Vantage Report

User's Guide

Default Login Details

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

Version 3.8
Edition 1, 2/2013

ZyXEL

www.zyxel.com

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Download software and documentation (User's Guide, Quick Start Guide, Datasheet, Support Notes) from one of the FTP sites:

  Europe: ftp://ftp.zyxel.dk/Vantage_Report

  Rest of World: ftp://ftp.zyxel.com/Vantage_Report
- Vantage Report Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

Contents Overview

Table of Contents

Chapter 6

Chapter 9

PART I

User’s Guide

1

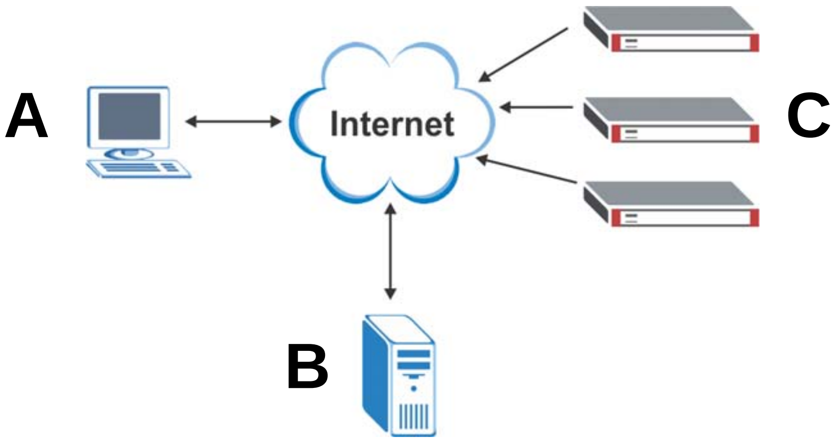
Introducing Vantage Report

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

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.

Table 1 Supported ZyXEL Devices

VANTAGE REPORT VERSION	SUPPORTED MODELS
Vantage Report 3.8	ZyWALL 110, ZyWALL 310, and ZyWALL 1100[A].

A. Models supported at the time of writing do not support anti-spam, anti-virus, content filtering, IDP, and ADP functions.

1.2 License Versions

This is independent from the version number, 3.8 for example. When you first install Vantage Report you get the trial version with full management authority for one device for 30 days. After the trial version expires you have a basic version with only limited management authority for one device.

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

Purchase license keys to use the full version with full management authority for more devices. See Section 14.5 on page 466 for more information.

1.3 Hardware Requirements

Minimum hardware requirements:

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

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

Table 2 Hardware Specification Recommendations

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

The Vantage Report Server

This chapter explains several characteristics of the Vantage Report server.

2.1 Starting and Stopping the Vantage Report Server

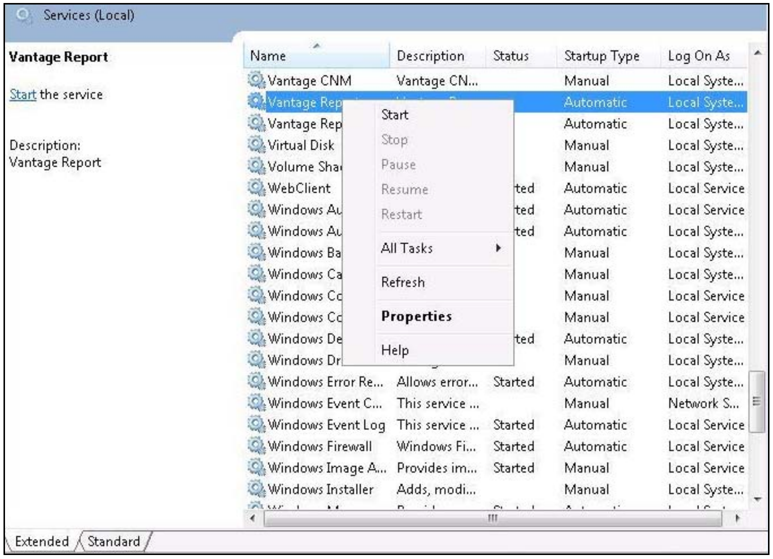
Note: Make sure the port Vantage Report uses for web services is not used by other applications, especially web servers.

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

1 In Windows 2000, click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**. The **Services** screen opens.

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

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



Services (Local)

Vantage Report

Start the service

Description:
Vantage Report

Name	Description	Status	Startup Type	Log On As
Vantage CNM	Vantage CN...		Manual	Local Syste...
Vantage Rep			Automatic	Local Syste...
Vantage Rep			Automatic	Local Syste...
Virtual Disk			Manual	Local Syste...
Volume Sha			Manual	Local Syste...
WebClient		ted	Automatic	Local Service
Windows Au		ted	Automatic	Local Service
Windows Au		ted	Automatic	Local Syste...
Windows Ba			Manual	Local Syste...
Windows Ca			Manual	Local Syste...
Windows Co			Manual	Local Service
Windows Co			Manual	Local Service
Windows De		ted	Automatic	Local Syste...
Windows Dr			Manual	Local Syste...
Windows Error Re...	Allows error...	Started	Automatic	Local Syste...
Windows Event C...	This service ...		Manual	Network S...
Windows Event Log	This service ...	Started	Automatic	Local Service
Windows Firewall	Windows Fi...	Started	Automatic	Local Service
Windows Image A...	Provides im...	Started	Manual	Local Service
Windows Installer	Adds, modi...		Manual	Local Syste...

4 Right-click on **Vantage Report**. A menu appears.

5 Select **Start** or **Stop** to start or stop the Vantage Report service. Select **Properties** to configure the service.

2.2 E-Mail in the Vantage Report Server

Note: Before the Vantage Report server can send e-mail to anyone, you have to configure the SMTP mail server. See Section 14.2 on page 461 for more information.

The Vantage Report server can use e-mail to send information in several situations. In some situations, it sends e-mail to the e-mail address that is associated with a specific user (see Section 14.3 on page 463). In other situations, it sends e-mail to any valid e-mail address.

- **scheduled report** - The Vantage Report server can send one or more statistical reports regularly or one-time to any valid e-mail address. See Chapter 12 on page 423 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. One of the threshold values can be configured. See Section 14.1 on page 457.
- **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 27 for an example of the **Login** screen.
- **test message** - The Vantage Report administrator tests the SMTP mail server settings. The Vantage Report server sends an e-mail message to the e-mail address associated with the **root** account. See Section 14.2 on page 461 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.

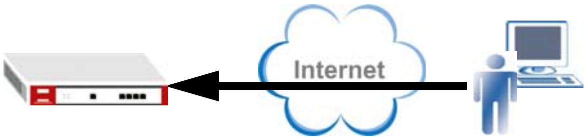
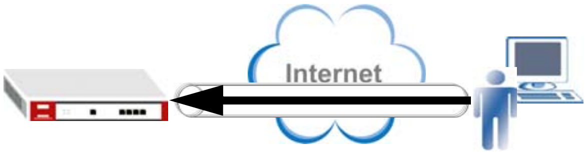
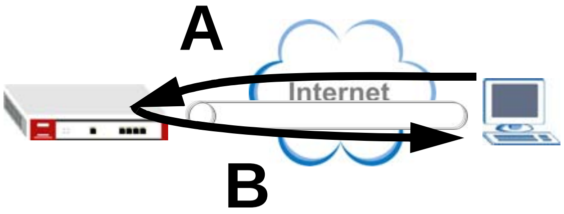
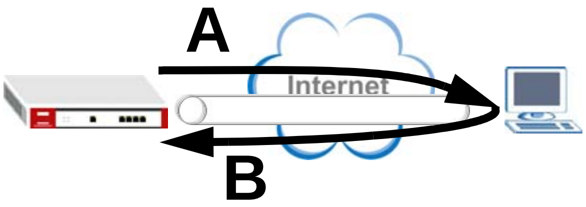
Table 3 Processing Times by Menu Item

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

2.4 Common Terms

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

Table 4 Common Terms

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

2.5 Common Icons

The following table describes common icons.

