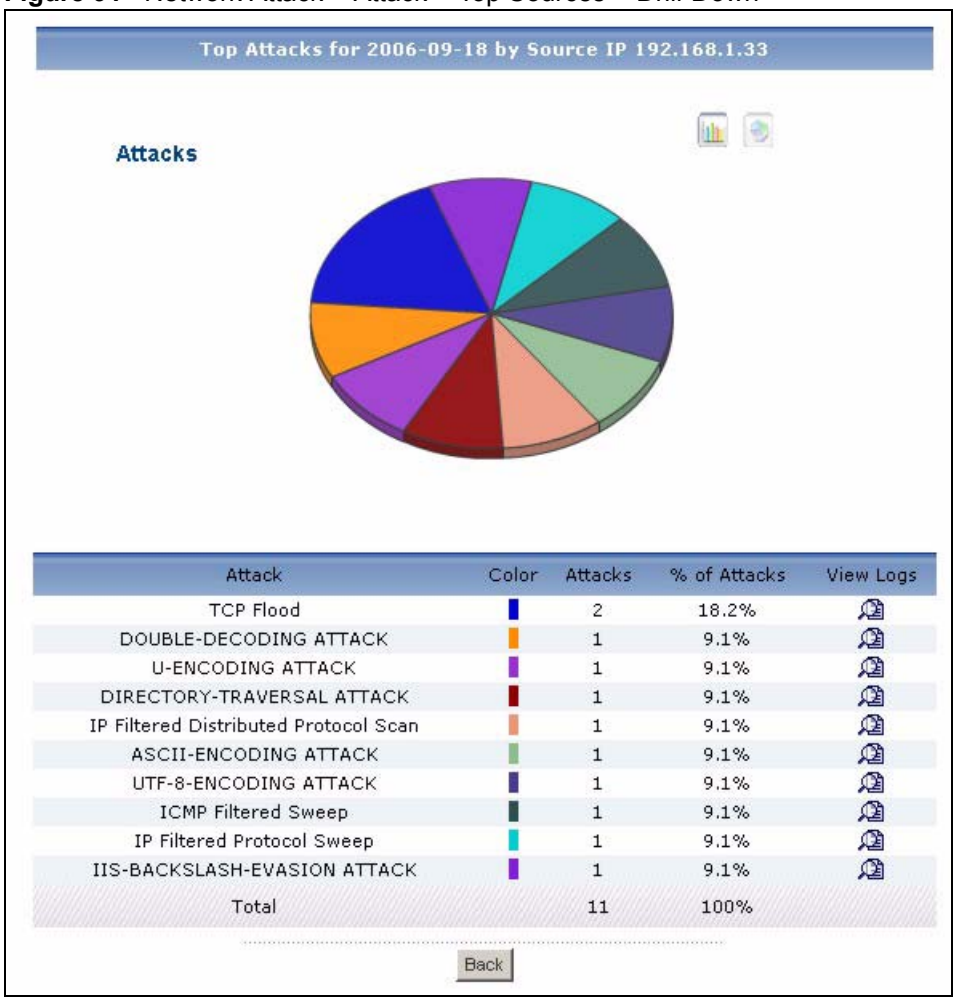
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of DoS attacks in the selected device, sorted by the number of attacks by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a source to look at the top categories of DoS attacks by the selected source. The **Top Attack Sources Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Attacks	This field displays the number of DoS attacks by each source.
% of Attacks	This field displays what percentage of all DoS attacks was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.1.6 Top Attack Sources Drill-Down

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

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

Figure 91 Network Attack > Attack > Top Sources > Drill-Down



Each field is described in the following table.

Table 85 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks from the selected source, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays the number of DoS attacks from each category that occurred from the selected source.
% of Attacks	This field displays what percentage of all DoS attacks from the selected source comes from each category.
View Logs	Click this icon to see the logs that go with the record.

Table 85 Network Attack > Attack > Top Sources > Drill-Down

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

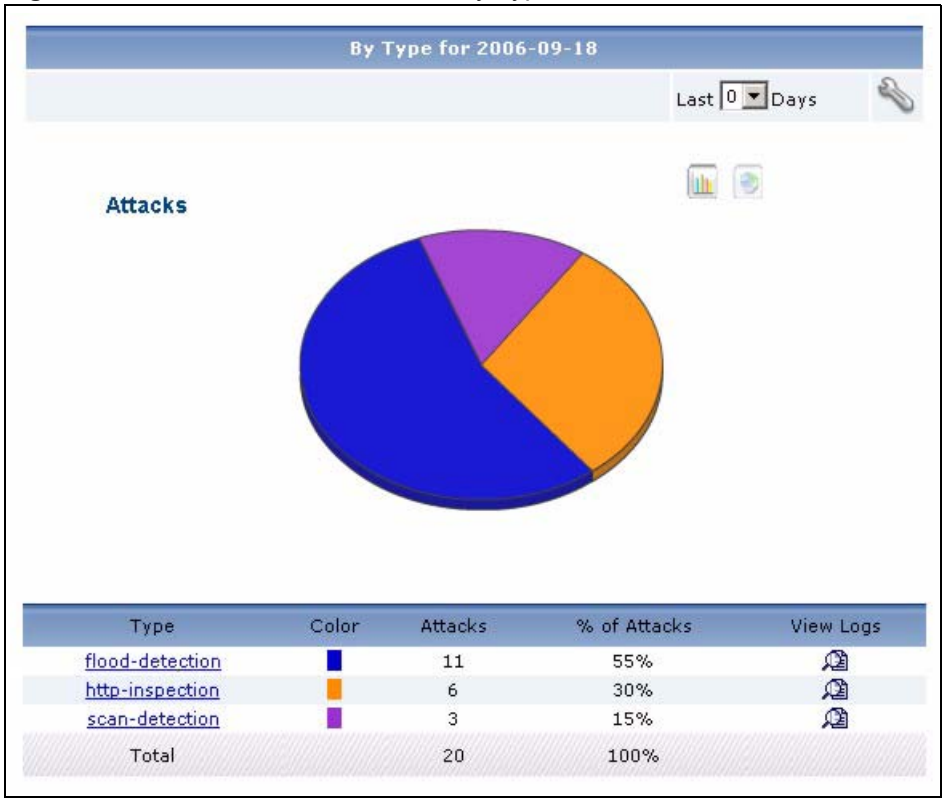
7.1.7 Attack Types

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

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.

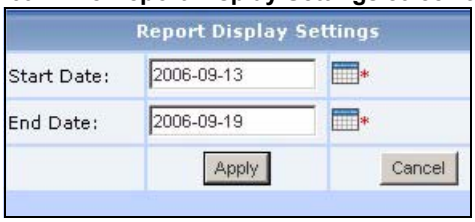
Click **Network Attack > Attack > By Type** to open this screen.

Figure 92 Network Attack > Attack > By Type



Each field is described in the following table.

Table 86 Network Attack > Attack > By Type

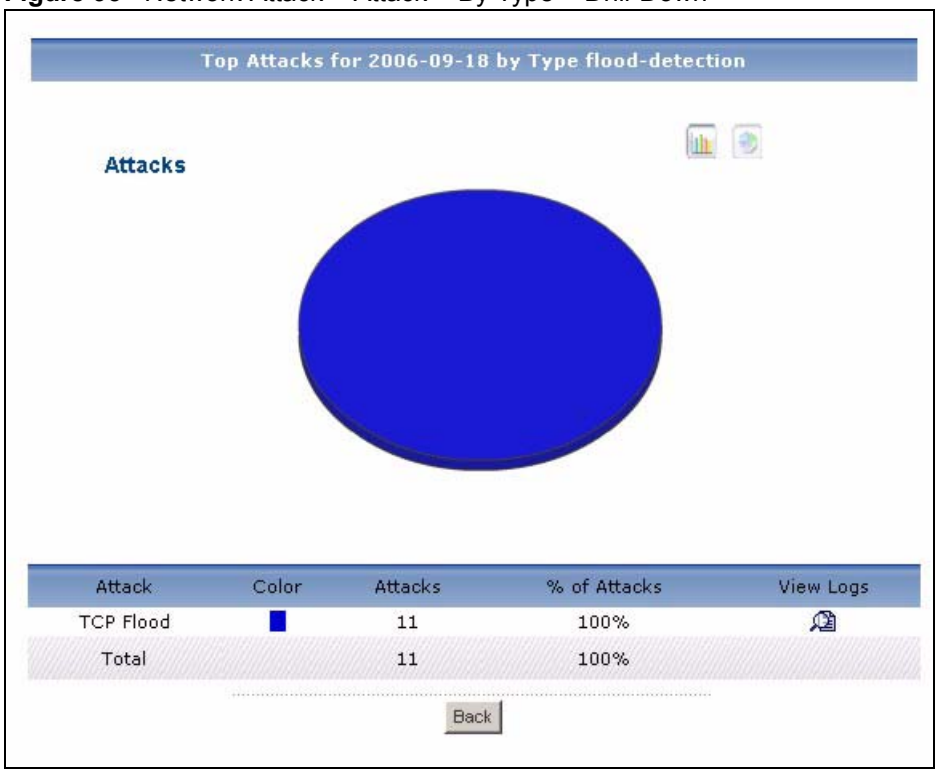
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Type	This field displays the categories of DoS attacks in the selected device, sorted by the number of attacks by each one. Click on a category to look at the DoS attacks in the selected category. The **Top Attack Types Drill-Down** report appears.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks from each category the device stopped.
% of Attacks	This field displays what percentage of all DoS attacks come from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

7.1.8 Attack Types Drill-Down

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

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

Figure 93 Network Attack > Attack > By Type > Drill-Down



Each field is described in the following table.

Table 87 Network Attack > Attack > By Type > Drill-Down

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

7.2 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 the selected device's IDP feature.

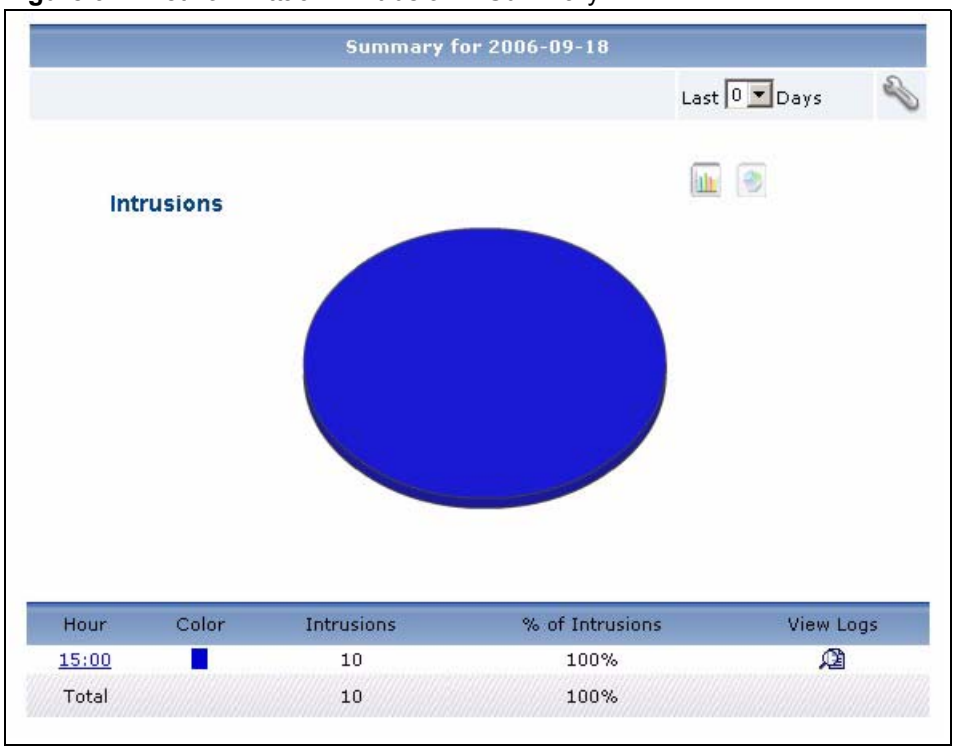
7.2.1 Intrusion Summary

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

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.

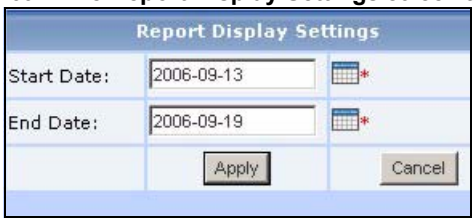
Click **Network Attack > Intrusion > Summary** to open this screen.

Figure 94 Network Attack > Intrusion > Summary



Each field is described in the following table.

Table 88 Network Attack > Intrusion > Summary

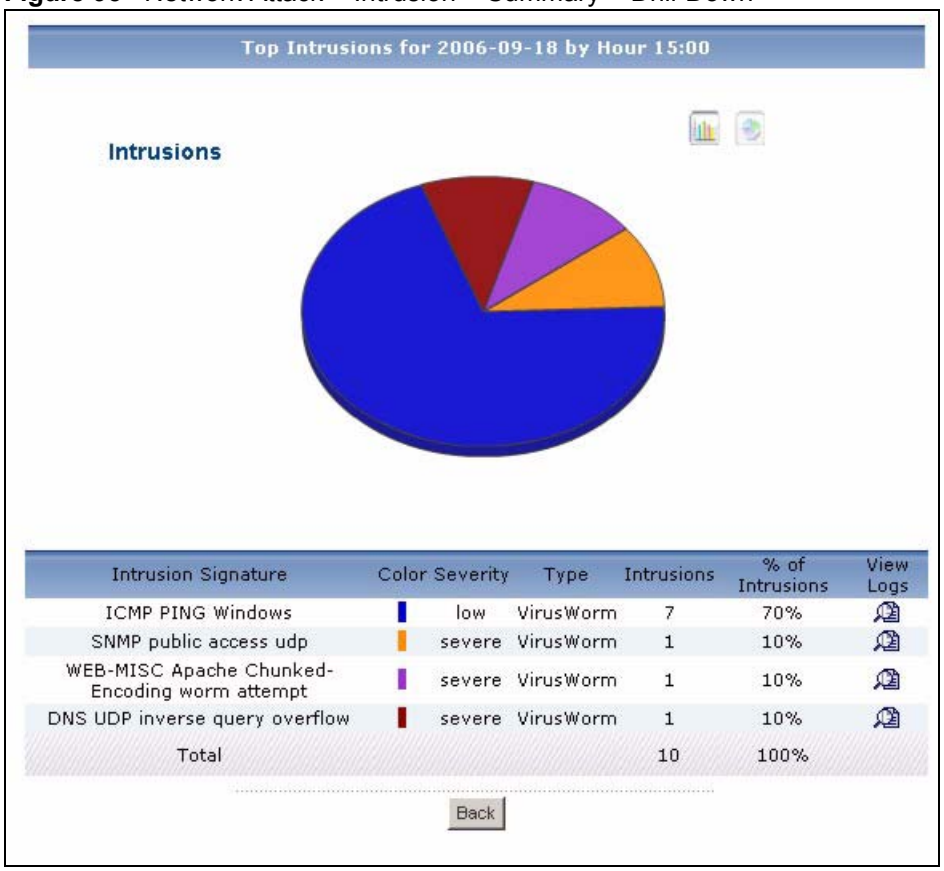
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days,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

7.2.2 Intrusion Summary Drill-Down

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

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

Figure 95 Network Attack > Intrusion > Summary > Drill-Down



Each field is described in the following table.

Table 89 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most ZyXEL devices.
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.

Table 89 Network Attack > Intrusion > Summary > Drill-Down

LABEL	DESCRIPTION
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

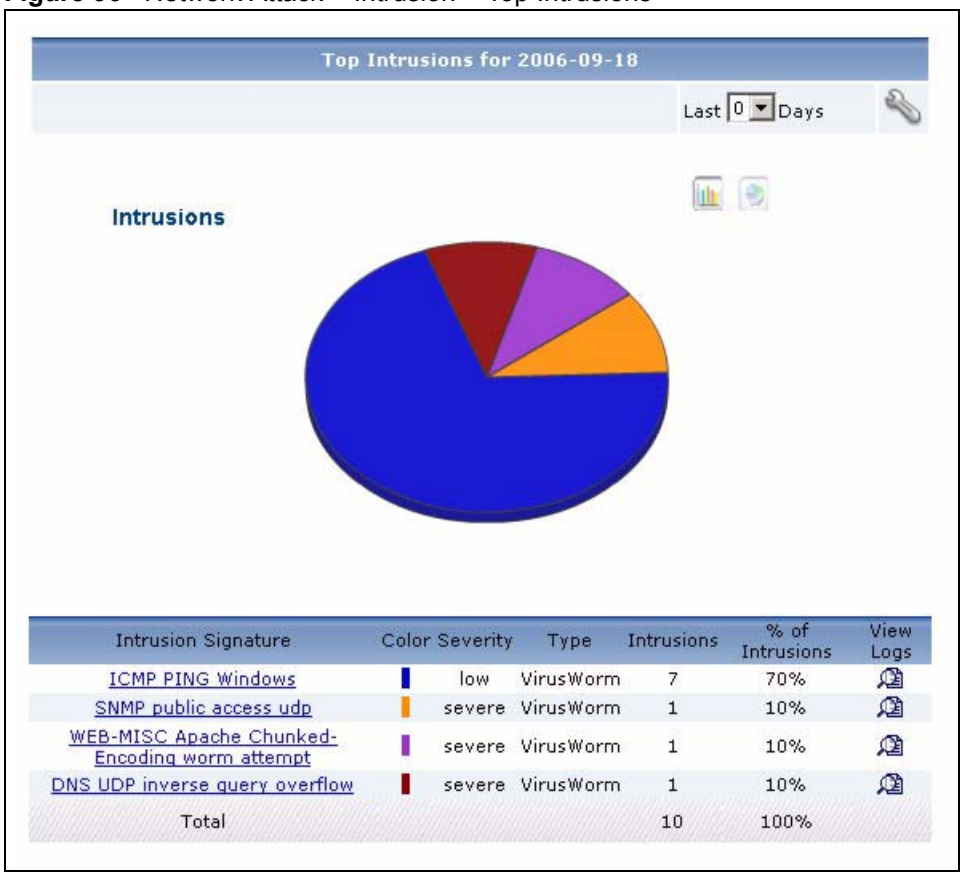
7.2.3 Top Intrusion Signatures

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

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.

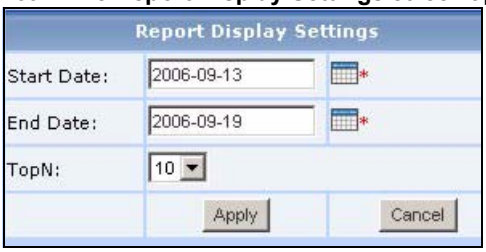
Figure 96 Network Attack > Intrusion > Top Intrusions



Intrusion Signature	Color Severity	Type	Intrusions	% of Intrusions	View Logs
ICMP PING Windows	low	VirusWorm	7	70%	
SNMP public access udp	severe	VirusWorm	1	10%	
WEB-MISC Apache Chunked-Encoding worm attempt	severe	VirusWorm	1	10%	
DNS UDP inverse query overflow	severe	VirusWorm	1	10%	
Total			10	100%	

Each field is described in the following table.

Table 90 Network Attack > Intrusion > Top Intrusions

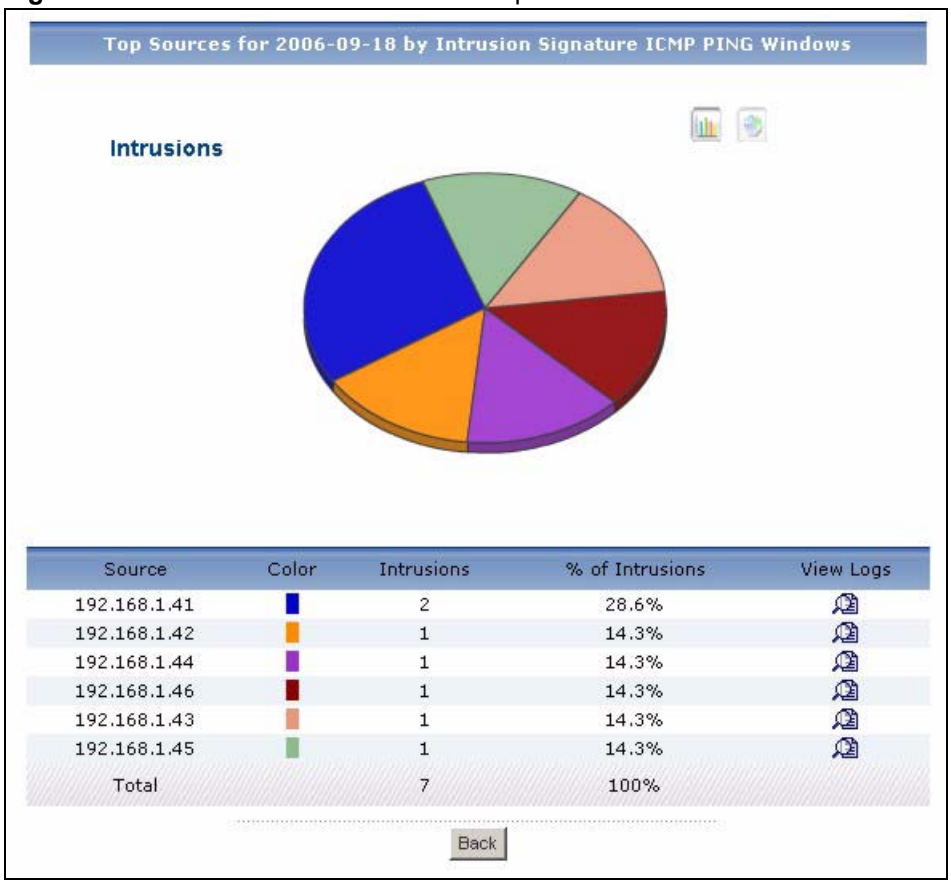
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature. The **Top Intrusion Signatures Drill-Down** report appears.
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.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

7.2.4 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 97 Network Attack > Intrusion > Top Intrusions > Drill-Down



Each field is described in the following table.

Table 91 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected intrusion signature, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).

Table 91 Network Attack > Intrusion > Top Intrusions > Drill-Down

LABEL	DESCRIPTION
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions using the selected intrusion signature was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of the selected intrusion signature is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

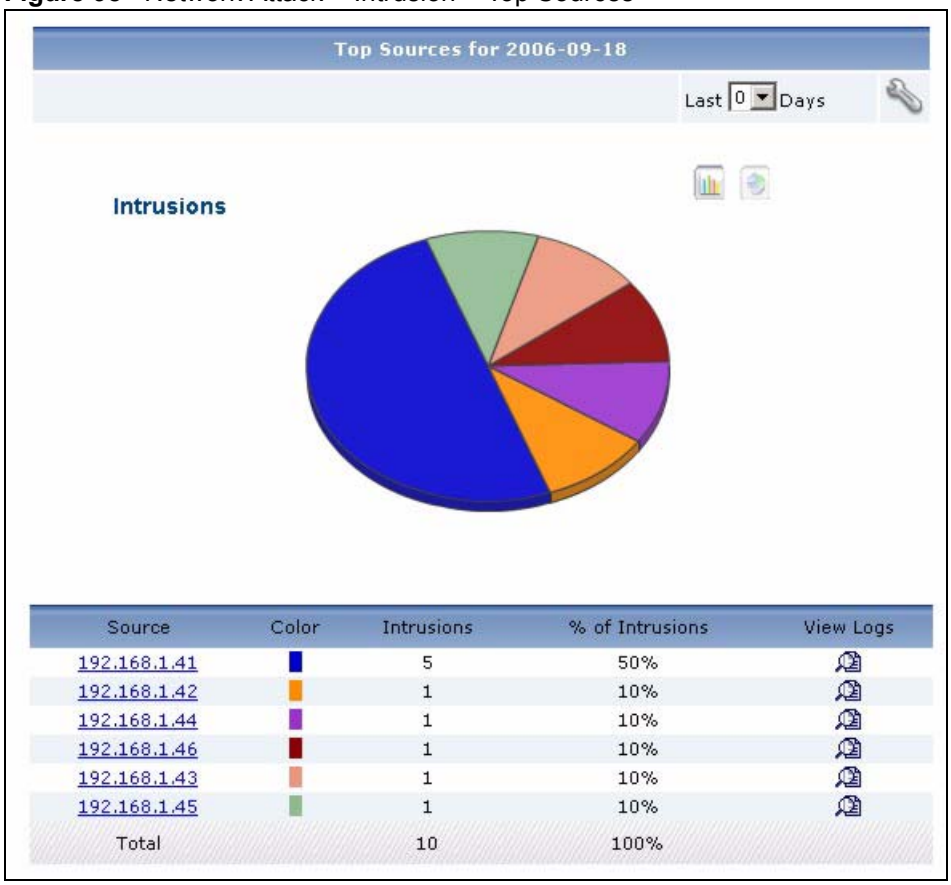
7.2.5 Top Intrusion Sources

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

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 98 Network Attack > Intrusion > Top Sources

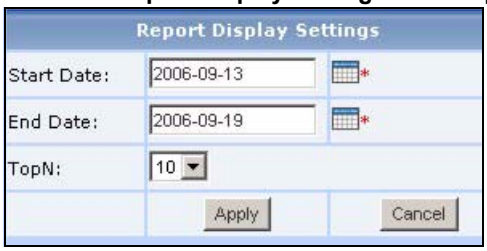


Each field is described in the following table.

Table 92 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 92 Network Attack > Intrusion > Top Sources

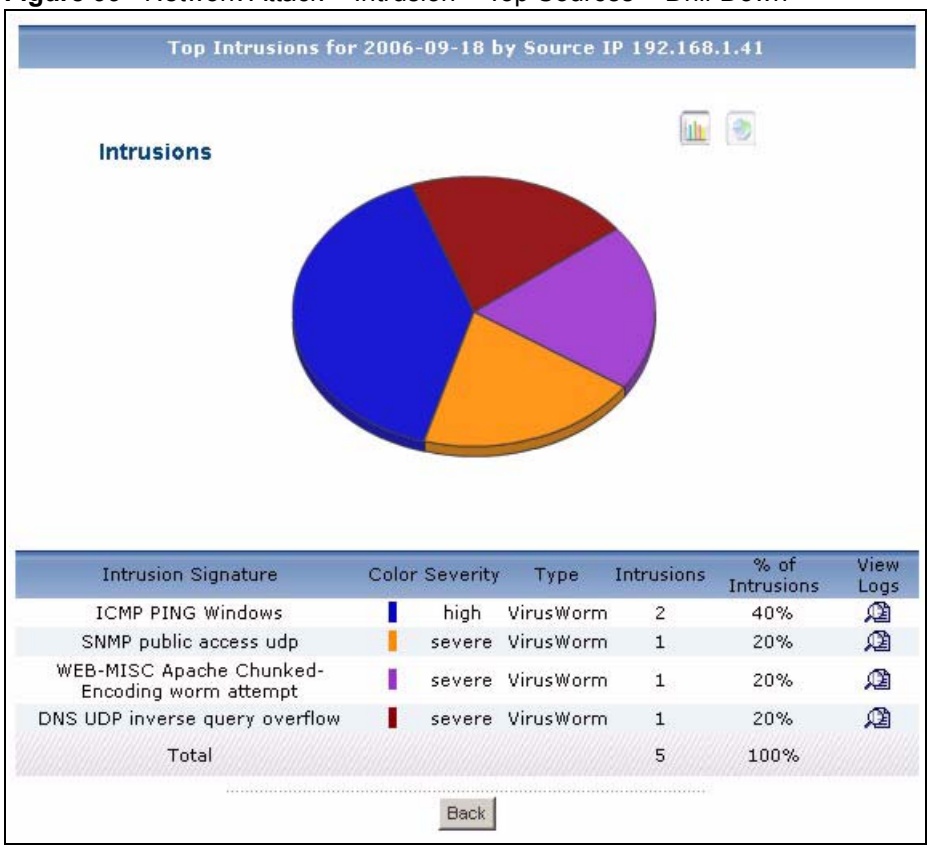
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a source to look at the top intrusion signatures for the selected source. The **Top Intrusion Sources Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.2.6 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 99 Network Attack > Intrusion > Top Sources > Drill-Down



Each field is described in the following table.

Table 93 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures from the selected source, sorted by the number of intrusions by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by the selected source using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions by the selected source was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.

Table 93 Network Attack > Intrusion > Top Sources > Drill-Down

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

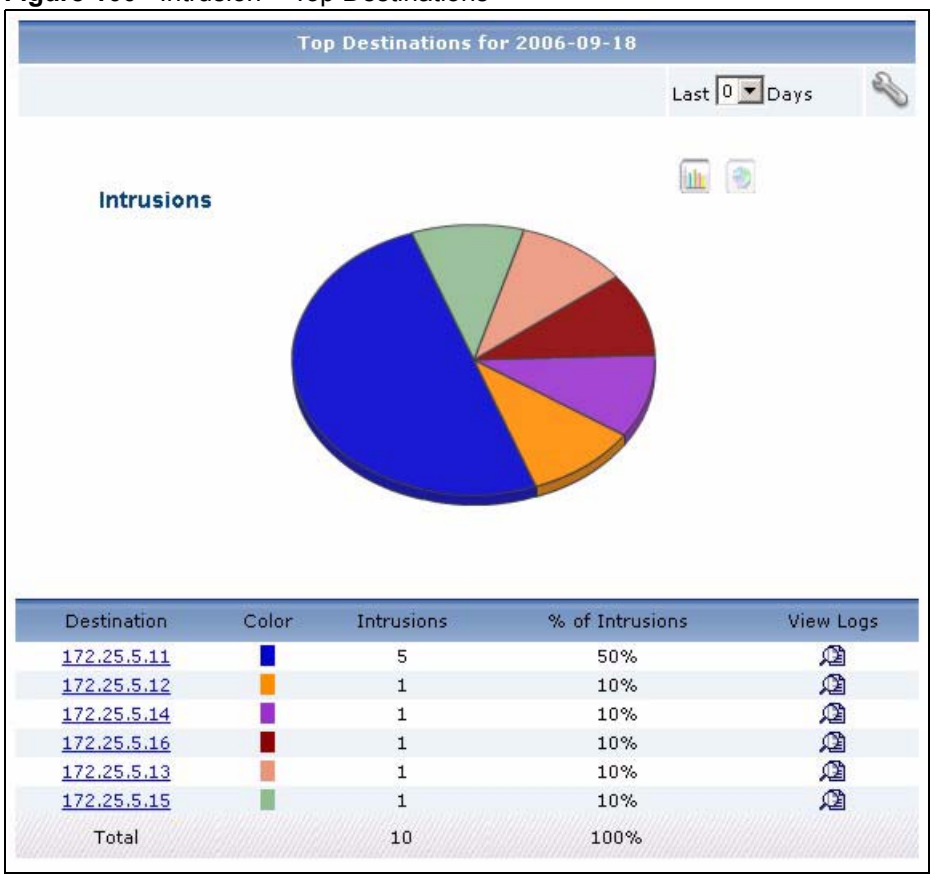
7.2.7 Top Intrusion Destinations

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

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.

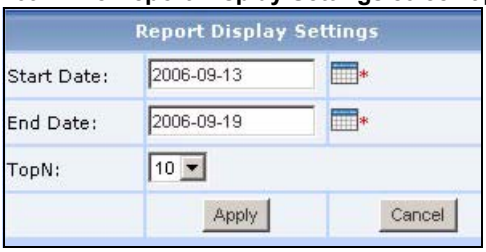
Click **Network Attack** > **Intrusion** > **Top Destinations** to open this screen.

Figure 100 Intrusion > Top Destinations



Each field is described in the following table.

Table 94 Intrusion > Top Destinations

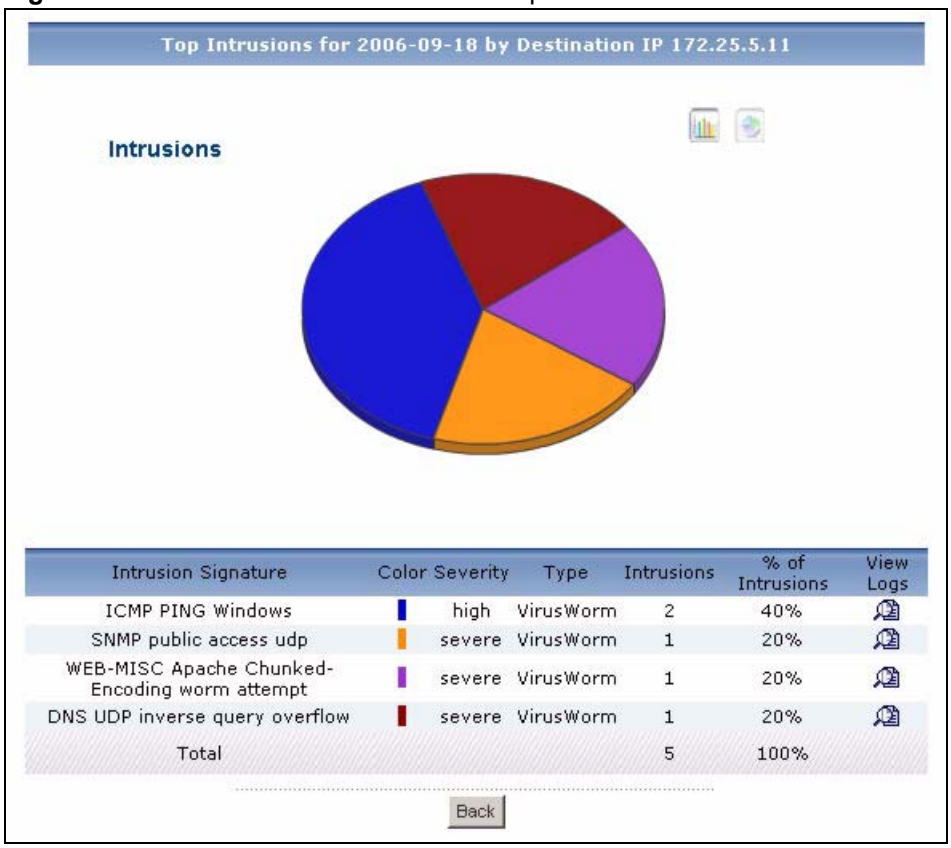
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a destination to look at the top intrusion signatures for the selected destination. The **Top Intrusion Destinations Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

7.2.8 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 101 Network Attack > Intrusion > Top Destinations > Drill-Down



Each field is described in the following table.

Table 95 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures sent to the selected destination, sorted by the number of intrusions at each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most ZyXEL devices.

Table 95 Network Attack > Intrusion > Top Destinations > Drill-Down

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

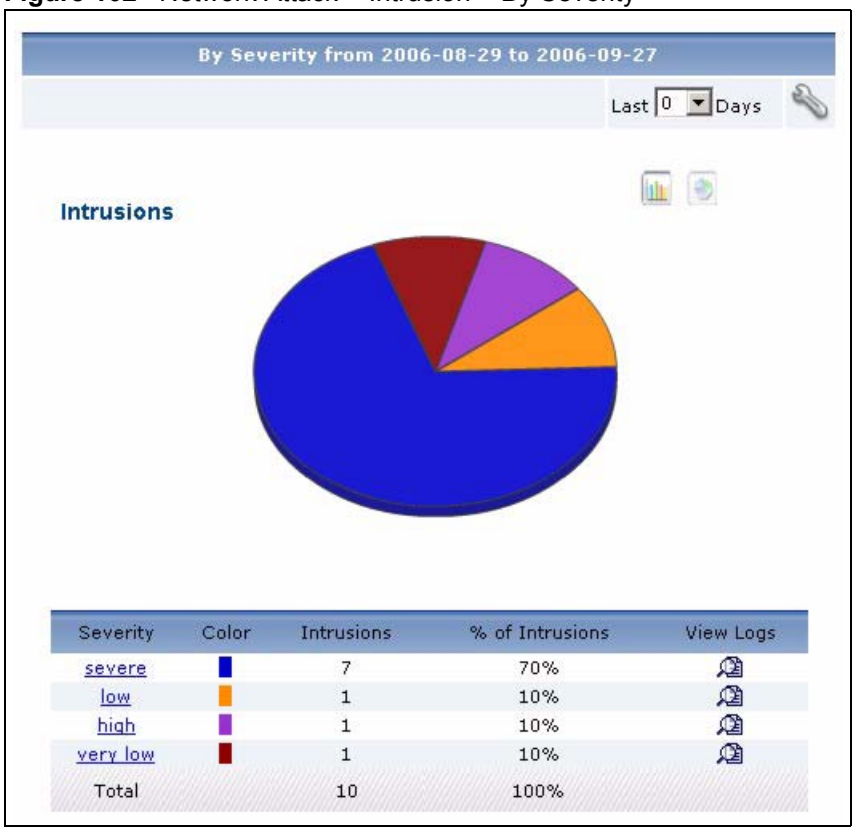
7.2.9 Intrusion Severities

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.

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 102 Network Attack > Intrusion > By Severity



Each field is described in the following table.

Table 96 Network Attack > Intrusion > By Severity

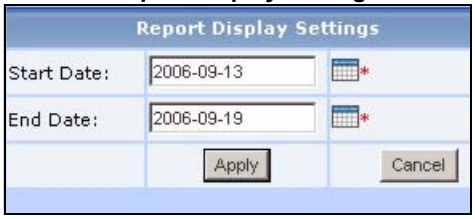
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.

Table 96 Network Attack > Intrusion > By Severity

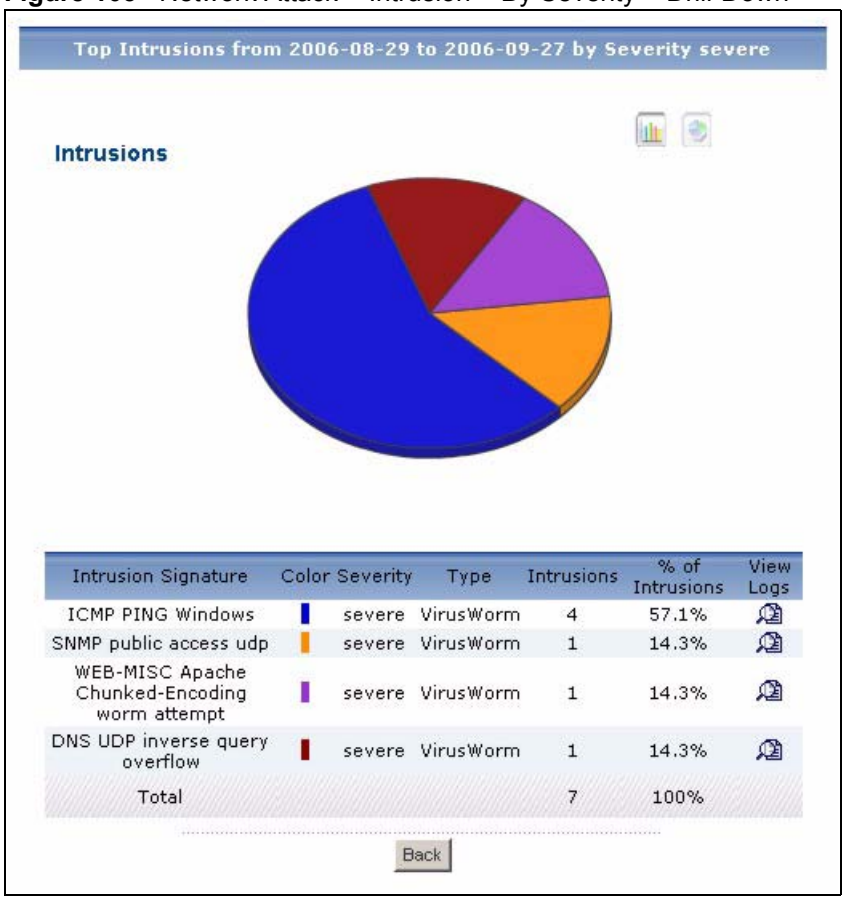
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity. The **Intrusion Severities Drill-Down** report appears.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

7.2.10 Intrusion Severities Drill-Down

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

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

Figure 103 Network Attack > Intrusion > By Severity > Drill-Down



Each field is described in the following table.

Table 97 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the intrusion signatures of the selected severity, sorted by the number of intrusions by each one.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of the selected severity using each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions of the selected severity was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.

Table 97 Network Attack > Intrusion > By Severity > Drill-Down

LABEL	DESCRIPTION
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

7.3 AntiVirus

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

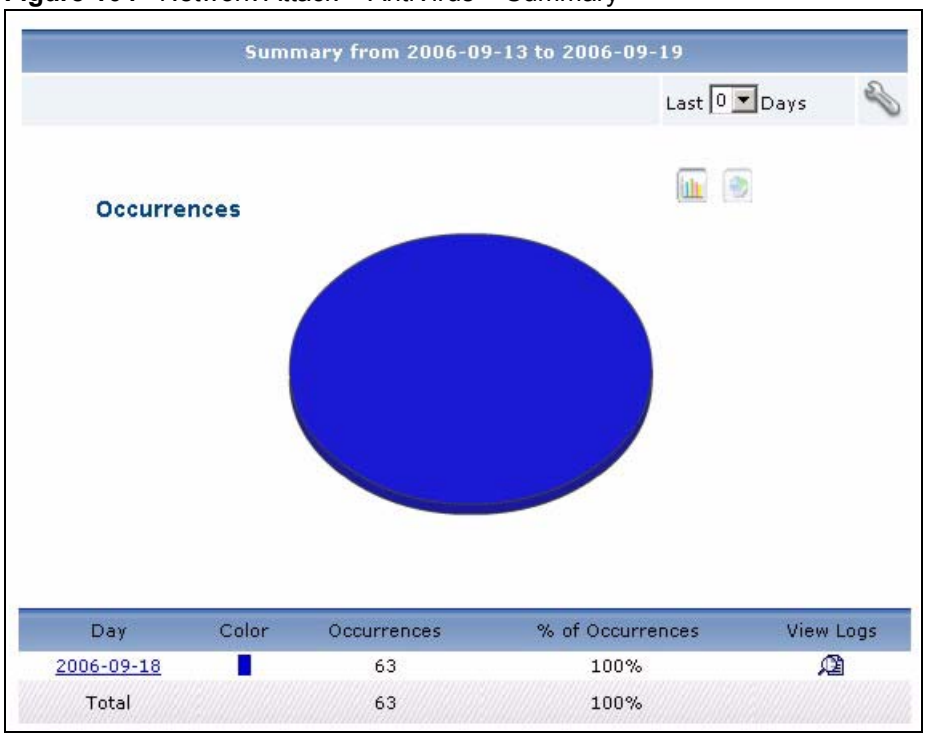
7.3.1 Virus Summary

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

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.

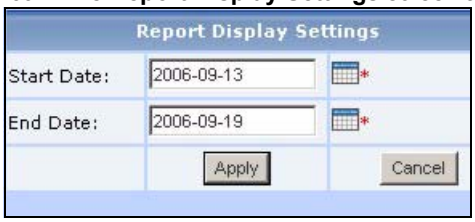
Click **Network Attack** > **AntiVirus** > **Summary** to open this screen.

Figure 104 Network Attack > AntiVirus > Summary



Each field is described in the following table.

Table 98 Network Attack > AntiVirus > Summary

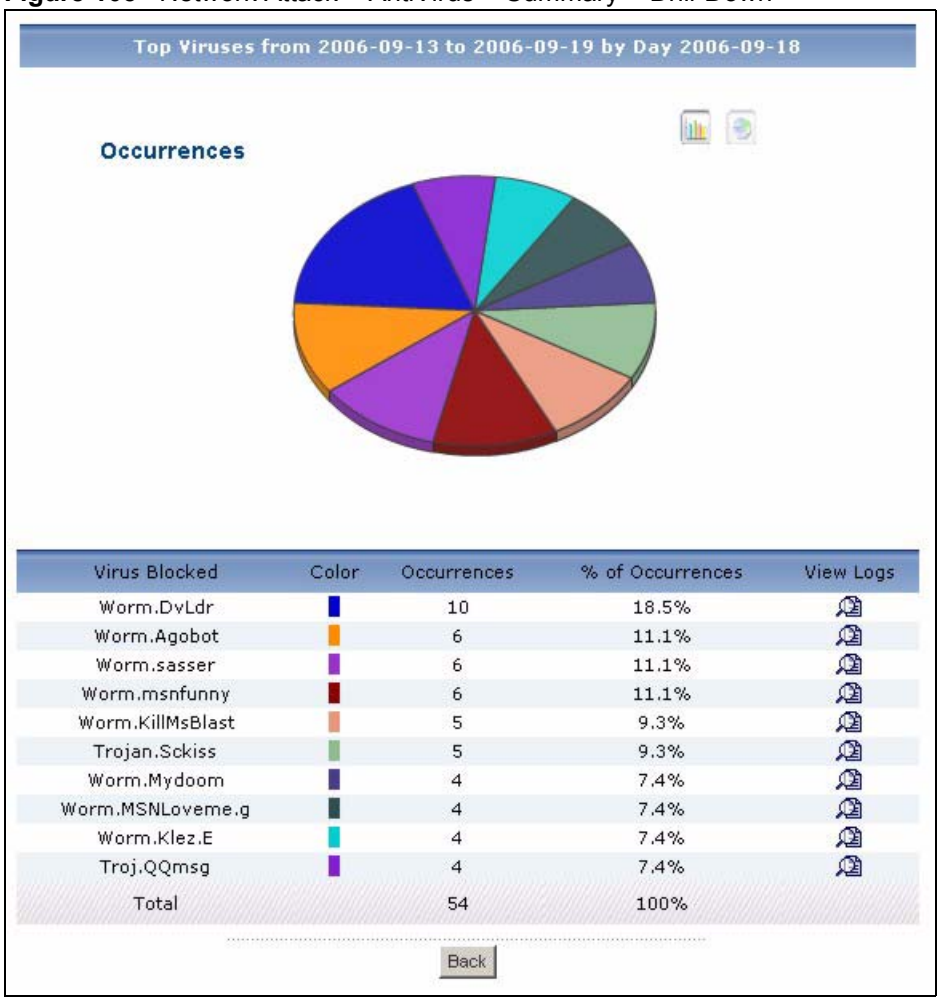
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval. The **Virus Summary Drill-Down** report appears.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.3.2 Virus Summary Drill-Down

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

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

Figure 105 Network Attack > AntiVirus > Summary > Drill-Down



Each field is described in the following table.

Table 99 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the viruses stopped in the selected time interval, sorted by the number of occurrences of each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences in the selected time interval was made by each virus.
View Logs	Click this icon to see the logs that go with the record.

Table 99 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.

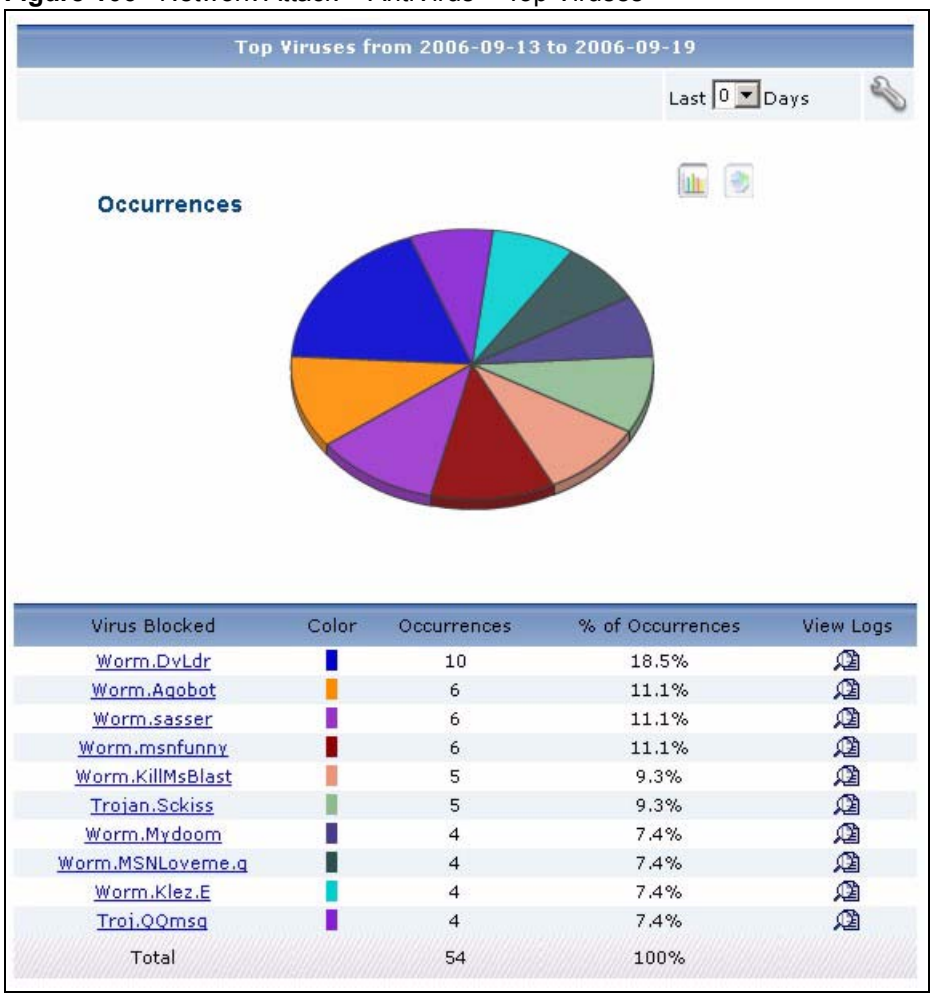
7.3.3 Top Viruses

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

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 106 Network Attack > AntiVirus > Top Viruses



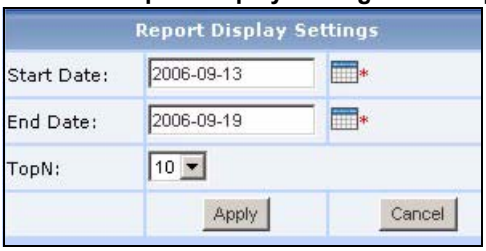
Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Worm.DvLdr		10	18.5%	
Worm.Agobot		6	11.1%	
Worm.sasser		6	11.1%	
Worm.msnfunny		6	11.1%	
Worm.KillMsBlast		5	9.3%	
Trojan.Sckiss		5	9.3%	
Worm.Mydoom		4	7.4%	
Worm.MSNLoveme.g		4	7.4%	
Worm.Klez.E		4	7.4%	
Troj.QQmsg		4	7.4%	
Total		54	100%	

Each field is described in the following table.

Table 100 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 100 Network Attack > AntiVirus > Top Viruses

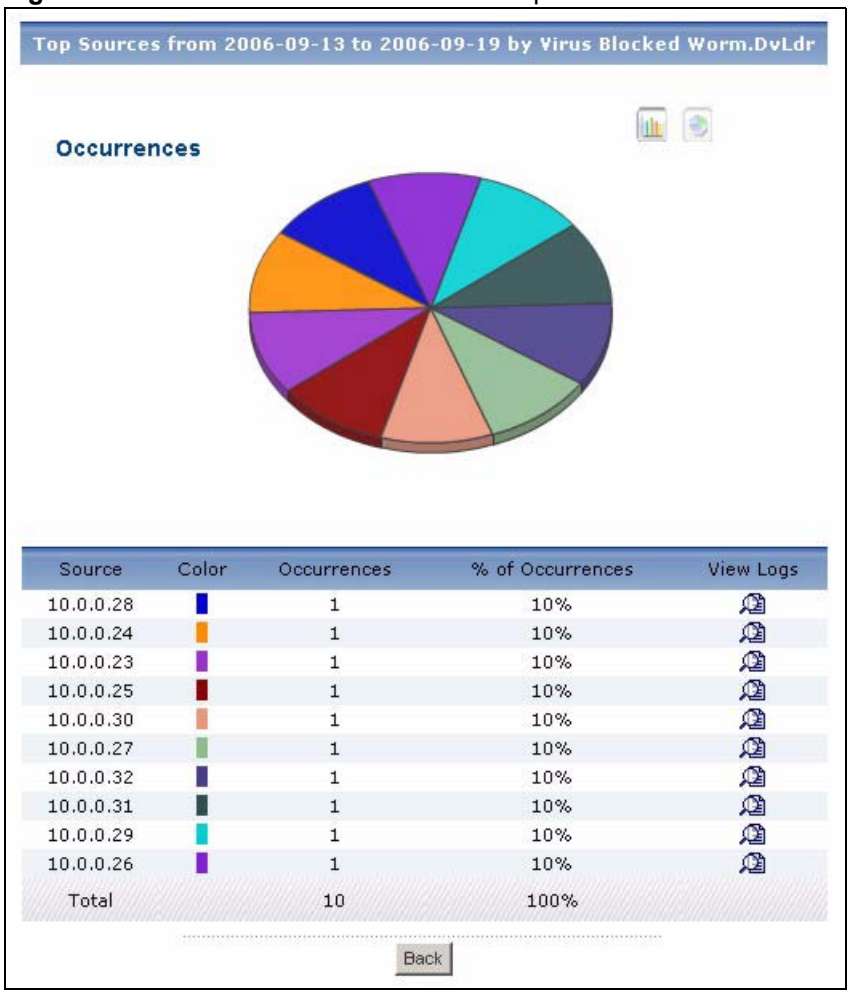
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus. The **Top Viruses Drill-Down** report appears.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.
% of Occurrences	This field displays what percentage each virus's occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

7.3.4 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 107 Network Attack > AntiVirus > Top Viruses > Drill-Down



Each field is described in the following table.

Table 101 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of the selected virus, sorted by the number of occurrences by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences of the selected virus from each source.

Table 101 Network Attack > AntiVirus > Top Viruses > Drill-Down

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

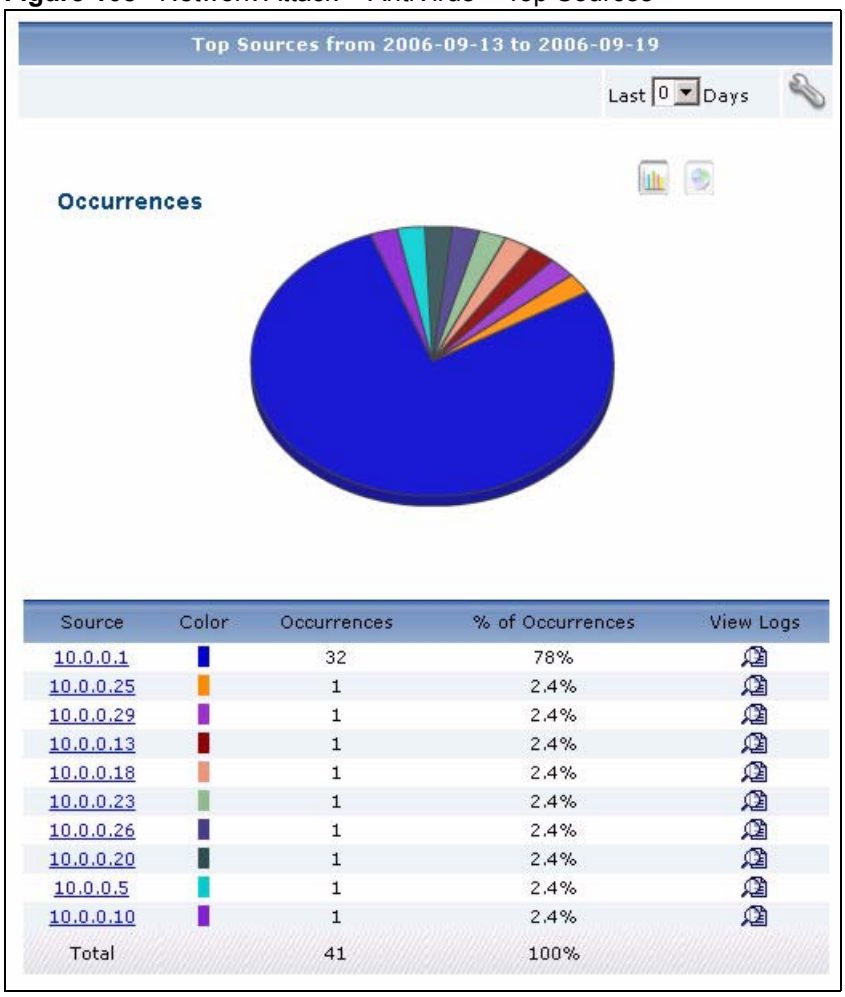
7.3.5 Top Virus Sources

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

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 108 Network Attack > AntiVirus > Top Sources

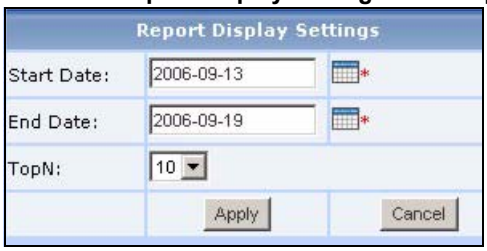


Each field is described in the following table.

Table 102 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 102 Network Attack > AntiVirus > Top Sources

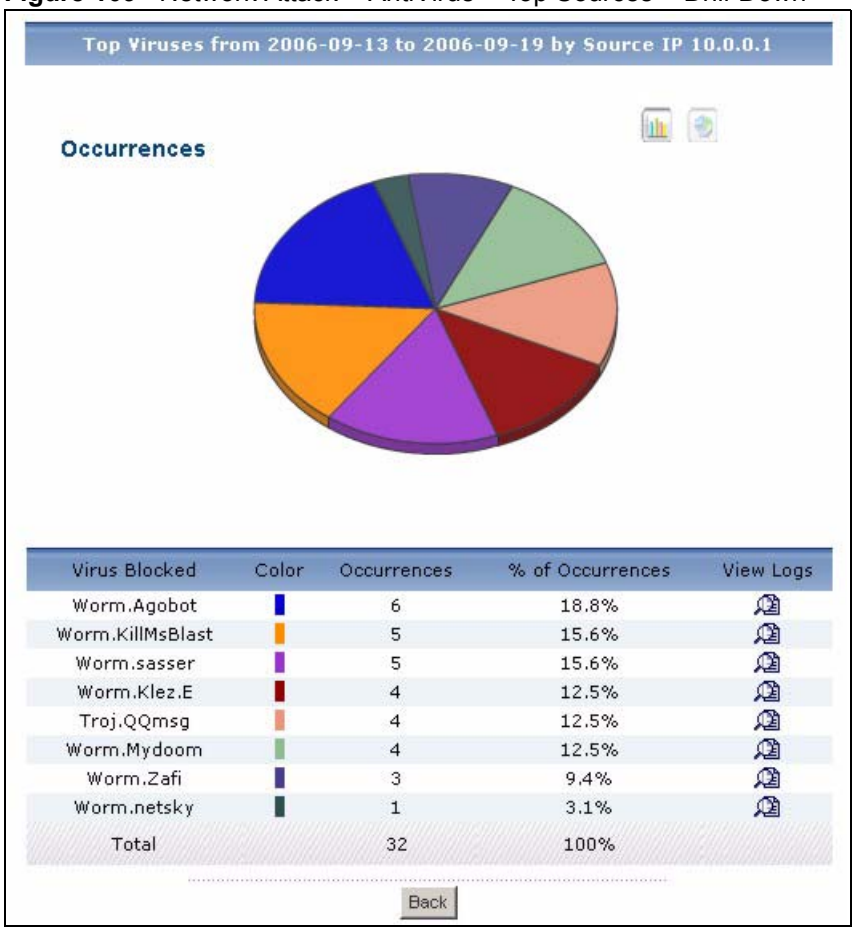
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”). Click on a source to look at the top viruses for the selected source. The **Top Virus Sources Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.3.6 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 109 Network Attack > AntiVirus > Top Sources > Drill-Down



Each field is described in the following table.

Table 103 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from the selected source, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences from the selected source by each virus.
% of Occurrences	This field displays what percentage of all occurrences from the selected source was made by each virus.
View Logs	Click this icon to see the logs that go with the record.

Table 103 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.

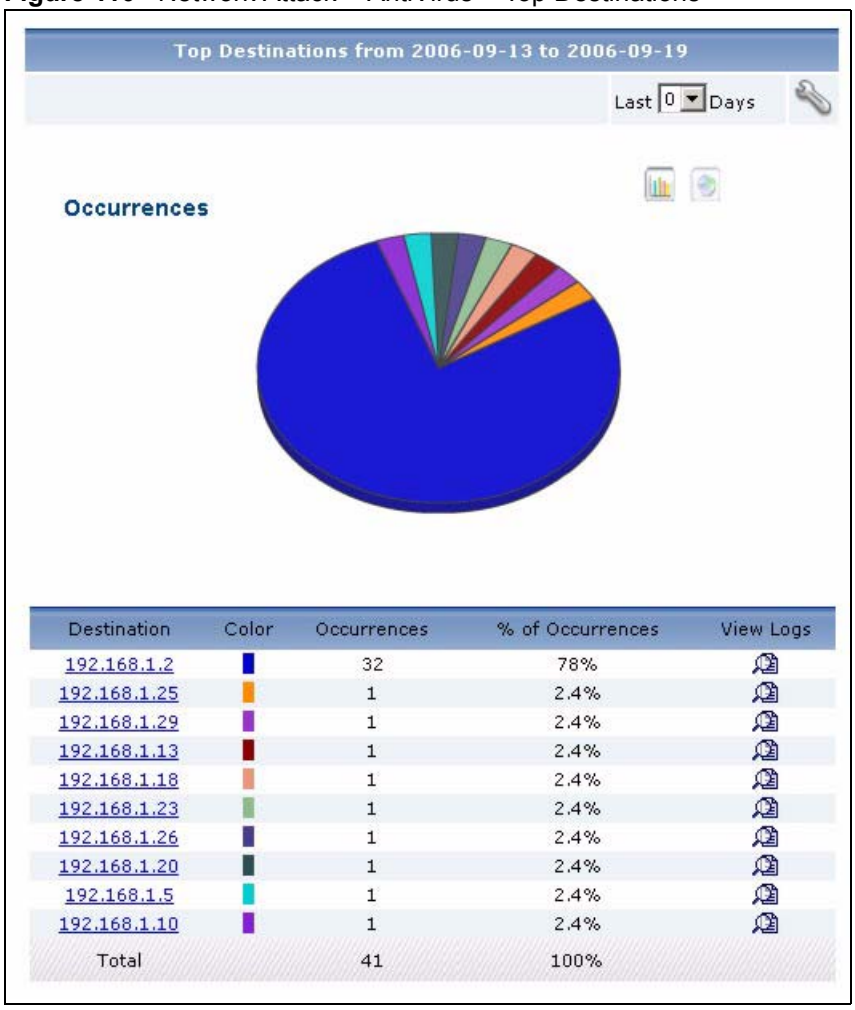
7.3.7 Top Virus Destinations

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

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 110 Network Attack > AntiVirus > Top Destinations

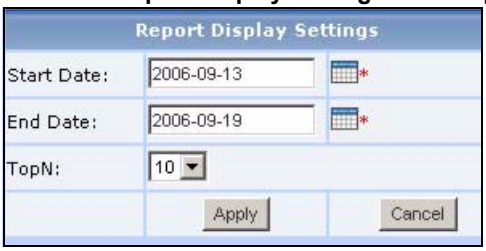


Each field is described in the following table.

Table 104 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 104 Network Attack > AntiVirus > Top Destinations

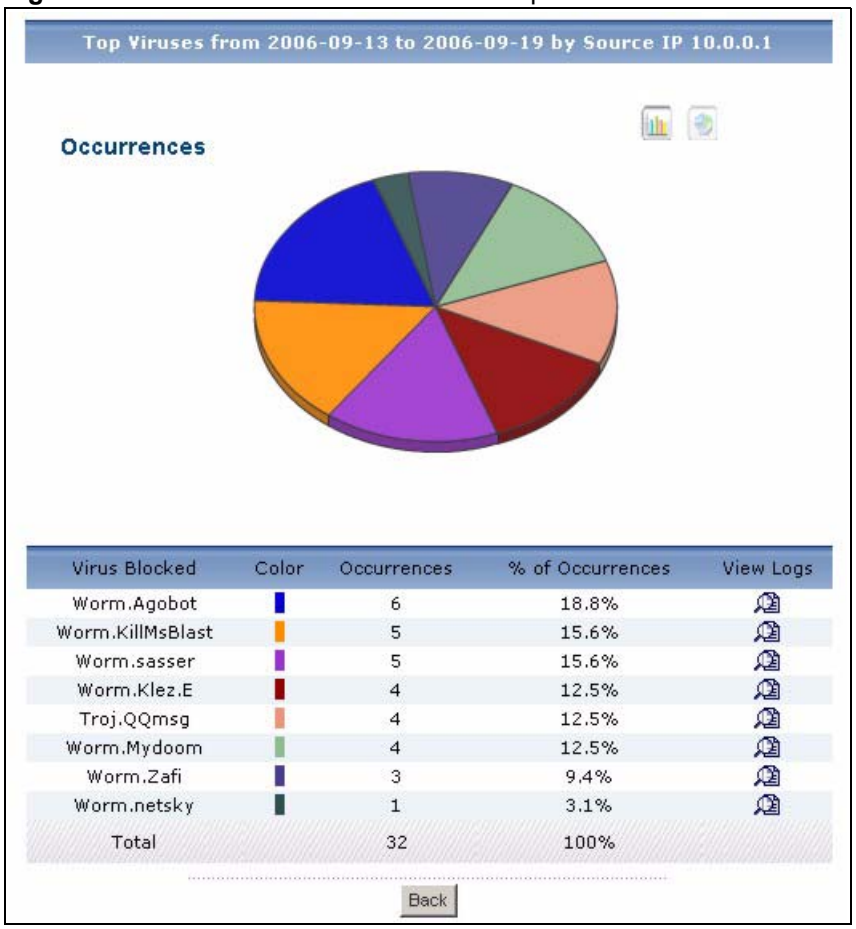
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

7.3.8 Top Virus Destinations Drill-Down

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

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

Figure 111 Network Attack > AntiVirus > Top Destinations > Drill-Down



Each field is described in the following table.

Table 105 Network Attack > AntiVirus > 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from going to the selected destination, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of times each virus was sent to the selected destination.
% of Occurrences	This field displays what percentage each virus made of the viruses sent to the selected destination.
View Logs	Click this icon to see the logs that go with the record.

Table 105 Network Attack > AntiVirus > Top Destinations > Drill-Down

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

7.4 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.

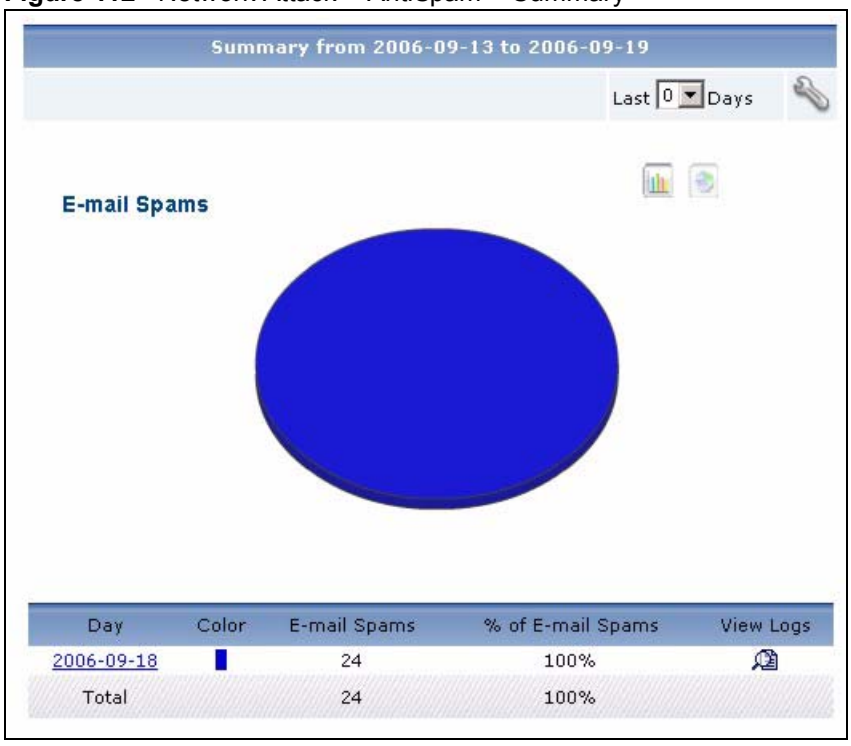
7.4.1 Spam Summary

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

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 112 Network Attack > AntiSpam > Summary



Each field is described in the following table.

Table 106 Network Attack > AntiSpam > Summary

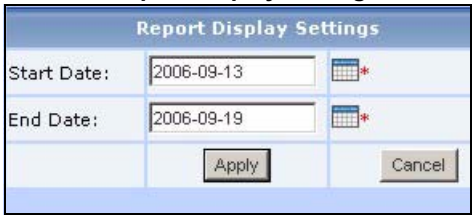
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.

Table 106 Network Attack > AntiSpam > Summary

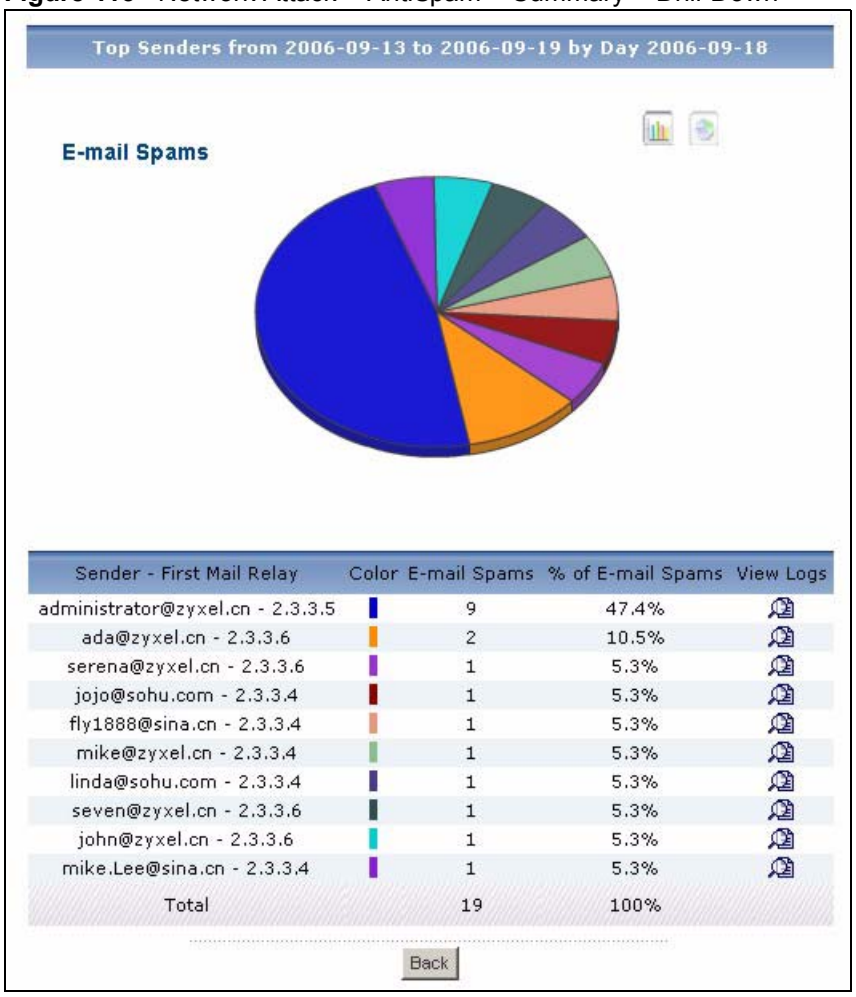
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top spam messages in the selected time interval. The **Spam Summary Drill-Down** report appears.
Color	This field displays what color represents each time interval in the graph.
E-mail Spams	This field displays the number of spam messages in the selected time interval.
% of E-mail Spams	This field displays what percentage of all spam messages was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.4.2 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 113 Network Attack > AntiSpam > Summary > Drill-Down



Each field is described in the following table.

Table 107 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	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Sender - 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.

Table 107 Network Attack > AntiSpam > Summary > Drill-Down

LABEL	DESCRIPTION
% of E-mail Spams	This field displays what percentage of all spam messages in the selected time interval was sent by each sender.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the senders above. If the number of senders in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

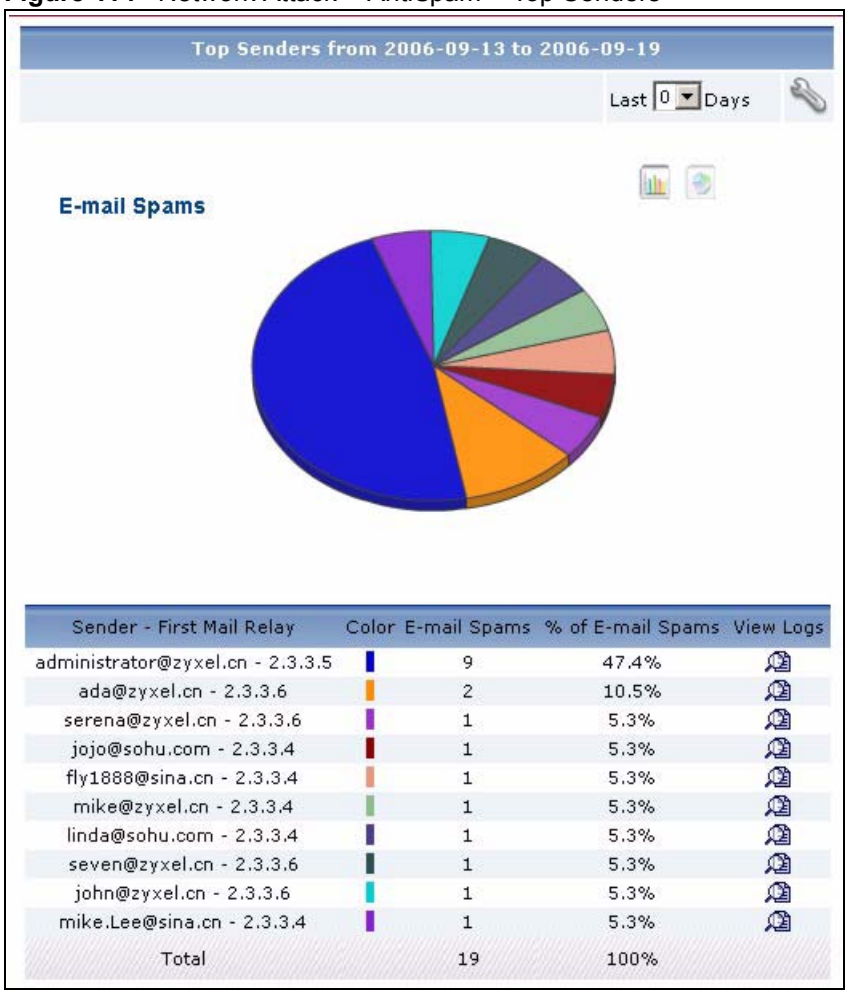
7.4.3 Top Spam Senders

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.

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 114 Network Attack > AntiSpam > Top Senders



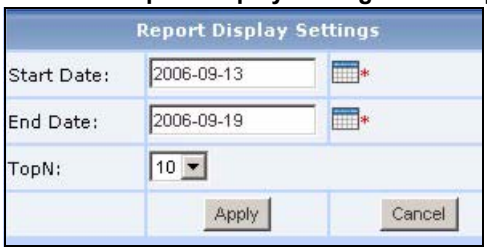
Sender - First Mail Relay	Color	E-mail Spams	% of E-mail Spams	View Logs
administrator@zyxel.cn - 2.3.3.5		9	47.4%	
ada@zyxel.cn - 2.3.3.6		2	10.5%	
serena@zyxel.cn - 2.3.3.6		1	5.3%	
jojo@sohu.com - 2.3.3.4		1	5.3%	
fly1888@sina.cn - 2.3.3.4		1	5.3%	
mike@zyxel.cn - 2.3.3.4		1	5.3%	
linda@sohu.com - 2.3.3.4		1	5.3%	
seven@zyxel.cn - 2.3.3.6		1	5.3%	
john@zyxel.cn - 2.3.3.6		1	5.3%	
mike.Lee@sina.cn - 2.3.3.4		1	5.3%	
Total		19	100%	

Each field is described in the following table.

Table 108 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 108 Network Attack > AntiSpam > Top Senders

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Sender - First Mail Relay	This field displays the top combinations of senders of spam and the first SMTP server to which the spam was sent, sorted by the number of spam messages sent for each combination. Each sender is identified by its e-mail address. Each SMTP server is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).
Color	This field displays what color represents each sender in the graph.
E-mail Spams	This field displays how many spam messages each sender sent.
% of E-mail Spams	This field displays what percentage of all spam messages was sent by each sender.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the senders above.

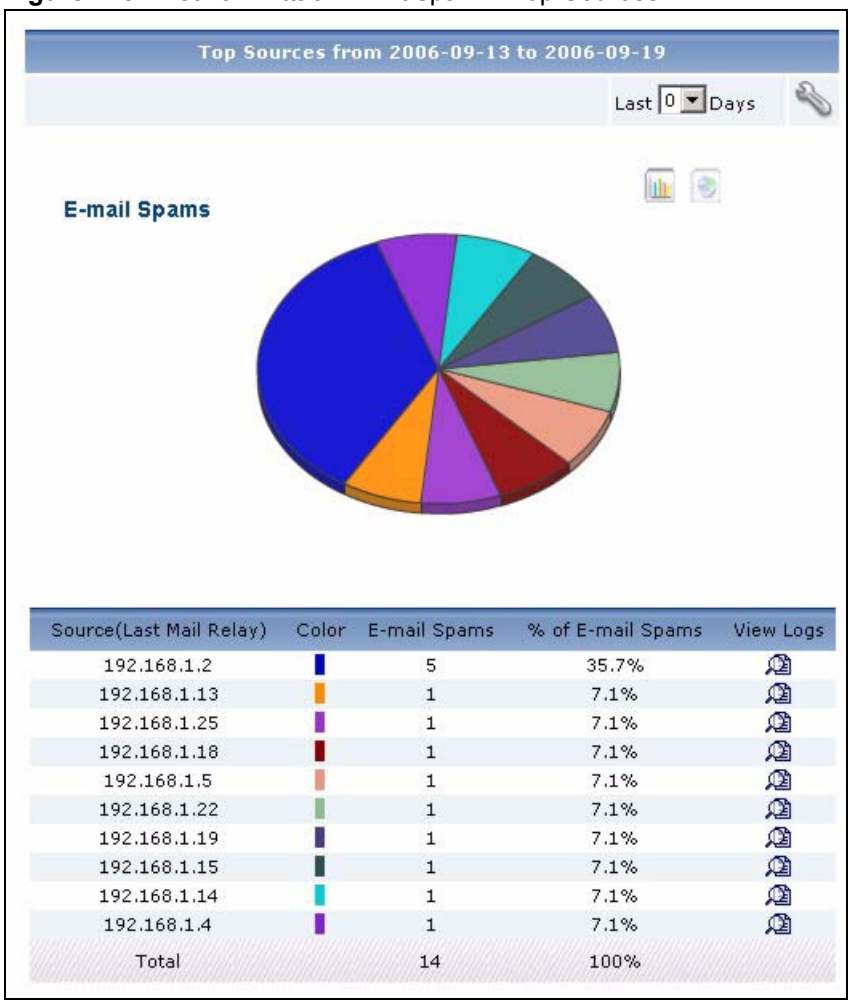
7.4.4 Top Spam Sources

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

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 115 Network Attack > AntiSpam > Top Sources

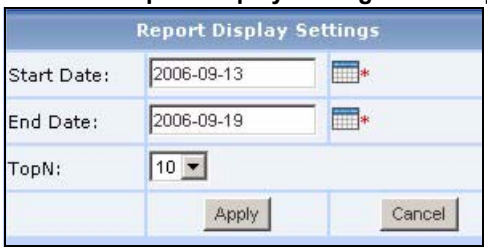


Each field is described in the following table.

Table 109 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 109 Network Attack > AntiSpam > Top Sources

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source (Last Mail Relay)	This field displays the top SMTP servers that sent spam to the selected device, sorted by the number of spam messages from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each SMTP server is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/ 200.100.20.10”).
Color	This field displays what color represents each source in the graph.
E-mail Spams	This field displays the number of spam messages from each source.
% of E-mail Spams	This field displays what percentage of all spam messages came from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

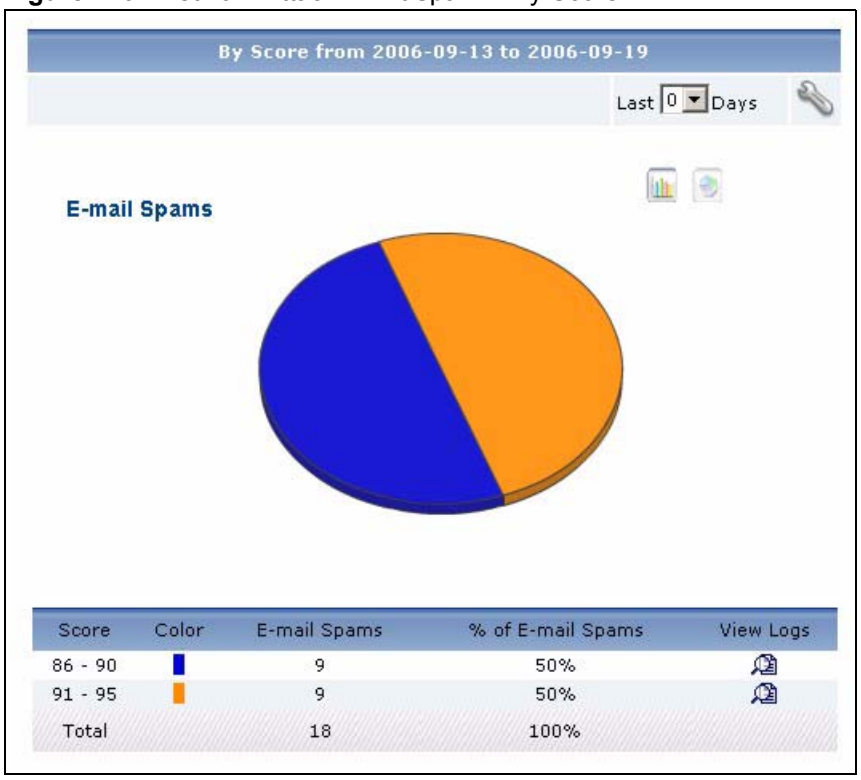
7.4.5 Spam Scores

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

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 116 Network Attack > AntiSpam > By Score



Each field is described in the following table.

Table 110 Network Attack > AntiSpam > By Score

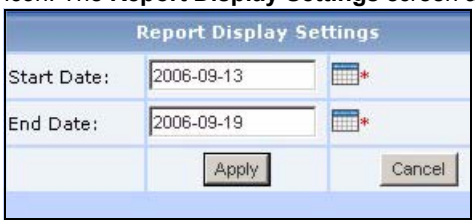
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.

Table 110 Network Attack > AntiSpam > By Score

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Score	This field displays the scores calculated for spam messages by the selected device, sorted by the number of spam messages from each score. If the number of scores is less than the maximum number of records displayed in this table, every score is displayed.
Color	This field displays what color represents each score in the graph.
E-mail Spams	This field displays the number of spam messages with each score.
% of E-mail Spams	This field displays what percentage of all spam messages had each score.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the scores above.

8

Security Policy

Use these screens to look at what users and traffic were allowed or blocked by the device's firewall, application patrol and content filtering policies.