Table 5 Common Icons

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

2.6 ZyXEL Device Configuration and Source Data

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

Table 6 ZyWALL Products Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	ZYWALL PRODUCTS		
	SOURCE DATA	LOG SETTINGS*	ADDITIONAL
Monitor > Hardware Status > CPU Usage	log entries	System Monitoring	--
Monitor > Hardware Status > Memory Usage	log entries	System Monitoring	--
Monitor > Network Traffic > Session Usage	log entries	System Monitoring	--
Monitor > Network Traffic > Bandwidth > Port Usage	log entries	INTERFACE STATISTICS	--
Monitor > Network Traffic > Bandwidth > Interface Usage	log entries	INTERFACE STATISTICS	--
Monitor > Network Traffic > Web	log entries	Traffic Log	--
Monitor > Network Traffic > FTP	log entries	Traffic Log	--
Monitor > Network Traffic > Mail	log entries	Traffic Log	--
Monitor > Secure Remote Access > Site-to-Site (IPSec)	log entries	Traffic Log	--
Monitor > Secure Remote Access > Client-to-Site (SSL)	log entries	Traffic Log	--
Monitor > Network Security > Firewall Access Control	log entries	Firewall	--
Monitor > Network Security > Attack	log entries	Attack (ADP)	--
Monitor > Network Security > Intrusion Hits	log entries	IDP	--
Monitor > Network Security > AntiVirus	log entries	Anti-Virus	--

Table 6 ZyWALL Products Configuration Requirements by Menu Item

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

Table 6 ZyWALL Products Configuration Requirements by Menu Item

VANTAGE REPORT MENU ITEM(S)	ZYWALL PRODUCTS		
	SOURCE DATA	**LOG SETTINGS***	**ADDITIONAL**
Report > Web Security > Security Threat > Top Hosts	log entries	Blocked web sites	--
Report > Web Security > Security Threat > By Category	log entries	Blocked web sites	--
Report > Web Security > Virus Found	log entries	Anti-Virus	--
Report > Web Security > Intrusion Hits	log entries	IDP	--
Report > Security Policy Enforcement > EPS	log entries	EPS	--
Report > Security Policy Enforcement > Content Filter (All) > Summary	log entries	Blocked web sites, Forward web sites, Warning web sites	--
Report > Security Policy Enforcement > Content Filter (All) > Top Sites	log entries	Blocked web sites, Forward web sites, Warning web sites	--
Report > Security Policy Enforcement > Content Filter (All) > Top Users	log entries	Blocked web sites, Forward web sites, Warning web sites	--
Report > Security Policy Enforcement > Content Filter (All) > Top Hosts	log entries	Blocked web sites, Forward web sites, Warning web sites	--
Report > Security Policy Enforcement > Content Filter (All) > By Category	log entries	Blocked web sites, Forward web sites, Warning web sites	--
Report > Security Policy Enforcement > Content Filter (Blocked) > Summary	log entries	Blocked web sites	--
Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites	log entries	Blocked web sites	--
Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users	log entries	Blocked web sites	--
Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts	log entries	Blocked web sites	--
Report > Security Policy Enforcement > Content Filter (Blocked) > By Category	log entries	Blocked web sites	--
Report > Security Policy Enforcement > Application Access Control	log entries	Application Patrol	--
Report > Event > DHCP Leasing > Summary	log entries	Traffic Log	--
Report > Event > DHCP Leasing > Top Host	log entries	Traffic Log	--
Logs > Log Viewer	log entries	**	**

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

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

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

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

- **Source Data** - Some screens use log entries; some screens use traffic statistics. Some ZyXEL devices do not track traffic statistics. If Vantage Report does not get one of these, the screens are empty. See the Quick Start Guide for detailed instructions.

- **Log Settings** - If ZyXEL devices do not record some categories of log entries, Vantage Report does not have any information to display either. For example, if you want to look at VPN traffic for a particular device, the device has to record log entries for **IPSec**.

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

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

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

The Web Configurator

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

3.1 Web Configurator Requirements

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

- Internet Explorer 6.0 or later, Firefox 1.0.7 or later, Google Chrome 23.0.1271.95 or later (local or remote)
- JavaScript enabled
- Macromedia Flash Player 11 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.)

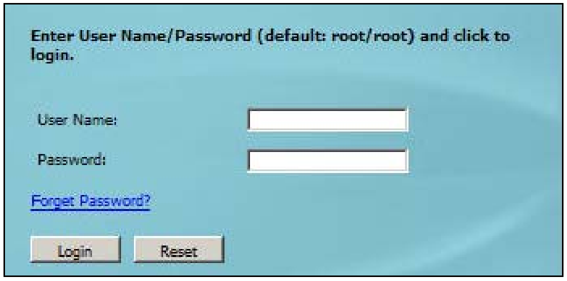
2 Open a browser window, and go to `http://a.b.c.d:xxxxx/vrpt`, where

- `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 (default is 8080).

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

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

Figure 6 Web Configurator Login Screen



Enter User Name/Password (default: root/root) and click to login.

User Name:

Password:

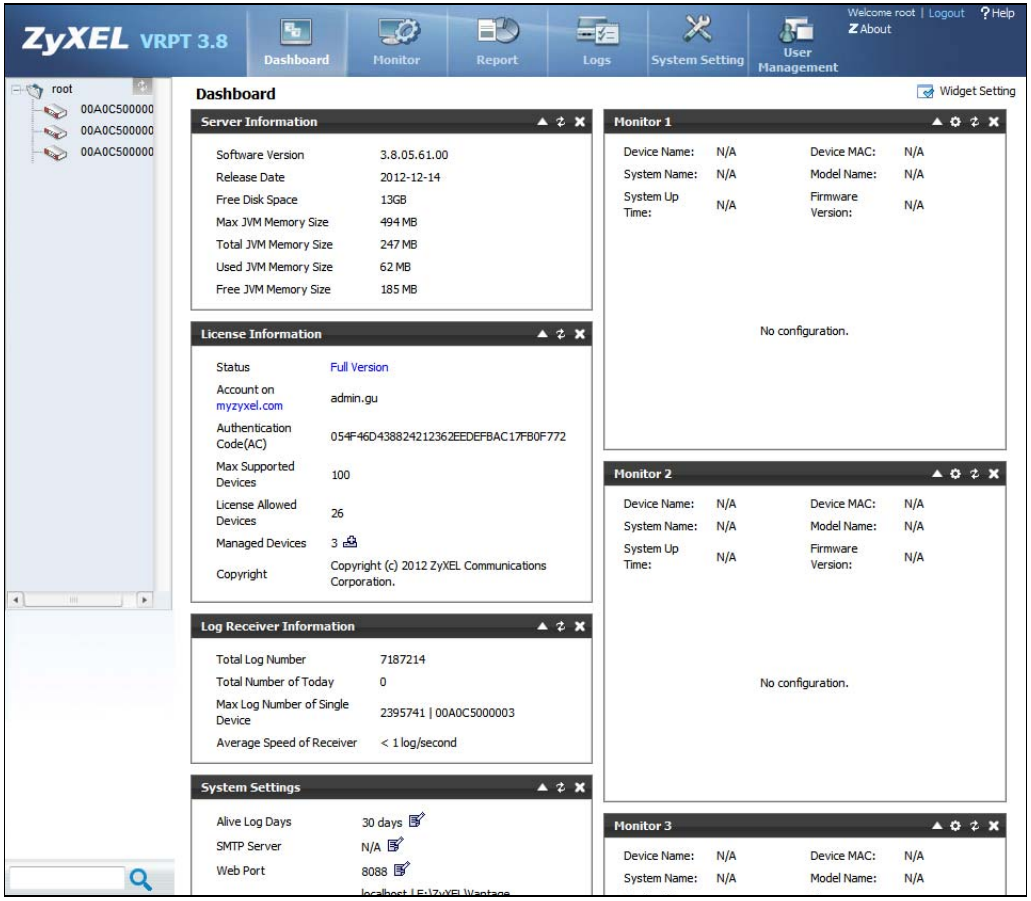
Note: If you forget your password, enter your user name, and click **Forget Password?**. Vantage Report sends your password to the e-mail address (if any) for your **User Name**. See Section 2.2 on page 20 for more information about e-mail in Vantage Report and Section 14.3 on page 463 for more information about SMTP configuration.