8.1 Firewall Access Control

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

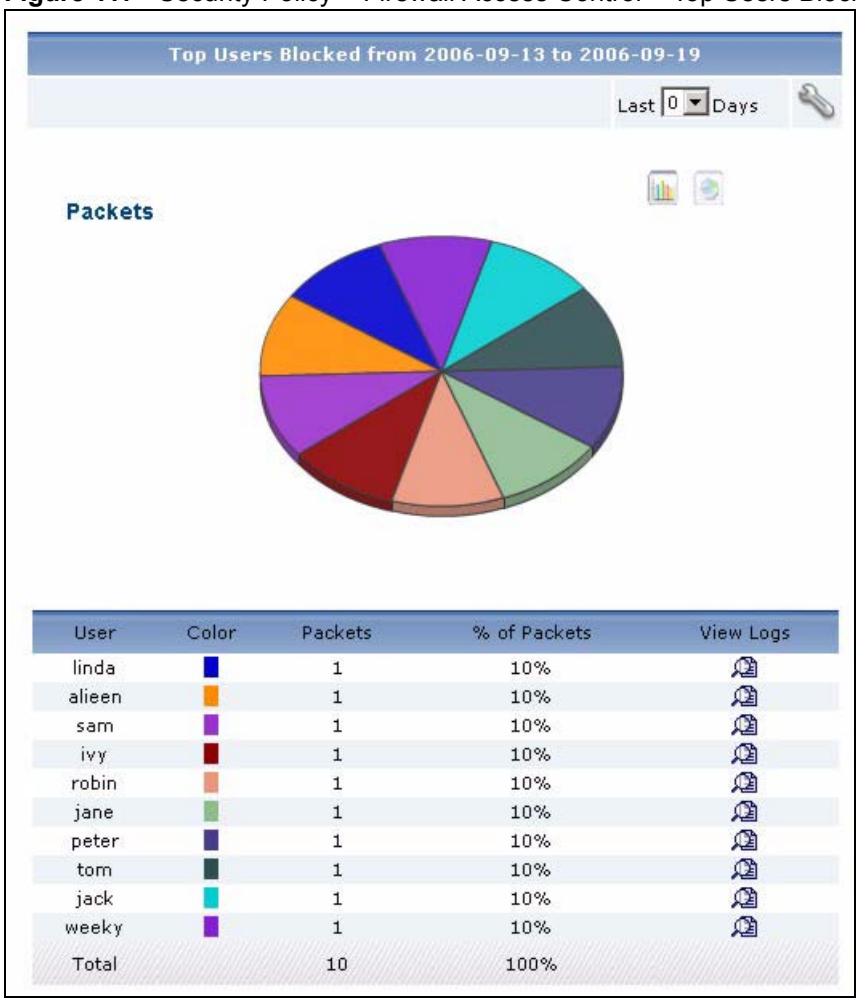
8.1.1 Top Users Blocked

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

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

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

Figure 117 Security Policy > Firewall Access Control > Top Users Blocked

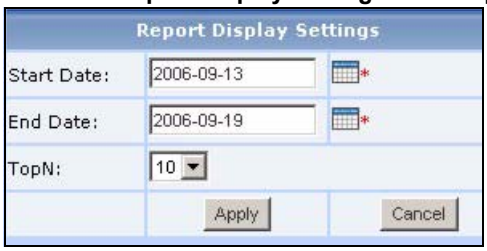


Each field is described in the following table.

Table 111 Security Policy > Firewall Access Control > Top Users Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 111 Security Policy > Firewall Access Control > Top Users Blocked

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users from which the selected device blocked the most traffic, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Packets	This field displays the number of packets the device blocked from each user.
% of Packets	This field displays what percentage each user's number of blocked packets makes out of the total number of blocked packets that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

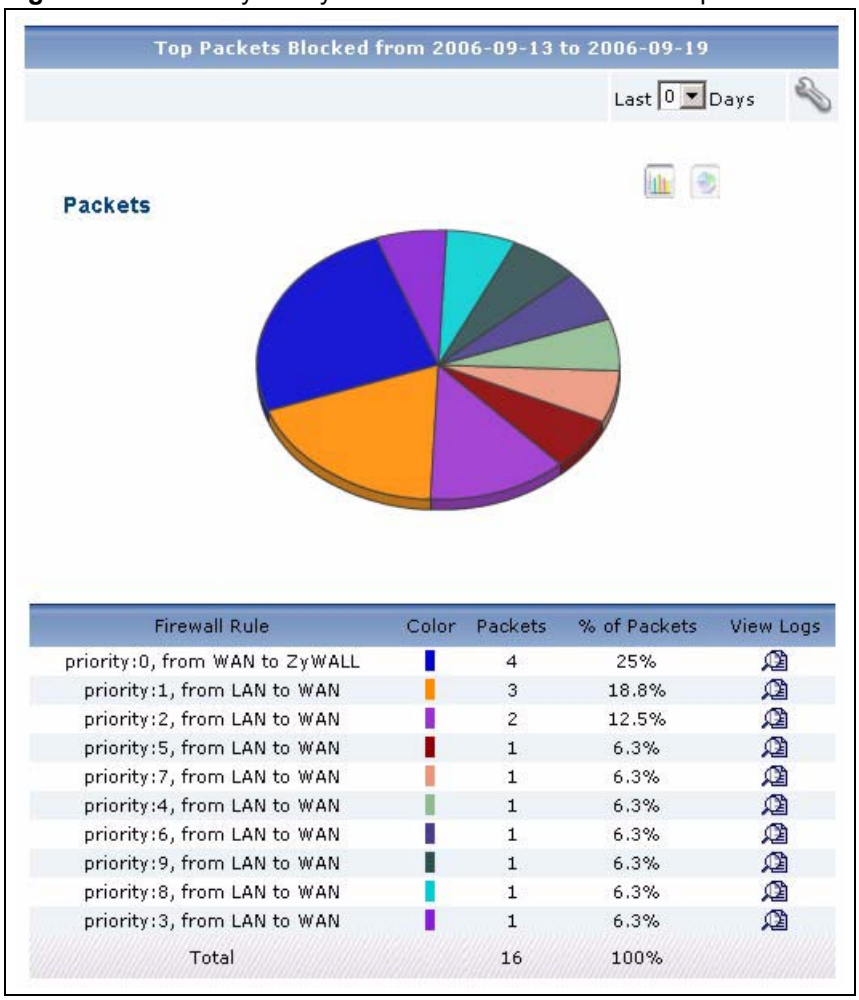
8.1.2 Top Packets Blocked

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

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

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

Figure 118 Security Policy > Firewall Access Control > Top Packets Blocked

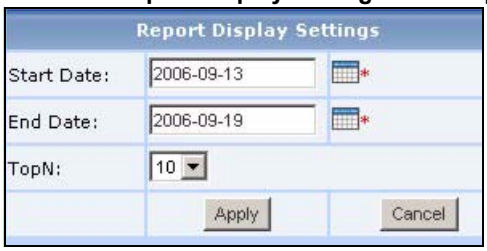


Each field is described in the following table.

Table 112 Security Policy > Firewall Access Control > Top Packets Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 112 Security Policy > Firewall Access Control > Top Packets Blocked

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Firewall Rule	This field displays the name of the firewall rule on the selected device that blocked packets, sorted by the number of packets for each one. Each firewall rule is identified by priority in the firewall rule list and the traffic direction to which it applies.
Color	This field displays what color represents each firewall rule in the graph.
Packets	This field displays the number of packets the firewall rule blocked from each user.
% of Packets	This field displays what percentage each firewall rule's number of blocked packets makes out of the total number of blocked packets that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the firewall rules above.

8.2 Application Access Control

Use these screens to display the most-often blocked applications.

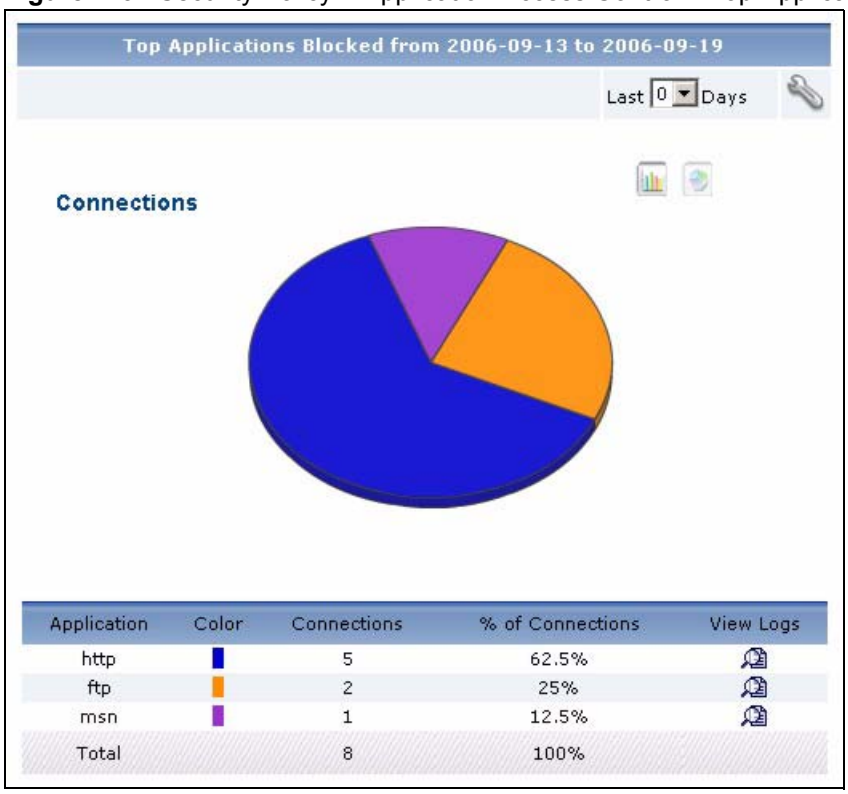
8.2.1 Top Applications Blocked

Use this report to look at the applications for which the device blocked the most connections.

To look at application access control reports, each ZyXEL device must record allowed applications and blocked applications and users in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Application Patrol is** enabled.

Click **Security Policy > Application Access Control** > **Top Applications Blocked** to open this screen.

Figure 119 Security Policy > Application Access Control > Top Applications Blocked

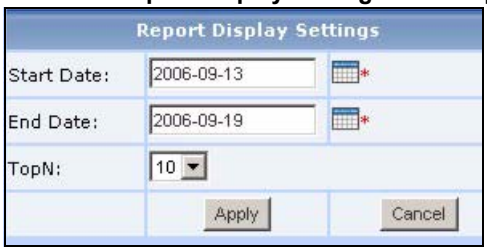


Each field is described in the following table.

Table 113 Security Policy > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 113 Security Policy > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the name of the application for which the selected device blocked the most traffic, sorted by the amount of traffic for each one. If the number of applications is less than the maximum number of records displayed in this table, every application is displayed.
Color	This field displays what color represents each application in the graph.
Connections	This field displays the number of traffic events the device blocked for each application.
% of Connections	This field displays what percentage each application's number of blocked connections makes out of the total number of blocked connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the applications above.

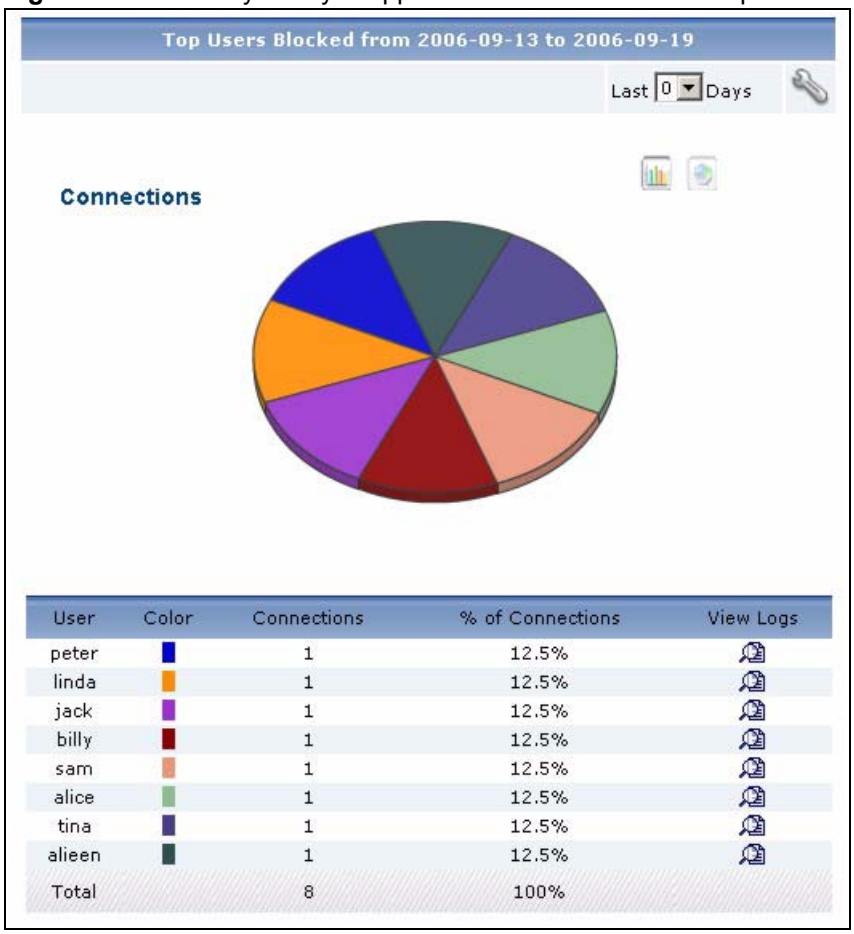
8.2.2 Top Users Blocked

Use this report to look at the users for which the device blocked the most connections.

To look at security policy reports, each ZyXEL device must record users blocked by the application patrol in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Application Patrol is** enabled.

Click **Security Policy > Application Access Control** > **Top Users Blocked** to open this screen.

Figure 120 Security Policy > Application Access Control > Top Users Blocked

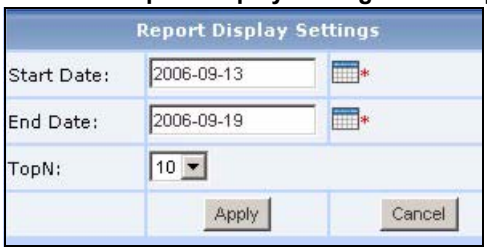


Each field is described in the following table.

Table 114 Security Policy > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 114 Security Policy > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users from which the selected device's application patrol blocked the most traffic, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Connections	This field displays the number of traffic events the device blocked for each user.
% of Connections	This field displays what percentage each user's number of blocked connections makes out of the total number of blocked connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

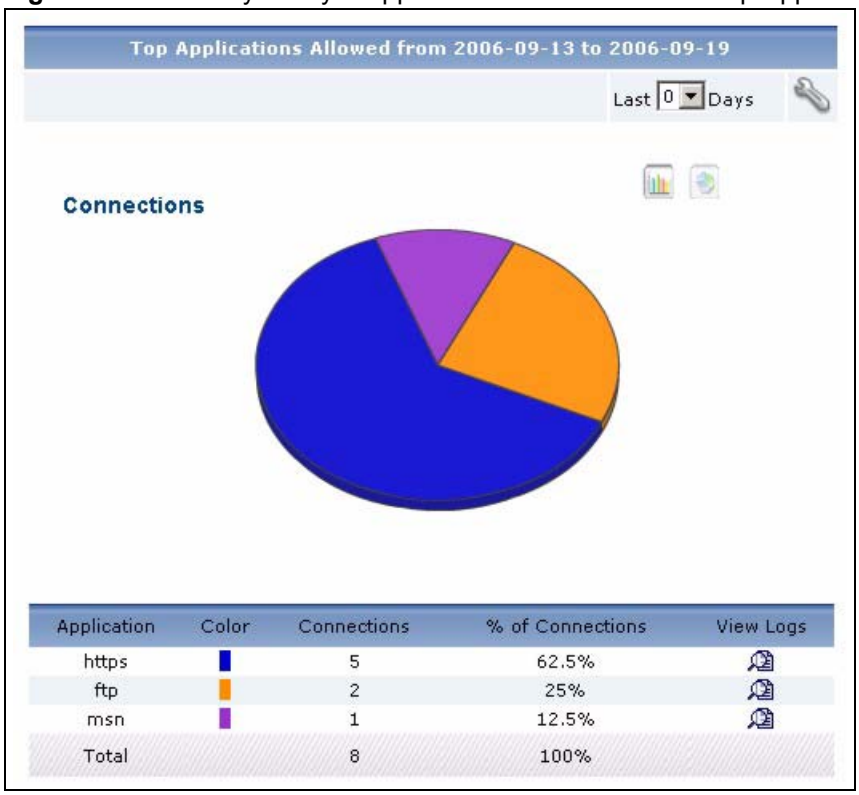
8.2.3 Top Applications Allowed

Use this report to look at the applications for which the device allowed the most connections.

To look at security policy reports, each ZyXEL device must record forwarded applications in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Application Patrol is** enabled.

Click **Security Policy > Application Access Control > Top Applications Allowed** to open this screen.

Figure 121 Security Policy > Application Access Control > Top Applications Allowed

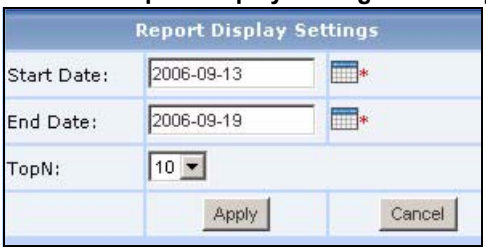


Each field is described in the following table.

Table 115 Security Policy > Application Access Control > Top Applications Allowed

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 115 Security Policy > Application Access Control > Top Applications Allowed

LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the name of the application for which the selected device permitted connections, sorted by the number of connections for each one.
Color	This field displays what color represents each application in the graph.
Connections	This field displays the number of connections the application patrol allowed for each application.
% of Connections	This field displays what percentage each application's number of allowed connections makes out of the total number of allowed connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the application rules above.

8.3 Blocked Web Accesses

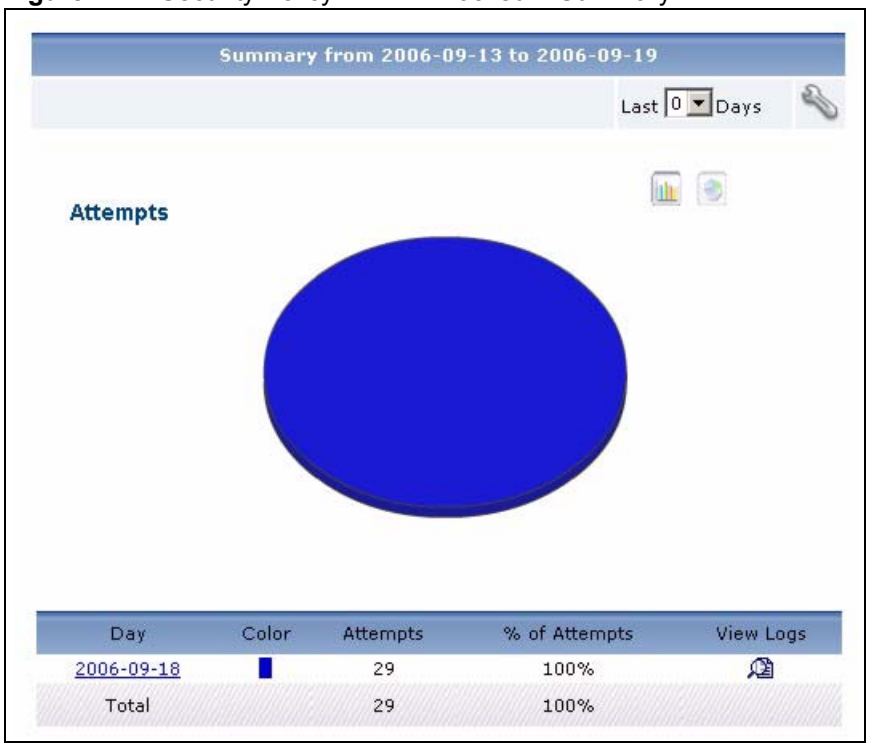
Use this report to look at the number of attempts to access blocked web sites by time interval as well as top blocked sites and hosts.

8.3.1 Web Block Summary

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 122 Security Policy > WEB Blocked > Summary

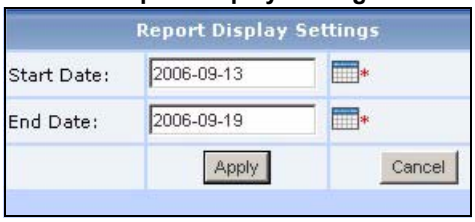


Each field is described in the following table.

Table 116 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 116 Security Policy > WEB Blocked > Summary

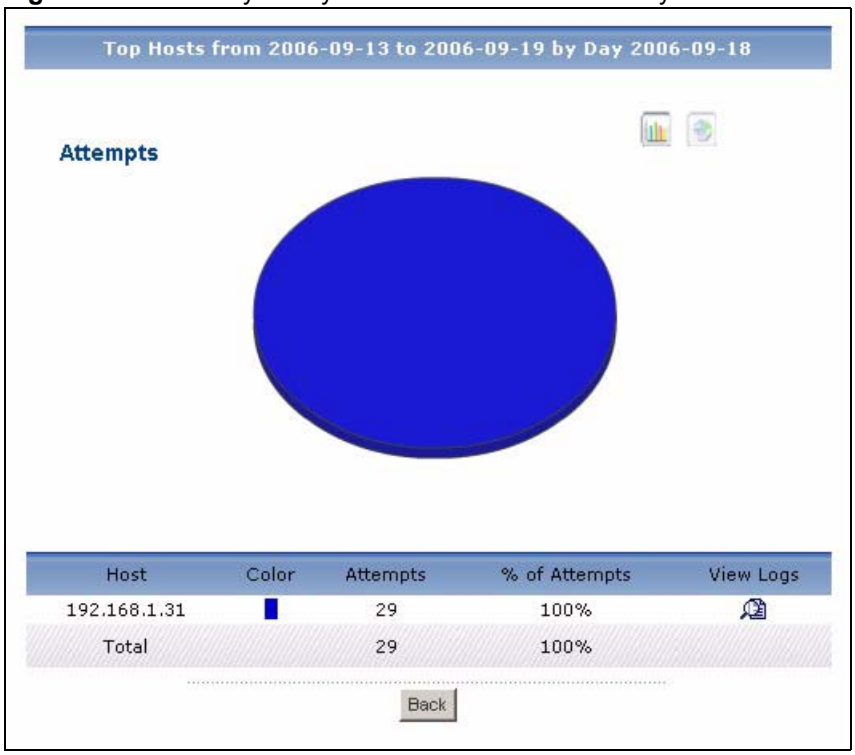
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval. The **Web Block Summary Drill-Down** report appears.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts by each source to access blocked web sites in the selected time interval.
% of Attempts	This field displays what percentage of all blocked web access attempts was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.3.2 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 123 Security Policy > WEB Blocked > Summary > Drill-Down



Each field is described in the following table.

Table 117 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of attempts to access blocked web sites in the selected time interval, sorted by the number of attempts by each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each host in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each host.
% of Attempts	This field displays what percentage of all blocked web access attempts in the selected time interval was attributed to each host.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

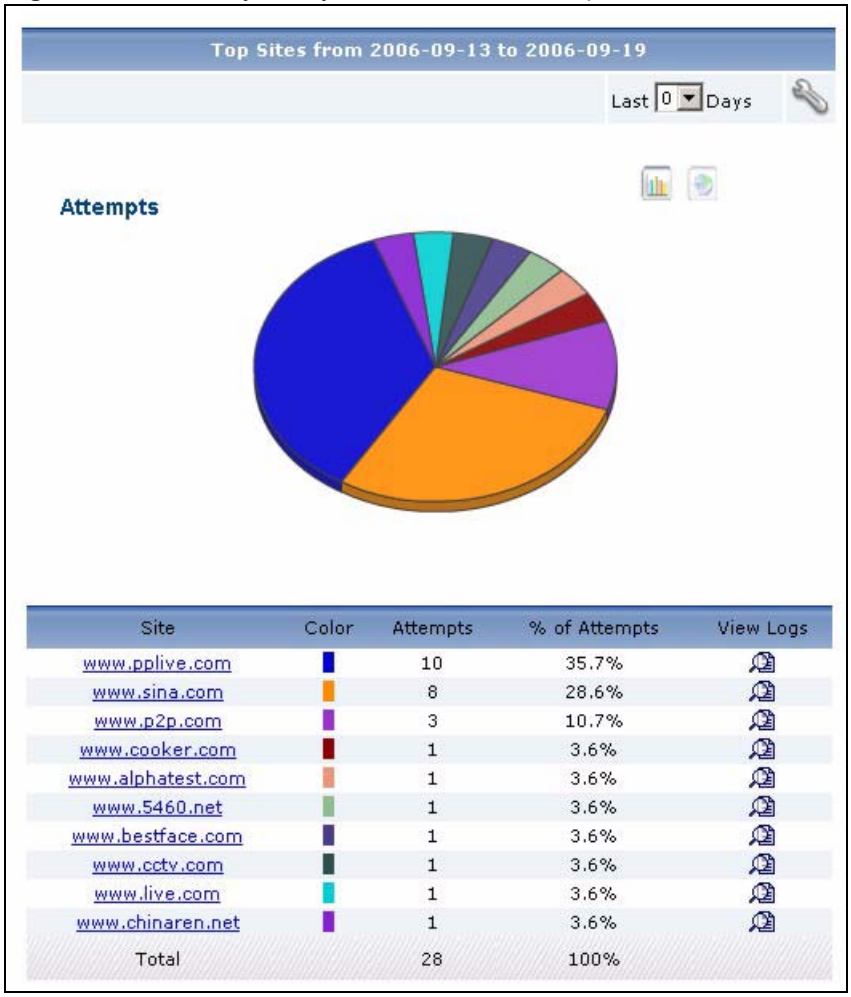
8.3.3 Top Blocked Web Sites

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

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.

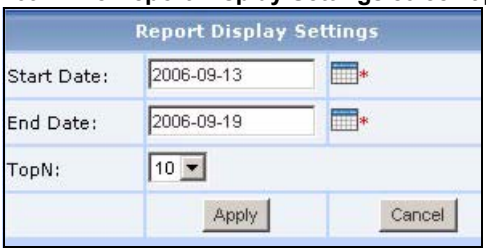
Figure 124 Security Policy > WEB Blocked > Top Sites



Site	Color	Attempts	% of Attempts	View Logs
www.pplive.com		10	35.7%	
www.sina.com		8	28.6%	
www.p2p.com		3	10.7%	
www.cooker.com		1	3.6%	
www.alphatest.com		1	3.6%	
www.5460.net		1	3.6%	
www.bestface.com		1	3.6%	
www.cctv.com		1	3.6%	
www.live.com		1	3.6%	
www.chinaren.net		1	3.6%	
Total		28	100%	

Each field is described in the following table.

Table 118 Security Policy > WEB Blocked > Top Sites

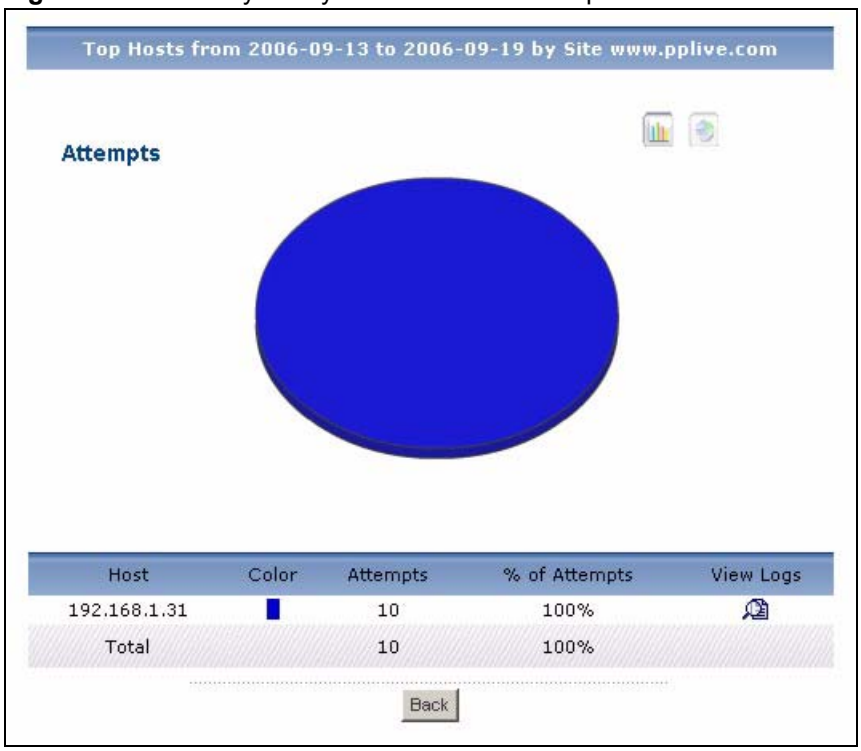
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of blocked web traffic for the selected destination. The **Top Blocked Web Sites Drill-Down** report appears.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays how much traffic (in megabytes) the device handled for each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

8.3.4 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 125 Security Policy > WEB Blocked > Top Sites > Drill-Down



Each field is described in the following table.

Table 119 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by each source to the selected destination.

Table 119 Security Policy > WEB Blocked > Top Sites > Drill-Down

LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the 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.

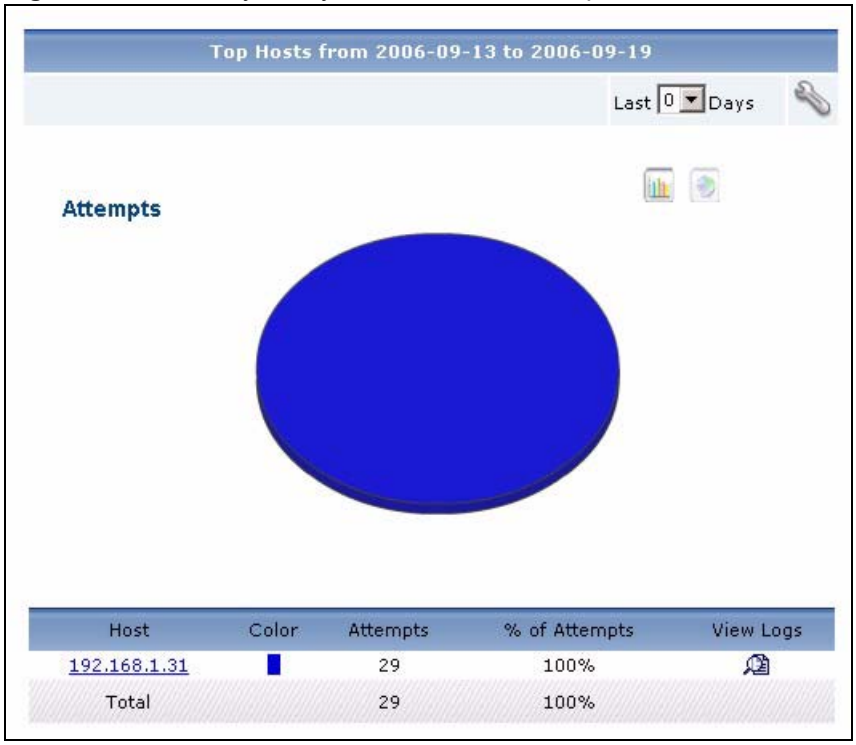
8.3.5 Top Blocked Web Hosts

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

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.

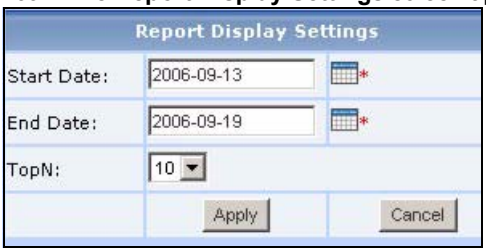
Click **Security Policy** > **WEB Blocked** > **Top Hosts** to open this screen.

Figure 126 Security Policy > WEB Blocked > Top Hosts



Each field is described in the following table.

Table 120 Security Policy > WEB Blocked > Top Hosts

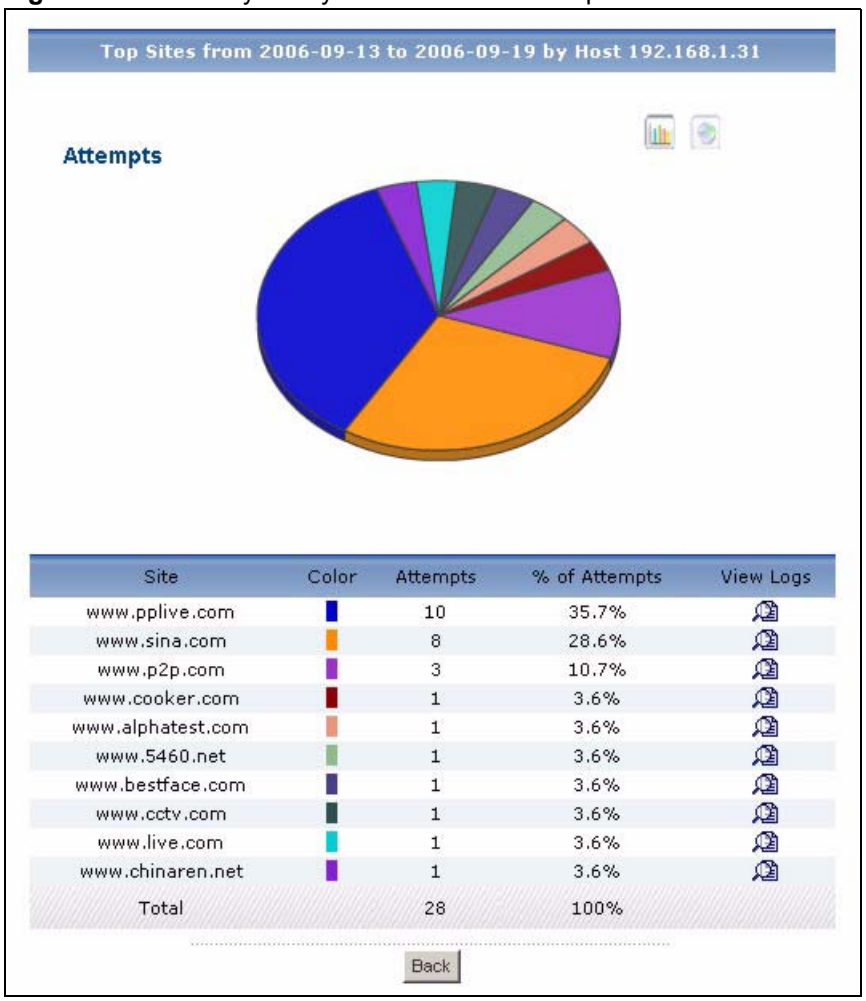
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source. The **Top Blocked Web Hosts Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of web site access attempts the device blocked from each source.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.3.6 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 127 Security Policy > WEB Blocked > Top Hosts > Drill-Down



Each field is described in the following table.

Table 121 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic from the selected source, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.

Table 121 Security Policy > WEB Blocked > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

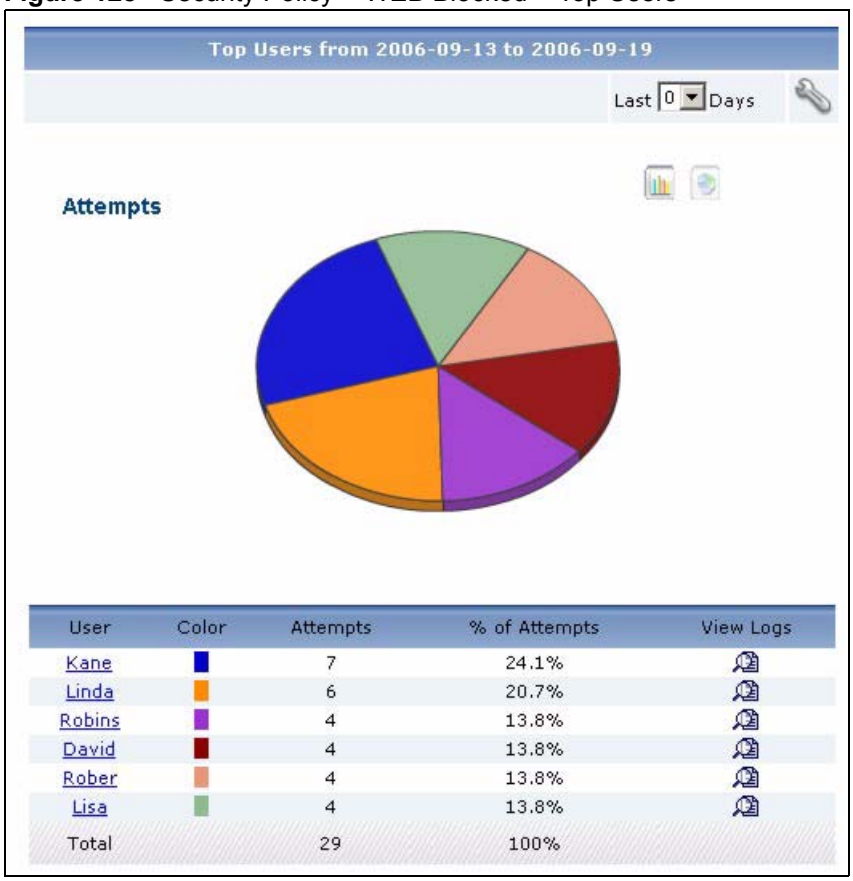
8.3.7 Top Blocked Web Users

Use this report to look at the users for which the device blocked the most web site access attempts.

To look at security policy Web blocked reports, each ZyXEL device must record forwarded web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Allow Web Sites** and **Block Web Sites** are enabled.

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

Figure 128 Security Policy > WEB Blocked > Top Users

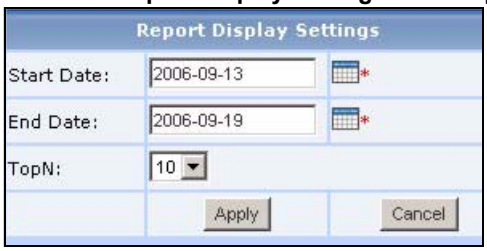


Each field is described in the following table.

Table 122 Security Policy > WEB Blocked > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 122 Security Policy > WEB Blocked > Top Users

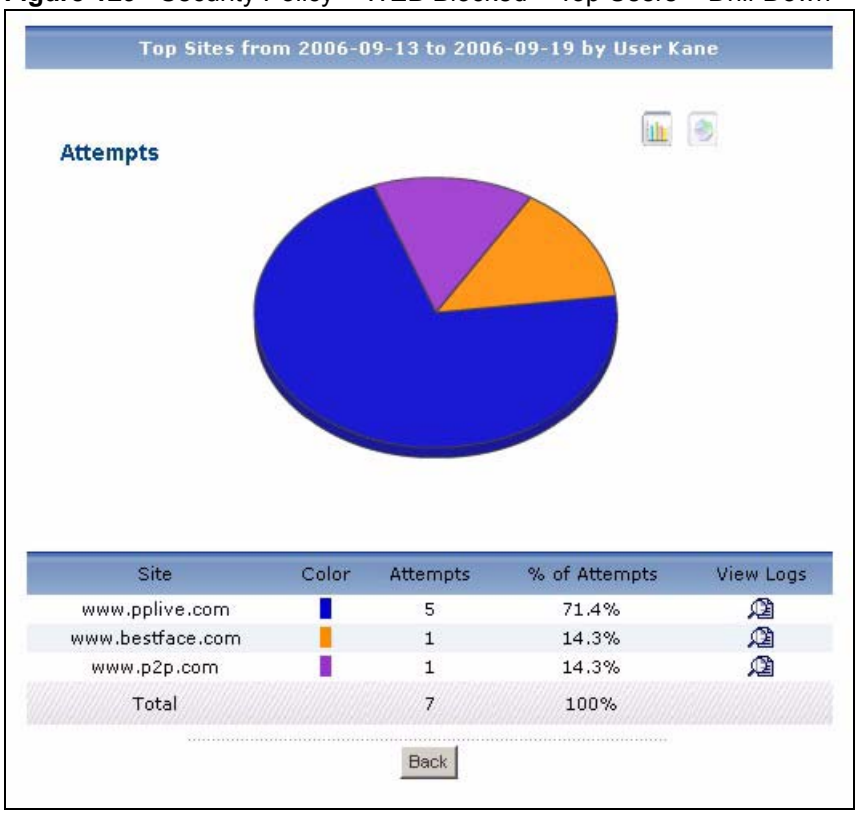
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users for which the device blocked the most web site access attempts, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source. The **Top Blocked Web Users Drill-Down** report appears.
Color	This field displays what color represents each user in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each user.
% of Attempts	This field displays what percentage the user had of all blocked attempts to access web sites.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.3.8 Top Blocked Web Users Drill-Down

Use this report to look at the top destinations for any user for which the device blocked the most web site access attempts.

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

Figure 129 Security Policy > WEB Blocked > Top Users > Drill-Down



Each field is described in the following table.

Table 123 Security Policy > WEB Blocked > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic from the selected user, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

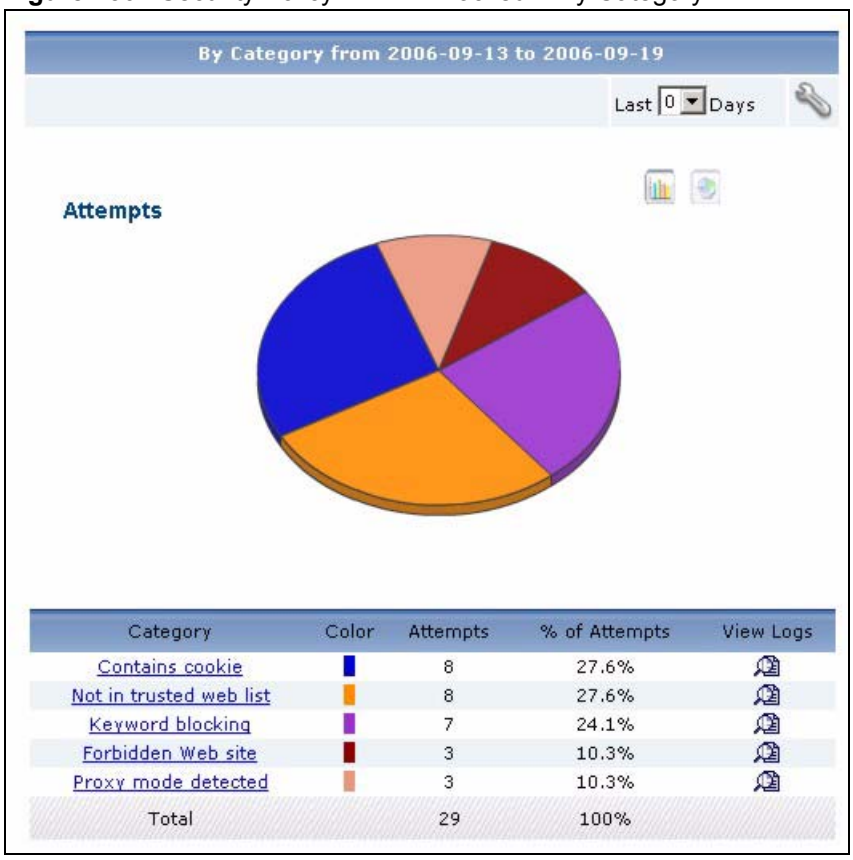
8.3.9 Blocked Web Categories

Use this report to look at the categories of blocked web traffic.

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.

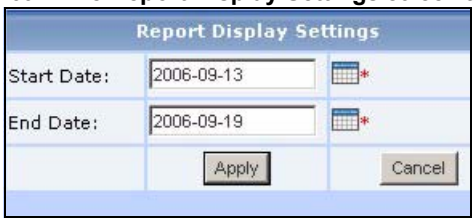
Figure 130 Security Policy > WEB Blocked > By Category



Category	Color	Attempts	% of Attempts	View Logs
Contains cookie		8	27.6%	
Not in trusted web list		8	27.6%	
Keyword blocking		7	24.1%	
Forbidden Web site		3	10.3%	
Proxy mode detected		3	10.3%	
Total		29	100%	

Each field is described in the following table.

Table 124 Security Policy > WEB Blocked > By Category

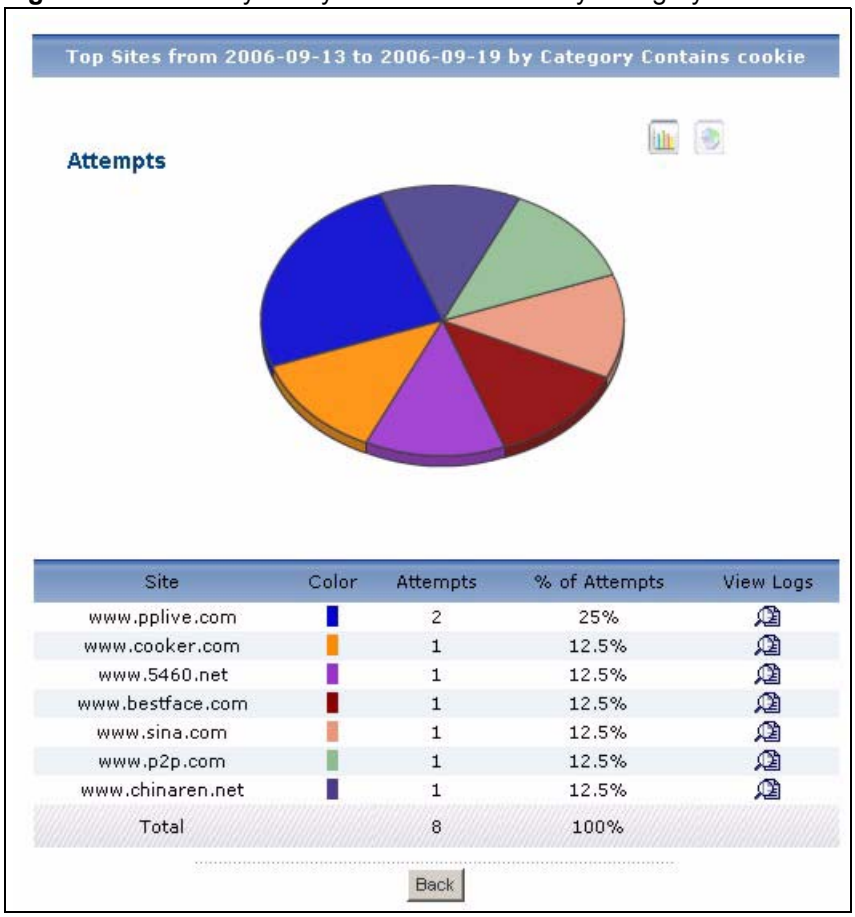
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category. The **Blocked Web Categories Drill-Down** report appears.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access allowed web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

8.3.10 Blocked Web Categories Drill-Down

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

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

Figure 131 Security Policy > WEB Blocked > By Category > Drill-Down



Each field is described in the following table.

Table 125 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the destinations of blocked web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts to each destination in the selected category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites in the selected category went to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.
Back	Click this to return to the main report.

8.4 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.

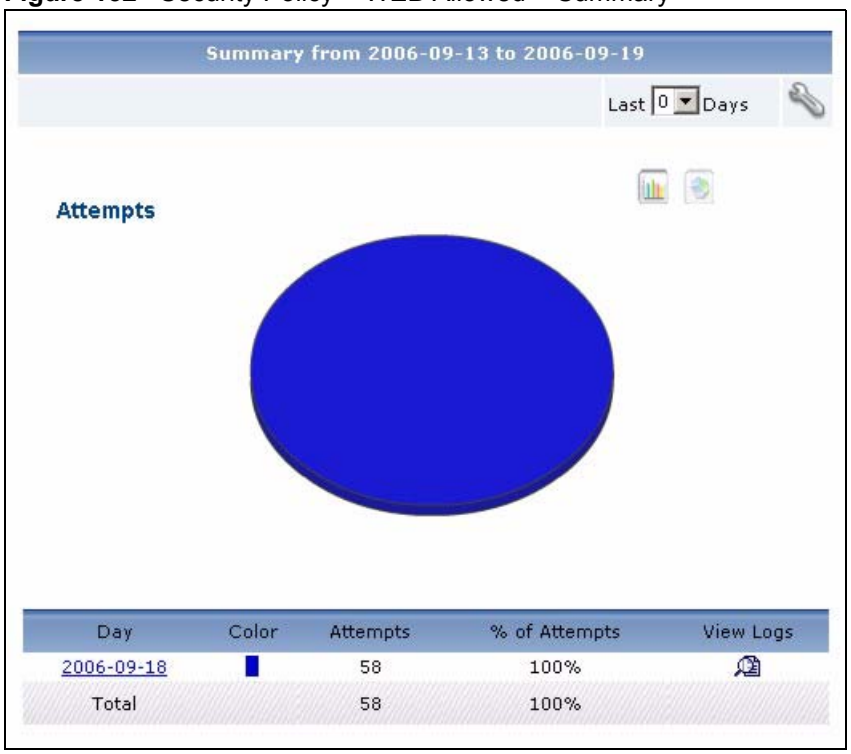
8.4.1 Web Allowed Summary

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

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.

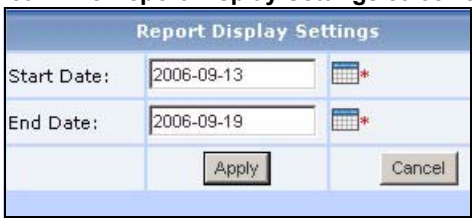
Click **Security Policy > WEB Allowed** > **Summary** to open this screen.

Figure 132 Security Policy > WEB Allowed > Summary



Each field is described in the following table.

Table 126 Security Policy > WEB Allowed > Summary

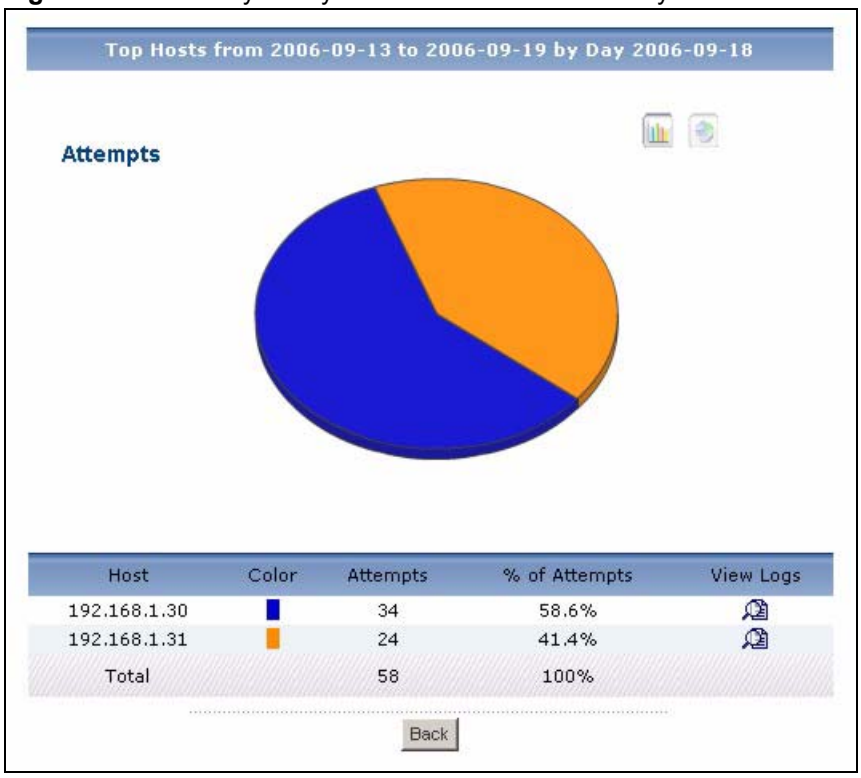
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour (Day)	This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access allowed web sites in the selected time interval. The **Web Allowed Summary Drill-Down** report appears.
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.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.4.2 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 133 Security Policy > WEB Allowed > Summary > Drill-Down



Each field is described in the following table.

Table 127 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of attempts to access 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. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts by each source to access 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.
View Logs	Click this icon to see the logs that go with the record.

Table 127 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.

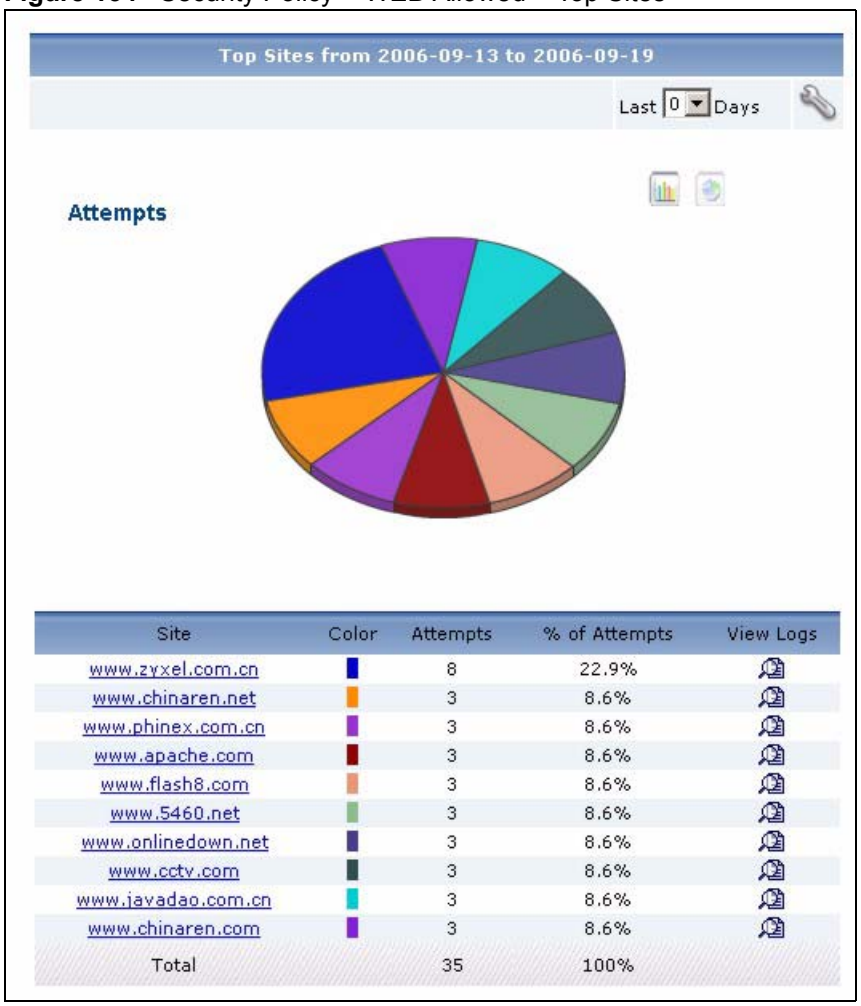
8.4.3 Top Allowed Web Sites

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

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 134 Security Policy > WEB Allowed > Top Sites



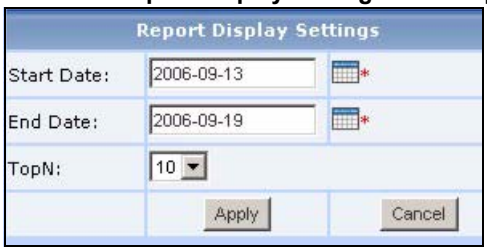
Site	Color	Attempts	% of Attempts	View Logs
www.zyxel.com.cn		8	22.9%	
www.chinaren.net		3	8.6%	
www.phinex.com.cn		3	8.6%	
www.apache.com		3	8.6%	
www.flash8.com		3	8.6%	
www.5460.net		3	8.6%	
www.onlinedown.net		3	8.6%	
www.cctv.com		3	8.6%	
www.javadao.com.cn		3	8.6%	
www.chinaren.com		3	8.6%	
Total		35	100%	

Each field is described in the following table.

Table 128 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	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 128 Security Policy > WEB Allowed > Top Sites

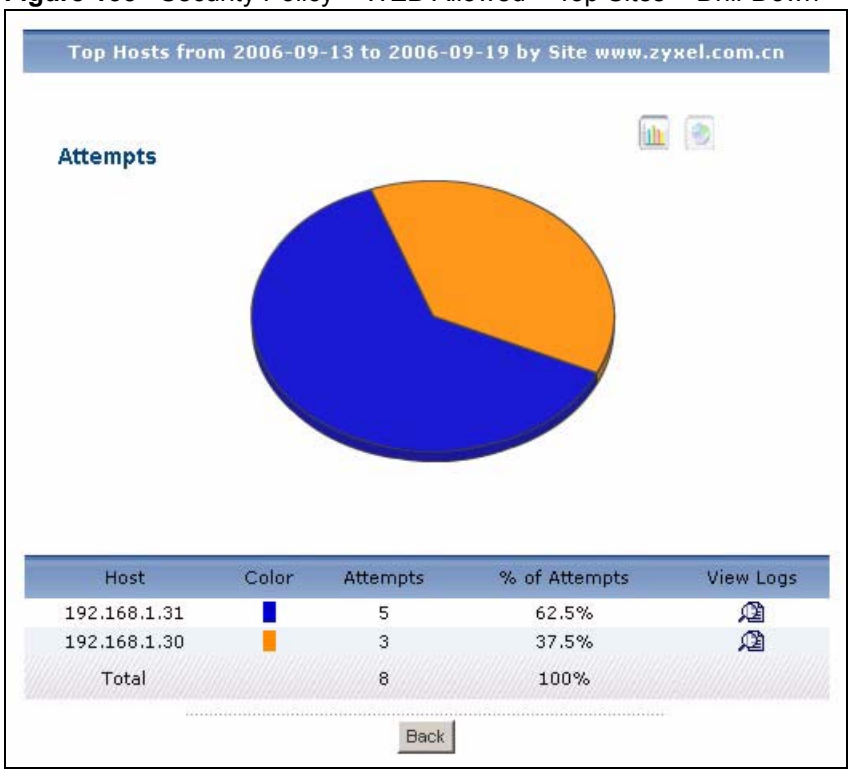
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of 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. 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.
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.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

8.4.4 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 135 Security Policy > WEB Allowed > Top Sites > Drill-Down



Each field is described in the following table.

Table 129 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of 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. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made by each source to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

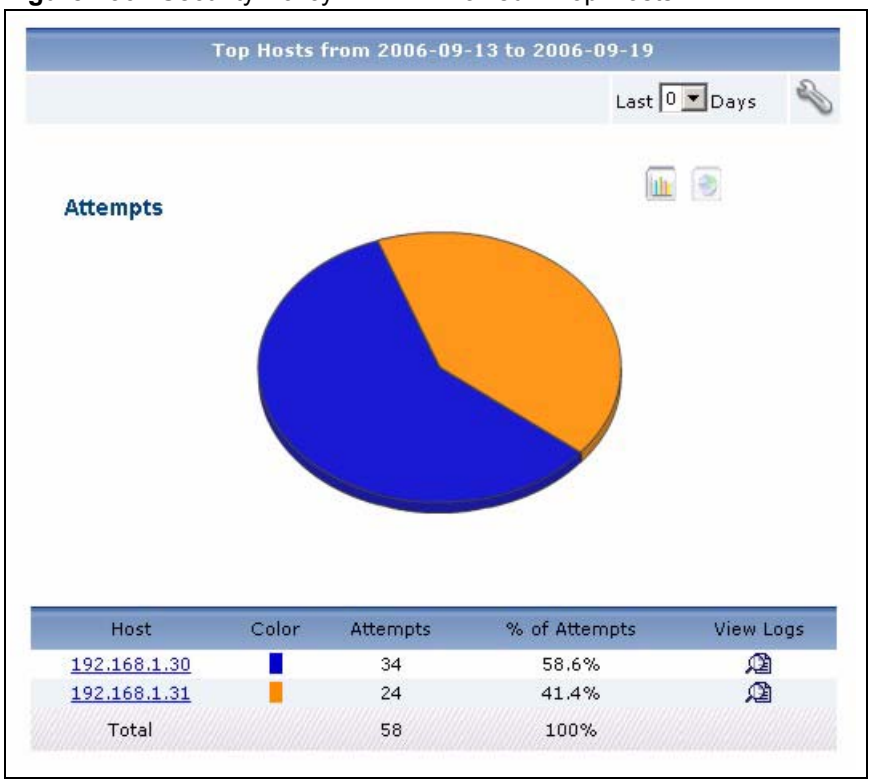
8.4.5 Top Allowed Web Hosts

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

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.

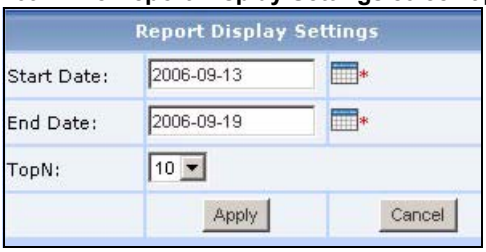
Click **Security Policy** > **WEB Allowed** > **Top Hosts** to open this screen.

Figure 136 Security Policy > WEB Allowed > Top Hosts



Each field is described in the following table.

Table 130 Security Policy > WEB Allowed > Top Hosts

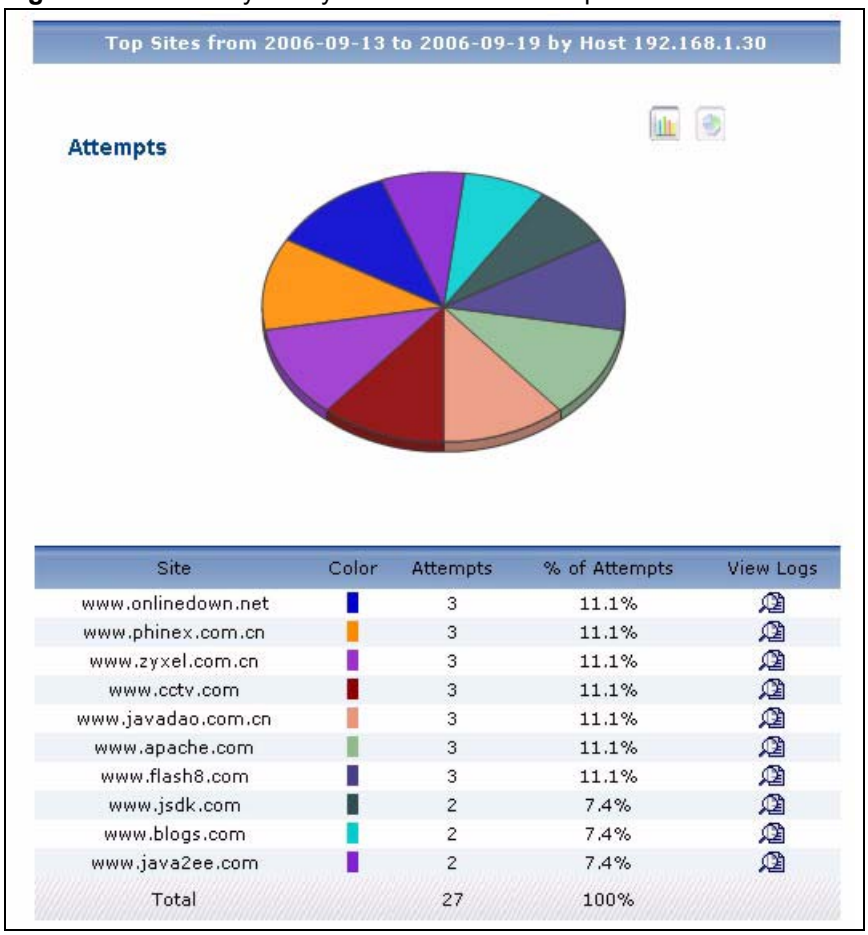
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of 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. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of forwarded web traffic for the selected source. The **Top Forwarded Web Hosts Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how times the device allowed each source to access web sites.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made from each sources.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.4.6 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 137 Security Policy > WEB Allowed > Top Hosts > Drill-Down



Each field is described in the following table.

Table 131 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. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of 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.

Table 131 Security Policy > WEB Allowed > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Attempts	This field displays the number of attempts from the selected source to each destination.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made by the selected source to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above. If the number of destinations of attempts from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

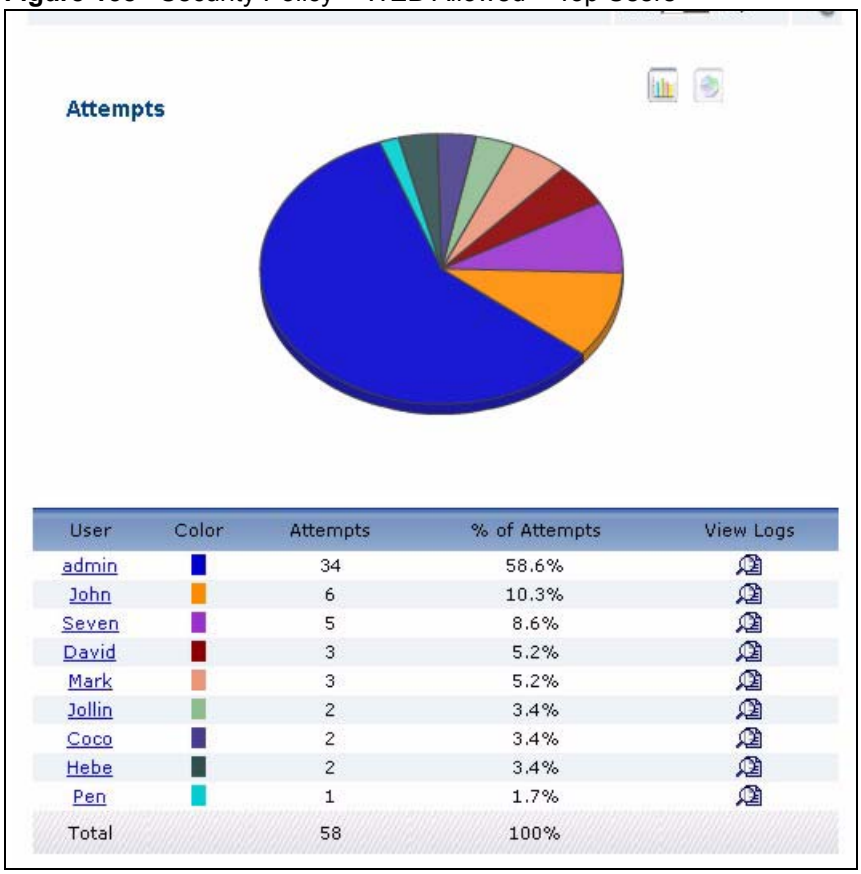
8.4.7 Top Allowed Web Users

Use this report to look at the top users for which the device forwarded web traffic.

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 Users** to open this screen.

Figure 138 Security Policy > WEB Allowed > Top Users

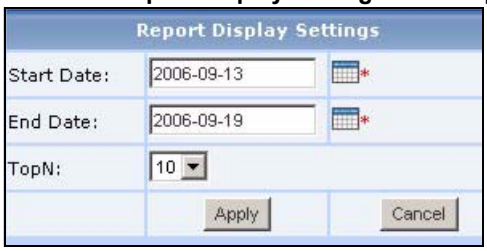


Each field is described in the following table.

Table 132 Security Policy > WEB Allowed > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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 132 Security Policy > WEB Allowed > Top Users

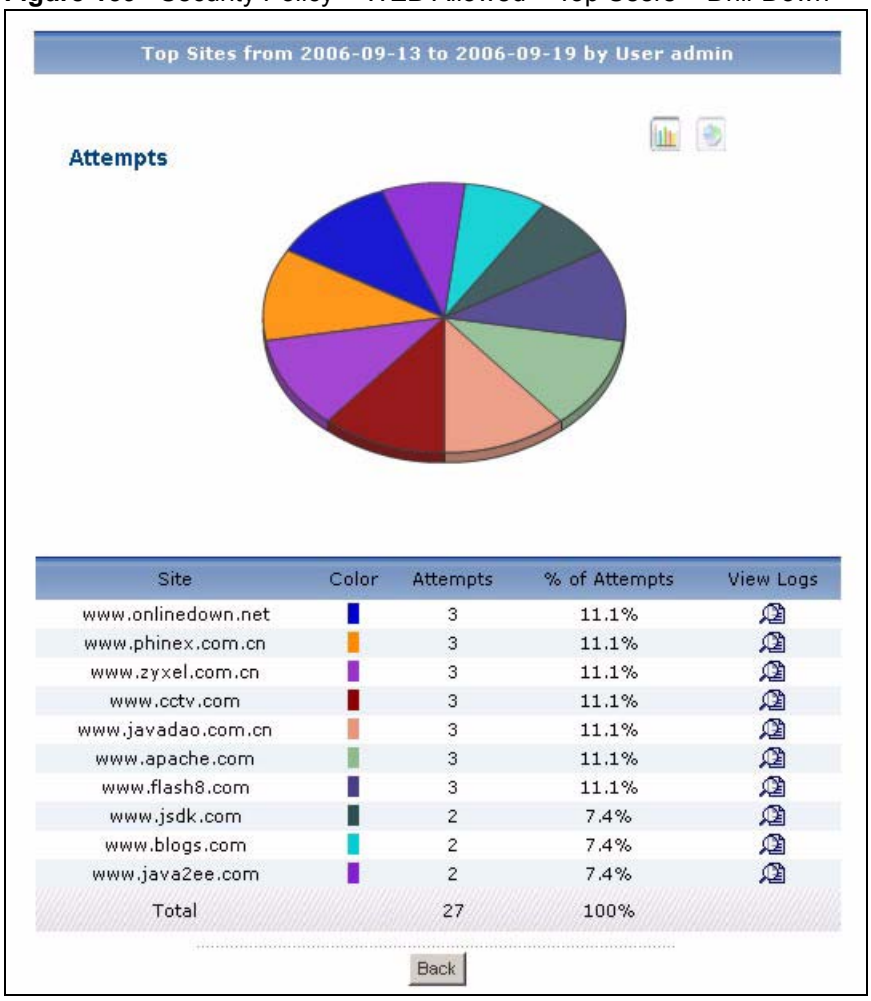
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users for which the device forwarded web traffic, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of forwarded web traffic for the selected user. The **Top Allowed Web Users Drill-Down** report appears.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how many times the device allowed each user to access web sites.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made by each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.4.8 Top Allowed Web Users 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 Users** to open this screen.

Figure 139 Security Policy > WEB Allowed > Top Users > Drill-Down



Each field is described in the following table.

Table 133 Security Policy > WEB Allowed > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of forwarded web traffic from the selected user, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected user to each destination.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made by the selected user to each destination.
View Logs	Click this icon to see the logs that go with the record.

Table 133 Security Policy > WEB Allowed > Top Users > Drill-Down

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

PART IV
Event, Log Viewer and Schedule Report

Event (287)
Log Viewer (295)
Schedule Report (299)

9

Event

Use these screens to look at who successfully logged into the ZyXEL device or who tried to log in but failed.

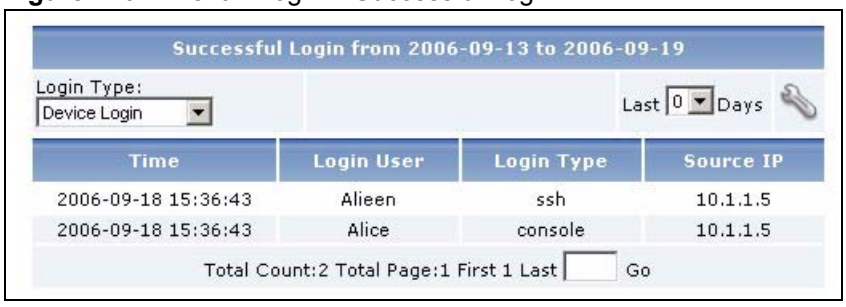
9.1 Successful Logins

Use this screen to look at who successfully logged into the ZyXEL device. See Section 2.4 on page 35 for more information about the source data used by the report.

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.

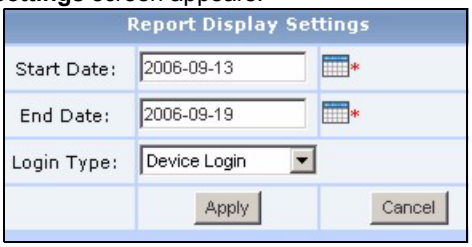
Click **Event** > **Login** > **Successful Login** to open the **Successful Login** screen.

Figure 140 Event > Login > Successful Login



Each field is described in the following table.

Table 134 Event > 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.
Login Type	Select **Device Login** to display a list of successful management logins to the ZyXEL device. Select **UserAware Login** to display a list of successful user logins to the ZyXEL device (to use the ZyXEL device's features such as Internet access or VPN tunnels). This field is not available with all models.
Last ... Days	Select how many more days of information, ending with current information today, you want to look at. Select **0** or **1** if you only want to look at today's information.
Settings	Click this if you want to specify the select any **Start Date** and **End Date**. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Login Type** field is the same as in the main screen. These fields reset to the default values when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user logged into the device.
Login User	This field displays who logged into the selected device.
Login Type	This field displays what type of connection the user used to log into the device.
Source IP	This field displays the IP address of the computer the user used to log into the selected device.
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**.

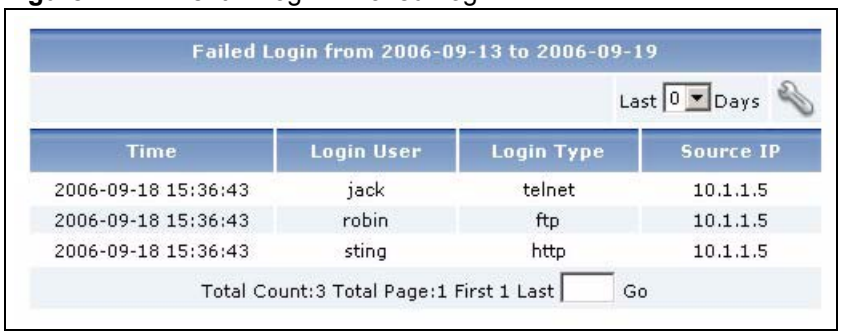
9.2 Failed Logins

Use this screen to look at who tried to log in into the ZyXEL device (for management or monitoring purposes) but failed. See Section 2.4 on page 35 for more information about the source data used by the report.

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 > Login > Failed Login** to open the **Failed Login** screen.

Figure 141 Event > Login > Failed Login



Each field is described in the following table.

Table 135 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** or **1** if you only want to look at today's information.
Settings	Click this if you want to specify the select any **Start Date** and **End Date**. The **Report Display Settings** screen appears.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user tried unsuccessfully to log into the device.
Login User	This field displays who tried unsuccessfully to log into the selected device.
Login Type	This field displays what type of connection the user unsuccessfully tried to use to log into the device.
Source IP	This field displays the IP address of the computer the user used to try to log into the selected device.
Total Count	This field displays how many records there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the records.
First .. Last	Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click **Go**.

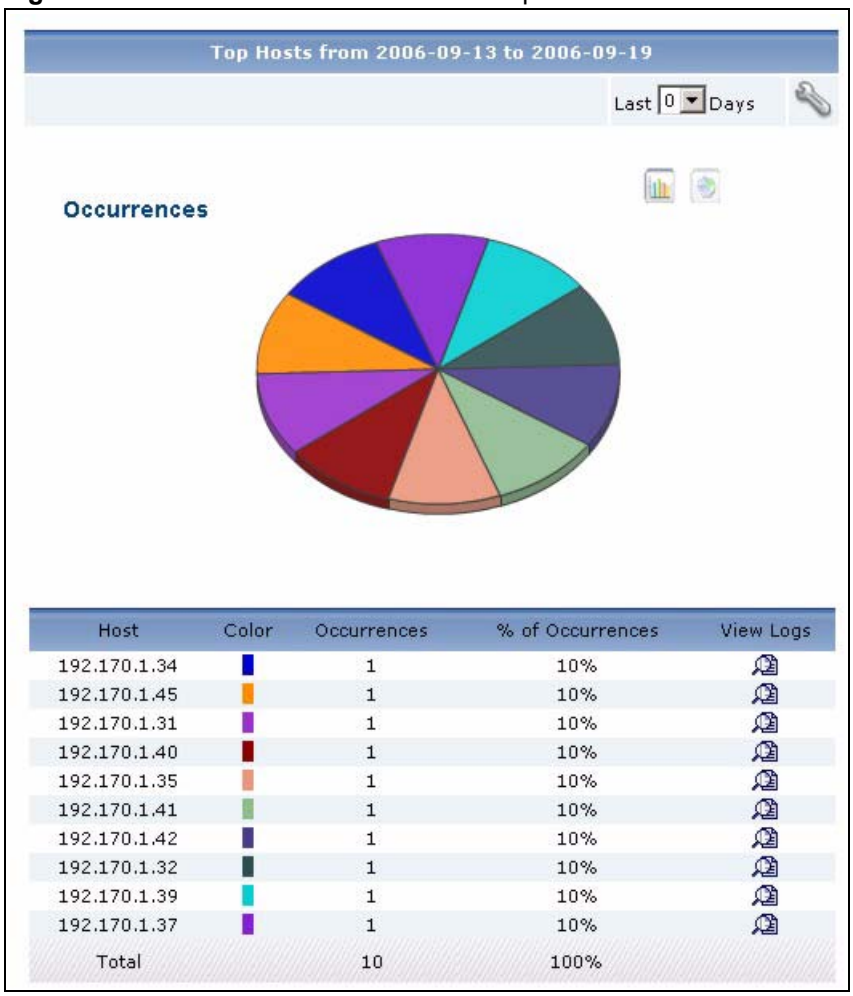
9.3 Top Sessions Per Host

Use this screen to see which hosts have most frequently gone over the maximum number of NAT sessions per host.

To use this screen, the ZyXEL device must record instances of hosts exceeding the maximum number of NAT sessions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **System Maintenance** is enabled.

Click **Event** > **Session Per Host** > **Top Hosts** to open this screen.

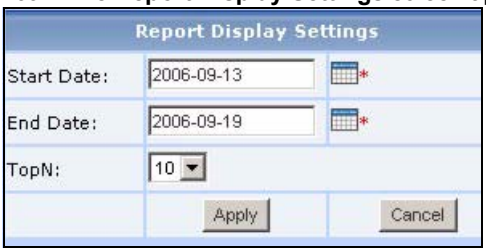
Figure 142 Event > Session Per Host > Top Hosts



Host	Color	Occurrences	% of Occurrences	View Logs
192.170.1.34		1	10%	
192.170.1.45		1	10%	
192.170.1.31		1	10%	
192.170.1.40		1	10%	
192.170.1.35		1	10%	
192.170.1.41		1	10%	
192.170.1.42		1	10%	
192.170.1.32		1	10%	
192.170.1.39		1	10%	
192.170.1.37		1	10%	
Total		10	100%	

Each field is described in the following table.

Table 136 Event > Session Per Host > 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources that have gone over the selected device's maximum number of NAT sessions per host, sorted by the number of occurrences for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of times each source has gone over the selected device's maximum number of NAT sessions per host.
% of Occurrences	This field displays what percentage each source's number of times it has exceeded the selected device's maximum number of NAT sessions per host makes out of the total number of times that it has occurred within the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

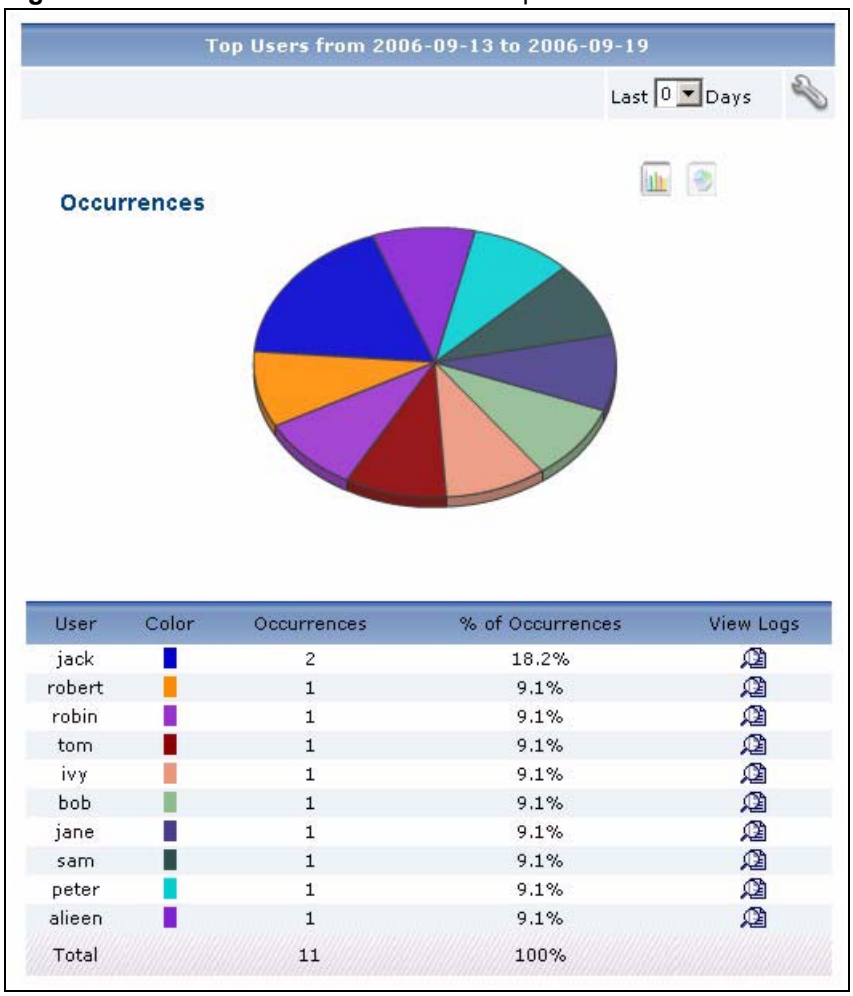
9.4 Top Sessions Per User

Use this screen to see which users have most frequently gone over the maximum number of NAT sessions per host.

To use this screen, the ZyXEL device must record instances of users exceeding the maximum number of NAT sessions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **System Maintenance** is enabled.

Click **Event > Session Per Host > Top Users** to open this screen.

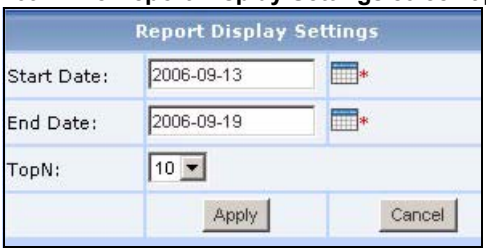
Figure 143 Event > Session Per Host > Top Users



User	Color	Occurrences	% of Occurrences	View Logs
jack		2	18.2%	
robert		1	9.1%	
robin		1	9.1%	
tom		1	9.1%	
ivy		1	9.1%	
bob		1	9.1%	
jane		1	9.1%	
sam		1	9.1%	
peter		1	9.1%	
alieen		1	9.1%	
Total		11	100%	

Each field is described in the following table.

Table 137 Event > Session Per Host > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. These fields reset to the default values 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.
graph	The graph displays the information in the table visually. • Click the pie view or the bar view icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users that have gone over the selected device's maximum number of NAT sessions per host, sorted by the number of occurrences for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Occurrences	This field displays the number of times each user has gone over the selected device's maximum number of NAT sessions per host.
% of Occurrences	This field displays what percentage each user's number of times it has exceeded the selected device's maximum number of NAT sessions per host makes out of the total number of times that it has occurred within the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

10

Log Viewer

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

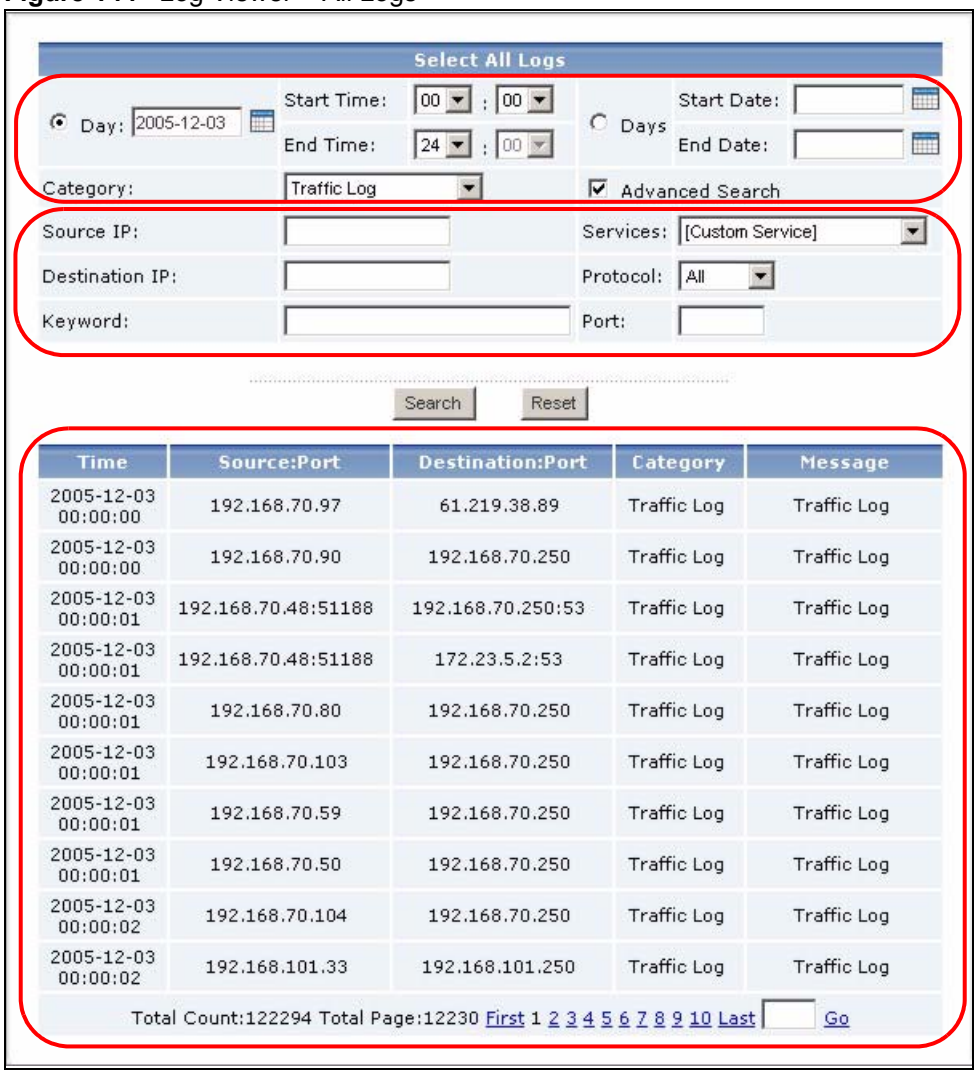
10.1 Log Viewer

Use this screen to view logs that the devices send to Vantage Report.