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

Note: See Section 14.3 on page 463 to change the password.

4 Click the **Login** button. The **System Dashboard** screen displays Vantage Report system and device information in widgets that you can re-arrange to suit your needs. You can also select what information the device monitor widgets display. See Section 3.6 on page 43 for details on the dashboard.

Figure 7 System Dashboard



Server Information

Software Version	3.8.05.61.00
Release Date	2012-12-14
Free Disk Space	13GB
Max JVM Memory Size	494 MB
Total JVM Memory Size	247 MB
Used JVM Memory Size	62 MB
Free JVM Memory Size	185 MB

License Information

Status	Full Version
Account on myzyxel.com	admin.gu
Authentication Code(AC)	054F46D438824212362EEDEFBAC17FB0F772
Max Supported Devices	100
License Allowed Devices	26
Managed Devices	3
Copyright	Copyright (c) 2012 ZyXEL Communications Corporation.

Log Receiver Information

Total Log Number	7187214
Total Number of Today	0
Max Log Number of Single Device	2395741 | 00A0C5000003
Average Speed of Receiver	< 1 log/second

System Settings

Alive Log Days	30 days
SMTP Server	N/A
Web Port	8088
	localhost | E:\ZyXEL\Vantage

Monitor 1

Device Name:	N/A	Device MAC:	N/A
System Name:	N/A	Model Name:	N/A
System Up Time:	N/A	Firmware Version:	N/A

No configuration.

Monitor 2

Device Name:	N/A	Device MAC:	N/A
System Name:	N/A	Model Name:	N/A
System Up Time:	N/A	Firmware Version:	N/A

No configuration.

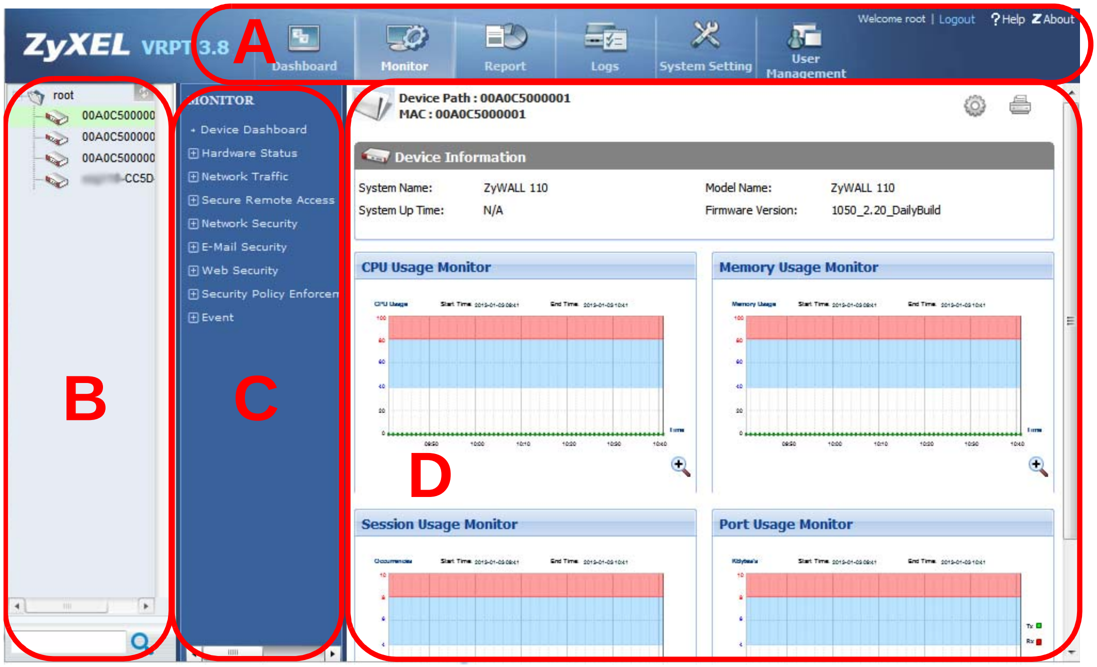
Monitor 3

Device Name:	N/A	Device MAC:	N/A
System Name:	N/A	Model Name:	N/A

5 Manually add a device to Vantage Report. See Table 8 on page 31 for how to add a device.

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

Figure 8 Web Configurator Main Screen



Device Path : 00A0C5000001
MAC : 00A0C5000001

System Name:	ZyWALL 110	Model Name:	ZyWALL 110
System Up Time:	N/A	Firmware Version:	1050_2.20_DailyBuild

The main screen is divided into four parts:

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

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

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

3.3 Main Menu Bar

The main menu bar links are explained in the table below.

Table 7 Main Menu Bar Links

LABEL	DESCRIPTION
Help	**Help** opens the help page for the current screen in Vantage Report.

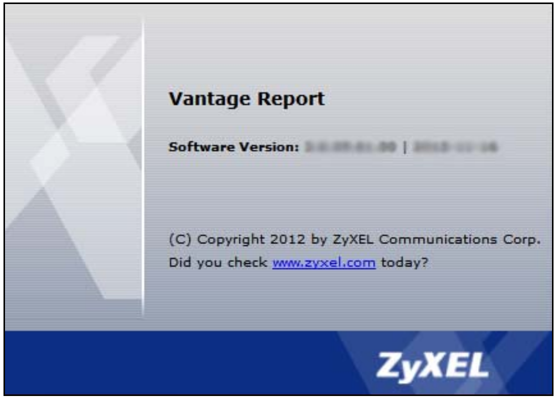
Table 7 Main Menu Bar Links

LABEL	DESCRIPTION
About	**About** opens a screen with the version of Vantage Report.
Logout	**Logout** logs you out of Vantage Report.

3.3.1 The About Screen

Use this screen to view Vantage Report release and copyright information.

Figure 9 About



Vantage Report

Software Version: [redacted] | [redacted]

(C) Copyright 2012 by ZyXEL Communications Corp.
Did you check www.zyxel.com today?

3.4 Device Window

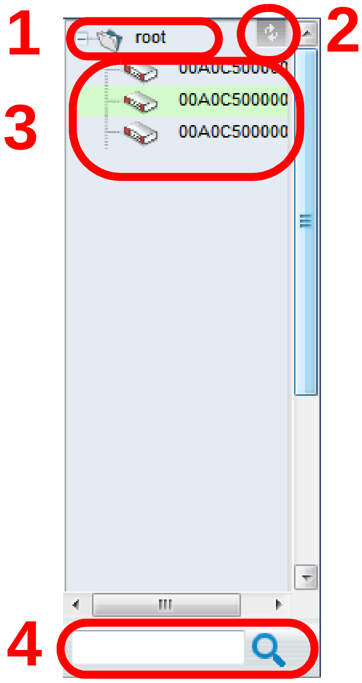
Use the device window to select which device(s) you want to include in a report, add devices to Vantage Report, and remove devices from Vantage Report.