Click **Log Viewer** > **All Logs** to look at all log entries. The screen is shown next. See Section 2.3 on page 34 for more information about update frequencies for log entries. See Section 2.4 on page 35 for more information about the source data used by the report.

Vantage Report consolidates log entries. See Appendix A on page 339 for Vantage Report's internal log consolidation frequency. See Appendix C on page 351 and Appendix D on page 375 for information on the logs.

Figure 144 Log Viewer > All Logs



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 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 138 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.
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.

Table 138 Log Viewer > All Logs

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

11

Schedule Report

Use the summary 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 34 for more information about e-mail in Vantage Report. Use the template screens to add and edit report templates.

11.1 Scheduled Report Summary Screen

To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 12.2 on page 322 for more information.

Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves three days of information, weekly reports only consist of information from these three days, not seven days. See Section 12.1 on page 317 for more information.

This feature can send e-mail messages with very large attachments (2+ MB). Some SMTP mail servers might not accept such large messages. In this case, there is a way to send e-mail messages without the attachments. See the **E-mail Attached Files** option in any of the **Customize ... Report** screens for more information. If you do not have Vantage Report send the attachments you can still view the reports. The Vantage Report server backs up all scheduled reports in the <vrpt_home>\vrpt\data\scheduler folder.

Click **Schedule Report** > **Summary** to open the **Schedule Report Summary** screen.

This screen lists the existing scheduled reports. Use the **Add** buttons to create new reports.

Figure 145 Schedule Report > Summary

Each field is described in the following table.

Table 139 Schedule Report > Summary

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	
#	Select this check box, and click **Delete** to delete the scheduled report.
Index	Click it to edit the scheduled report next to it. The **Customize Scheduled Report** screen appears. Otherwise, this field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
To E-mail Address	This field displays the first e-mail address to which the scheduled report is sent. If there are more, this field displays a couple of punctuation marks at the end.
E-mail Subject	This field displays the subject line in the e-mail message Vantage Report sends.
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. It is recommended that you vary the times for your reports.
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.

Table 139 Schedule Report > Summary

LABEL	DESCRIPTION
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**.

11.2 Customize Daily Report Screen

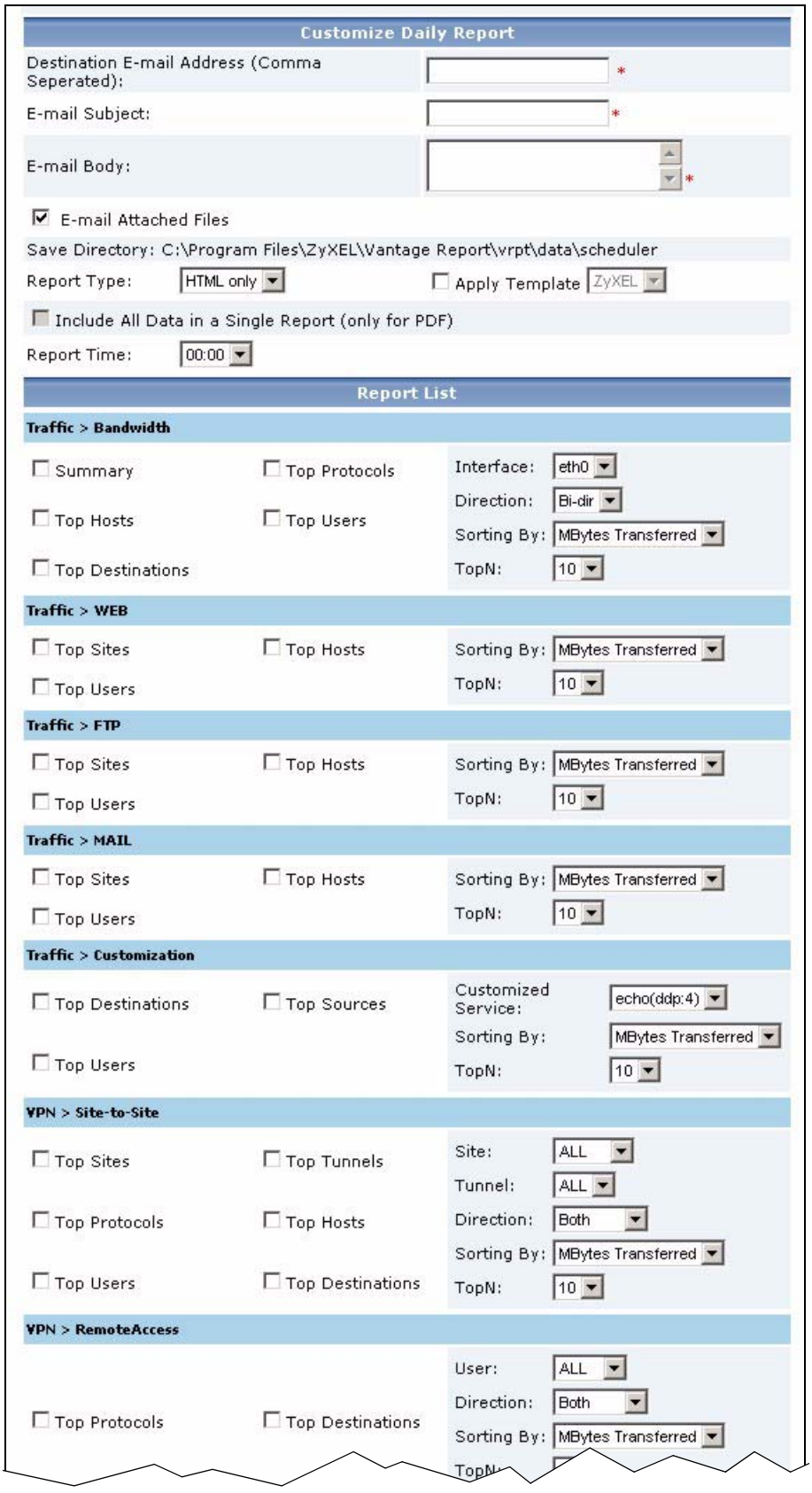
To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 12.2 on page 322 for more information.

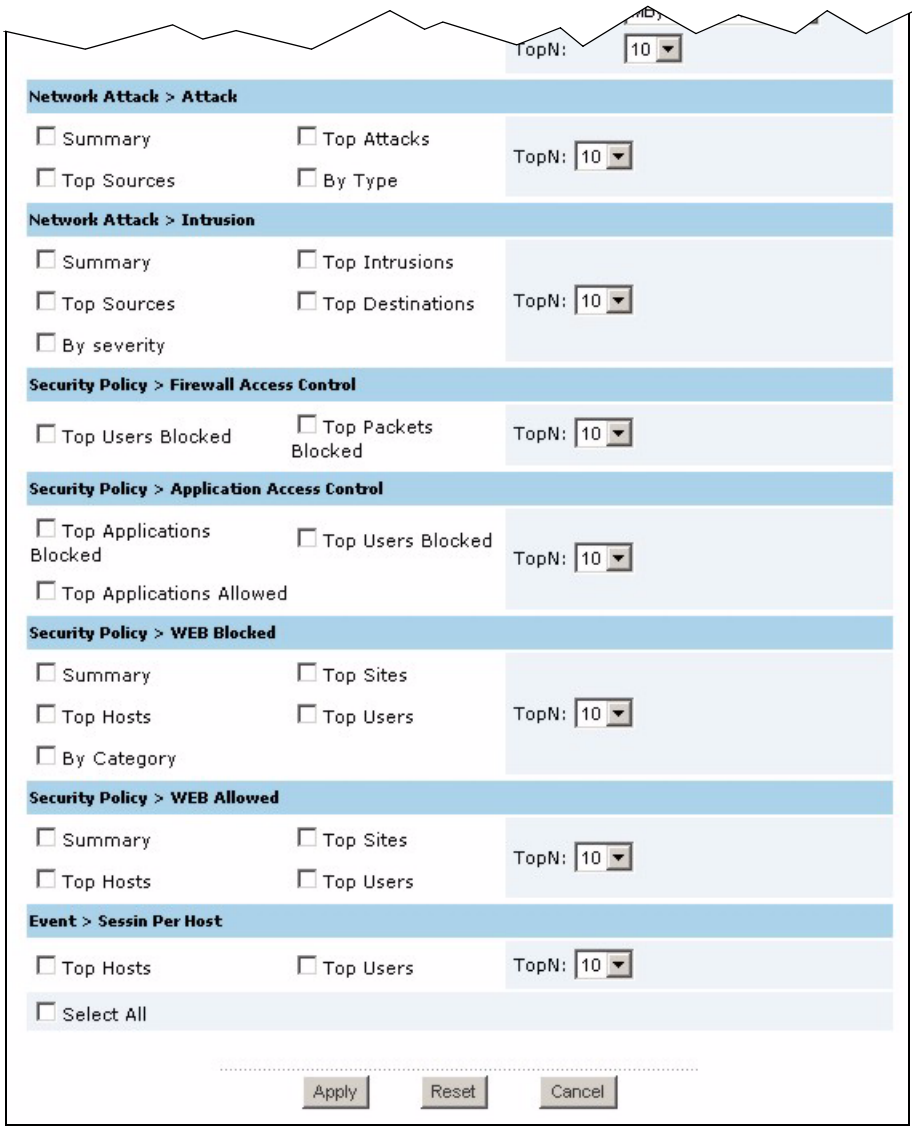
Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves three days of information, weekly reports only consist of information from these three days, not seven days. See Section 12.1 on page 317 for more information.

This feature can send e-mail messages with very large attachments (2+ MB). Some SMTP mail servers might not accept such large messages. In this case, there is a way to send e-mail messages without the attachments. See the **E-mail Attached Files** option in any of the **Customize ... Report** screens for more information. If you do not have Vantage Report send the attachments you can still view the reports. The Vantage Report server backs up all scheduled reports in the <vrpt_home>\vrpt\data\scheduler folder.

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

Figure 146 Schedule Report > Summary > Add (Daily Report))





Each field is described in the following table.

Table 140 Schedule Report > Summary > 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.

Table 140 Schedule Report > Summary > Add (Daily Report)

LABEL	DESCRIPTION
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 `data\schedule` 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.
Apply Template	Select the check box and a template if you want to use a customized report format.
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 Time	Select the hour to start generating the report. Vantage Report sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having Vantage Report generate too many reports at the same time can affect performance. It is recommended that you vary the times for your reports.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report.
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.

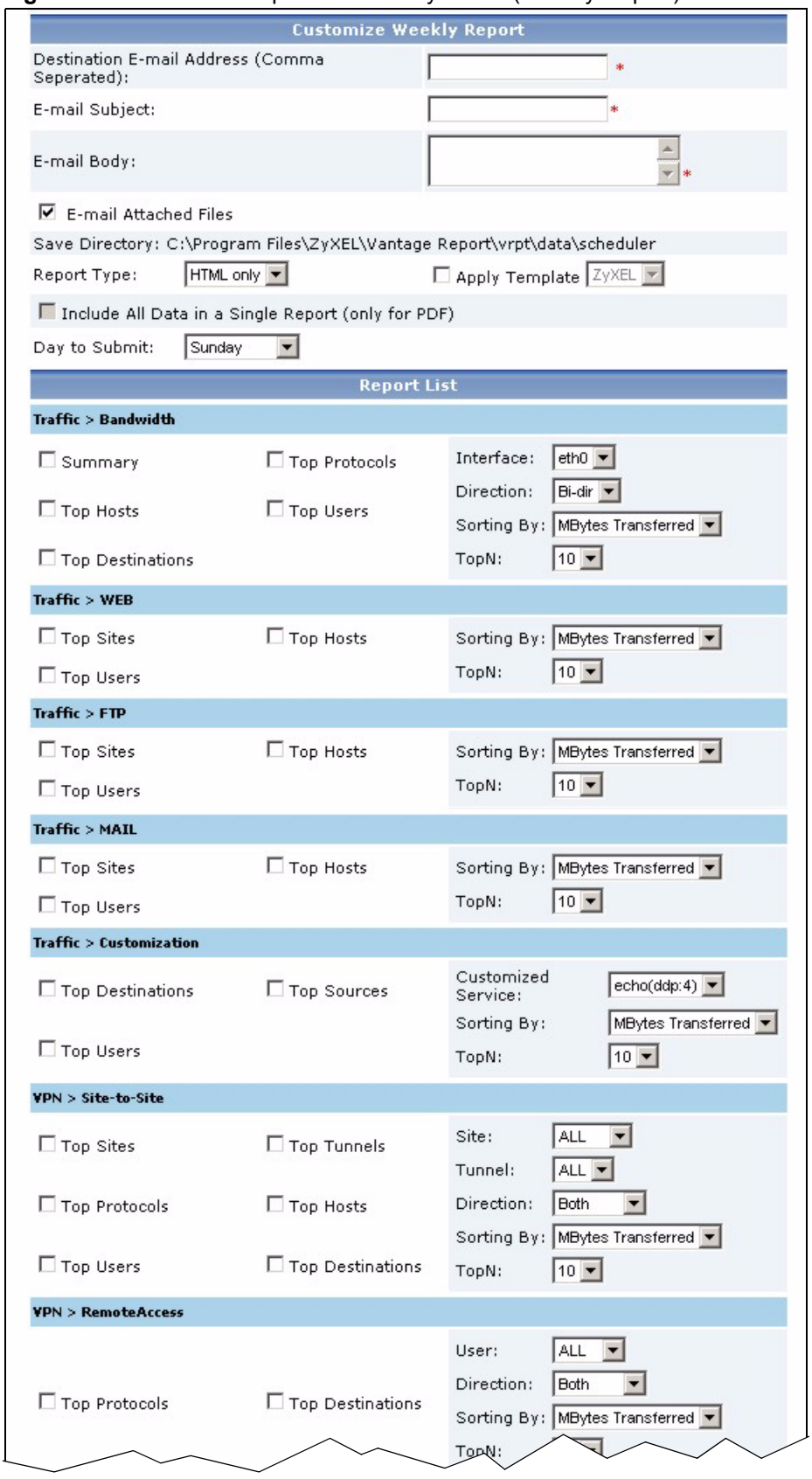
11.3 Customize Weekly Report Screen

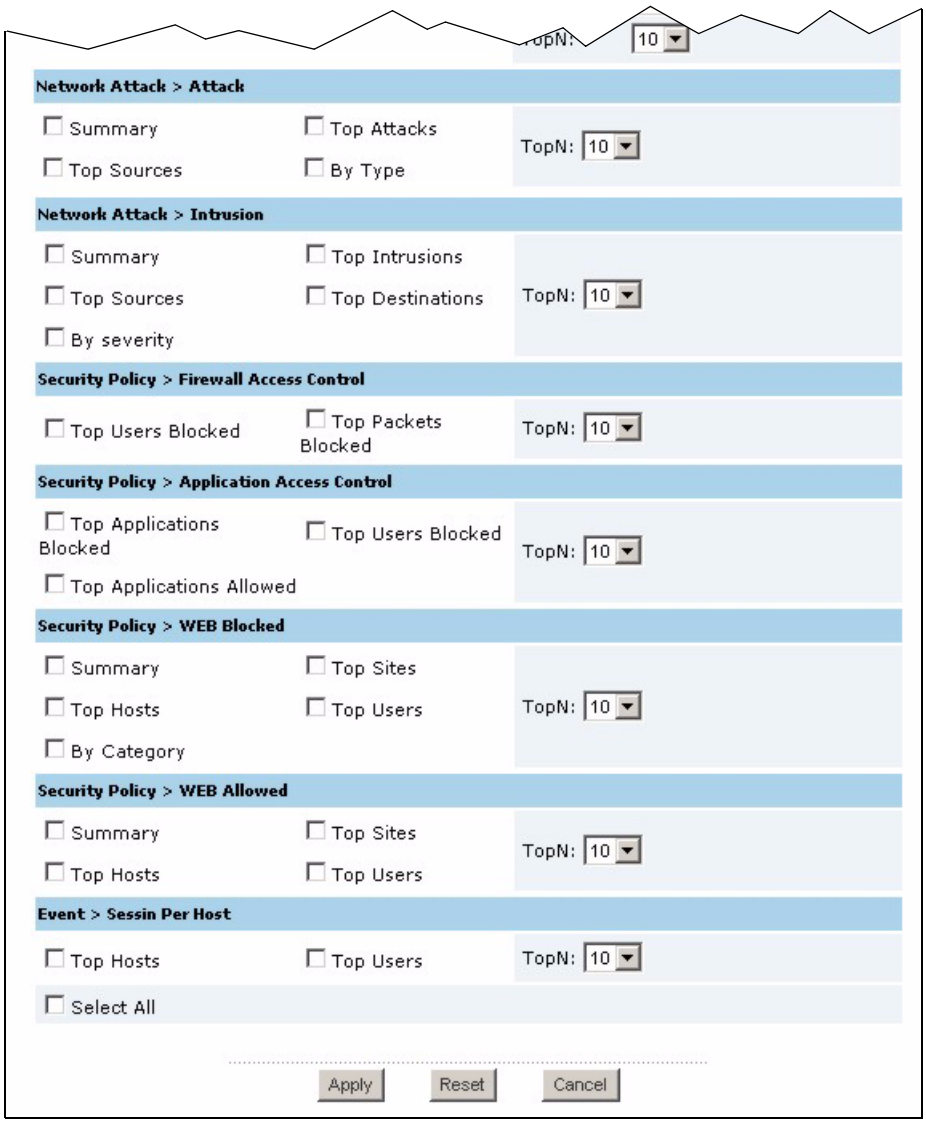
To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 12.2 on page 322 for more information.

Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves three days of information, weekly reports only consist of information from these three days, not seven days. See Section 12.1 on page 317 for more information.

This feature can send e-mail messages with very large attachments (2+ MB). Some SMTP mail servers might not accept such large messages. In this case, there is a way to send e-mail messages without the attachments. See the **E-mail Attached Files** option in any of the **Customize ... Report** screens for more information. If you do not have Vantage Report send the attachments you can still view the reports. The Vantage Report server backs up all scheduled reports in the <vrpt_home>\vrpt\data\scheduler folder.

Figure 147 Schedule Report > Summary > Add (Weekly Report)





Each field is described in the following table.

Table 141 Schedule Report > Summary > 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.

Table 141 Schedule Report > Summary > Add (Weekly Report)

LABEL	DESCRIPTION
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.
Apply Template	Select the check box and a template if you want to use a customized report format.
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).
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report.
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.

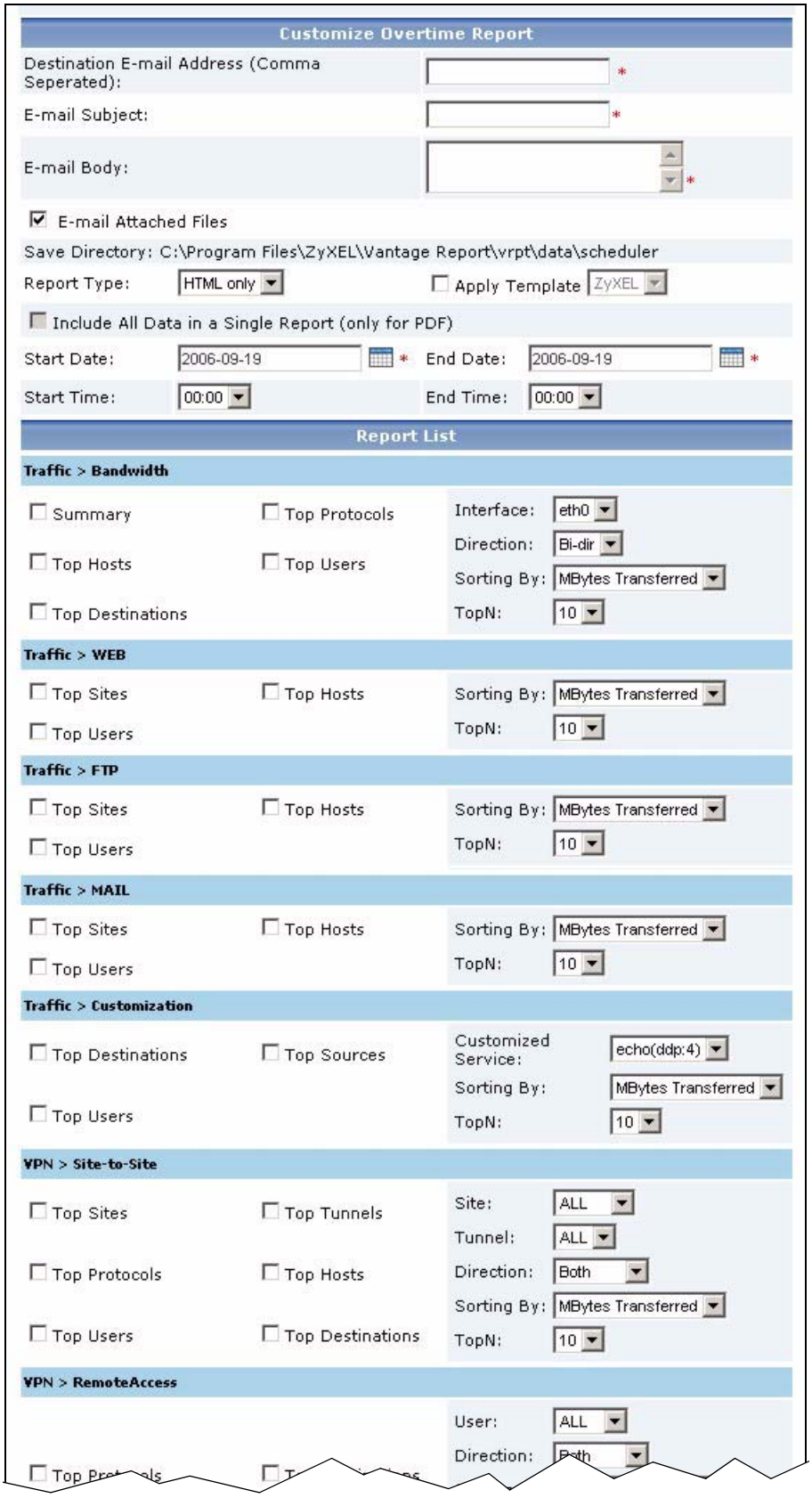
11.4 Customize Overtime Report Screen

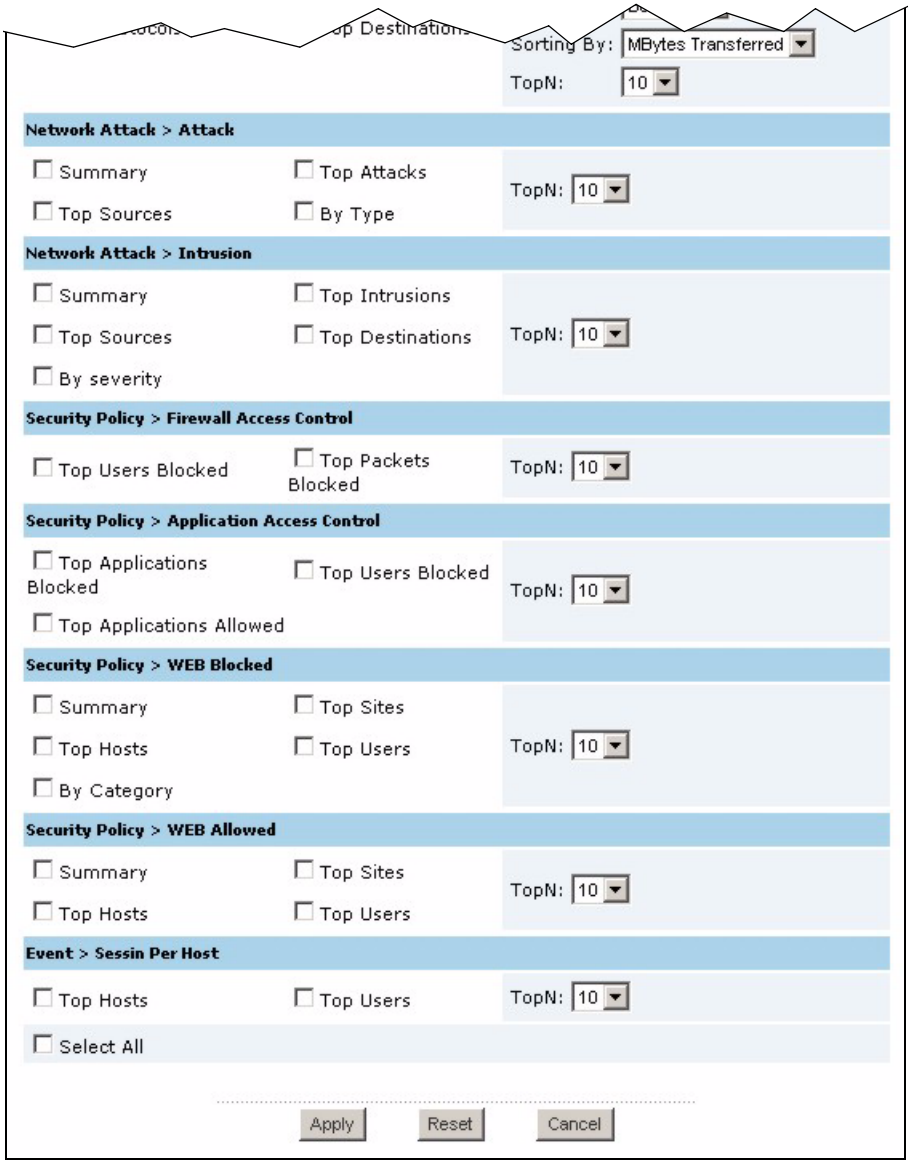
To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 12.2 on page 322 for more information.

Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves three days of information, weekly reports only consist of information from these three days, not seven days. See Section 12.1 on page 317 for more information.

This feature can send e-mail messages with very large attachments (2+ MB). Some SMTP mail servers might not accept such large messages. In this case, there is a way to send e-mail messages without the attachments. See the **E-mail Attached Files** option in any of the **Customize ... Report** screens for more information. If you do not have Vantage Report send the attachments you can still view the reports. The Vantage Report server backs up all scheduled reports in the <vrpt_home>\vrpt\data\scheduler folder.

Figure 148 Schedule Report > Summary > Add (Overtime Report)





Each field is described in the following table.

Table 142 Schedule Report > Summary > 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.

Table 142 Schedule Report > Summary > Add (Overtime Report)

LABEL	DESCRIPTION
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.
Apply Template	Select the check box and a template if you want to use a customized report format.
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).
End Date	Select the day to stop collecting information for the selected report(s).
Start Time	Select the hour to start collecting information for the selected report(s). Vantage Report starts collecting information at the beginning of this hour.
End Time	Select the hour to stop collecting information for the selected report(s). Vantage Report stops collecting information at the end of this hour and generates the report. Vantage Report sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having Vantage Report generate too many reports at the same time can affect performance.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report.
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.

11.5 Template List

Click **Schedule Report** > **Template** to open the **Schedule Report Template List** screen.

This screen lists the existing report templates.

Figure 149 Schedule Report > Template

Each field is described in the following table.

Table 143 Schedule Report > Template

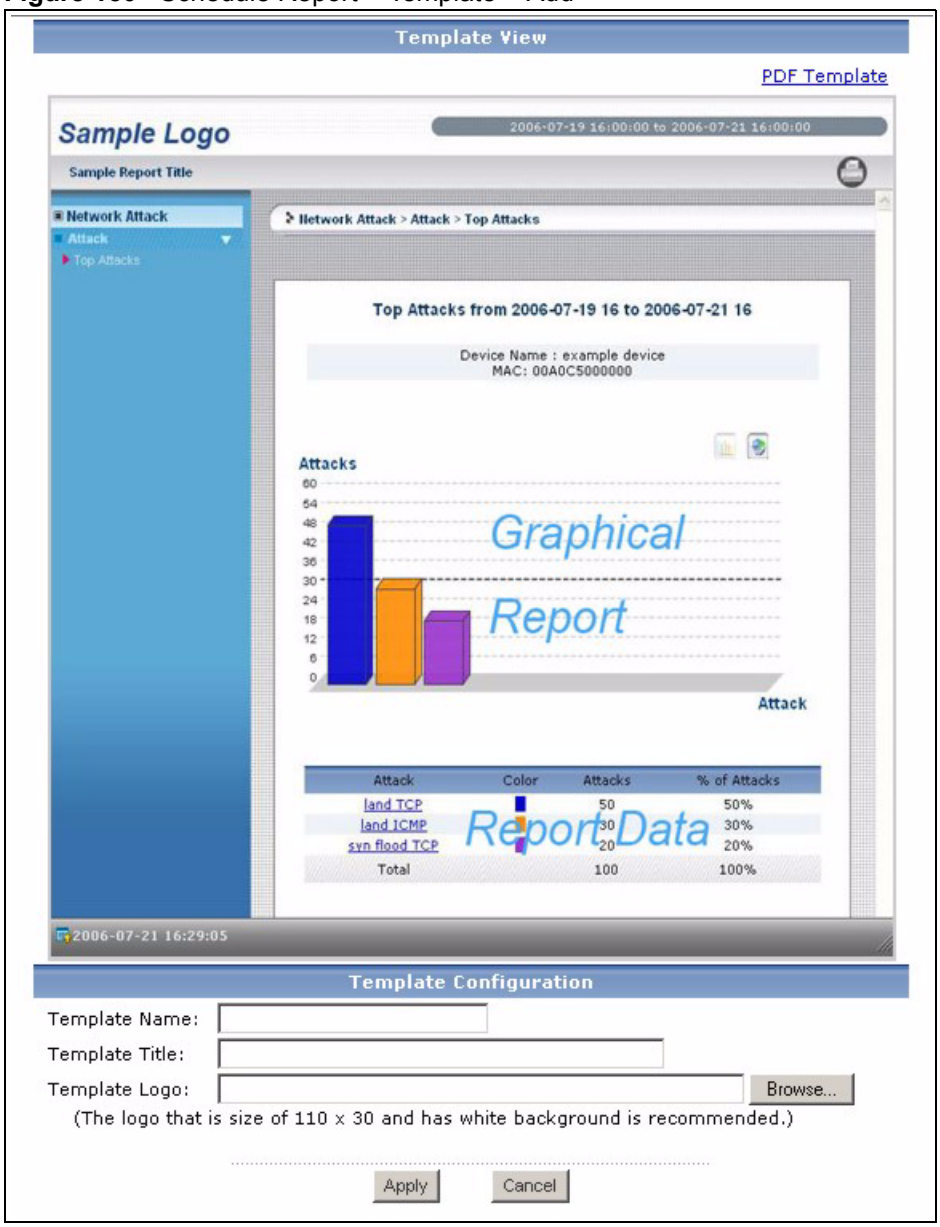
LABEL	DESCRIPTION
#	Select this check box, and click **Delete** to delete the report template.
Index	This is the number of this template in the list. This field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
Template Name	This is the name that identifies the template inside Vantage Report. Click it to edit the template.
Template Title	This field displays the title that appears at the top of the reports generated using this template.
Sample Report	Click the **Download** button to save a sample file using the report template to your computer.
Total Count	This field displays how many report templates there are.
Total Page	This field displays how many screens it takes to display all the scheduled reports.
First .. Last	Click **First**, **Last**, or a specific page number to look at the scheduled reports on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click **Go**.
Add	Click this to go to another screen to create a new report template.
Delete	Select the check box next to a template and click delete to remove the report template.

11.6 Template Add/Edit

To access this screen, click **Add** in the **Schedule Report** > **Template** screen.

This screen lists the existing report templates.

Figure 150 Schedule Report > Template > Add



Each field is described in the following table.

Table 144 Schedule Report > Template > Add

LABEL	DESCRIPTION
Template View	This section of the screen displays a sample of the report layout.
PDF Template	Click this button to view a sample of a report in PDF format.
HTML Template	Click this button to view a sample of a report in HTML format.
Template Configuration	Use this section of the screen to configure the template's name and the report title and upload a logo to display on the reports.
Template Name	Enter a name to identify the template inside Vantage Report. Numbers (0-9), letters (a-zA-Z), periods (.) and the underscore (_) are allowed. Spaces are not allowed. The name must start with a number or letter. Use up to 28 characters.

Table 144 Schedule Report > Template > Add

LABEL	DESCRIPTION
Template Title	Enter the title that you want to appear at the top of the reports generated using this template. Use up to 50 ASCII characters. Spaces are allowed.
Template Logo	Type the location of the file that you want to display as the logo in the report or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. The template logo file must be .gif or .jpg.
Apply	Click this to save your settings and close the screen.
Cancel	Click this to close the screen without saving any changes.

PART V
System and Troubleshooting

System (317)
Troubleshooting (335)

12 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 full version, or increase the number of devices Vantage Report supports.
- Monitor the number of logs received by time or by device.
- Get basic information about Vantage Report

Other users can use the system screens to

- Edit their user account settings, including the password
- Get basic information about Vantage Report

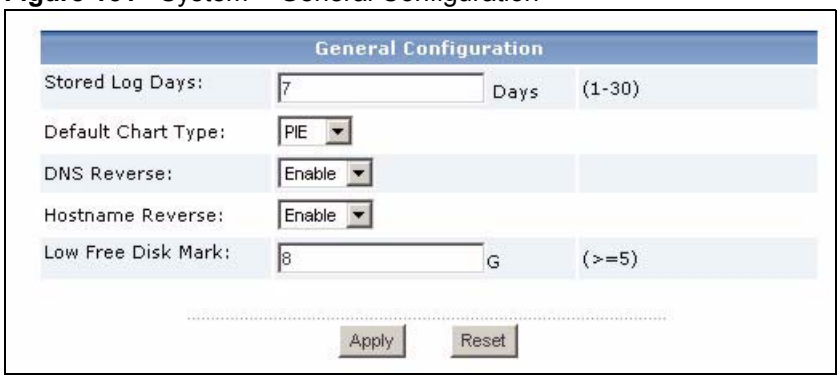
12.1 General Configuration Screen

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 151 System > General Configuration



Each field is described in the following table.

Table 145 System > General Configuration

LABEL	DESCRIPTION
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. When Vantage Report deletes data older than the time specified in this field, the raw data (raw logs) is exported as a CSV file (.csv) and compressed into a .zip file. These .zip files are stored in `<Vantage Report installation directory>\data\backup\csv`.
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.
Hostname Reverse	Select **Enable** if you want Vantage Report to display the host names for local computers instead of IP addresses. It has no effect in **Log Viewer**. In hostname reverse lookups, Vantage Report looks for the host name associated with local IP addresses that it displays. If Vantage Report finds the host name, it displays the host name and the IP address in the field. If it does not find the host name, it only displays the IP address. This feature might increase the amount of time it takes to display statistical reports, however. You also need to configure the host computers and ZyXEL device (see Section 12.1.1 on page 318).
Low Free Disk Mark	When the amount of available disk space falls below this number of gigabytes, Vantage Report sends a notification to the e-mail address (if any) for the **root** user account.
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.

12.1.1 Configuring for Hostname Reverse

Besides enabling hostname Do the following to allow the hostname reverse function to work.

- Turn on hostname reverse in Vantage Report.

- Enable the default NetBIOS setting in the host computers.
- Configure any software firewalls installed on the host computers to allow NetBIOS packets from the Vantage server.
- Set the ZyXEL device to allow NetBIOS traffic between interfaces. You need to configure both the individual interface screens (like LAN, WAN, DMZ) and the firewall to allow NetBIOS packets from the Vantage server.

12.1.1.1 Enabling the Default NetBIOS Setting in Host Computers

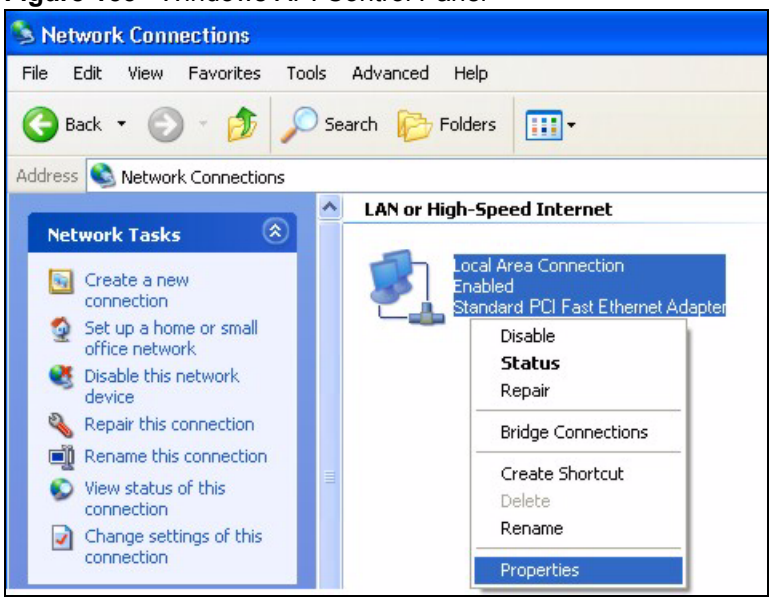
The following procedure gives an example of how to enable the default NetBIOS settings in host computers using Windows 2000, NT or XP.

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

Figure 152 Windows XP: Start Menu

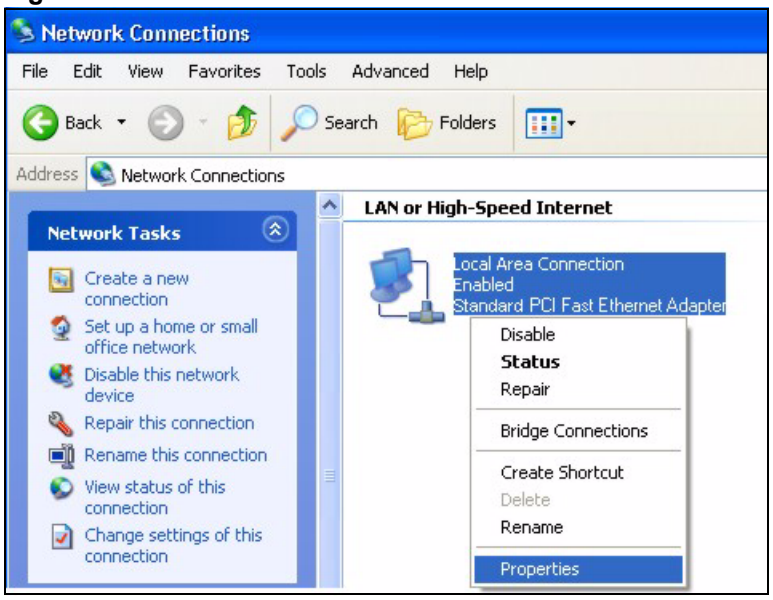
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 153 Windows XP: Control Panel



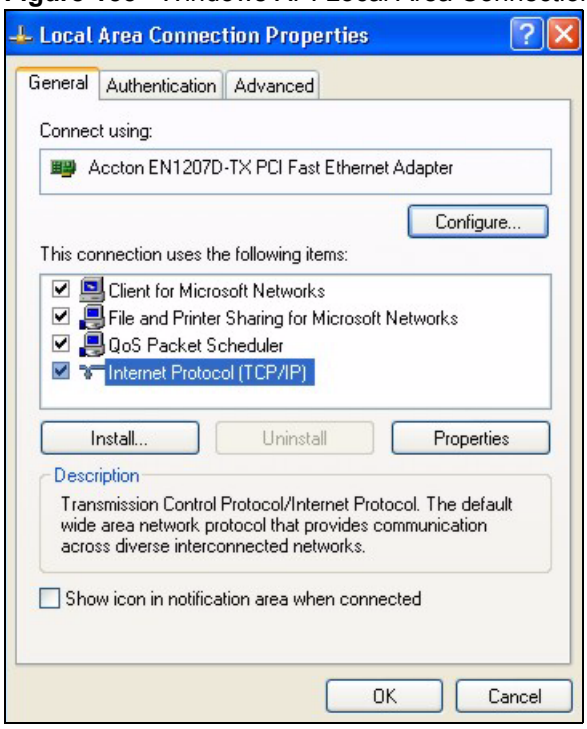
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 154 Windows XP: Control Panel: Network Connections: Properties



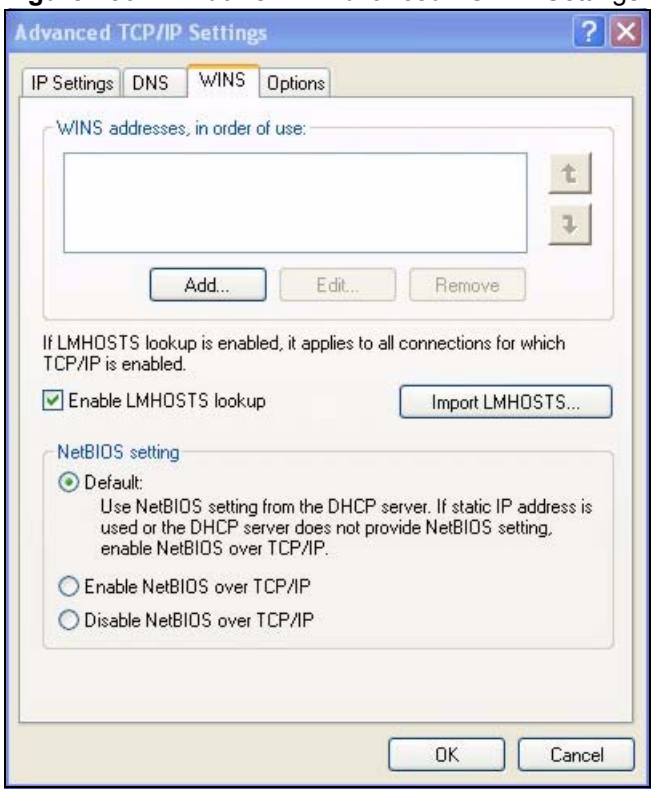
4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 155 Windows XP: Local Area Connection Properties



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

Figure 156 Windows XP: Advanced TCP/IP Settings: WINS



6 Select the **Default** NetBIOS setting and click **OK**.

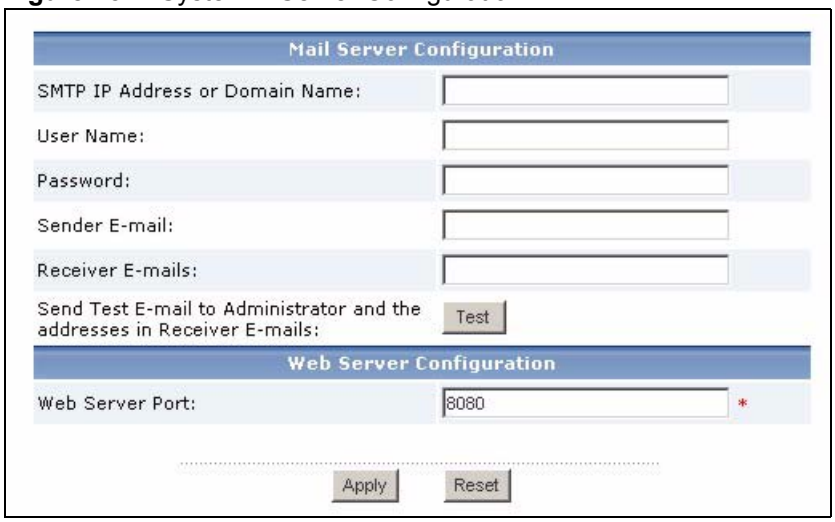
7 Click **OK** to close the **Local Area Connection Properties** window.
8 Turn on your ZyXEL device and restart your computer (if prompted).