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

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

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

Figure 10 Device Window



Each numbered section above is described in the following table.

Table 8 Device Window

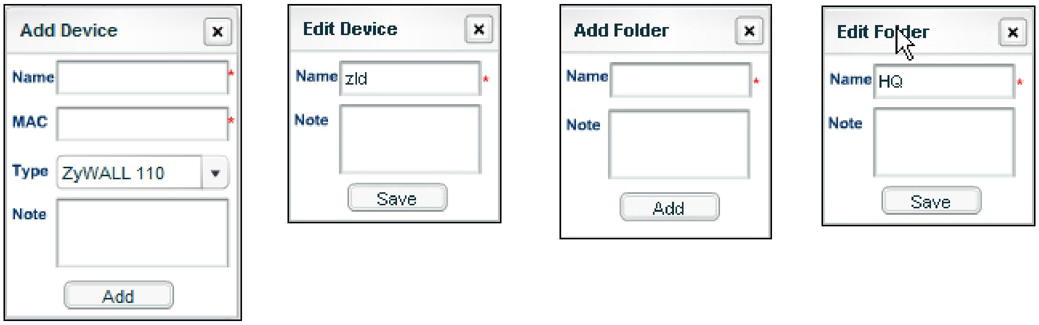
SECTION	DESCRIPTION
1	**To add a device to Vantage Report,** • right click on **root**, and select **Add Device**. The **Add Device** screen appears in the device window. (See Figure 11.) **To add a folder to Vantage Report,** • right click on root, and select **Add Folder**. The **Add Folder** screen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

Table 8 Device Window

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

When you add a device to Vantage Report, you can specify the name, MAC address, type, and any notes for the device. When you click on the device, this information is displayed in the report and setting window (see Section 3.7.1 on page 47). When you edit a device, however, you can only edit the name and the notes. If you want to update the MAC address or device type, you have to delete the current device and add it again. These screens are discussed in more detail together in Figure 11 on page 32.

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



Type: ZyWALL 110

Name: zld

Name: HQ

Each field is explained in the following table.

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

LABEL	DESCRIPTION
Name	Enter the name of the device or folder you want to add to Vantage Report. The device name can consist of alphanumeric characters, underscores(_), periods(.), or dashes(-), and it must be 1-28 characters long. This name is used to refer to the device (or folder) in Vantage Report, and it has to be different than other device (or folder) names in Vantage Report. You can use the system name of a device as the name for that device.
MAC	This field is not available in the **Edit Device** screen. Enter the LAN MAC address of the device you want to add. 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. See Table 1 on page 17 for a list of the supported ZyXEL devices. Not all reports (and fields in reports) are available with all models.
Note	Enter any additional notes you want to make for the device or folder here.
Add	This field is available in the **Add Device** screen. Click this to add the device to Vantage Report. It takes time before Vantage Report displays information received from this device.
Save	This field is available in the **Edit Device** screen. Click this to save your changes to Vantage Report.

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

Figure 12 Device Window Right-Click Menu

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

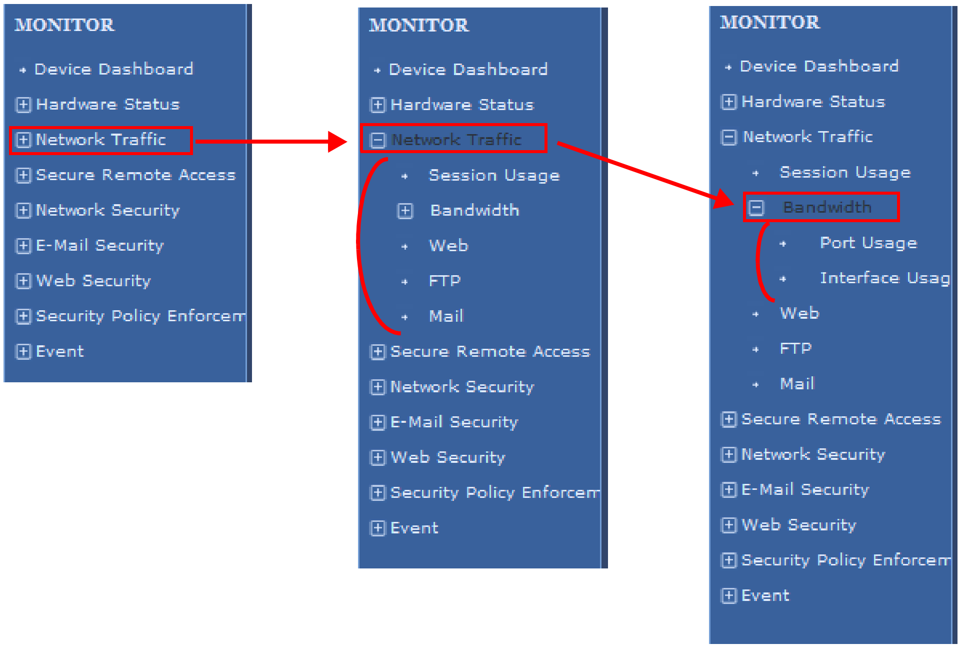
3.5 Menu Panel

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

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

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

Figure 13 Menu Panel



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

The following table expands the menu panel and introduces each monitor, statistical report, and screen. In addition, it also indicates if you can drill down into each statistical report.

Note: Not every report (or fields in a report) is available with every model of device and firmware version.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
Dashboard		Displays server information and device monitor summaries.
Monitor		Use monitors to check the status of ZyXEL devices.
Dashboard		The dashboard gives a quick top level summary of activity across devices that you pre-configured. The dashboard is available with the full version of Vantage Report.
Hardware Status		
	CPU Usage	Use this report to monitor the CPU usage on the selected device.
	Memory Usage	Use this report to monitor the memory usage on the selected device.
Network Traffic		
	Session Usage	Use this report to monitor the number of sessions change status on the selected device.
	Bandwidth	

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Port Usage	Use this report to monitor the throughput statistics on a selected device's port.
	Interface Usage	Use this report to monitor the throughput statistics on a selected device's interface.
	Web	Use this report to monitor the amount of traffic generated by web services in the selected device.
	FTP	Use this report to monitor the amount of traffic generated by FTP services in the selected device.
	Mail	Use this report to monitor the amount of traffic generated by mail services in the selected device.
Secure Remote Access		
	Site-to-site (IPSec)	Use this report to monitor the amount of traffic generated by site-to-site IPSec VPN services in the selected device.
	Client-to-site (IPSec)	Use this report to monitor the amount of traffic generated by client-to-site IPSec VPN services in the selected device.
	Client-to-site (SSL)	Use this report to monitor the amount of traffic generated by SSL VPN services in the selected device.
Network Security		
	Firewall Access Control	Use this report to monitor the number of occurrences of firewall access attempts.
	Attack	Use this report to monitor the number of Denial-of-Service (DoS) attacks detected by the selected device's firewall.
	Intrusion Hits	Use this report to monitor the number of intrusions detected by the selected device's IDP feature.
	Antivirus	Use this report to monitor the number of virus occurrences prevented by the selected device.
E-Mail Security		
	Virus Found	Use this report to monitor the number of email virus occurrences prevented by the selected device.
	Spam	Use this report to monitor the number of spam messages stopped by the selected device.
	Intrusion Hits	Use this report to monitor the number of email intrusions detected by the selected device's IDP feature.
Web Security		
	Security Threat	Use this report to monitor the number of occurrences of web security related access attempts to web sites specified in the content filter.
	Virus Found	Use this report to monitor the number of web virus occurrences prevented by the selected device.
	Intrusion Hits	Use this report to monitor the number of web intrusions detected by the selected device's IDP feature.
Security Policy Enforcement		
	Content Filter	Use this report to monitor the number of occurrences of all access attempts to web sites specified in the content filter.
	App Patrol	Use this report to monitor the number of occurrences of applications allowed and blocked.
Event		

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	DHCP Leasing	Use this screen to monitor the number of DHCP requests over a time period.
Report		Use reports to view various and detailed statistic report of ZyXEL devices.
Network Traffic		
	Bandwidth	
	Summary	Use this report to look at the amount of traffic handled by the selected device by time interval. You can also use this report to look at the top services in a specific time interval.
	Top Protocols	Use this report to look at the top services generating traffic through the selected device. You can also use this report to look at the top sources of traffic for any top service.
	Top Hosts	Use this report to look at the top sources of traffic in the selected device. You can also use this report to look at the top services for any top source.
	Top Users	Use this report to look at the top users generating traffic through the selected device. You can also use this report to look at the top services used by any top bandwidth user.
	Top Destinations	Use this report to look at the top destinations of traffic in the selected device. You can also use this report to look at the services that were used the most to access the top destination IP addresses.
	WEB	
	Top Sites	Use this report to look at the top destinations of web traffic. You can also use this report to look at the top sources of web traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of web traffic. You can also use this report to look at the top destinations of web traffic for any top source.
	Top Users	Use this report to look at the top sources of web traffic by user. You can also use this report to look at the top destinations of web traffic for any top user.
	FTP	
	Top Sites	Use this report to look at the top destinations of FTP traffic. You can also use this report to look at the top sources of FTP traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of FTP traffic. You can also use this report to look at the top destinations of FTP traffic for any top source.
	Top Users	Use this report to look at the top sources of FTP traffic by user. You can also use this report to look at the top destinations of FTP traffic for any top user.
	MAIL	
	Top Sites	Use this report to look at the top destinations of mail traffic. You can also use this report to look at the top sources of mail traffic for any top destination.
	Top Hosts	Use this report to look at the top sources of mail traffic. You can also use this report to look at the top destinations of mail traffic for any top source.
	Top Users	Use this report to look at the top sources of mail traffic by user. You can also use this report to look at the top destinations of mail traffic for any top user.
	Customization	
	Customization	Use this screen to select the ZyXEL firmware platform that the device uses.
	Top Destinations	Use this report to look at the top destinations of traffic for other services. You can also use this report to look at the top sources of traffic for other services for any top destination.
	Top Sources	Use this report to look at the top sources of traffic for other services. You can also use this report to look at the top destinations of traffic for other services for any top source.

Table 10 Menu Panel

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

Table 10 Menu Panel

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

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Top Destinations	Use this report to look at the top destinations of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top destination.
	By Severity	Use this report to look at the top severities (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug. You can also use this report to look at the top intrusion signatures for any severity.
	Antivirus	
	Summary	Use this report to look at the number of virus occurrences by time interval. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
E-Mail Security		
	Virus Found	
	Summary	Use this report to look at the number of virus occurrences by time interval. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
	Spam	
	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 drill-down 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 drill-down report to look at the top sources (last mail relay) of spam messages by number of messages.
	Top Senders	Use this report to look at the e-mail addresses of the top senders of spam messages and how many spam e-mails they sent.
	Top Sender IPs	Use this report to look at the IP addresses of the top senders of spam messages and how many spam e-mails they sent.
	Top Subjects	Use this report to look at the subject lines of the most common spam e-mails.
	By Category	Use this report to look at the most common spam categories.
	Intrusion Hits	
	Summary	Use this report to look at the number of intrusions by time interval. You can also use this report to look at the top intrusion signatures in a specific time interval.

Table 10 Menu Panel

LEVEL 1/2	LEVEL 3	FUNCTION
	Top Intrusions	Use this report to look at the top intrusion signatures by number of intrusions. You can also use this report to look at the top sources of intrusions for any top signature.
	Top Sources	Use this report to look at the top sources of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top source.
	Top Destinations	Use this report to look at the top destinations of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top destination.
	By Severity	Use this report to look at the top severities (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug. You can also use this report to look at the top intrusion signatures for any severity.
Web Security		
	Security Threat	
	Summary	Use this report to look at the number of attempts to access unsafe web sites by time interval. You can also use this report to look at the top sources of attempts to access unsafe web sites in a specific time interval.
	Top Sites	Use this report to look at the top destinations of attempts to access unsafe web sites by number of attempts. You can also use this report to look at the top sources of attempts to access unsafe web sites for any top destination.
	Top Users	Use this report to look at the top users accessing unsafe web traffic. You can also use this report to look at the top destinations for any top source of unsafe web traffic.
	Top Hosts	Use this report to look at the top sources of attempts to access unsafe web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access unsafe web sites for any top source.
	By Category	Use this report to look at the top categories of destinations in attempts to access unsafe web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access unsafe web sites for any top category.
	Virus Found	
	Summary	Use this report to look at the number of virus occurrences by time interval. You can also use this report to look at the top viruses in a specific time interval.
	Top Viruses	Use this report to look at the top viruses by number of occurrences. You can also use this report to look at the top sources of any top virus.
	Top Dangerous URLs	Use this report to to look at the top dangerous URLs the device blocked by number of occurrences. You can also use this report to look at the top sources of attempts to access dangerous URLs.
	Top Sources	Use this report to look at the top sources of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top source.
	Top Destination	Use this report to look at the top destinations of virus occurrences by number of occurrences. You can also use this report to look at the top viruses for any top destination.
	Intrusion Hits	
	Summary	Use this report to look at the number of intrusions by time interval. You can also use this report to look at the top intrusion signatures in a specific time interval.
	Top Intrusions	Use this report to look at the top intrusion signatures by number of intrusions. You can also use this report to look at the top sources of intrusions for any top signature.

Table 10 Menu Panel

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

Table 10 Menu Panel

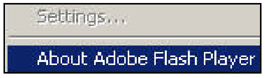
LEVEL 1/2	LEVEL 3	FUNCTION
	Application Access Control	
	Top Applications Blocked	Use this report to look at the applications for which the device blocked the most connections.
	Top Users Blocked	Use this report to look at the users for which the device blocked the most connections.
	Top Applications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