12.2 Server Configuration Screen

Only the `root` account can open this screen.

Use the **Server Configuration** screen to set up mail server and web server configuration for Vantage Report. See Section 2.2 on page 34 for more information. Click **System** > **Server Configuration** to open the **Server Configuration** screen.

Figure 157 System > Server Configuration



Each field is described in the following table.

Table 146 System > Server Configuration

LABEL	DESCRIPTION
Mail Server Configuration	Use this part of the screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports.
SMTP IP Address or Domain Name	Enter the IP address or domain name of the SMTP mail server on which Vantage Report has an account to send e-mail messages.
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.
Receiver E-mails	Enter the e-mail address you want to be the receiver when Vantage Report sends e-mail. This is the e-mail address to which Vantage Report e-mail appears to be sent.

Table 146 System > Server Configuration

LABEL	DESCRIPTION
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 **root** user account.
Web Server Configuration	Use this part of the screen to configure the port number Vantage Report uses for web services.
Web Server Port	Enter the port number you want Vantage Report to use for web services. Make sure this port number does not conflict with other services in your network.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.

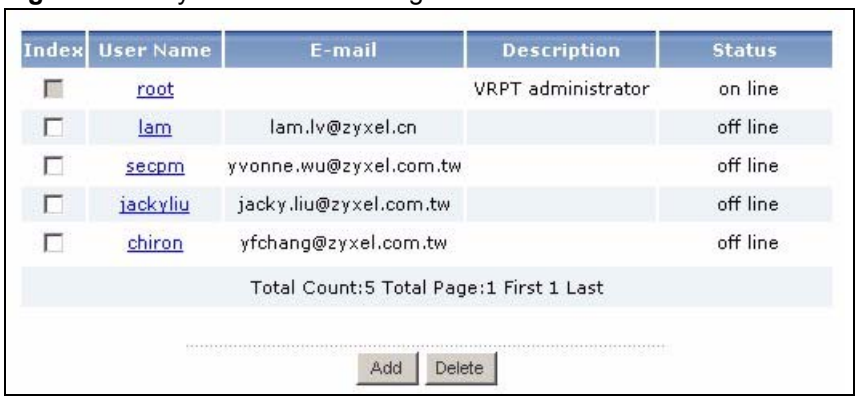
12.3 User Management Screens

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.

12.3.1 User Management Summary Screen

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

Figure 158 System > User Management



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

Table 147 System > User Management

LABEL	DESCRIPTION
Index	Select the check box next to a user account, and click **Delete** to remove the account. This does not apply to the **root** account since you cannot delete it.
User Name	This field displays the user name used to log in. You can also click this to edit the account settings. The **Add/Edit User Account** screen appears.
E-mail	This field displays the e-mail address associated with the user account. This address is used for notifications (**root** only) and forgotten passwords.

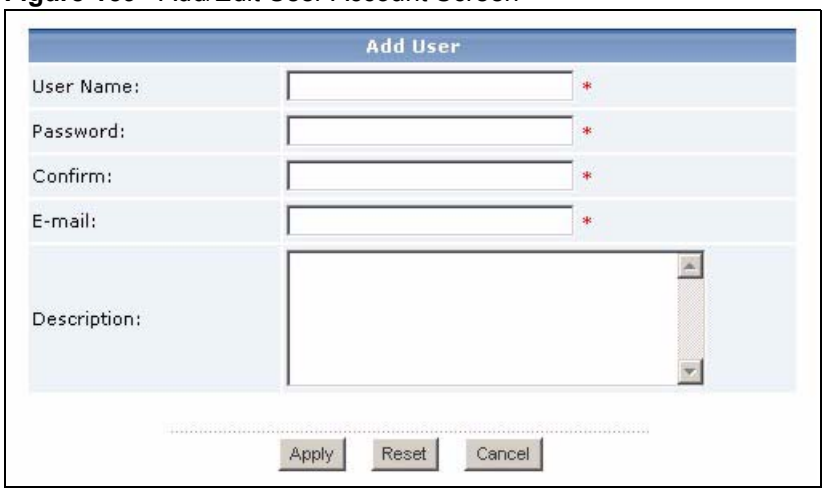
Table 147 System > User Management

LABEL	DESCRIPTION
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.

12.3.2 Add/Edit User Account Screen

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

Figure 159 Add/Edit User Account Screen



Each field is described in the following table.

Table 148 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 (**root** only) and forgotten passwords.

Table 148 Add/Edit User Account Screen

LABEL	DESCRIPTION
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.

12.4 Data Maintenance Screens

Only the `root` account can open these screens.

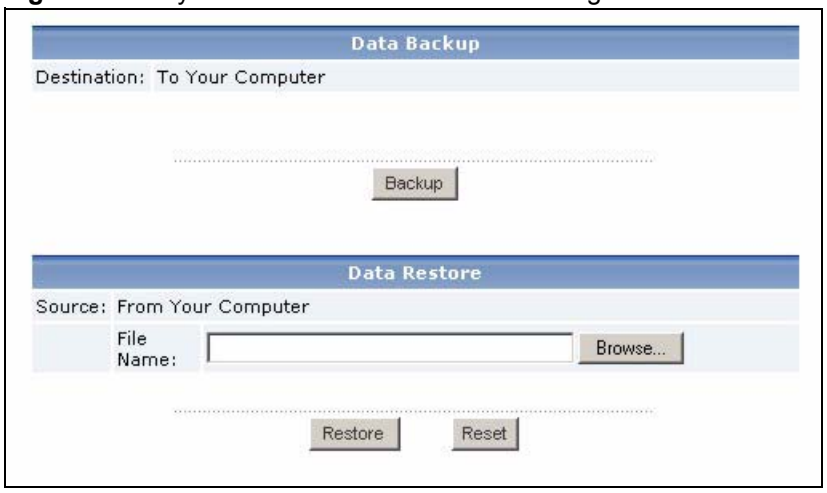
Use the data maintenance screens to backup the current configuration, restore a different configuration, export the device window, or import a different device window.

12.4.1 Data Backup and Data Restore Screen

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 Management** 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**.

Figure 160 System > Data Maintenance > Configuration



Each field is described in the following table.

Table 149 System > Data Maintenance > Configuration

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

12.4.2 Device List Export and Device List Import Screen

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**.

Figure 161 System > Data Maintenance > Device List

Each field is described in the following table.

Table 150 System > Data Maintenance > Device List

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.

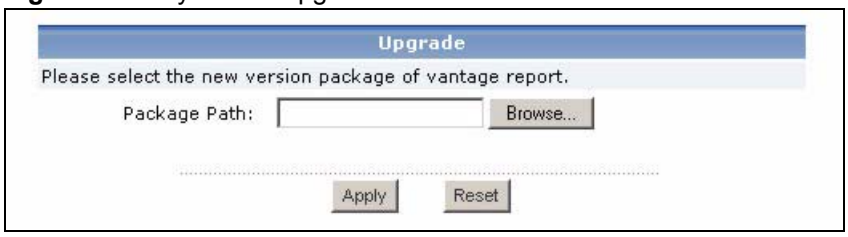
12.5 Upgrade Screen

Only the `root` account can open this screen.

Before you use this screen, read the documentation for the new release to make sure you understand the upgrade process.

Use this screen to install new releases of Vantage Report. Do not use this screen to upgrade to the full version. To access this screen, click **System** > **Upgrade**.

Figure 162 System > Upgrade



Each field is described in the following table.

Table 151 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.

12.6 Registration Screens

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 full version of Vantage Report; or
- increase the number of devices in Vantage Report.

Vantage Report uses myZyXEL.com for registration and activation. You have to use the registration screens to log into myZyXEL.com. You cannot log in to myZyXEL.com separately to register or activate Vantage Report.

The following information may be required for registration.

Table 152 Information for Using an Existing MyZyXEL.com Account

If you want to use an existing myZyXEL.com account, you need your ...
• myZyXEL.com user name • myZyXEL.com password

Table 153 Information for Upgrading the Version or Number of Devices

If you want to upgrade to the full version or increase the number of devices, you need your ...
• license key (iCard for the upgrade or increase)

12.6.1 Registration Summary Screen

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

Figure 163 System > Registration

The fields in this screen depend on what version (basic or full) of Vantage Report you have and whether or not you have used the registration screens to log into myZyXEL.com. All the fields are described in the following table.

Table 154 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 basic version.

Table 154 System > Registration

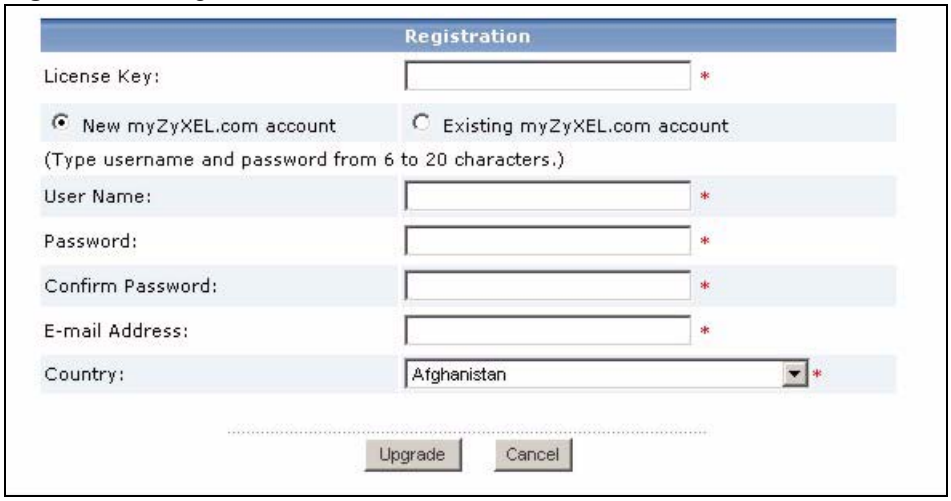
LABEL	DESCRIPTION
Supported Maximum Nodes	This field appears if you have the full version. It displays the maximum number of devices Vantage Report can currently support, regardless of the number of licenses you purchase. You can never increase the number of devices in Vantage Report higher than this value, regardless of how many licenses you have. In other words, this is the maximum value of **License Allowed Nodes**.
License Allowed Nodes	This field appears if you have the full version. It displays the number of devices you can add in Vantage Report based on your current license(s).
Used Nodes	This field appears if you have the full version. It displays the number of devices you currently have added in Vantage Report.
Refresh	Click this to update the information in this screen.
Trial	This field appears if you have the basic version and if you have not installed the trial version yet. Click this to get the trial version of Vantage Report. The **Registration** screen appears.
Upgrade	Click this to upgrade to the full version of Vantage Report or to increase the number of devices in Vantage Report. If you cannot upgrade Vantage Report further (in other words, if you can already add the maximum number of devices in Vantage Report), an error message is displayed. Otherwise, the **Registration** screen appears.

12.6.2 Registration Screen

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 164 Registration Screen



Some fields do not appear if you have already used this screen to log into myZyXEL.com, if you have a myZyXEL.com account, or if you are getting the trial version.The fields are described in the following table.

Table 155 Registration Screen

LABEL	DESCRIPTION
License Key	This field appears if you are upgrading to the full 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.
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 full version, or increase the number of devices in Vantage Report.
Cancel	Click this to return to the **Registration** summary screen without registering.

12.7 Log Receiver Screens

Only the `root` account can open these screens.

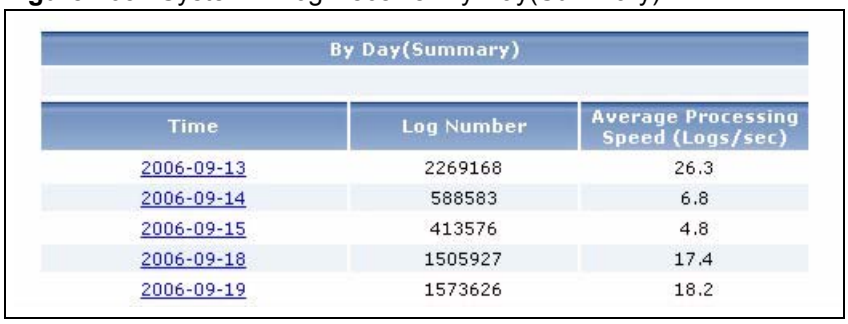
Use these screens to monitor the log receiver by time or by device.

12.7.1 Log Receiver By Day Screen

Use this screen to look at the total number of logs that Vantage Report received by day. It also displays how many logs Vantage Report processed per second (on average).

To access this screen, click **System** > **Log Receiver > By Day(Summary)**.

Figure 165 System > Log Receiver By Day(Summary)



All the fields are described in the following table.

Table 156 System > Log Receiver By Day(Summary)

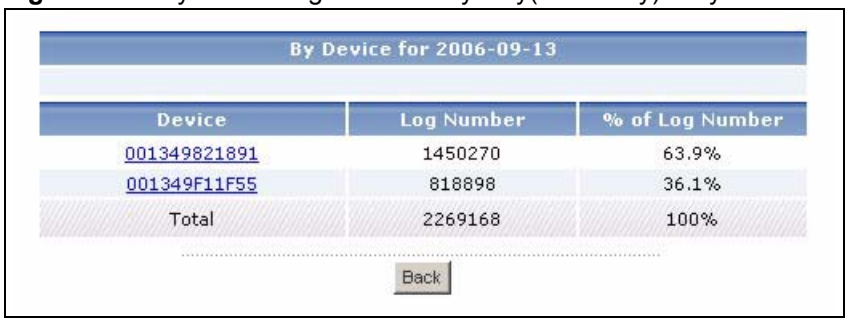
LABEL	DESCRIPTION
Time	This field displays the day for which the logs were collected. Click the date to go to a screen that lists how many logs were received from each device on that day.
Log Number	This field displays how many logs were received on each day.
Average Processing Speed (Logs/sec)	This field displays the average number of logs the Vantage Report server processed per second on each day.

12.7.2 Log Receiver By Day > By Device Screen

Use this screen to look at the total number of logs that Vantage Report received from each device on a particular day.

Click on the link in an entry in **System** > **Log Receiver > By Day(Summary)** to access this screen.

Figure 166 System > Log Receiver By Day(Summary) > By Device



All the fields are described in the following table.

Table 157 System > Log Receiver By Day(Summary) > By Device

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date you clicked in the summary screen.
Device	This field displays the MAC addresses of the devices that sent logs on the day you clicked. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected day.

Table 157 System > Log Receiver By Day(Summary) > By Device

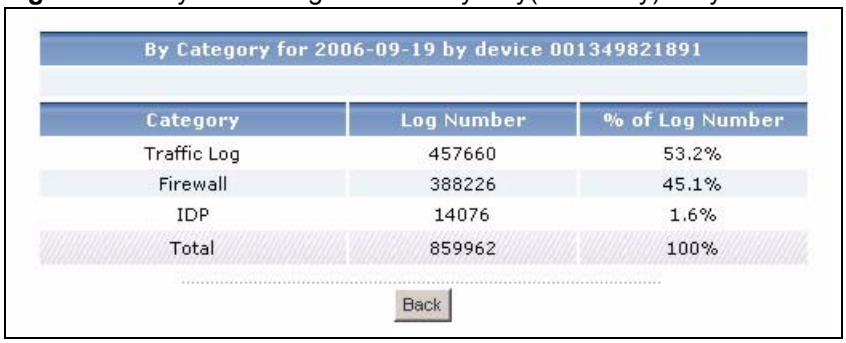
LABEL	DESCRIPTION
Log Number	This field displays how many logs were received from each device on the day you clicked.
% of Log Number	This field displays what percent of the day's total logs came from each device.

12.7.3 Log Receiver By Day > By Device > By Category Screen

Use this screen to look at the number of logs in each category that Vantage Report received from an individual device on a particular day.

Click on the link in an entry in **System** > **Log Receiver > By Day(Summary) > By Device** to access this screen.

Figure 167 System > Log Receiver By Day(Summary) > By Device > By Category



All the fields are described in the following table.

Table 158 System > Log Receiver By Day(Summary) > By Device > By Category

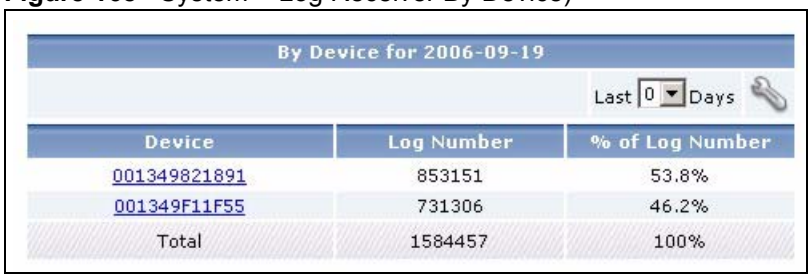
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date you clicked in the summary screen and the MAC address of the device that you clicked in the previous screen.
Category	This field displays the types of logs that the device sent to Vantage Report MAC during the selected day.
Log Number	This field displays how many of the device's logs belonged to each category.
% of Log Number	This field displays what percent of the day's total logs came from each category.

12.7.4 Log Receiver By Device Screen

Use this screen to look at the number of logs that Vantage Report received from each device over a selected range of days.

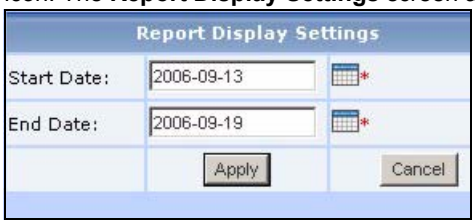
To access this screen, click **System** > **Log Receiver > By Device**.

Figure 168 System > Log Receiver By Device)



All the fields are described in the following table.

Table 159 System > Log Receiver By Device

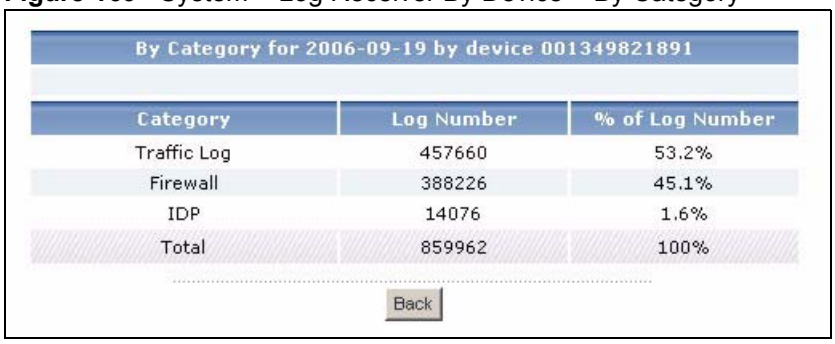
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Last ... Days	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, 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.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
Device	This field displays the MAC addresses of the devices that sent logs on the days you selected. They are sorted by the number of logs from each. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected days.
Log Number	This field displays how many logs Vantage Report received from each device.
% of Log Number	This field displays what percent of the selected time period's total logs came from each category.

12.7.5 Log Receiver By Device > By Category Screen

Use this screen to look at the number of logs in each category that Vantage Report received from an individual device over a selected range of days.

To access this screen, click the link in an entry in the **System** > **Log Receiver > By Device** screen.

Figure 169 System > Log Receiver By Device > By Category



All the fields are described in the following table.

Table 160 System > Log Receiver By Device > By Category

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the dates you specified in the summary screen and the MAC address of the device that you selected.
Category	This field displays the types of logs that the device sent to Vantage Report MAC during the selected day.
Log Number	This field displays how many logs Vantage Report received from the device during the selected time period.
% of Log Number	This field displays what percent of the device's logs came from each category.

12.8 About Screen

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

Figure 170 System > About

13

Troubleshooting

Table 161 Troubleshooting

PROBLEM	CORRECTIVE ACTION
There is no information in any report for my device.	If you just added the device, wait. See Table 2 on page 34 for the amount of time it takes for information to appear in each report. Look for the device's MAC address in `vrpt\log\LogRecord.log` in the Vantage Report installation directory. This file keeps track of all the log entries received by the syslog server in Vantage Report, including log entries for devices that are not set up in Vantage Report. • If the MAC address is in the file, Vantage Report is receiving information from the device. Wait. If the **Attribute** is **Unregistered**, however, the MAC address is not set up correctly in Vantage Report. See section 3.4. • If the MAC address is not in the file, Vantage Report is not receiving information from the device. Make sure you have configured the ZyXEL devices correctly. See section 2.4. Check the amount of available disk space on the Vantage Report server. If it is less than the value in Appendix A on page 339, the Vantage Report server stops receiving log entries. Make sure your ZyXEL devices support Vantage Report. Check the release notes for the current firmware version. Check the connections between the ZyXEL devices and Vantage Report server. If the problem continues, contact your local vendor.
There is information in some reports, but there is no information in others.	Make sure your ZyXEL devices support these reports. Check the release notes for the current firmware version. Make sure you have configured the ZyXEL devices correctly. See section 2.4. Make sure there are log entries or traffic statistics for the report dates you selected. For example, if there were no attacks yesterday, yesterday's attack report is empty. If the problem continues, contact your local vendor.

PART VI Appendices and Index

This part contains the following chapters.

- Product Specifications (339)
- Setting up Your Computer's IP Address (345)
- ZyNOS Log Descriptions (351)
- Open Software Announcements (417)
- Legal Information (447)
- Customer Support (449)
- Index (453)

A

Product Specifications

All values are accurate at the time of writing.

See Table 2 on page 34 for specifications about the time it takes the Vantage Report server to process information from ZyXEL devices.

Table 162 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 163 System Notifications Specifications

FEATURE	SPECIFICATION
Maximum number of logs for each device	15,000,000
Warning: Maximum number of logs for each device	10,000,000
Minimum amount of free disk space required to run Vantage Report	800 MB
Warning: Minimum amount of free disk space required to run Vantage Report	Per Low free disk Mark.

Table 164 Feature Specifications

FEATURE	SPECIFICATION
Maximum Number of Entries in the Table at the Bottom of Each Statistical Report	30
Log Consolidation Frequency	4 minutes

Table 165 Key Features

FEATURE	DESCRIPTION
Executive Dashboard	Get a quick top level summary of activity across devices. You can also easily drill-down to get more details on any area of interest. Select which reports or monitors you want Vantage Report to display first when you login.
Customizable Reports	Display company logos, record information and edit report titles to match customer accounts.

Table 165 Key Features (continued)

FEATURE	DESCRIPTION
Device Monitors and Logs	Monitor the status of all your ZyXEL devices in one application. You can also look at the logs for all your ZyXEL devices in Vantage Report. In normal operation, this information should be no older than five minutes, worst-case.
Real-time Syslog Viewer	As soon as events are shown in the monitors and reports, you can see the log details in the log viewer.
Statistical Reports	Generate reports for historical analysis. These reports include bandwidth usage, service usage, 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.
Reverse Hostname Lookup	Where possible, see host names, instead of IP addresses, in statistical reports.
Scheduled Reports	Set up regular times to generate and e-mail statistical reports.
Registration, Activation, and Upgrades	Register and activate on myZyXEL.com through Vantage Report. This makes getting the trial version and upgrading simpler.
System Service	Run and manage Vantage Report as a system service.
Administration	Create separate accounts for network administrators and device administrators. These accounts do not give access to administration screens for Vantage Report.
File Management and Data Maintenance	Backup Vantage Report configurations, including various statistical "snapshots," and restore them later.

The following table lists which features Vantage Report supports with various firmware versions of various devices.

Table 166 VRPT 3.0 Device and Feature Support

MENU ITEM			ZYWALL				P-	IDP
			3.62 ZYWALL 2 / 10W	3.63 / 3.64 / 3.65 ZYWALL 5 / 35 / 70	4.00 ZYWALL 5 / 35 / 70	1.01 ZYWALL 1050	3.40 P-662 P-652	2.00 IDP 10
Monitor								
	Bandwidth		N / A	Y	Y	Y	N / A	Y
	Service		N / A	Y	Y	Y	N / A	Y
	Attack		Y	Y	Y	Y	Y	N / A
	Intrusion		N / A	N / A	Y	Y	N / A	Y
	AntiVirus		N / A	N / A	Y	N / A	N / A	N / A
	AntiSpam		N / A	N / A	Y	N / A	N / A	N / A
Traffic								
	Bandwidth							

Table 166 VRPT 3.0 Device and Feature Support

MENU ITEM			ZYWALL				P-	IDP
			3.62 ZYWALL 2 / 10W	3.63 / 3.64 / 3.65 ZYWALL 5 / 35 / 70	4.00 ZYWALL 5 / 35 / 70	1.01 ZYWALL 1050	3.40 P-662 P-652	2.00 IDP 10
		Summary	N / A	Y	Y	Y	N / A	Y
		Top Protocols	N / A	Y	Y	Y	N / A	Y
		Top Hosts	N / A	Y	Y	Y	N / A	Y
		Top Users	N / A	N / A	N / A	Y	N / A	N / A
		Top Destinations	N / A	Y	Y	Y	N / A	Y
	WEB							
		Top Sites	N / A	Y	Y	Y	N / A	Y
		Top Hosts	N / A	Y	Y	Y	N / A	Y
		Top Users	N / A	N / A	N / A	Y	N / A	Y
	FTP							
		Top Sites	N / A	Y	Y	Y	N / A	Y
		Top Hosts	N / A	Y	Y	Y	N / A	Y
		Top Users	N / A	N / A	N / A	Y	N / A	Y
	MAIL							
		Top Sites	N / A	Y	Y	Y	N / A	Y
		Top Hosts	N / A	Y	Y	Y	N / A	Y
		Top Users	N / A	N / A	N / A	Y	N / A	Y
	Customization							
		Top Sites	N / A	Y	Y	Y	N / A	Y
		Top Hosts	N / A	Y	Y	Y	N / A	Y
		Top Users	N / A	N / A	N / A	Y	N / A	Y
VPN								
	Site to Site							
		Link Status	N / A	N / A	N / A	Y	N / A	N / A
		Traffic Monitor	N / A	N / A	N / A	Y	N / A	N / A
		Top Peer Gateways	N / A	Y	Y	N / A	N / A	N / A
		Top Sites	N / A	N / A	N / A	Y	N / A	N / A
		Top Tunnels	N / A	N / A	N / A	Y	N / A	N / A
		Top Hosts	N / A	Y	Y	Y	N / A	N / A
		Top Users	N / A	N / A	N / A	Y	N / A	N / A
		Top Destinations	N / A	N / A	N / A	Y	N / A	N / A
	Remote Access							

Table 166 VRPT 3.0 Device and Feature Support

MENU ITEM			ZYWALL				P-	IDP
			3.62 ZYWALL 2 / 10W	3.63 / 3.64 / 3.65 ZYWALL 5 / 35 / 70	4.00 ZYWALL 5 / 35 / 70	1.01 ZYWALL 1050	3.40 P-662 P-652	2.00 IDP 10
		Total Users & Traffic	N / A	N / A	N / A	Y	N / A	N / A
		User Status	N / A	N / A	N / A	Y	N / A	N / A
		Top Protocols	N / A	N / A	N / A	Y	N / A	N / A
		Top Destinations	N / A	N / A	N / A	Y	N / A	N / A
	Xauth							
		Successful Login	Y	Y	Y	Y	N / A	N / A
		Failed Login	Y	Y	Y	Y	N / A	N / A
Network Attack								
	Attack							
		Summary	Y	Y	Y	Y	Y	N / A
		Top Attacks	Y	Y	Y	Y	Y	N / A
		Top Sources	Y	Y	Y	Y	Y	N / A
		By Type	N / A	N / A	N / A	N / A	N / A	N / A
	Intrusion							
		Summary	N / A	N / A	Y	Y	N / A	Y
		Top Intrusions	N / A	N / A	Y	Y	N / A	Y
		Top Sources	N / A	N / A	Y	Y	N / A	Y
		Top Destinations	N / A	N / A	Y	Y	N / A	Y
		By Severity	N / A	N / A	Y	Y	N / A	Y
	AntiVirus							
		Summary	N / A	N / A	Y	N / A	N / A	N / A
		Top Viruses	N / A	N / A	Y	N / A	N / A	N / A
		Top Sources	N / A	N / A	Y	N / A	N / A	N / A
		Top Destinations	N / A	N / A	Y	N / A	N / A	N / A
	AntiSpam							
		Summary	N / A	N / A	Y	N / A	N / A	N / A
		Top Senders	N / A	N / A	Y	N / A	N / A	N / A
		Top Sources	N / A	N / A	Y	N / A	N / A	N / A
Security Policy								

Table 166 VRPT 3.0 Device and Feature Support

MENU ITEM			ZYWALL				P-	IDP
			3.62 ZYWALL 2 / 10W	3.63 / 3.64 / 3.65 ZYWALL 5 / 35 / 70	4.00 ZYWALL 5 / 35 / 70	1.01 ZYWALL 1050	3.40 P-662 P-652	2.00 IDP 10
	Firewall Access Control							
		Top Users Blocked	N / A	N / A	N / A	Y	N / A	N / A
		Top Packets Blocked	Y	Y	Y	Y	N / A	N / A
	Application Access Control							
		Top Applications Blocked	N / A	N / A	N / A	Y	N / A	N / A
		Top Users Blocked	N / A	N / A	N / A	Y	N / A	N / A
		Top Applications Allowed	N / A	N / A	N / A	Y	N / A	N / A
	Web Blocked							
		Summary	Y	Y	Y	Y	N / A	N / A
		Top Sites	Y	Y	Y	Y	N / A	N / A
		Top Hosts	Y	Y	Y	Y	N / A	N / A
		Top Users	N / A	N / A	N / A	Y	N / A	N / A
		By Category	Y	Y	Y	Y	N / A	N / A
	Web Allowed							
		Summary	Y	Y	Y	Y	N / A	N / A
		Top Sites	Y	Y	Y	Y	N / A	N / A
		Top Hosts	Y	Y	Y	Y	N / A	N / A
		Top Users	N / A	N / A	N / A	Y	N / A	N / A
Event								
	Login							
		Successful Login	Y	Y	Y	Y	N / A	N / A
		Failed Login	Y	Y	Y	Y	N / A	N / A
	Sessions Per Host							
		Top Hosts	Y	Y	Y	Y	N / A	N / A
		Top Users	N / A	N / A	N / A	Y	N / A	N / A

Table 166 VRPT 3.0 Device and Feature Support

MENU ITEM			ZYWALL				P-	IDP
			3.62 ZYWALL 2 / 10W	3.63 / 3.64 / 3.65 ZYWALL 5 / 35 / 70	4.00 ZYWALL 5 / 35 / 70	1.01 ZYWALL 1050	3.40 P-662 P-652	2.00 IDP 10
Log Viewer								
	All Logs		Y	Y	Y	Y	Y	Y

B

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.

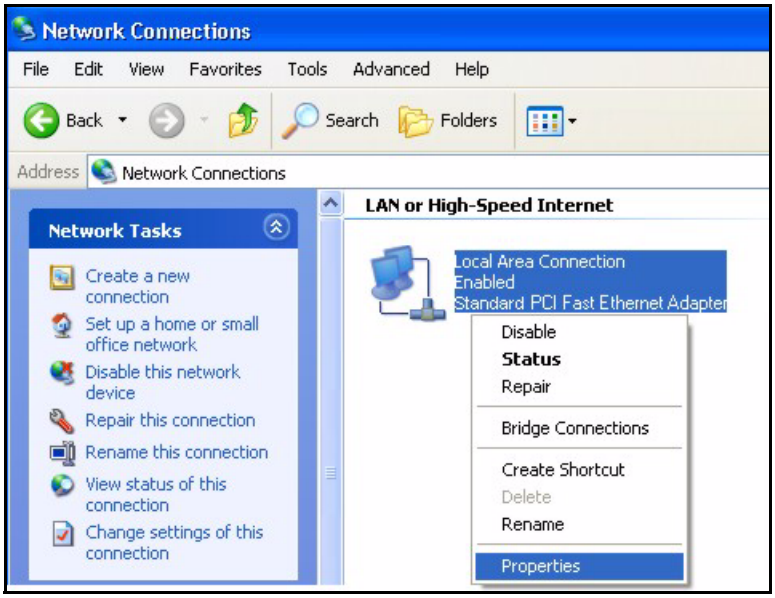
Windows 2000/NT/XP

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

Figure 171 Windows XP: Start Menu

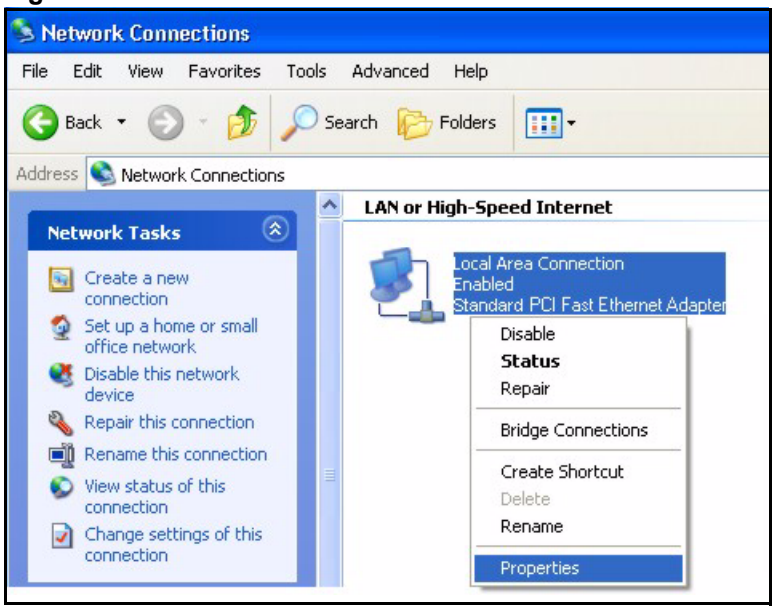
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 172 Windows XP: Control Panel



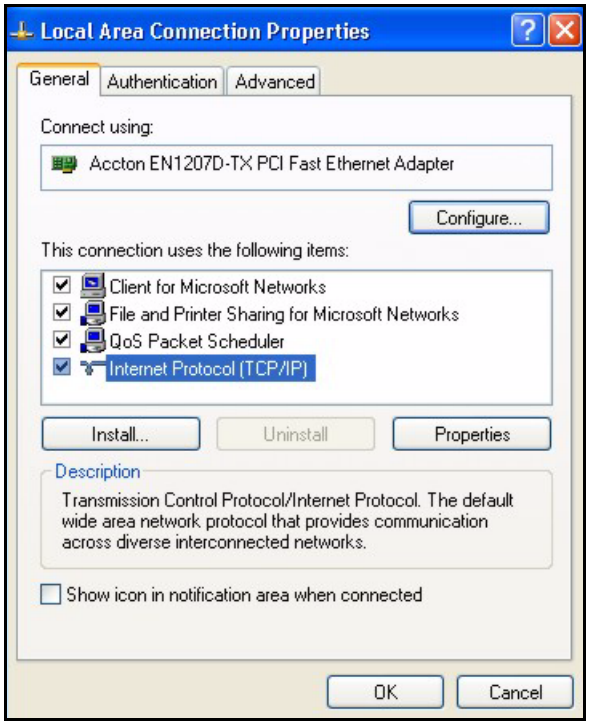
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 173 Windows XP: Control Panel: Network Connections: Properties



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

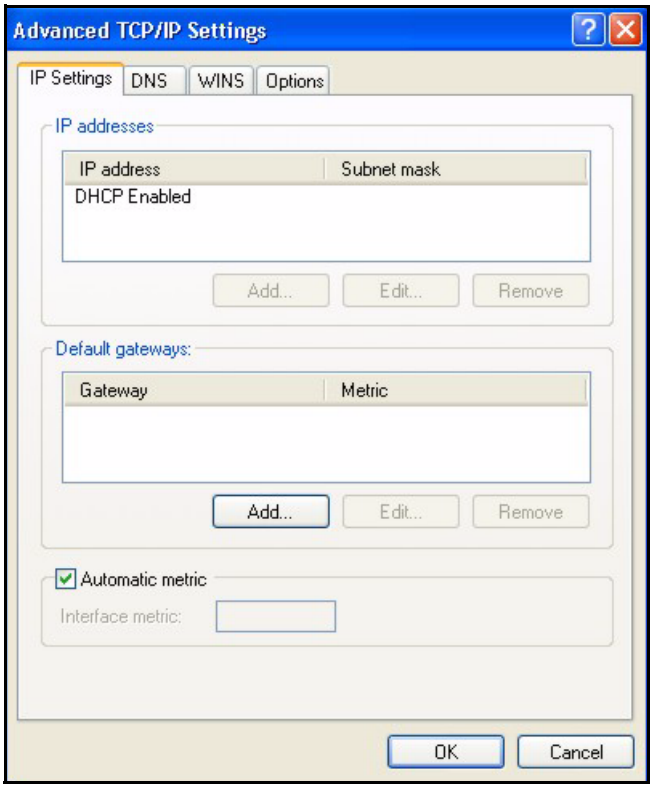
Figure 174 Windows XP: Local Area Connection Properties



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 175 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 Setting**s tab and click **OK**.

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

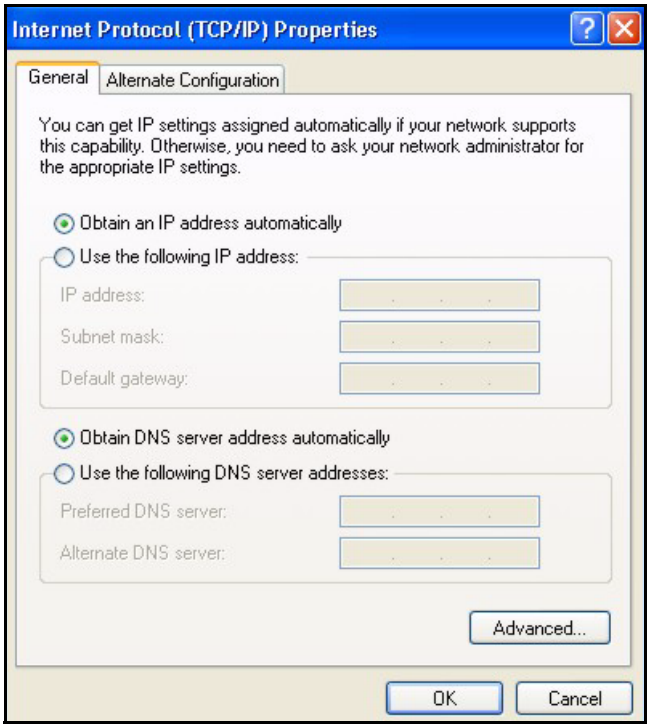
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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 176 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 ZyXEL device 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.

C

ZyNOS Log Descriptions

This appendix provides descriptions of example log messages for ZyNOS-based devices. Log messages vary by device.

Table 167 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.

Table 167 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
SMT Session Begin	An SMT management session has started.
SMT Session End	An SMT management session has ended.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.
DNS server %s was not responding to last 32 consecutive queries…	The specified DNS server did not respond to the last 32 consecutive queries.
DDNS update IP:%s (host %d) successfully	The device updated the IP address of the specified DDNS host name.
SMTP successfully	The device sent an e-mail.
myZyXEL.com registration successful	Registration of the device with myZyXEL.com was successful.
Trial service registration successful	Registration for a trial service was successful.
Service upgrade successful	Registration for a service upgrade was successful.
Service refresh successful.	The device successfully refreshed service information from myZyXEL.com.
Content Filter trial service activation successfully	The content filtering trial service was successfully activated for this device.
Anti-Spam trial service activation successfully	The anti-spam trial service was successfully activated for this device.
IDP/Anti-Virus trial service activation successfully	The IDP and anti-virus trial service was successfully activated for this device.
%s	The myZyXEL.com service registration failed due to the error listed. If you are unable to register for services at myZYXEL.com, the error message displayed in this log may be useful when contacting customer support.

Table 168 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.
Dial Backup starts	Dial backup started working.
Dial Backup ends	Dial backup stopped working.
DHCP Server cannot assign the static IP %S (out of range).	The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid.
The DHCP static IP %s is conflict.	The static DHCP IP address conflicts with another host.
SMTP fail (%s)	The device failed to send an e-mail (error message included).
SMTP authentication fail (%s)	The device failed to authenticate with the SMTP server (error message included).
%s	The device will send a Gratuitous ARP to detect the IP collision. If the collision happens, there will be a log in centralized log.

Table 169 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.

Table 169 Access Control Logs (continued)

LOG MESSAGE	DESCRIPTION
Firewall allowed a packet that matched a NAT session: [TCP | UDP]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.
Firewall matches a dynamic ACL rule of an ALG session	The firewall allowed access for a packet that matched a dynamic ACL rule of an ALG session.
Maximum number of dynamic ACL rules exceeded.	
Dynamic ACL rule, listening port : %d, peer port : %d already exists.	

Table 170 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
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 CI command: "sys firewall tcprst").

Table 171 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 185 on page 366.

Table 172 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 173 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 174 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 175 UPnP Logs

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

Table 176 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.

Table 176 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The Vantage Report cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The Vantage Report cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see Table 185 on page 366.

Table 177 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.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.

Table 177 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.
IP address in FTP port command is different from the client IP address. It maybe a bounce attack.	The IP address in an FTP port command is different from the client IP address. It may be a bounce attack.
Fragment packet size is smaller than the MTU size of output interface.	The fragment packet size is smaller than the MTU size of output interface.

Table 178 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.

Table 178 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: SNMP denied	Attempted use of SNMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

Table 179 Wireless Logs

LOG MESSAGE	DESCRIPTION
WLAN MAC Filter Fail	The MAC filter blocked a wireless station from connecting to the device.
WLAN MAC Filter Success	The MAC filter allowed a wireless station to connect to the device.
WLAN STA Association	A wireless station associated with the device.
WLAN STA Association List Full	The maximum number of associated wireless clients has been reached.
WLAN STA Association Again	The SSID and time of association were updated for an wireless station that was already associated.

Table 180 IPSec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPSec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed.
Inbound packet decryption failed	Please check the algorithm configuration.
Cannot find outbound SA for rule <%d>	A packet matches a rule, but there is no phase 2 SA for outbound traffic.
Rule [%s] sends an echo request to peer	The device sent a ping packet to check the specified VPN tunnel's connectivity.

Table 180 IPSec Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%s] receives an echo reply from peer	The device received a ping response when checking the specified VPN tunnel's connectivity.
Delete all tunnels	The device disconnected all IPSec tunnels.

Table 181 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.
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.

Table 181 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
XAUTH succeed! Remote user: <Username>	The router used extended authentication to authenticate the listed remote username.
XAUTH fail! Remote user: <Username>	The router was not able to use extended authentication to authenticate the listed remote username.
XAUTH succeed! My name: <Username>	The router used extended authentication to authenticate the listed username.

Table 181 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
XAUTH fail! My name: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
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 1verification 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 181 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.
Remote Gateway Addr in rule [%s] is changed to %s"	The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address.
New My Vantage Report Addr in rule [%s] is changed to %s	The IP address for the domain name of the Vantage Report in the listed rule changed to the listed IP address.
Remote Gateway Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the remote gateway's IP address changed.
My Vantage Report Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the Vantage Report's IP address changed.

Table 182 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.

Table 182 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 183 on page 364 for the corresponding descriptions of the codes.

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
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).

CODE	DESCRIPTION
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 183 802.1X 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 mothed.	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.

Table 183 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 184 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/ Vantage Report	ACL set for packets traveling from the LAN to the LAN or the Vantage Report.
(W to W/ZW)	WAN to WAN/ Vantage Report	ACL set for packets traveling from the WAN to the WAN or the Vantage Report.
(D to D/ZW)	DMZ to DMZ/ Vantage Report	ACL set for packets traveling from the DMZ to the DM or the Vantage Report.
(L to WL)	LAN to WLAN	ACL set for packets traveling from the LAN to the WLAN.
(WL to L)	WLAN to LAN	ACL set for packets traveling from the WLAN to the LAN.
(W to WL)	WAN to WLAN	ACL set for packets traveling from the WAN to the WLAN.
(WL to W)	WLAN to WAN	ACL set for packets traveling from the WLAN to the WAN.
(D to WL)	DMZ to WLAN	ACL set for packets traveling from the DMZ to the WLAN.
(WL to D)	WLAN to DMZ	ACL set for packets traveling from the WLAN to the DMZ.
(WL to WL)	WLAN to WLAN/ Vantage Report	ACL set for packets traveling from the WLAN to the WLAN or the Vantage Report.

Table 185 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable

Table 185 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
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 186 IDP Logs

LOG MESSAGE	DESCRIPTION
The buffer size is too small!	The buffer for holding IDP information such as the signature file version was too small to hold any more information.
The format of the user config file is incorrect!	There was a format error in the configuration backup file that someone attempted to load into the system.
The system is doing signature update now , please wait!	The device is updating the signature file.
No data!	The system could not find any IDP signatures that matched a search.
IDP %s!	The device detected an intrusion event in a connection. The format of %s is “ID” followed by the IDP ID signature number and the IDP signature name. For example, ID:10001,Window Ping.
Can not find the signature , please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.
Signature update OK - New signature version: <Signature version> Release Date: <Release date>!	The device updated the signature file successfully. The signature file’s version and release date are included.
The turbo card is not ready , please insert the card and reboot!	The turbo card is not installed.

Table 187 AV Logs

LOG MESSAGE	DESCRIPTION
HTTP Virus infected - %s!	The device detected a virus in an HTTP connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
FTPDATA Virus infected - %s!	The device detected a virus in a FTPDATA connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.

Table 187 AV Logs (continued)

LOG MESSAGE	DESCRIPTION
SMTP Virus infected - %s!	The device detected a virus in a SMTP connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
POP3 Virus infected - %s!	The device detected a virus in a POP3 connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
HTTP Bypass - %s!	The device bypassed the scanning of files in HTTP connections. %s is the filename. For example, game.zip.
FTPDATA Bypass - %s!	The device bypassed the scanning of files in FTP data connections. %s is the filename. For example, game.zip.
SMTP Bypass - %s!	The device bypassed the scanning of files in SMTP connections. %s is the filename. For example, game.zip.
POP3 Bypass - %s!	The device bypassed the scanning of files in POP3 connections. %s is the filename. For example, game.zip.
Can not find the signature , please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.
Update the signature file successfully.	The device updated the signature file successfully.
The turbo card is not ready , please insert the card and reboot!	The turbo card is not installed.
The system is doing signature update now , please wait!	The device is updating the signature file.
HTTP Block. The session is over maximun ZIP sessions - %s!	The system blocked scanning files in HTTP connections. The format of %s is %FILENAME%. For example, game.zip."
FTPDATA Block. The session is over maximun ZIP sessions - %s!	The system blocked scanning files in FTPDATA connections. The format of %s is %FILENAME%. For example, game.zip."
SMTP Block. The session is over maximun ZIP sessions - %s!	The system blocked scanning files in SMTP connections. The format of %s is %FILENAME%. For example, game.zip."

Table 187 AV Logs (continued)

LOG MESSAGE	DESCRIPTION
POP3 Block. The session is over maximun ZIP sessions - %s!	The system blocked scanning files in POP3 connections. The format of %s is %FILENAME%. For example, game.zip."
Zip file unsupported - %s!	The system destroyed unsupported zip files.

Table 188 AS Logs

LOG MESSAGE	DESCRIPTION
Mail is in the Black List - Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!%MAIL_DIRECTION%	An e-mail with the listed source and subject matched an anti-spam blacklist entry.
Mail score is higher than threshold - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!%MAIL_DIRECTION%	The spam score (listed) for the e-mail with the listed source and subject was higher than or equal to the spam score threshold.
Exceed maximum mail sessions (%d).%MAIL_DIRECTION%	The number of concurrent mail sessions went over the limit (%d).
Remove rating server [%Rating Server IP Address%] from server list!%MAIL_DIRECTION%	The listed server IP address has been removed from the list of anti-spam external database servers.
"This is a phishing mail - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!"%MAIL_DIRECTION%	The spam score (listed) for the e-mail with the listed source and subject was higher than the spam score threshold. The anti-spam external database identified the e-mail as a phishing mail.
Invalid parameter for AsEngine!	There was an internal AS system error. This type of error causes the device to restart.
Mail Parser buffer is overflow!%MAIL_DIRECTION%	There were too many characters in a single line of an e-mail header that the device was attempting to parse.
Initialized the link list for IP list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Initialized the link list for Email list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Initialized the link list for MIME list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Initialized the link list for subject list failed - rule:%d, ret_code:%d	The runtime structure cannot be initialized correctly.
Convert the string to the PCRE pattern failed - ret_code:%d	Convert the string to regular expression failed.
Compile the string for PCRE failed - rule:%d	Compile the regular expression by PCRE library failed.

Table 188 AS Logs (continued)

LOG MESSAGE	DESCRIPTION
`Load the anti-spam fixed runtime settings failed - ret_code:%d`	Load the anti-spam fixed runtime settings failed.
`Load the anti-spam variable runtime settings failed - rule:%d, ret_code:%d`	Load the anti-spam variable runtime settings failed.
`AS checking bypassed as a mail header line exceeds 1024 characters!%MAIL_DIRECTION%`	AS checking bypassed as a mail header line exceeds 1024 characters. See

Table 189 AS Directions for Multiple WAN Devices

FROM\TO	LAN	WAN1	DMZ	WAN2	WLAN
LAN	(L to L)	(L to W1)	(L to D)	(L to W2)	(L to WL)
WAN1	(W1 to L)	(W1 to W1)	(W1 to D)	(W1 to W2)	(W1 to WL)
DMZ	(D to L)	(D to W1)	(D to D)	(D to W2)	(D to WL)
WAN2	(W2 to L)	(W2 to W1)	(W2 to D)	(W2 to W2)	(W2 to WL)
WLAN	(WL to L)	(WL to W1)	(WL to D)	(WL to W2)	(WL to WL)

Table 190 AS Directions for Single WAN Devices

FROM\TO	LAN	WAN	DMZ	WLAN
LAN	(L to L)	(L to W)	(L to D)	(L to WL)
WAN	(W to L)	(W to W)	(W to D)	(W to WL)
DMZ	(D to L)	(D to W)	(D to D)	(D to WL)
WLAN	(WL to L)	(WL to W)	(WL to D)	(WL to WL)

13.1 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 191 Syslog Logs

LOG MESSAGE	DESCRIPTION
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"`	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
`Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"`	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DMZ", "LAN:DEV" for example).
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC.
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0|1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu | b64 >"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions.

Table 191 Syslog Logs (continued)

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid> act="<idp action>" count="1"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Spam" 1stReIP="<IP>"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. 1stReIP is the IP address of the first mail relay server. The definition of messages and notes are defined in the Anti-Spam log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" act="<idp action>" sid="<idp sid> count="1"	This message is sent by the "RAS" at the time when this syslog is generated. The facility is defined in the web **MAIN MENU, LOGS, Log Settings** page. The severity is the centralized log type. The definition of messages and notes are defined in the IDP categories.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 192 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce

Table 192 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
NOTFY	Notification
DEL	Delete
VID	Vendor ID

D

ZyWALL 1050 Log Descriptions

This appendix provides descriptions of example log messages for the ZyWALL 1050.

Table 193 Content Filter Logs

LOG MESSAGE	DESCRIPTION
`Content filter has been enabled`	An administrator turned the content filter on.
`Content filter has been disabled`	An administrator turned the content filter off.

Table 194 Forward Web Site Logs

LOG MESSAGE	DESCRIPTION
`%s: Trusted Web site`	The device allowed access to a web site in a trusted domain. %s: website host
`%s`	The device allowed access to a web site. The content filtering service is registered and activated or the service is not activated in a profile, this is a web site that is not blocked according to a profile and the default policy is not set to block. %s: website host
`%s: Service is not registered`	The device allowed access to a web site. The content filtering service is unregistered and the default policy is not set to block. %s: website host

Table 195 Blocked Web Site Logs

LOG MESSAGE	DESCRIPTION
`%s :%s`	The rating server responded that the web site is in a specified category and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
`%s: Unrated`	The rating server responded that the web site cannot be categorized and access was blocked according to a content filter profile. %s: website host

Table 195 Blocked Web Site Logs (continued)

LOG MESSAGE	DESCRIPTION
`%s: Service is unavailable`	Content filter rating service is temporarily unavailable and access to the web site was blocked due to: 1. Can't resolve rating server IP (No DNS) 2. Invalid service license 4. Rating service is restarting 5. Can't connect to rating server 6. Query failed 7. Query timeout 8. Too many queries 9. Unknown reason %s: website host
`%s: %s(cache hit)`	The web site's category exists in the device's local cache and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
`%s: Not in trusted web list`	The web site is not a trusted host/domain, and the device blocks all traffic except for trusted web sites. %s: website host
`%s: Contains ActiveX`	The web site contains ActiveX and access was blocked according to a profile. %s: website host
`%s: Contains Java applet`	The web site contains Java applet and access was blocked according to a profile. %s: website host
`%s: Contains cookie`	The web site contains a cookie and access was blocked according to a profile. %s: website host
`%s: Proxy mode is detected`	The system detected a proxy connection and blocked access according to a profile. %s: website host
`%s: Forbidden Web site`	The web site is in forbidden web site list. %s: website host
`%s: Keyword blocking`	The web content matched a user defined keyword. %s: website host
`%s: Blocking by default policy`	No content filter policy is applied and access was blocked since the default action is block. %s: website host

Table 196 User Logs

LOG MESSAGE	DESCRIPTION
%s %s has logged in from %s	The specified user signed in. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s has logged out from %s	The specified user signed out. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s from %s has been logged out (re-auth timeout)	The specified user was signed out by the device due to a re-authentication timeout. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s from %s has been logged out (lease timeout)	The specified user was signed out by the device due to a lease timeout. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
%s %s from %s has been logged out (idle timeout)	The specified user was signed out by the device due to an idle timeout. 1st %s: Administrator|Limited-Admin|User|Ext-User|Guest 2nd %s: username 3rd %s: service name (HTTP/HTTPS, FTP, telnet, SSH, console) NOTE field: %s means username.
Console is put into lockout	Too many failed login attempts were made on the console port so the device is blocking login attempts on the console port.
Address %u.%u.%u.%u is put into lockout	Too many failed login attempts were made from an IP address so the device is blocking login attempts from that IP address. %u.%u.%u.%u: the source address of the user's login attempt
Login attempt is made on a lockout address from %s	A login attempt came from an IP address that the device has locked out. %u.%u.%u.%u: the source address of the user's login attempt
Failed %s login attempt (reach the maximum number of user)	The device blocked a login because the maximum login capacity has already been reached. %s: service name
Failed %s login attempt (reach the maximum number of simultaneous logon)	The device blocked a login because the maximum simultaneous login capacity for the administrator or access account has already been reached. %s: service name

Table 197 myZyXEL.com Logs

LOG MESSAGE	DESCRIPTION
Send registration message to MyZyXEL.com server has failed.	The device was not able to send a registration message to MyZyXEL.com.
Get server response has failed.	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
Timeout for get server response.	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
User has existed.	The user name already exists in MyZyXEL.com's database. So the user can't use it for device registration and needs to specify another one.
User does not exist.	The user name does not yet exist in MyZyXEL.com's database. So the user can use it for device registration.
Internal server error.	MyZyXEL.com's database had an error when checking the user name.
Device registration has failed:%s.	Device registration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by the myZyXEL.com server
Device registration has succeeded.	The device registered successfully with the myZyXEL.com server.
Registration has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
%s:Trial service activation has failed:%s.	Trail service activation failed for the specified service, an error message returned by the MyZyXEL.com server will be appended to this log. 1st %s: service name 2nd %s: error message returned by the myZyXEL.com server
%s:Trial service activation has succeeded.	Trail service was activated successfully for the specified service. %s: service name
Trial service activation has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
Standard service activation has failed:%s.	Standard service activation failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by the myZyXEL.com server
Standard service activation has succeeded.	Standard service activation has succeeded.
Standard service activation has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.

Table 197 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Service expiration check has failed:%s.	The service expiration day check failed, this log will append an error message returned by the MyZyXEL.com server. %s: error message returned by myZyXEL.com server
Service expiration check has succeeded.	The service expiration day check was successful.
Service expiration check has failed. Because of lack must fields.	The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device.
Server setting error.	The device could not retrieve the myZyXEL.com server's IP address or FQDN from local.
Resolve server IP has failed.	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
Verify server's certificate has failed.	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate.
Connect to MyZyXEL.com server has failed.	The device could not connect to the MyZyXEL.com server.
Do account check.	The device started to check whether or not the user name in MyZyXEL.com's database.
Do device register.	The device started device registration.
Do trial service activation.	The device started trail service activation.
Do standard service activation.	The device started standard service activation.
Do expiration check.	The device started the service expiration day check.
Build query message has failed.	Some information was missing in the packets that the device sent to the MyZyXEL.com server.
Parse receive message has failed.	The device cannot parse the response returned by the MyZyXEL.com server. Maybe some required fields are missing.
Resolve server IP has failed. Update stop.	The update has stopped because the device couldn’t resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
Verify server's certificate has failed. Update stop.	The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate. The update has stopped.
Send download request to update server has failed.	The device’s attempt to send a download message to the update server failed.
Get server response has failed.	The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal.
Timeout for get server response.	zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout.
Send update request to update server has failed.	The device could not send an update message to the update server.

Table 197 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Update has failed. Because of lack must fields.	The device received an incomplete response from the update server and it caused a parsing error for the device.
Update server is busy now. File download after %d seconds.	The update server was busy so the device will wait for the specified number of seconds and send the download request to the update server again.
Device has latest file. No need to update.	The device already has the latest version of the file so no update is needed.
Device has latest signature file; no need to update	The device already has the latest version of the signature file so no update is needed.
Connect to update server has failed.	The device cannot connect to the update server.
Wrong format for packets received.	The device cannot parse the response returned by the server. Maybe some required fields are missing.
Server setting error. Update stop.	The device could not resolve the update server's FQDN to an IP address through gethostbyname(). The update process stopped.
Build query message failed.	Some information was missing in the packets that the device sent to the server.
Starting signature update.	The device started an IDP signature update.
Signature download has succeeded.	The device successfully downloaded a signature file.
Signature update has succeeded.	The device successfully downloaded and applied an IDP signature file.
Signature update has failed:%s.	The signature update signature failed, an error message returned by the update server will be appended to this log. %s: error message returned by update server
Signature download has failed.	The device still can't download the IDP signature after 3 retries.
Signature update has failed. Do %d retry.	The IDP signature update failed, so the device will process 3 retries. %d: retry times (1~3)
Resolve server IP has failed.	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
Connect to MyZyXEL.com server has failed.	The device could not connect to the MyZyXEL.com server.
Build query message has failed.	Some information was missing in the packets that the device sent to the server.
Verify server's certificate has failed.	The device could not process an HTTPS connection because it could not verify the server's certificate.
Get server response has failed.	The device sent packets to the server, but did not receive a response. The root cause may be that the connection is abnormal.

Table 197 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
Expiration daily-check has failed:%s.	The daily check for service expiration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by myZyXEL.com server
Do expiration daily-check has failed. Because of lack must fields.	The device received an incomplete response to the daily service expiration check and the packets caused a parsing error for the device.
Server setting error.	The device could not retrieve the server's IP address or FQDN from local.
Do expiration daily-check has failed.	The daily check for service expiration failed.
Do expiration daily-check has succeeded.	The daily check for service expiration was successful.
Expiration daily-check will trigger PPP interface. Do self-check.	Before the device sends an expiration day check packet, it needs to check whether or not it will trigger a PPP connection.
System bootup. Do exipration daily-check.	The device processes a service expiration day check immediately after it starts up.
After register. Do expiration daily-check immediately.	The device processes a service expiration day check immediately after device registration.
Time is up. Do exipration daily-check.	The processes a service expiration day check every 24 hrs.
Read MyZyXEL.com storage has failed.	Read data from EEPROM has failed.
Open /proc/MRD has failed.	This error message is shown when getting MAC address.
IDP service has expired.	The IDP service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count.
Content-Filter service has expired.	The content filtering service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count.
Unknown TLS/SSL version: %d.	The device only supports SSLv3 protocol. %d: SSL version assigned by client.
Load trusted root certificates has failed.	The device needs to load the trusted root certificate before the device can verify a server's certificate. This log displays if the device failed to load it.
Certificate has expired.	Verification of a server's certificate failed because it has expired.
Self signed certificate.	Verification of a server's certificate failed because it is self-signed.

Table 197 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Self signed certificate in certificate chain.`	Verification of a server's certificate failed because there is a self-signed certificate in the server's certificate chain.
`Verify peer certificates has succeeded.`	The device verified a server's certificate while processing an HTTPS connection.
`Certification verification failed: Depth: %d, Error Number(%d):%s.`	Verification of a server's certificate failed while processing an HTTPS connection. This log identifies the reason for the failure. 1st %d: certificate chain level 2nd %d: error number %s: error message
`Certificate issuer name:%s.`	Verification of the specified certificate failed because the device could not get the certificate's issuer name. %s is the certificate name.
`The wrong format for HTTP header.`	The header format of a packet returned by a server is wrong.
`Timeout for get server response.`	After the device sent packets to a server, the device did not receive any response from the server. The root cause may be a network delay issue.
`Download file size is wrong.`	The file size downloaded for AS is not identical with content-length
`Parse HTTP header has failed.`	Device can't parse the HTTP header in a response returned by a server. Maybe some HTTP headers are missing.

Table 198 IDP Logs

LOG MESSAGE	DESCRIPTION
`System internal error. Detect IDP engine status failed.`	System internal error. Get IDP engine activation flag failed.
`System internal error. Enable IDP failed.`	Enable IDP engine activation flag failed.
`System internal error.Disable IDP failed.`	Disable IDP engine activation flag failed.
`Enable IDP succeeded.`	Enable IDP engine succeeded.
`Disable IDP succeeded.`	Disable IDP engine succeeded.
`Enable IDP engine failed.`	Insert IDP engine failed.
`Disable IDP engine failed.`	Remove IDP engine failed.
`Enable IDP engine succeeded.`	Insert IDP engine succeeded.
`Disable IDP engine succeeded.`	Remove IDP engine succeeded.

Table 198 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
IDP service is not registered. Packet Inspection feature will not be activated.	IDP service is not registered. IDP service packet inspection feature and signature update will both be deactivated.
IDP service trial license is expired. Packet Inspection feature will not be activated.	IDP service trial license is expired. IDP service packet inspection feature and signature update will both be deactivated.
IDP service standard license is expired. Update signature failed.	IDP service standard license is expired. IDP signature cannot update.
IDP service standard license is not registered. Update signature failed.	IDP service standard license is not registered. IDP signature cannot update.
IDP service trial license is expired. Update signature failed.	IDP service trial license is expired. IDP signature cannot update.
IDP service trial license is not registered. Update signature failed.	IDP service trial license is expired. IDP signature cannot update.
Custom signature add error: sid <*sid*>, <*error_message*>.	Custom signature adding failed. Error sid and message will be shown.
Custom signature import error: line <*line*>, sid <*sid*>, <*error_message*>.	Custom signature importing failed. Error line number of file, sid and message will be shown
Custom signature replace error: line <*line*>, sid <*sid*>, <*error_message*>.	Custom signature replacing failed. Error line number of file, sid and message will be shown
Custom signature edit error: sid <*sid*>, <*error_message*>.	Custom signature editing failed. Error sid and message will be shown.
Custom signature more than <*num*>. Replacement custom signature number is <*num*>.	Custom signature replacement failed. Display maximum rule number and replacement rule number.
Custom signature more than <*num*>. Remaining custom signature number is <*num*>. Adding custom signature number is <*num*>.	Custom signature adding failed. Display maximum rule number, remaining rule number and adding rule number.

Table 198 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Get custom signature number error.`	Get custom rule number failed.
`Add custom signature error: signature <sid> is over length.`	Custom signature adding failed. Rule content length is too long.
`Edit custom signature error: signature <sid> is over length.`	Custom signature editing failed. Rule content length is too long.
`IDP off-line update failed. File damaged.`	IDP signature off-line update failed. Signature file maybe corrupt.
`IDP signature update failed. File crashed.`	IDP signature update failed. Decrypt signature file failed.
`IDP signature update failed. File damaged.`	IDP signature update failed. Decompress signature file failed.
`IDP signature update failed. File update failed.`	IDP signature update failed. Update signature file filed.
`IDP signature update failed. Can not update last update time.`	IDP signature update failed. Update last update time failed.
`IDP signature update failed. Can not update synchronized file.`	IDP signature update failed. Rebuild IDP DHA synchronized file failed.
`IDP signature update successful. Signature version: <version>.`	IDP signature update successful.
`System internal error. Create IDP debug directory failed`	System internal error. Create IDP debug directory failed.
`System internal error. Create IDP statistics entry failed.`	System internal error. Create IDP statistics entry failed.
`System internal error. Out of memory. IDP activation unchanged.`	System internal error. System is out of memory. IDP activation unchanged.
`System internal error. Create IDP proc failed. IDP activation failed.`	System internal error. Create IDP proc failed. IDP activation failed.
`[type=<type>] <message>, Action: <action>, Severity: <severity>`	IDP triggered event log. *<type>* = {sig(*<id>*) | scan-detection(*<attack>*) | flood-detection(*<attack>*) | http-inspection(*<attack>*) | tcp-decoder(*<attack>*) | udp-decoder(*<attack>*) | icmp-decoder(*<attack>*) }, *<attack>* = attack type. <severity> = {very low | low | medium | high | severe}
`Program DFA failed.`	IDP program DFA to hardware search engine failed.
`IDP sigature update failed. Fail to create temporary directory`	IDP signature update failed. Create /tmp/sig directory failed

Table 198 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
IDP sigature update failed. Fail to extract temporary file.	IDP signature update failed. Extract signature package to /tmp/sig failed.
IDP signature update failed. Invalid IDP config file.	IDP signature update failed. Sig_check_update check failed.
IDP signature update failed. Invalid signature content.	IDP signature update failed. Sigquery check signature content failed.
System internal error. Create IDP traffic anomaly entry failed.	System internal error. Create IDP traffic anomaly entry failed.
Query signature version failed.	Unable to get signature version from new signature package download from update server
Can not get signature version.	Unable to get signature version from new signature package download from update server

Table 199 Application Patrol Logs

LOG MESSAGE	DESCRIPTION
System fatal error: 60005001.	Application patrol zysh initialization failed. Protocol file import error.
System fatal error: 60005002.	Application patrol zysh initialization failed. Shared memory failed.
System fatal error: 60005017.	Application patrol zyio failed. Fail to do zyio operation.
System fatal error: 60005018.	Application patrol kernel error. Fail to communicate with kernel module.
System fatal error: 60005019.	Application patrol configuration group error. Fail to retrieve use group from use object.
System fatal error: 60006004.	Application patrol daemon (process) shared memory key generating fail.
System fatal error: 60006021.	Error generating application patrol semaphore key.
System fatal error: 60006031.	Warning application patrol resources ran out! New configuration of affected rule [%s:%d] is discarded.
System fatal error: 60018001.	Application patrol daemon (process) out of share memory address pool.
System fatal error: 60018002.	Application patrol daemon (process) ran out of pre-allocated share memory.
System fatal error: 60018003.	Application patrol daemon (process) failed to lock shared memory.

Table 199 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
System fatal error: 60018004.	Application patrol daemon (process) failed to unlock shared memory.
System fatal error: 60018005.	Error generating application patrol semaphore key.
System fatal error: 60018006.	Application patrol daemon (process) fails to create share memory.
System fatal error: 60018007.	Error opening /dev/l7_action device.
System fatal error: 60018008.	Error when do ioctl L7_ACTION_IOCTL_ADDR_USAGE.
System fatal error: 60018009.	Error when do ioctl L7_ACTION_IOCTL_ADDR_USAGE.
System fatal error: 60018010.	Error when do ioctl L7_ACTION_IOCTL_PROTO_ADDR_NUMS.
System fatal error: 60018011.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018012.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018013.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018014.	Fail to user lib user_profile to retrieve current login user.
System fatal error: 60018015.	Fail to retrieve user event from uamd.
System fatal error: 60018016.	Application patrol daemon (process) shared memory generate failed.
System fatal error: 60018017.	Fail to get share memory.
System fatal error: 60018018.	Fail to get attach memory.
System fatal error: 60018019.	Application patrol daemon receive restart signal.
System fatal error: 60018020.	Application patrol daemon signal handler failed.
System fatal error: 60018021.	Application patrol daemon initialization failed.
System fatal error: 60018022.	Application patrol daemon startup failed.
System fatal error: 60018023.	Application patrol daemon stop.
Activate App. Patrol has succeeded.	Activate application patrol has succeeded.
No '%s' protocol.	The protocol %s does not exist. %s: Protocol Name
Service %s has been activated.	Protocol %s is active. %s: Protocol Name

Table 199 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
Deactivate App Patrol has succeeded.	Deactivation of application patrol has succeeded.
Initialize App. Patrol has succeeded.	Initialization application patrol has succeeded.
App Patrol Name=%s Type=%s %s=%d Protocol=%s Action=%s	Packets logging. 1st %s: Protocol Name, 2nd %s: Category Name, 3rd %s: Default Rule or Exception Rule, 1st %d: Rule Index, 4th %s: TCP or UDP, 5th %s: Action.
App Patrol resources ran out. User %s is unrestricted by rule [%s:%d]. 1st %s: User Name, 2nd %s: Protocol Name, 1% %d: Rule Index	The application patrol daemon (process) resource pool is full, current login user %s is unrestricted by rule %d of protocol %s. 1st %s: User Name, 1st %d: Rule Index, 2nd %s: Protocol Name.

Table 200 IKE Logs

LOG MESSAGE	DESCRIPTION
%s:%s has not announced DPD capability	%s:%s is the peer IP:Port. Peer has not announced capability.
[COOKIE] Invalid cookie, no sa found	Cannot find SA according to the cookie.
[DPD] No response from "%s:%s using existing Phase-1 SA in %u seconds. Trying with Phase-1 rekey.	%s:%s is the peer IP:Port. %u is the retry time. Dead Peer Detection (DPD) detected no response from peer.
[HASH] : Tunnel [%s] Phase 1 hash mismatch	%s is the tunnel name. When negotiating Phase-1, the exchange hash did not match.
[HASH] : Tunnel [%s] Phase 2 hash mismatch"	%s is the tunnel name. When negotiating Phase-2, the calculated quick mode authentication hash did not match.
[ID] : Invalid ID information	ID payload is not valid (in Phase-1 is local/peer ID, in Phase-2 is local/ remote policy).
[ID] : Tunnel [%s] Local IP mismatch	%s is the tunnel name. When negotiating Phase-1, the local tunnel IP did not match the My IP in VPN gateway.
[ID] : Tunnel [%s] My IP mismatch	%s is the tunnel name. When negotiating Phase-1 and selecting matched proposal, My IP Address could not be resolved.
[ID] : Tunnel [%s] Phase 1 ID mismatch	%s is the tunnel name. When negotiating Phase-1, the peer ID did not match.
[ID] : Tunnel [%s] Phase 2 Local ID mismatch	%s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.

Table 200 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
[ID] : Tunnel [%s] Phase 2 Remote ID mismatch	%s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID.
[ID] : Tunnel [%s] Remote IP mismatch	%s is the tunnel name. When negotiating Phase-1, the peer tunnel IP did not match the secure gateway address in VPN gateway.
[SA] : Malformed IPSec SA proposal	When selecting a matched proposal, some protocol was given more than once.
[SA] : No proposal chosen	When selecting a matched proposal in phase-1 or phase-2, so proposal was selected.
[SA] : Tunnel [%s] Phase 1 authentication algorithm mismatch	%s is the tunnel name. When negotiating Phase-1, the authentication algorithm did not match.
[SA] : Tunnel [%s] Phase 1 authentication method mismatch	%s is the tunnel name. When negotiating Phase-1, the authentication method did not match.
[SA] : Tunnel [%s] Phase 1 encryption algorithm mismatch	%s is the tunnel name. When negotiating Phase-1, the encryption algorithm did not match.
[SA] : Tunnel [%s] Phase 1 invalid protocol	%s is the tunnel name. When negotiating Phase-1, the packet was not a ISKAMP packet in the protocol field.
[SA] : Tunnel [%s] Phase 1 invalid transform	%s is the tunnel name. When negotiating Phase-1, the transform ID was invalid.
[SA] : Tunnel [%s] Phase 1 key group mismatch	%s is the tunnel name. When negotiating Phase-1, the DH group of the attribute list `attrs' did not match the security policy.
[SA] : Tunnel [%s] Phase 1 negotiation mode mismatch	%s is the tunnel name. When negotiating Phase-1, the negotiation mode did not match.
[SA] : Tunnel [%s] Phase 2 authentication algorithm mismatch	%s is the tunnel name. When negotiating Phase-2, the authentication algorithm did not match.
[SA] : Tunnel [%s] Phase 2 encapsulation mismatch	%s is the tunnel name. When negotiating Phase-2, the encapsulation did not match.
[SA] : Tunnel [%s] Phase 2 encryption algorithm mismatch	%s is the tunnel name. When negotiating Phase-2, the encryption algorithm did not match.
[SA] : Tunnel [%s] Phase 2 pfs mismatch	%s is the tunnel name. When negotiating Phase-2, the PFS specified did not match.
[SA] : Tunnel [%s] Phase 2 pfs unsupported: %d	%s is the tunnel name. When negotiating Phase-2, this device does not support the PFS specified.
[SA] : Tunnel [%s] Phase 2 SA encapsulation mismatch	%s is the tunnel name. When negotiating Phase-2, the SA encapsulation did not match.

Table 200 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
[SA] : Tunnel [%s] Phase 2 SA protocol mismatch	%s is the tunnel name. When negotiating Phase-2, the SA protocol did not match.
[SA] : Tunnel [%s] SA sequence size mismatch	%s is the tunnel name. When negotiating Phase-2, the SA sequence size did not match.
[XCHG] exchange type is not IP, AGGR, or INFO	This device is the responder and this is the initiator's first packet, but exchange type is not IP, AGGR, or INFO and the packet is ignored.
Cannot resolve My IP Addr %s for Tunnel [%s]	1st %s is my ip address. 2nd %s is the tunnel name. When selecting a matched proposal in phase-1, the engine could not get My-IP address.
Cannot resolve Secure Gateway Addr %s for Tunnel [%s]	1st %s is my ip address. 2nd %s is the tunnel name; When selecting a matched proposal in phase-1, the engine could not get the correct secure gateway address.
Could not dial dynamic tunnel "%s"	%s is the tunnel name. The tunnel is a dynamic tunnel and the device cannot dial it.
Could not dial incomplete tunnel "%s"	%s is the tunnel name. The tunnel setting is not complete.
Could not dial manual key tunnel "%s"	%s is the tunnel name. The manual key tunnel cannot be dialed.
DPD response with invalid ID	When receiving a DPD response with invalid ID ignored.
DPD response with no active request	When receiving a DPD response with no active query.
IKE Packet Retransmit	When retransmitting the IKE packets.
Phase 1 IKE SA process done	When Phase 1 negotiation is complete.
Recv Main Mode request from [%s]	%s is the remote name; When receiving a request to enter Main mode.
Recv Aggressive Mode request from [%s]	%s is the remote name; When receiving a request to enter Aggressive mode.
Recv DPD request from "%s:%s"	%s:%s is peer IP:Port. The device received a Dead Peer Detection request.
Recv DPD response from "%s:%s"	%s:%s is peer IP:Port. The device received a Dead Peer Detection response.
Recv:[SA]%s[KE]%s[ID]%s[CERT]%s[CR]%s[HASH]%s[SIG]%s[NONCE]%s[DEL]%s[VID]%s[ATTR]%s	This is a combined message for incoming IKE packets.
Send Main Mode request to [%s]	%s is the remote name. The device sent a request to enter Main Mode.
Send Aggressive Mode request to [%s]	%s is the remote name. The device sent a request to enter Aggressive Mode.
Send DPD request to "%s:%s"	%s:%s is peer IP:Port. The device sent a Dead Peer Detection request to the peer.

Table 200 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Send DPD response to "%s:%s"	%s:%s is peer IP:Port. The device sent a DPD response sent to the peer.
Send:[ID]%s[SA]%s[KE]%s[ID]%s[CERT]%s[CR]%s[HASH]%s[SIG]%s[NONCE]%s[DEL]%s[VID]%s[ATTR]%s[	This is a combined message for outgoing IKE packets.
Start Phase 2: Quick Mode	Indicates the beginning of phase 2 using quick mode.
The cookie pair is : 0x%08x%08x / 0x%08x%08x	Indicates the initiator/responder cookie pair.
The IPSec tunnel "%s" is already established	%s is the tunnel name. When dialing a tunnel, the tunnel is already dialed.
Tunnel [%s] built successfully	%s is the tunnel name. The phase-2 tunnel negotiation is complete.
Tunnel [%s] Phase 1 pre-shared key mismatch	%s is the tunnel name. When negotiating phase-1, the pre-shared key did not match.
Tunnel [%s] Recving IKE request	%s is the tunnel name. The device received an IKE request.
Tunnel [%s] Sending IKE request	%s is the tunnel name. The device sent an IKE request.
Tunnel [%s] IKE Negotiation is in process	%s is the tunnel name. When IKE request is already sent but still attempting to dial a tunnel.
VPN gateway %s was disabled	%s is the gateway name. An administrator disabled the VPN gateway.
VPN gateway %s was enabled	%s is the gateway name. An administrator enabled the VPN gateway.
XAUTH fail! My name: %s	%s is the my xauth name. This indicates that my name is invalid.
XAUTH fail! Remote user: %s	%s is the remote xauth name. This indicates that a remote user's name is invalid.
XAUTH succeed! My name: %s	%s is the my xauth name. This indicates that my name is valid.
XAUTH succeed! Remote user: %s	%s is the remote xauth name. This indicate that a remote user's name is valid
Dynamic Tunnel [%s:%s:0x%x:%s] built successfully	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.
Dynamic Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
Tunnel [%s:%s:0x%x:%s] built successfully	The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete.

Table 200 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully	The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully.
Tunnel [%s:%s] Phase 1 pre-shared key mismatch	The variables represent the phase 1 name and tunnel name. When negotiating phase-1, the pre-shared keys did not match.
Tunnel [%s:%s] Recving IKE request	The variables represent the phase 1 name and tunnel name. The device received an IKE request.
Tunnel [%s:%s] Sending IKE request	The variables represent the phase 1 name and tunnel name. The device sent an IKE request.
Tunnel [%s:0x%x] is disconnected	The variables represent the tunnel name and the SPI of a tunnel that was disconnected.
Tunnel [%s] rekeyed successfully	%s is the tunnel name. The tunnel was rekeyed successfully.

Table 201 IPSec Logs

LOG MESSAGE	DESCRIPTION
Corrupt packet, Inbound transform operation fail	The device received corrupt IPsec packets and could not process them.
Encapsulated packet too big with length	An outgoing packet needed to be transformed but was longer than 65535.
Get inbound transform fail	When performing inbound processing for incoming IPSEC packets and ICMPs related to them, the engine cannot obtain the transform context.
Get outbound transform fail	When outgoing packet need to be transformed, the engine cannot obtain the transform context.
Inbound transform operation fail	After encryption or hardware accelerated processing, HWAccel dropped packet (resource shortage, corrupt packet, invalid MAC, and so on).
Outbound transform operation fail	After encryption or hardware accelerated processing, Hwaccel dropped packet (e.g., resource overflow, corrupt packet, and so on).
Packet too big with Fragment Off	An outgoing packet needed to be transformed, but the fragment flag was off and the packet was too big.
SPI:0x%x SEQ:0x%x Execute transform step fail, ret=%d	The variables represent the SPI, sequence number and the error number. When trying to perform transforming, the engine returned an error.
SPI:0x%x SEQ:0x%x No rule found, Dropping packet	The variables represent the SPI and the sequence number. The packet did not match the tunnel policy and was dropped.
SPI:0x%x SEQ:0x%x Packet Anti-Replay detected	The variables represent the SPI and the sequence number. The device received a packet again (that it had already received).

Table 201 IPSec Logs (continued)

LOG MESSAGE	DESCRIPTION
VPN connection %s was disabled.	%s is the VPN connection name. An administrator disabled the VPN connection.
VPN connection %s was enabled.	%s is the VPN connection name. An administrator enabled the VPN connection.

Table 202 Firewall Logs

LOG MESSAGE	DESCRIPTION
priority:%lu, from %s to %s, service %s, %s	1st variable is the global index of rule, 2nd is the from zone, 3rd is the to zone, 4th is the service name, 5th is ACCEPT/DROP/ REJECT.
%s:%d: in %s():	Firewall is dead, trace to %s is which file, %d is which line, %s is which function
Firewall has been %s.	%s is enabled/disabled
Firewall rule %d has been moved to %d.	1st %d is the old global index of rule, 2nd %d is the new global index of rule
Firewall rule %d has been deleted.	%d is the global index of rule
Firewall rules have been flushed.	Firewall rules were flushed
Firewall rule %d was %s.	%d is the global index of rule, %s is appended/inserted/modified
Firewall %s %s rule %d was %s.	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule 3rd %s is appended/inserted/modified
Firewall %s %s rule %d has been moved to %d.	1st %s is from zone, 2nd %s is to zone, 1st %d is the old index of the rule 2nd %d is the new index of the rule
Firewall %s %s rule %d has been deleted.	1st %s is from zone, 2nd %s is to zone, %d is the index of the rule
Firewall %s %s rules have been flushed.	1st %s is from zone, 2nd %s is to zone
abnormal TCP flag attack detected	Abnormal TCP flag attack detected
invalid state detected	Invalid state detected
The Asymmetrical Route has been enabled.	Asymmetrical route has been turned on.
The Asymmetrical Route has been disabled.	Asymmetrical Route has been turned off.

Table 203 Sessions Limit Logs

LOG MESSAGE	DESCRIPTION
Maximum sessions per host (%d) was exceeded.	%d is maximum sessions per host.