Table 10 Menu Panel

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

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

Figure 14 Menu Panel Right-Click Menu



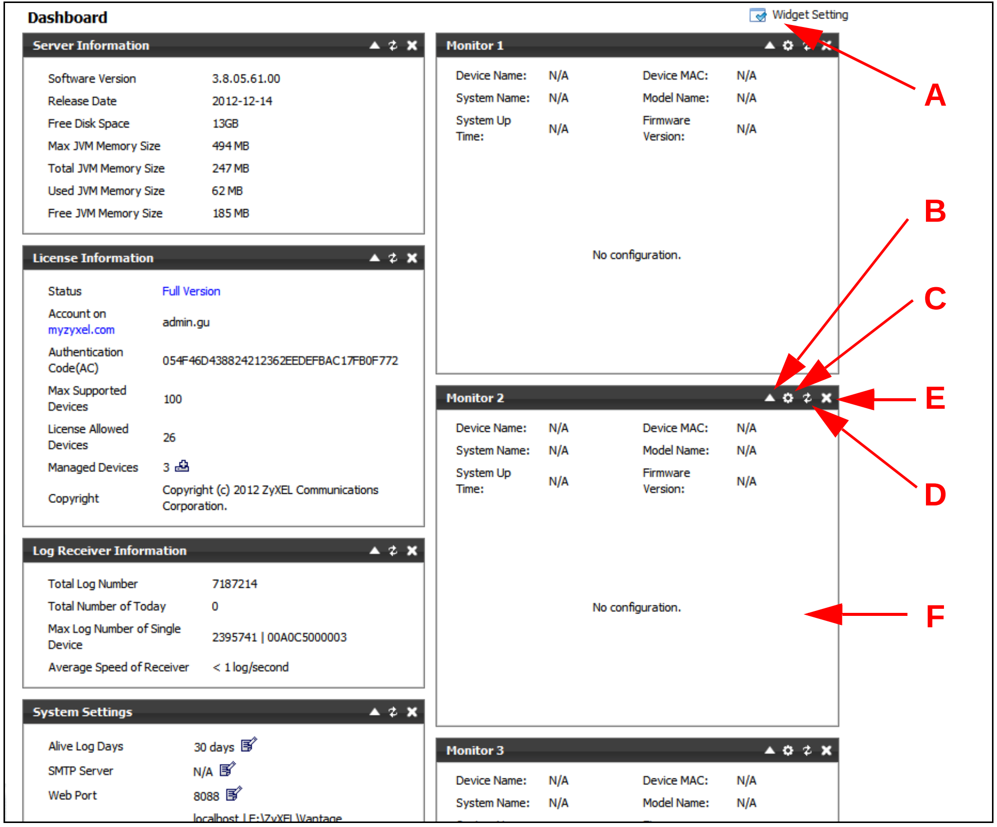
Click **About Adobe Flash Player ...** to get information about the current version of Flash.

3.6 System Dashboard

The **System Dashboard** screen summarizes the Vantage Report system, license, log received and system settings information in widgets. It also displays configurable device monitor widgets with the device information you select. You can re-arrange the widgets to suit your needs. Click the

Dashboard menu at the top to open this screen when you are in another screen. See Section 3.6.1 on page 46 for details on the device monitor widgets.

Figure 15 System Dashboard



Dashboard

Widget Setting

Server Information

Software Version	3.8.05.61.00
Release Date	2012-12-14
Free Disk Space	13GB
Max JVM Memory Size	494 MB
Total JVM Memory Size	247 MB
Used JVM Memory Size	62 MB
Free JVM Memory Size	185 MB

License Information

Status	Full Version
Account on myzyxel.com	admin.gu
Authentication Code(AC)	054F46D438824212362EEDEFBAC17FB0F772
Max Supported Devices	100
License Allowed Devices	26
Managed Devices	3
Copyright	Copyright (c) 2012 ZyXEL Communications Corporation.

Log Receiver Information

Total Log Number	7187214
Total Number of Today	0
Max Log Number of Single Device	2395741 | 00A0C5000003
Average Speed of Receiver	< 1 log/second

System Settings

Alive Log Days	30 days
SMTP Server	N/A
Web Port	8088
	localhost | E:\ZyXEL\Vantage

Monitor 1

Device Name:	N/A	Device MAC:	N/A
System Name:	N/A	Model Name:	N/A
System Up Time:	N/A	Firmware Version:	N/A

No configuration.

Monitor 2

Device Name:	N/A	Device MAC:	N/A
System Name:	N/A	Model Name:	N/A
System Up Time:	N/A	Firmware Version:	N/A

No configuration.

Monitor 3

Device Name:	N/A	Device MAC:	N/A
System Name:	N/A	Model Name:	N/A

Each field is described in the following table.

Table 11 System Dashboard

LABEL	DESCRIPTION
Widget Setting (A)	Use this link to open or close widgets by selecting/clearing the associated checkbox.
Collapse (B)	Click this to collapse a widget. It then becomes a down arrow. Click it again to enlarge the widget again.
Edit Widget (C)	Click this to select the information a device monitor widget displays.
Refresh Widget (D)	Click this to update the widget's information immediately.
Close Widget (E)	Click this to close the widget. Use **Widget Setting** to re-open it.
View Detail (F)	Click this to go to the monitor or summary report's related **Monitor** screen.
Server Information	
Software Version	This field displays the Vantage Report version.
Release Date	This field displays the date the Vantage Report software version is released.
Free Disk Space	This field displays the available disk space in the computer your Vantage Report is installed.
Max JVM Memory Size	This field displays the maximum memory size the Vantage Report's Java Virtual Machine (JVM) can allocate on the computer where the Vantage Report is installed. You can configure the memory size according to the computer's RAM (Random Access Memory) size. Java applications request memory to the computer through the JVM.

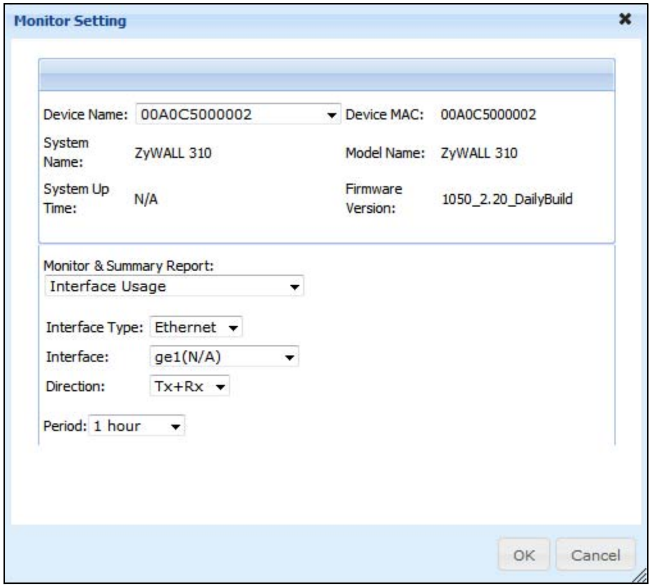
Table 11 System Dashboard

LABEL	DESCRIPTION
Total JVM Memory Size	This field displays the total amount of memory the computer has allocated for the Vantage Report's JVM.
Used JVM Memory Size	This field displays the amount of memory size the Java applications are using.
Free JVM Memory Size	This field displays the amount of memory size available for Java applications.
Log Receiver Information	
Total Log Number	This field displays the total number of log entries the Vantage Report stores.
Total Number of Today	This field displays the total number of log entries the Vantage Report has received today.
Max Log Number of Single Device	This field displays the number of a device's log entries and the device's name which sends the most number of logs to the Vantage Report.
Average Speed of Receiver	This field displays the average time in seconds the Vantage Report received a log entry since it is last started.
License Information	
Status	This field displays the type of Vantage Report license: **Trial Version** (and the days remaining), **Full Version**, or **Basic Version**. Click the hyperlink to view more information about the license status in the **System Setting** > **Registration** screen.
Account on myzyxel.com	This field displays the user account you used to register your Vantage Report to the www.zyxel.com website. Click the **myzyxel.com** hyperlink to take you to the website. www.myzyxel.com is a central product registration website owned by ZyXEL.
Authentication Code	This field displays the string generated during the registration of your Vantage Report to www.zyxel.com.
Max Supported Devices	This field displays the maximum number of ZyXEL devices your Vantage Report version supports.
License Allowed Devices	This field displays the maximum ZyXEL devices you are allowed to manage in the Vantage Report. The number depends on the license you have entered in the **System Setting** > **Registration**. See Section 14.5.1 on page 467.
Managed Devices	This field displays the number of ZyXEL devices you can manage in the Vantage Report. Click the **Add Device** icon to add more devices in the Vantage Report.
Copyright	This field displays the copyright of the Vantage Report.
System Settings	
Alive Log Days	This field displays the number of days the Vantage Report stores logs. The Vantage Report automatically deletes logs over this configured days.
SMTP Server	This field displays the mail server you configured for the Vantage Report to send reports through emails. Click the edit icon to take you to the **System Setting** > **Server Configuration** screen where you can configure the related settings.
Web Port	This field displays the port number the Vantage Report listens for user's web interface access. Click the edit icon to take you to the **System Setting** > **Server Configuration** screen where you can change the setting.
Archived Log Location	This field displays the location where the Vantage Report stores its archived logs currently. Click the edit icon to take you to the **Logs** > **Log Archiving** > **File Archiving Settings** screen where you can configure the related settings.

3.6.1 Device Monitor Widget Settings

In the **System Dashboard**, click a device monitor widget's **Edit Widget** icon to open a screen like where you can configure it's settings.

Figure 16 Edit Widget Screen



Device Name: 00A0C5000002

Device MAC: 00A0C5000002

System Name: ZyWALL 310

Model Name: ZyWALL 310

System Up Time: N/A

Firmware Version: 1050_2.20_DailyBuild

Monitor & Summary Report: Interface Usage

Interface Type: Ethernet

Interface: ge1(N/A)

Direction: Tx+Rx

Period: 1 hour

Each field is explained in the following table.

Table 12 Device Information Screen Fields

LABEL	DESCRIPTION
Device Name	Select the device for which to display information.
Device MAC	This is the LAN MAC address of the device.
System Name	This is the name of the device you configured.
Model Name	This is the model type of the device.
System Up Time	This is the total amount of time the ZyXEL device has been running since it last restarted.
Firmware Version	This is the firmware version the ZyXEL device currently uses.
Monitor & Summary Report	Select the monitor or summary report information to display for the device. See Section 3.7.2 on page 48 for more on monitors and reports.

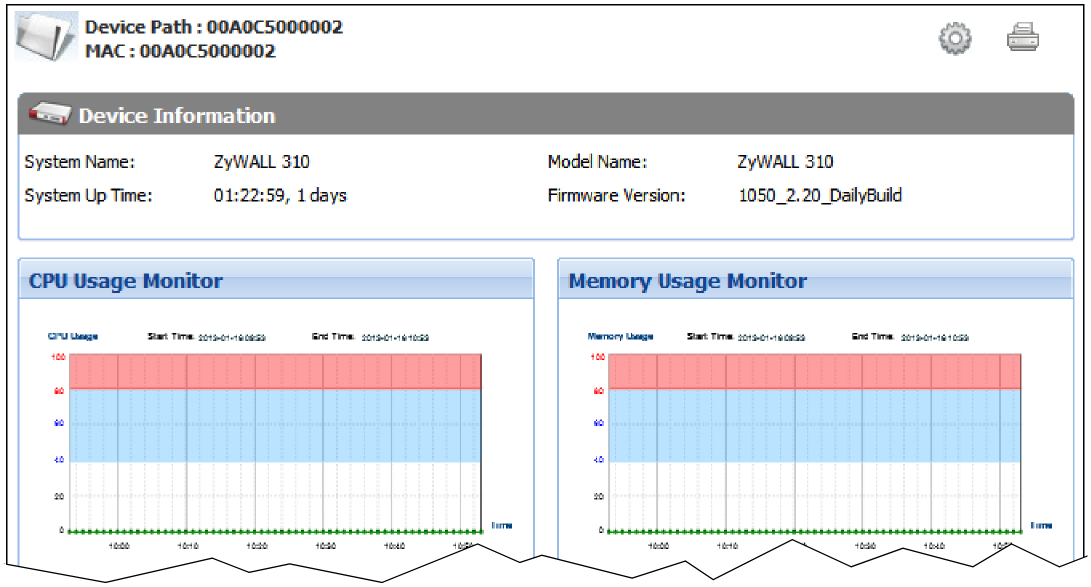
3.7 Report and Setting Window

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

3.7.1 Device Information Screen

When you first click on a device in the device window, the information you configured for the device displays in the report and setting window. See Section 3.4 on page 30 for how to add and edit device information.

Figure 17 Device Information Screen



Device Path : 00A0C5000002
MAC : 00A0C5000002

Device Information

System Name: ZyWALL 310
System Up Time: 01:22:59, 1 days
Model Name: ZyWALL 310
Firmware Version: 1050_2.20_DailyBuild

Each field is explained in the following table.

Table 13 Device Information Screen Fields

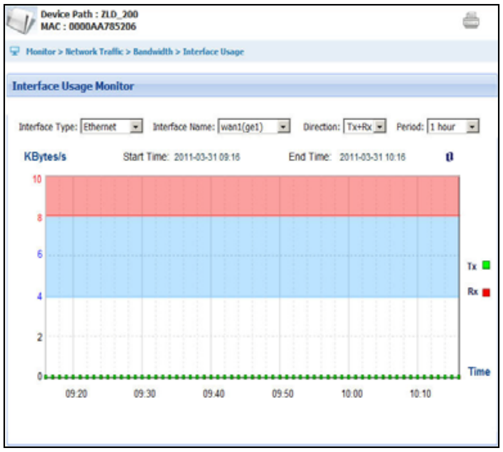
LABEL	DESCRIPTION
Device Path	You can create multiple layers of folders for devices. This field displays the name used to refer to the device in Vantage Report and the folders that the device is in. For example, if the device path is “folder1/folder2/myZyWALL”, “folder1” is in the root folder, “folder2” is in folder1 and “myZyWALL” is the name of the device and it is in folder2.
MAC	This is the LAN MAC address of the device.
System Name	This is the name of the device you configured.
System Up Time	This is the total amount of time the ZyXEL device has been running since it last restarted.
Model Name	This is the model type of the device.
Firmware Version	This is the firmware version the ZyXEL device currently uses.

3.7.2 Monitors and Statistical Reports

The layout in the report and setting window is similar for all monitors. Similarly, the layout is similar for all statistical reports. For other screens, the layout is different for each one. Typical examples of monitors and statistical reports are shown in Figure 18.

Figure 18 Report and Setting Window: Monitor and Statistical Report Examples

Monitor



Device Path : ZLD_200
MAC : 0000AA785206

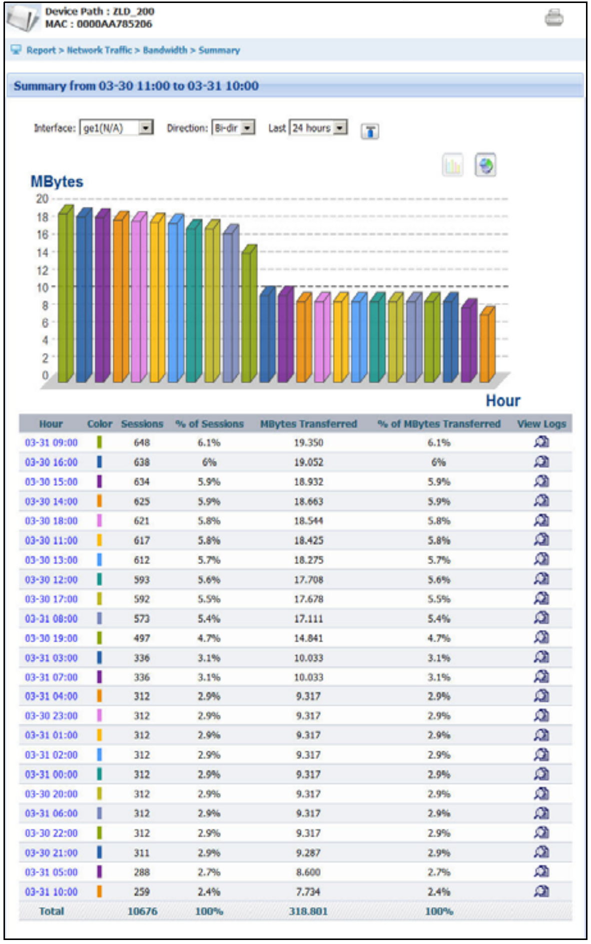
Monitor > Network Traffic > Bandwidth > Interface Usage