Table 204 Policy Route Logs

LOG MESSAGE	DESCRIPTION
Cann't open bwm_entries	Policy routing can't activate BWM feature.
Cann't open link_down	Policy routing can't detect link up/down status.
Cannot get handle from UAM, user-aware PR is disabled	User-aware policy routing is disabled due to some reason.
mblock: allocate memory failed!	Allocating policy routing rule fails: insufficient memory.
pt: allocate memory failed!	Allocating policy routing rule fails: insufficient memory.
To send message to policy route daemon failed!	Failed to send control message to policy routing manager.
The policy route %d allocates memory fail!	Allocating policy routing rule fails: insufficient memory. %d: the policy route rule number
The policy route %d uses empty user group!	Use an empty object group. %d: the policy route rule number
The policy route %d uses empty source address group!	Use an empty object group. %d: the policy route rule number
The policy route %d uses empty destination address group!	Use an empty object group. %d: the policy route rule number
The policy route %d uses empty service group	Use an empty object group. %d: the policy route rule number
Policy-route rule %d was inserted.	Rules is inserted into system. %d: the policy route rule number
Policy-route rule %d was appended.	Rules is appended into system. %d: the policy route rule number
Policy-route rule %d was modified.	Rule is modified. %d: the policy route rule number

Table 204 Policy Route Logs (continued)

LOG MESSAGE	DESCRIPTION
Policy-route rule %d was moved to %d.	Rule is moved. 1st %d: the original policy route rule number 2nd %d: the new policy route rule number
Policy-route rule %d was deleted.	Rule is deleted. %d: the policy route rule number
Policy-route rules were flushed.	Policy routing rules are cleared.

Table 205 Built-in Services Logs

LOG MESSAGE	DESCRIPTION
User on %u.%u.%u.%u has been denied access from %s	HTTP/HTTPS/TELNET/SSH/FTP/SNMP access to the device was denied. %u.%u.%u.%u is IP address %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET
HTTPS certificate:%s does not exist. HTTPS service will not work.	An administrator assigned a nonexistent certificate to HTTPS. %s is certificate name assigned by user
HTTPS port has been changed to port %s.	An administrator changed the port number for HTTPS. %s is port number
HTTPS port has been changed to default port.	An administrator changed the port number for HTTPS back to the default (443).
HTTP port has changed to port %s.	An administrator changed the port number for HTTP. %s is port number assigned by user
HTTP port has changed to default port.	An administrator changed the port number for HTTP back to the default (80).
SSH port has been changed to port %s.	An administrator changed the port number for SSH. %s is port number assigned by user
SSH port has been changed to default port.	An administrator changed the port number for SSH back to the default (22).
SSH certificate:%s does not exist. SSH service will not work.	An administrator assigned a nonexistent certificate to SSH. %s is certificate name assigned by user
SSH certificate:%s format is wrong. SSH service will not work.	After an administrator assigns a certificate for SSH, the device needs to convert it to a key used for SSH. %s is certificate name assigned by user
TELNET port has been changed to port %s.	An administrator changed the port number for TELNET. %s is port number assigned by user
TELNET port has been changed to default port.	An administrator changed the port number for TELNET back to the default (23).

Table 205 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
FTP certificate:%s does not exist.	An administrator assigned a nonexistent certificate to FTP. %s is certificate name assigned by user
FTP port has been changed to port %s.	An administrator changed the port number for FTP. %s is port number assigned by user
FTP port has been changed to default port.	An administrator changed the port number for FTP back to the default (21).
SNMP port has been changed to port %s.	An administrator changed the port number for SNMP. %s is port number assigned by user
SNMP port has been changed to default port.	An administrator changed the port number for SNMP back to the default (161).
Console baud has been changed to %s.	An administrator changed the console port baud rate. %s is baud rate assigned by user
Console baud has been reset to %d.	An administrator changed the console port baud rate back to the default (115200). %d is default baud rate
DHCP Server on Interface %s will not work due to Device HA status is Stand-By	If interface is stand-by mode for device HA, DHCP server can't be run. Otherwise it has conflict with the interface in master mode. %s is interface name
DHCP Server on Interface %s will be reapplied due to Device HA status is Active	When an interface has become the HA master, the DHCP server needs to start operating. %s is interface name
DHCP's DNS option:%s has changed.	DHCP pool's DNS option support from WAN interface. If this interface is unlink/disconnect or link/connect, this log will be shown. %s is interface name. The DNS option of DHCP pool has retrieved from it
Set timezone to %s.	An administrator changed the time zone. %s is time zone value
Set timezone to default.	An administrator changed the time zone back to the default (0).
Enable daylight saving.	An administrator turned on daylight saving.
Disable daylight saving.	An administrator turned off daylight saving.
DNS access control rules have been reached the maximum number.	An administrator tried to add more than the maximum number of DNS access control rules (64).
DNS access control rule %u of DNS has been appended.	An administrator added a new rule. %u is rule number

Table 205 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
DNS access control rule %u has been inserted.	An administrator inserted a new rule. %u is rule number
DNS access control rule %u has been appended	An administrator appended a new rule. %u is rule number
DNS access control rule %u has been modified	An administrator modified the rule %u. %u is rule number
DNS access control rule %u has been deleted.	An administrator removed the rule %u. %u is rule number
DNS access control rule %u has been moved to %d.	An administrator moved the rule %u to index %d. %u is previous index %d variable is current index
The default record of Zone Forwarder have reached the maximum number of 128 DNS servers.	The default record DNS servers is more than 128.
Interface %s ping check is successful. Zone Forwarder adds DNS servers in records.	Ping check ok, add DNS servers in bind. %s is interface name
Interface %s ping check is failed. Zone Forwarder removes DNS servers in records.	Ping check failed, remove DNS servers from bind. %s is interface name
Interface %s ping check is disabled. Zone Forwarder adds DNS servers in records.	Ping check disabled, add DNS servers in bind. %s is interface name
Wizard apply DNS server failed.	Wizard apply DNS server failed.
Wizard adds DNS server %s failed because DNS zone setting has conflictd.	Wizard apply DNS server failed because DNS zone conflicted. %s is the IP address of the DNS server
Wizard adds DNS server %s failed because Zone Forwarder numbers have reached the maximum number of 32.	Wizard apply DNS server fail because the device already has the maximum number of DNS records configured. %s is IP address of the DNS server.
Access control rules of %s have reached the maximum number of %u	The maximum number of allowable rules has been reached. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. %u is the maximum number of access control rules.

Table 205 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
Access control rule %u of %s was appended.	A new built-in service access control rule was appended. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %u of %s was inserted.	An access control rule was inserted successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %u of %s was modified.	An access control rule was modified successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %u of %s was deleted.	An access control rule was removed successfully. %u is the index of the access control rule. %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.
Access control rule %d of %s was moved to %d.	An access control rule was moved successfully. 1st %d is the previous index . %s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. 2nd %d is current previous index.
SNMP trap can not be sent successfully	Cannot send a SNMP trap to a remote host due to network error

Table 206 System Logs

LOG MESSAGE	DESCRIPTION
Port %d is up!!	When LINK is up, %d is the port number.
Port %d is down!!	When LINK is down, %d is the port number.
%s is dead at %s	A daemon (process) is gone (was killed by the operating system). 1st %s: Daemon Name, 2nd %s: date+time
%s process count is incorrect at %s	The count of the listed process is incorrect. 1st %s: Daemon Name, 2nd %s: date+time
%s becomes Zombie at %s	A process is present but not functioning. 1st %s: Daemon Name, 2nd %s: date+time When memory usage exceed threshold-max, memory usage reaches %d%% :mem-threshold-max. When disk usage exceeds threshold-max, %s: Partition name file system usage reaches %d%%: disk-threshold-max. When memory usage drops below threshold-min, System Memory usage drops below the threshold of %d%%: mem-threshold-min. When disk usage drops below threshold-min, %s: partition_name file system drops below the threshold of %d%%: disk-threshold-min.
DHCP Server executed with cautious mode enabled	DHCP Server executed with cautious mode enabled.
DHCP Server executed with cautious mode disabled	DHCP Server executed with cautious mode disabled.

Table 206 System Logs (continued)

LOG MESSAGE	DESCRIPTION
Received packet is not an ARP response packet	A packet was received but it is not an ARP response packet.
Receive an ARP response	The device received an ARP response.
Receive ARP response from %s (%s)	The device received an ARP response from the listed source.
The request IP is: %s, sent from %s	The device accepted a request.
Received ARP response NOT for the request IP address	The device received an ARP response that is NOT for the requested IP address.
Receive an ARP response from the client issuing the DHCP request	The device received an ARP response from the client issuing the DHCP request.
Receive an ARP response from an unknown client	The device received an ARP response from an unknown client.
In total, received %d arp response packets for the requested IP address	The device received the specified total number of ARP response packets for the requested IP address.
Clear arp cache successfully.	The ARP cache was cleared successfully.
Client MAC address is not an Ehernet address	A client MAC address is not an Ethernet address.
DHCP request received via interface %s (%s:%s), src_mac: %s with requested IP: %s	The device received a DHCP request through the specified interface.
IP confliction is detected. Send back DHCP-NAK.	IP conflict was detected. Send back DHCP-NAK.
Clear ARP cache done	Clear ARP cache done.
NTP update successful, current time is %s	The device successfully synchronized with a NTP time server . %s is the time format.
NTP update failed	The device was not able to synchronize with the NTP time server successfully.
Device is rebooted by administrator!	An administrator restarted the device.
Insufficient memory.	Cannot allocate system memory.
Connect to dyndns server has failed.	Cannot connect to members.dyndns.org to update DDNS.

Table 206 System Logs (continued)

LOG MESSAGE	DESCRIPTION
Update the profile %s has failed because of strange server response.	Update profile failed because the response was strange, %s is the profile name.
Update the profile %s has succeeded because the IP address of FQDN %s was not changed.	Update profile succeeded, because the IP address of profile is unchanged, %s is the profile name.
Update the profile %s has succeeded.	Update profile succeeded, %s is the profile name.
Update the profile %s has failed because the FQDN %s is invalid.	Update profile failed because FQDN for the profile is invalid for DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because the FQDN %s is malformed.	The FQDN format is malformed for DynDNS server, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because the FQDN %s is not under your control.	The owner of this FQDN is not the user, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because the FQDN %s was blocked for abuse.	The FQDN is blocked by DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because of authentication fail.	Try to update profile, but failed, because of authentication fail, %s is the profile name.
Update the profile %s has failed because of invalid system parameters.	Some system parameters are invalid to update FQDN, %s is the profile name.
Update the profile %s has failed because the FQDN %s was blocked.	The FQDN is blocked by DynDNS , 1st %s is the profile name, 2nd %s is the FQDN of the profile.
Update the profile %s has failed because too many or too few hosts found.	%s is the profile name.
Update the profile %s has failed because of dyndns internal error	Update profile failed because of a dynsdns internal error, %s is the profile name.
Update the profile %s has failed because the feature requested is only available to donators.	Update profile failed because the feature requested is only available to donators, %s is the profile name.
Update the profile %s has failed because of error response.	Update profile failed because the response is incorrect, %s is the profile name.

Table 206 System Logs (continued)

LOG MESSAGE	DESCRIPTION
Update the profile %s has failed because %s.	Update profile failed, and show the response message, 1st %s is the profile name, 2nd %s is the reason.
Update the profile %s has failed because of unknown error.	Update profile failed because unknown error. Sometimes, the force authentication will result in this error, 1st %s is the profile name.
Update the profile %s has failed because Username was empty.	DDNS profile needs username, %s is the profile name.
Update the profile %s has failed because Password was empty.	DDNS profile needs password, %s is the profile name.
Update the profile %s has failed because Domain name was empty.	DDNS profile needs domain name, %s is the profile name.
Update the profile %s has failed because Custom IP was empty.	The DDNS profile's IP select type is custom, and a custom IP was not defined, %s is the profile name.
Update the profile %s has failed because WAN interface was empty.	If the DDNS profile's IP select type is iface, it needs a WAN iface, %s is the profile name.
The profile %s has been paused because the VRRP status of WAN interface was standby.	The profile is paused by device-HA, because the VRRP status of that iface is standby, %s is the profile name.
Update the profile %s has failed because WAN interface was link-down.	DDNS profile cannot be updated for WAN IP because WAN iface is link-down, %s is the profile name.
Update the profile %s has failed because WAN interface was not connected.	DDNS profile cannot be updated for WAN IP because WAN iface is PPP and not connected, %s is the profile name.
Update the profile %s has failed because IP address of WAN interface was empty.	DDNS profile cannot be updated because the IP of WAN iface is 0.0.0.0, 1st %s is the profile name.
Update the profile %s has failed because ping-check of WAN interface has failed.	DDNS profile cannot be updated because the ping-check for WAN iface failed , %s is the profile name.
The profile %s has been paused because the HA interface of VRRP status was standby.	The profile is paused by Device-HA, because the VRRP status of that HA iface is standby, %s is the profile name.
Update the profile %s has failed because HA interface was link-down.	DDNS profile cannot be updated for HA IP address because HA iface is link-down, %s is the profile name.

Table 206 System Logs (continued)

LOG MESSAGE	DESCRIPTION
Update the profile %s has failed because the HA interface was not connected.	DDNS profile cannot be updated for HA IP address because HA iface is PPP and not connected, %s is the profile name.
Update the profile %s has failed because IP address of HA interface was empty.	DDNS profile cannot be updated because the IP address of HA iface is 0.0.0.0, %s is the profile name.
Update the profile %s has failed because ping-check of HA interface has failed.	DDNS profile cannot be updated because the fail of ping-check for HA iface, %s is the profile name
DDNS has been disabled by Device-HA.	DDNS is disabled by Device-HA, because all VRRP groups are standby.
DDNS has been enabled by Device-HA.	DDNS is enabled by Device-HA, because one of VRRP groups is active.
Disable DDNS has succeeded.	Disable DDNS.
Enable DDNS has succeeded.	Enable DDNS.
DDNS profile %s has been renamed as %s.	Rename DDNS profile, 1st %s is the original profile name, 2nd %s is the new profile name.
DDNS profile %s has been deleted.	Delete DDNS profile, %s is the profile name,
DDNS Initialization has failed.	Initialize DDNS failed,
All DDNS profiles are deleted	All DDNS profiles have been removed.

Table 207 Connectivity Check Logs

LOG MESSAGE	DESCRIPTION
Cann't open link_up2	Can not recover routing status which is link-down.
Can not open %s.pid	Can not open connectivity check process ID file. %s: interface name
Can not open %s.arg	Can not open configuration file for connectivity check process. %s: interface name
The connectivity-check is activate for %s interface	The link status of interface is still activate after check of connectivity check process. %s: interface name
The connectivity-check is fail for %s interface	The link status of interface is fail after check of connectivity check process. %s: interface name

Table 207 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
Can't get gateway IP of %s interface	The connectivity check process can't get the gateway IP address for the specified interface. %s: interface name
Can't alloc memory	The connectivity check process can't get memory from OS.
Can't load %s module	The connectivity check process can't load module for check link-status. %s: the connectivity module, currently only ICMP available.
Can't handle 'isalive' function of %s module	The connectivity check process can't execute 'isalive' function from module for check link-status. %s: the connectivity module, currently only ICMP available.
Create socket error	The connectivity check process can't get socket to send packet.
Can't get IP address of %s interface	The connectivity check process can't get IP address of interface. %s: interface name.
Can't get flags of %s interface	The connectivity check process can't get interface configuration. %s: interface name
Can't get remote address of %s interface	The connectivity check process can't get remote address of PPP interface %s: interface name
Can't get NETMASK address of %s interface	The connectivity check process can't get netmask address of interface. %s: interface name
Can't get BROADCAST address of %s interface	The connectivity check process can't get broadcast address of interface %s: interface name
Can't use MULTICAST IP for destination	The connectivity check process can't use multicast address to check link-status.
The destination is invalid, because destination IP is broadcast IP	The connectivity check process can't use broadcast address to check link-status.
Can't get MAC address of %s interface!	The connectivity check process can't get MAC address of interface. %s: interface name
To send ARP REQUEST error!	The connectivity check process can't send ARP request packet.
The %s routing status seted to DEAD by connectivity-check	The interface routing can't forward packet. %s: interface name
The %s routing status seted ACTIVATE by connectivity-check	The interface routing can forward packet. %s: interface name

Table 208 Device HA Logs

LOG MESSAGE	DESCRIPTION
Device HA VRRP Group %s has been added.	An VRRP group has been created, %s: the name of VRRP group.
Device HA VRRP group %s has been modified.	An VRRP group has been modified, %s: the name of VRRP group.
Device HA VRRP group %s has been deleted.	An VRRP group has been deleted, %s: the name of VRRP group.
Device HA VRRP interface %s for VRRP Group %s has changed.	Configuration of an interface that belonged to a VRRP group has been changed, 1st %s: VRRP interface name, 2ed %s: %s: the name of VRRP group.
Device HA syncing from %s starts.	Device HA Syncing from Master starts when user click "Sync Now" using Auto Sync, %s: The IP of FQDN of Master.
%s has no file to sync, Skip syncing it for %s.	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2ed %s: The feature name for the syncing object.
Master configuration is the same with Backup. Skip updating it.	The System Startup configuration file synchronized from the Master is the same with the one in the Backup, so the configuration does not have to be updated.
%s file not existed, Skip syncing it for %s	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2ed %s: The feature name for the syncing object.
Master firmware version can not be recognized. Stop syncing from Master.	Synchronizing stopped because the firmware version file was not found in the Master. A Backup device only synchronizes from the Master if the firmware versions are the same between the Master and the Backup.
Device HA Sync has failed when syncing %s for %s due to bad \"Sync Password\".	The synchronization password was incorrect when attempting to synchronize a certain object (AV/AS/IDP/Certificate/System Configuration). 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
Device HA Sync has failed when syncing %s for %s due to bad \"Sync From\" or \"Sync Port\".	The Sync From IP address or Sync Port may be incorrect when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration).
Device HA Sync has failed when syncing %s for %s.	Synchronization failed when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration) due to an unknown reason, 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
Sync Failed: Cannot connect to Master when syncing %s for %s.	Synchronization failed because the Backup could not connect to the Master. The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.

Table 208 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
Backup firmware version can not be recognized. Stop syncing from Master.	The firmware version on the Backup cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Sync failed: Remote Firmware Version Unknown	The firmware version on the Master cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Master firmware version should be the same with Backup.	The Backup and Master have different firmware versions. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Update %s for %s has failed.	Updating a certain object failed when updating (AS/AV/IDP/Certificate/ System Configuration). 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
Update %s for %s has failed: %s.	Updating a certain object failed when updating (AS/AV/IDP/Certificate/ System Configuration) due to some reason. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized.
Device HA has skipped syncing %s since %s is %s.	A certain service has no license or the license is expired, so it was not synchronized from the Master. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized, 3rd %s: unlicensed or license expired.
Device HA authentication type for VRRP group %s maybe wrong.	A VRRP group's Authentication Type (Md5 or IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Device HA authenticaton string of text for VRRP group %s maybe wrong.	A VRRP group's Simple String (Md5) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Device HA authentication string of AH for VRRP group %s maybe wrong.	A VRRP group's AH String (IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Retrying to update %s for %s. Retry: %d.	An update failed. Retrying to update the failed object again. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized, %d: the retry count.
Recovring to Backup original state for %s has failed.	An update failed. The device will try to recover the failed update feature to the original state before Device HA synchronizes the specified object.
Recovering to Backup original state for %s has succeeded.	Recovery succeeded when an update for the specified object failed.
One of VRRP groups has became avtive. Device HA Sync has aborted from Master %s.	%s: IP or FQDN of Master

Table 208 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
Master configuration file does not exist. Skip updating ZySH Startup Configuration.	
System internal error: %s. Skip updating %s.	1st %s: error string, 2ed %s: the syncing object
Master configuration file is empty. Skip updating ZySH Startup Configuration.	
Device HA Sync has failed when syncing %s for %s due to transnission timeout.	1st %s: the syncing object, 2ed %s: the feature name for the syncing object

Table 209 Routing Protocol Logs

LOG MESSAGE	DESCRIPTION
RIP on interface %s has been stopped because Device-HA binds this interface.	Device-HA is currently running on the interface %s, so all the local service have to be stopped including RIP. %s: Interface Name
RIP on all interfaces have been stopped	Got the CLI command 'no router rip' to shut down RIP on all interfaces
Invalid RIP md5 authentication	RIP md5 authentication has been set without setting md5 authentication id and key first
Invalid RIP text authentication.	RIP text authentication has been set without setting authentication key first
RIP on interface %s has been activated.	RIP on interface %s has been activated. %s: Interface Name
RIP direction on interface %s has been changed to In-Only.	RIP direction on interface %s has been changed to In-Only. %s: Interface Name
RIP direction on interface %s has been changed to Out-Only.	RIP direction on interface %s has been changed to Out-Only. %s: Interface Name
RIP authentication mode has been changed to %s.	RIP authentication mode has been changed to text or md5.
RIP text authentication key has been changed.	RIP text authentication key has been changed.
RIP md5 authentication id and key have been changed.	RIP md5 authentication id and key have been changed.

Table 209 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
RIP global version has been changed to %s.	RIP global version has been changed to version 1 or 2.
RIP redistribute OSPF routes has been enabled.	RIP redistribute OSPF routes has been enabled.
RIP redistribute static routes has been enabled.	RIP redistribute static routes has been enabled.
RIP on interface %s has been deactivated.	RIP on interface %s has been deactivated. %s: Interface Name
RIP direction on interface %s has been changed to BiDir.	RIP direction on interface %s has been changed to BiDir. %s: Interface Name
RIP authentication has benn disabled.	RIP text or md5 authentication has been disabled.
RIP text authentication key has been deleted.	RIP text authentication key has been deleted.
RIP md5 authentication id and key have been deleted.	RIP md5 authentication id and key have been deleted.
RIP global version has been deleted.	RIP global version has been deleted.
RIP redistribute OSPF routes has been disabled.	RIP redistribute OSPF routes has been disabled.
RIP redistribute static routes has been disabled.	RIP redistribute static routes has been disabled.
RIP v2-broadcast on interface %s has been enabled.	RIP v2-broadcast on interface %s has been enabled. %s: Interface Name.
RIP send-version on interface %s has been changed to %s.	RIP send-version on interface %s has been changed to version 1 or 2 or both 1 2. %s: Interface Name.
RIP receive-version on interface %s has been changed to %s.	RIP receive-version on interface %s has been changed to version 1 or 2 or both 1 2. 2nd%s: Interface Name.
RIP send-version on interface %s has been reset to current global version %s.	RIP send-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP Version
RIP receive-version on interface %s has been reset to current global version %s.	RIP receive-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP

Table 209 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
RIP v2-broadcast on interface %s has been disabled.	RIP v2-broadcast on interface %s has been disabled. %s: Interface Name
OSPF on interface %s has been stopped because Device-HA binds this interface.	Device-HA is currently running on the interface %s, so all the local service have to be stopped including OSPF. %s: Interface Name
Area %s cannot be removed. This area is in use.	One or more interfaces are still using this area, so area %s cannot be removed. %s: OSPF Area
Invalid OSPF %s authentication of area %s.	OSPF md5 or text authentication has been set without setting md5 authentication id and key, or text authentication key first.
Invalid OSPF virtual-link %d md5 authentication of area %s.	Virtual-link %s md5 authentication has been set without setting md5 authentication id and key first. %s: Virtual-Link ID
Invalid OSPF virtual-link %s text authentication of area %s.	Virtual-link %s text authentication has been set without setting text authentication key first. %s: Virtual-Link ID
Invalid OSPF virtual-link %s authentication of area %s.	Virtual-link %s authentication has been set to same-as-area but the area has invalid authentication configuration. %s: Virtual-Link ID
Invalid OSPF md5 authentication on interface %s.	Invalid OSPF md5 authentication is set on interface %s. %s: Interface Name
Invalid OSPF text authentication on interface %s.	Invalid OSPF text authentication is set on interface %s. %s: Interface Name
Interface %s does not belong to any OSPF area.	Interface %s has been set OSPF authentication same-as-area, however the interface does not belong to any OSPF area. %s: Interface Name
Invalid OSPF authentication of area %s on interface %s.	Interface %s has been set OSPF authentication same-as-area, however the area has invalid text authentication configuration. %s: Interface Name

Table 210 NAT Logs

LOG MESSAGE	DESCRIPTION
The NAT range is full	The NAT mapping table is full.
%s FTP ALG has succeeded.	The FTP Application Layer Gateway (ALG) has been turned on or off. %s: Enable or Disable

Table 210 NAT Logs (continued)

LOG MESSAGE	DESCRIPTION
Extra signal port of FTP ALG has been modified.	Extra FTP ALG port has been changed.
Signal port of FTP ALG has been modified.	Default FTP ALG port has been changed.
%s H.323 ALG has succeeded.	The H.323 ALG has been turned on or off. %s: Enable or Disable
Extra signal port of H.323 ALG has been modified.	Extra H.323 ALG port has been changed.
Signal port of H.323 ALG has been modified.	Default H.323 ALG port has been changed.
%s SIP ALG has succeeded.	The SIP ALG has been turned on or off. %s: Enable or Disable
Extra signal port of SIP ALG has been modified.	Extra SIP ALG port has been changed.
Signal port of SIP ALG has been modified.	Default SIP ALG port has been changed.
Register SIP ALG extra port=%d failed.	SIP ALG apply additional signal port failed. %d: Port number
Register SIP ALG signal port=%d failed.	SIP ALG apply signal port failed. %d: Port number
Register H.323 ALG extra port=%d failed.	H323 ALG apply additional signal port failed. %d: Port number
Register H.323 ALG signal port=%d failed.	H323 ALG apply signal port failed. %d: Port number
Register FTP ALG extra port=%d failed.	FTP ALG apply additional signal port failed. %d: Port number
Register FTP ALG signal port=%d failed.	FTP ALG apply signal port failed. %d: Port number

Table 211 PKI Logs

LOG MESSAGE	DESCRIPTION
Generate X509certifiate "%s" successfully	The router created an X509 format certificate with the specified name.
Generate X509 certifiate "%s" failed, errno %d	The router was not able to create an X509 format certificate with the specified name. See Table 214 on page 410 for details about the error number.

Table 211 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Generate certifiate request "%s" successfully	The router created a certificate request with the specified name.
Generate certifiate request "%s" failed, errno %d	The router was not able to create a certificate request with the specified name. See Table 214 on page 410 for details about the error number.
Generate PKCS#12 certificate "%s" successfully	The router created a PKCS#12 format certificate with the specified name.
Generate PKCS#12 certificate "%s" failed, errno %d	The router was not able to create anPKCS#12 format certificate with the specified name. See Table 214 on page 410 for details about the error number.
Prepare to import "%s" into "My Certificate"	%s is the name of a certificate request.
Prepare to import "%s" into Trusted Certificate"	%s is the name of a certificate request.
CMP enrollment "%s" successfully, CA "%s", URL "%s"	The device used CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
CMP enrollment "%s" failed, CA "%s", URL "%s"	The device was unable to use CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
SCEP enrollment "%s" successfully, CA "%s", URL "%s"	The device used SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL .
SCEP enrollment "%s" failed, CA "%s", URL "%s"	The device was unable to use SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL
Import X509 certificate "%s" into My Certificate successfully	The device imported a x509 format certificate into My Certificates. %s is the certificate request name.
Import X509 certificate "%s" into Trusted Certificate successfully	The device imported a x509 format certificate into Trusted Certificates. %s is the certificate request name.
Import PKCS#12 certificate "%s" into "My Certificate" successfully	The device imported a PKCS#12 format certificate into My Certificates. %s is the certificate request name.
Import PKCS#7 certificate "%s" into "My Certificate" successfully	The device imported a PKCS#7 format certificate into My Certificates. %s is the certificate request name.

Table 211 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Import PKCS#7 certificate "%s" into "Trusted Certificate" successfully	The device imported a PKCS#7 format certificate into Trusted Certificates. %s is the certificate request name.
Decode imported certificate "%s" failed	The device was not able to decode an imported certificate. %s is certificate the request name
Export PKCS#12 certificate "%s" from "My Certificate" successfully	The device exported a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
Export PKCS#12 certificate "%s" from "My Certificate" failed	The device was not able to export a PKCS#12 format certificate from My Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "My Certificate" failed	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "Trusted Certificate" failed	The device was not able to export a x509 format certificate from Trusted Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "My Certificate" successfully	The device exported a x509 format certificate from My Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "Trusted Certificate" successfully	The device exported a x509 format certificate from Trusted Certificates. %s is the certificate request name.
Export X509 certificate "%s" from "My Certificate" failed	The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name.
Import PKCS#12 certificate "%s" with incorrect password	An administrator used the wrong password when trying to import a PKCS#12 format certificate. %s is the certificate name.
Cert trusted: %s	%s is the subject.
Due to %d, cert not trusted: %s	%d is an error number (see Table 214 on page 410), %s is the certificate subject.

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.

CODE	DESCRIPTION
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 212 Interface Logs

LOG MESSAGE	DESCRIPTION
Interface %s has been deleted.	An administrator deleted an interface. %s is the interface name.
AUX Interface dialing failed. This AUX interface is not enabled.	A user tried to dial the AUX interface, but the AUX interface is not enabled.
AUX Interface disconnecting failed. This AUX interface is not enabled.	The AUX interface is not enabled and a user tried to use the disconnect aux command.

Table 212 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
Please type phone number of interface AUX first then dial again.	A user tried to dial the AUX interface, but the AUX interface does not have a phone number set.
Please type phone number of Interface AUX first then disconnect again.	The AUX interface does not have a phone number set and a user tried to use the disconnect aux command.
Interface %s will reapply because Device HA become active status.	Device-ha became active and is using a PPP base interface, the PPP interface must reapply, %s is the interface name.
Interface %s will reapply because Device HA is not running.	Device-ha was deleted and free PPP base interface, PPP interface must reapply, %s is the interface name.
Interface %s will stop connect because Device HA become standby status.	When device-ha is stand-by and use PPP base interface, PPP interface connection will stop, %s: interface name.
Create interface %s has been failed.	When PPP can't running fail, %s: interface name.
Base interface %s is disabled. Interface %s is disabled now.	When user disable ethernet, vlan or bridge interface and this interface is base interface of PPP or virtual interface. PPP and virtual will disable too. 1st %s is interface name, 2nd %s is interface.
Interface %s has been changed.	An administrator changed an interface's configuration. %s: interface name.
Interface %s has been added.	An administrator added a new interface. %s: interface name.
Interface %s is enabled.	An administrator enabled an interface. %s: interface name.
Interface %s is disabled.	An administrator disabled an interface. %s: interface name.
%s MTU > (%s MTU - 8), %s may not work correctly.	An administrator configured a PPP interface, PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface ans peer will not receive correct PPP packets. 1st %s: PPP interface name, 2nd %s: ethernet interface name.
(%s MTU - 8) < %s MTU, %s may not work correctly.	An administrator configured ethernet, vlan or bridge and this interface is base interface of PPP interface. PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and peer will not receive correct PPP packets.1st %s: Ethernet interface name, 2nd %s: PPP interface name.
Interface %s links down. Default route will not apply until interface %s links up.	An administrator set a static gateway in interface but this interface is link down. At this time the configuration will be saved but route will not take effect until the link becomes up.1st %s: interface name, 2nd %s: interface name.

Table 212 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u,UpTime=%s	Port statistics log. This log will be sent to the VRPT server. 1st %s: physical port name, 2nd %s: physical port status, 1st %u: physical port Tx packets, 2nd %u: physical port Rx packets, 3rd %u: physical port packets collisions, 4th %u: physical port Tx Bytes/s, 5th %u: physical port Rx Bytes/s, 3rd %s: physical port up time.
name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u	Interface statistics log. This log will be sent to the VRPT server. 1st %s: interface name, 2nd %s: interface status, 1st %u variable: interface Tx packets, 2nd %u variable: interface Rx packets, 3rd %u: interface packets collisions, 4th %u: interface Tx Bytes/s, 5th %u: interface Rx Bytes/s.
Interface %s start dailing.	A PPP or aux interface started dailing to a server. %s: interface name.
Interface %s connect failed: Connect to server failed.	A PPTP interface failed to connect to the PPTP server. %s: interface name.
Interface %s connection terminated.	A PPP or AUX connection will terminate. %s: interface name.
Interface %s connection terminated: idle timeout.	An idle PPP or AUX connection timed out.1%s: interface name.
Interface %s connect failed: MS-CHAPv2 mutual authentication failed.	MS-CHAPv2 authentication failed (the server must support mS-CHAPv2 and verify that the authentication failed, this does not include cases where the servers does not support MS-CHAPv2). %s: interface name.
Interface %s connect failed: MS-CHAP authentication failed.	MS-CHAP authentication failed (the server must support MS-CHAP and verify that the authentication failed, this does not include cases where the server does not support MS-CHAP). %s: interface name.
Interface %s connect failed: CHAP authentication failed.	CHAP authentication failed (the server must support CHAP and verify that the authentication failed, this does not include cases where the server does not support CHAP). CHAP: interface name.
Interface %s is connected.	A PPP or AUX interface connected successfully. %s: interface name.
Interface %s is disconnected.	A PPP or AUX interface disconnected successfully. %s: interface name.
Interface %s connect failed: Peer not responding.	The interface's connection will be terminated because the server did not send any LCP packets. %s: interface name.
Interface %s connect failed: PAP authentication failed.	PAP authentication failed (the server must support PAP and verify verify that the authentication failed, this does not include cases where the server does not support PAP). %s: PPP interface name.
Interface %s connect failed: Connect timeout.	A PPPOE connection timed out due to a lack of response from the PPPOE server. %s: PPP interface name.
Interface %s create failed because has no member.	A bridge interface has no member. %s: bridge interface name.

Table 213 Account Logs

LOG MESSAGE	DESCRIPTION
Account %s %s has been deleted.	A user deleted an ISP account profile. 1st %s: profile type, 2nd %se: profile name.
Account %s %s has been changed.	A user changed an ISP account profile's options. 1st %s: profile type, 2nd %s: profile name.
Account %s %s has been added.	A user added a new ISP account profile. 1st %s: profile type, 2nd %s: profile name.

Table 214 Port Grouping Logs

LOG MESSAGE	DESCRIPTION
`Interface %s links up because of changing Port Group. Enable DHCP client.`	An administrator used port-grouping to assign a port to a representative Interface and this representative interface is set to DHCP client and only has one member. In this case the DHCP client will be enabled. %s: interface name.
`Interface %s links down because of changing Port Group. Disable DHCP client.`	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has no members in its group. In this case the DHCP client will be disabled. %s: interface name.
`Port Group on %s is changed. Renew DHCP client.`	An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has more than one member in its group. In this case the DHCP client will renew. %s: interface name.
`Port Grouping %s has been changed.`	An administrator configured port-grouping, %s: interface name.

Table 215 Force Authentication Logs

LOG MESSAGE	DESCRIPTION
`Force User Authentication will be enabled due to http server is enabled.`	Force user authentication will be turned on because HTTP server was turned on.
`Force User Authentication will be disabled due to http server is disabled.`	Force user authentication will be turned off because HTTP server was turned off.
`Force User Authentication may not work properly!`	

Table 216 File Manager Logs

LOG MESSAGE	DESCRIPTION
ERROR:#%s, %s	Apply configuration failed, this log will be what CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
WARNING:#%s, %s	Apply configuration failed, this log will be what CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
ERROR:#%s, %s	Run script failed, this log will be what wrong CLI command is and what error message is. 1st %s is CLI command. 2nd %s is error message when apply CLI command.
WARNING:#%s, %s	Run script failed, this log will be what wrong CLI command is and what warning message is. 1st %s is CLI command. 2nd %s is warning message when apply CLI command.
Resetting system...	Before apply configuration file.
System resetted. Now apply %s..	After the system reset, it started to apply the configuration file. %s is configuration file name.
Running %s...	An administrator ran the listed shell script. %s is script file name.

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 t he Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so t hat distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

ONE LINE TO GIVE THE PROGRAM'S NAME AND A BRIEF IDEA OF WHAT IT DOES.

Copyright (C) YYYY NAME OF AUTHOR

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this

when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19YY NAME OF AUTHOR

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

SIGNATURE OF TY COON, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary

applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

This product includes 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/OROTHER 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 JavaTM 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

"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 UNINTERUPTED 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.

F

Legal Information

Copyright

Refer also to the Open Software Announcements on page 417.

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.

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.

G

Customer Support

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

Required Information

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

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-0
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: ftp.us.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

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

Index

A

about icon 40
Add Device screen 42
additional ZyXEL device configuration 36
allowed web access 35, 270
anti-spam
  monitors 70
  source data 35, 36
  statistical reports 232
  ZyXEL device configuration 35, 36
anti-virus
  monitors 69
  source data 35, 36
  statistical reports 217
  ZyXEL device configuration 35, 36
attacks
  monitors 68
  source data 35, 36
  statistical reports 185
  ZyXEL device configuration 35, 36
authentication
  failed login 288
  source data 35, 36
  successful login 287
  ZyXEL device configuration 35, 36
authentication code 328

B

bandwidth
  monitors 65
  source data 35, 36
  ZyXEL device configuration 35, 36
bandwidth. See device traffic.
basic version 31

C

clock time 34
configuration
  backup 325
  e-mail 322
  general 317
  restore 325
  screens 317
  SMTP mail server 322
  users 323
contact information 449
copyright 447
customer support 449
customized report templates 310
customized service field
  where configured 126
  where used 128, 131, 135
customized service traffic. See other service traffic.

D

dashboard 57
data backup 325
data restore 325
Device Information screen 52
device list
  export 326
  import 326
device traffic
  direction in statistical reports 74
  statistical reports 73
device window 39
  export 326
  import 326
  refresh 41
  right-click 43
devices 340
DNS reverse. See reverse DNS.
drill-down 56, 340

E

Edit Device screen 43
e-mail 34
  forget password 34
  low free disk mark 318
  scheduled reports 34
  SMTP settings 34, 322

system notification 34
test SMTP mail server 34, 323

F

failed login 288
source data 35, 36
ZyXEL device configuration 35, 36
features 340
firmware
platform 126
versions 340
folder
add 41
edit folder information 42
remove 42
forget password 34, 38
FTP
monitors 67
FTP traffic
statistical reports 104
full version 31
function window 39, 43
list of screens 44
right-click 51

H

help icon 40
hostname reverse 318
HTTP/HTTPS. See web traffic.

I

iCard 328
idle timeout 39
intrusions
monitors 68
source data 35, 36
statistical reports 200
ZyXEL device configuration 35, 36
IPSec VPN traffic. See VPN traffic.

L

license key 328
list of screens 44
log entries 31, 295
how used 36
log settings requirements 36
log viewer
regular log entries. See regular log viewer.
Login screen 37
logout icon 40
low free disk mark 318

M

MAC 43, 52
mail traffic
monitors 67
statistical reports 115
main screen 38
parts of 39
monitors 340
anti-spam 70
anti-virus 69
attacks 68
bandwidth 65
end time 54
FTP 67
graph 54
intrusions 68
mail traffic 67
next refresh time 54
printing 54
processing time 34
right-click 54
service traffic 66
source data 35, 36
start time 54
typical layout 53
VPN traffic 67
web traffic 67
ZyXEL device configuration 35, 36
myZyXEL.com 328

N

network attacks 185
number of devices
currently allowed 329
currently used 329

increase allowed 327
maximum allowed 329

O

other service traffic
configure customized service field 126
statistical reports 127

P

password
default value 38
platform 126
POP3/SMTP traffic. See mail traffic.
port number 33
print icon 61
printing
monitors 54
statistical reports 55
processing time 34

Q

Quick Start Guide 31

R

registration 340
authentication code 328
iCard 328
license key 328
myZyXEL.com 328
regular log viewer
processing time 35
source data 35, 36
ZyXEL device configuration 35, 36
related documentation 3
report templates 310
report window 39, 52
typical layouts 52
reverse DNS 56, 318, 340
reverse hostname 340

S

scheduled reports 34, 318, 340
daily 301
generation time 300
one-time 307
overtime 307
requirements 299
store log days 299, 301, 304, 307
summary 299
templates 310
weekly 304
security timeout 39
service traffic
monitors 66
setting icon 61
SMTP mail server 34
test 34, 323
software release
upgrade 327
source data 35
how used in screens 36
log entries 36
traffic statistics 36
spam. See anti-spam.
statistical reports 340
anti-spam 232
anti-virus 217
attacks 185
dates 55
default chart type 56, 318
device traffic 73
end date 56
FTP traffic 104
graph 56
graph type 56
intrusions 200
last X days 56
mail traffic 115
mouse over 56
other service traffic 127
printing 55
processing time 35
right-click 56
settings 56
start date 56
table 56
title 55
typical layout 54
VPN traffic 139
web allowed 270
web blocked 253
web traffic 93
store log days 318
effects of 56
scheduled reports 299, 301, 304, 307, 318

setting 318
successful login 287
source data 35, 36
ZyXEL device configuration 35, 36
syntax conventions 4
system notification 34
low free disk mark setting 318

T

templates 310
time 34
clock time 34
processing time 34
title bar 39, 40
top level summary 57
traffic statistics
how used 36
in typical application 31
trial version 32
typical application 31

U

upgrade
software release 327
versions 327
user name
default value 38
users
add 324
change password 324
edit 324
list 323
on line vs off line 324
password 324
screens 323

V

Vantage Report
license key 328
typical application 31
users. See users.
Vantage Report server 31, 33
as service 33, 340
clock time in 34
configuration. See configuration.
e-mail in 34
port number 33
processing time 34
source data 35
starting 33
stopping 33
time in 34
Vantage Report users. See users.
versions 31
basic 31
differences 32
full 31, 327
trial 32, 327, 328
upgrade 327
view detail icon 61
view logs icon 56
virus. See anti-virus.
VPN traffic
monitors 67
source data 35, 36
statistical reports 139
ZyXEL device configuration 35, 36

W

web allowed
source data 35
statistical reports 270
ZyXEL device configuration 35
web block
source data 35, 36
ZyXEL device configuration 35, 36
web blocked
statistical reports 253
web configurator 37
default password 38
default user name 38
in typical application 31
minimum requirements 37
starting 37
timeout 39
URL 37
web forward
source data 36
ZyXEL device configuration 36
web traffic
monitors 67
statistical reports 93

Z

ZLD **126**
ZyNOS **126**
ZyWALL 1050 **126**, **340**
ZyXEL device
  add **41**, **42**, **326**
  configuration **35**
  device type setting **43**, **52**
  edit basic information **42**
  feature support **340**
  import **326**
  in typical application **31**
  MAC setting **43**, **52**
  move **42**
  remove **42**
  search for **42**
  select **42**
  source data. See source data.
  view basic information **42**