Interface Usage Monitor

Interface Type: Ethernet   Interface Name: wan1(ge1)   Direction: Tx+Rx   Period: 1 hour

Start Time: 2011-03-31 09:16   End Time: 2011-03-31 10:16

Statistical Report



Device Path : ZLD_200
MAC : 0000AA785206

Report > Network Traffic > Bandwidth > Summary

Summary from 03-30 11:00 to 03-31 10:00

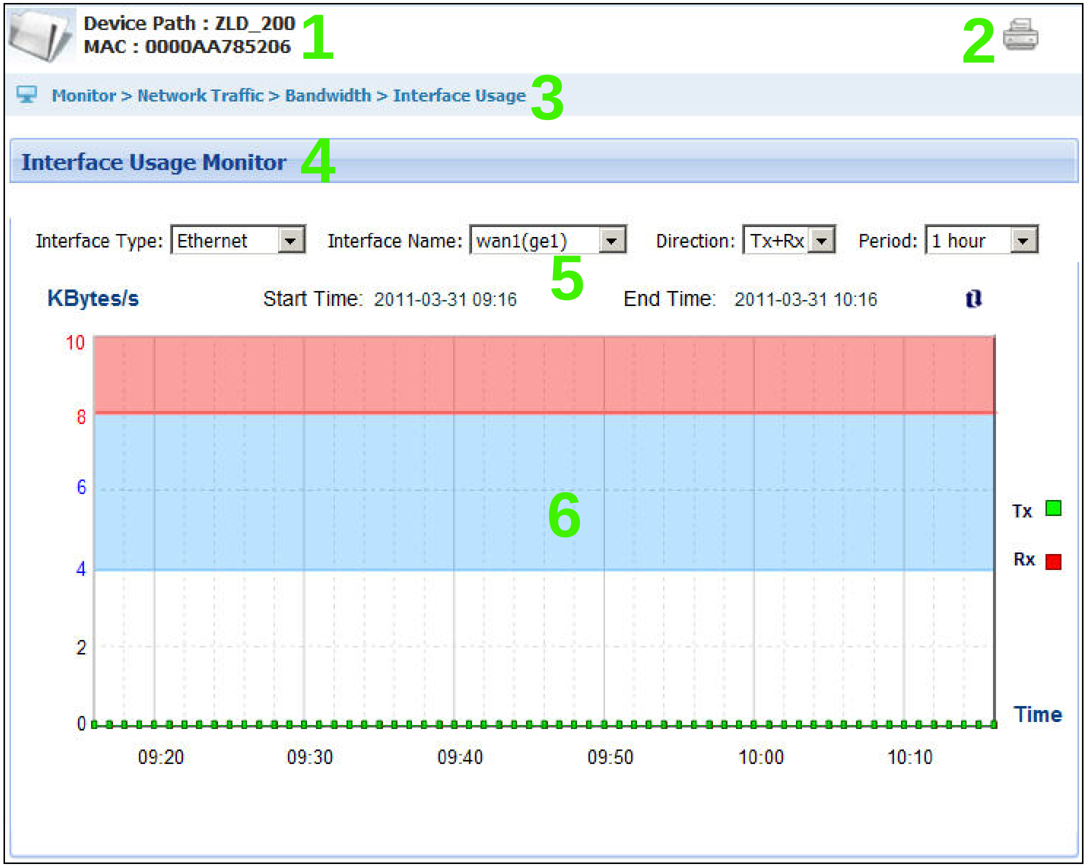
Interface: ge1(N/A)   Direction: Bi-dir   Last 24 hours

Hour	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
03-31 09:00	▮	648	6.1%	19.350	6.1%	🔍
03-30 16:00	▮	638	6%	19.052	6%	🔍
03-30 15:00	▮	634	5.9%	18.932	5.9%	🔍
03-30 14:00	▮	625	5.9%	18.663	5.9%	🔍
03-30 18:00	▮	621	5.8%	18.544	5.8%	🔍
03-30 11:00	▮	617	5.8%	18.425	5.8%	🔍
03-30 13:00	▮	612	5.7%	18.275	5.7%	🔍
03-30 12:00	▮	593	5.6%	17.708	5.6%	🔍
03-30 17:00	▮	592	5.5%	17.678	5.5%	🔍
03-31 08:00	▮	573	5.4%	17.111	5.4%	🔍
03-30 19:00	▮	497	4.7%	14.841	4.7%	🔍
03-31 03:00	▮	336	3.1%	10.033	3.1%	🔍
03-31 07:00	▮	336	3.1%	10.033	3.1%	🔍
03-31 04:00	▮	312	2.9%	9.317	2.9%	🔍
03-30 23:00	▮	312	2.9%	9.317	2.9%	🔍
03-31 01:00	▮	312	2.9%	9.317	2.9%	🔍
03-31 02:00	▮	312	2.9%	9.317	2.9%	🔍
03-31 00:00	▮	312	2.9%	9.317	2.9%	🔍
03-30 20:00	▮	312	2.9%	9.317	2.9%	🔍
03-31 06:00	▮	312	2.9%	9.317	2.9%	🔍
03-30 22:00	▮	312	2.9%	9.317	2.9%	🔍
03-30 21:00	▮	311	2.9%	9.287	2.9%	🔍
03-31 05:00	▮	288	2.7%	8.600	2.7%	🔍
03-31 10:00	▮	259	2.4%	7.734	2.4%	🔍
Total		10676	100%	318.801	100%	

3.7.2.1 Monitor Layout

A typical monitor is shown in Figure 10.

Figure 19 Typical Monitor Layout



Device Path : ZLD_200
MAC : 0000AA785206

Monitor > Network Traffic > Bandwidth > Interface Usage

Interface Usage Monitor

Interface Type: Ethernet
Interface Name: wan1(ge1)
Direction: Tx+Rx
Period: 1 hour

Start Time: 2011-03-31 09:16
End Time: 2011-03-31 10:16

Each numbered section above is described in the following table.

Table 14 Typical Monitor Features

SECTION	DESCRIPTION
1	**Device Path**, **MAC**: These fields display the path you added the ZyXEL device in the Vantage Report and the device's MAC address.
2	**Print** icon: Click this icon to print the current screen.
3	This field shows the menu items you selected to open this monitor.
4	This field displays the title of the monitor.
5	**Start Time**: the time of the earliest traffic information in the graph **End Time**: the time of the latest traffic information in the graph. **Refresh** icon: Click this icon to update the screen immediately.
6	The graph shows how the status changes over time. The X-axis (horizontal) is time. See Section 2.3 on page 20 for more information about clock time in Vantage Report. The Y-axis (vertical) depends on the type of monitor you select. In Figure 19, the Y-axis is the amount of traffic in kilobytes the ge1 Ethernet interface has transmitted and received in the past one hour. See Section 2.6 on page 22 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.

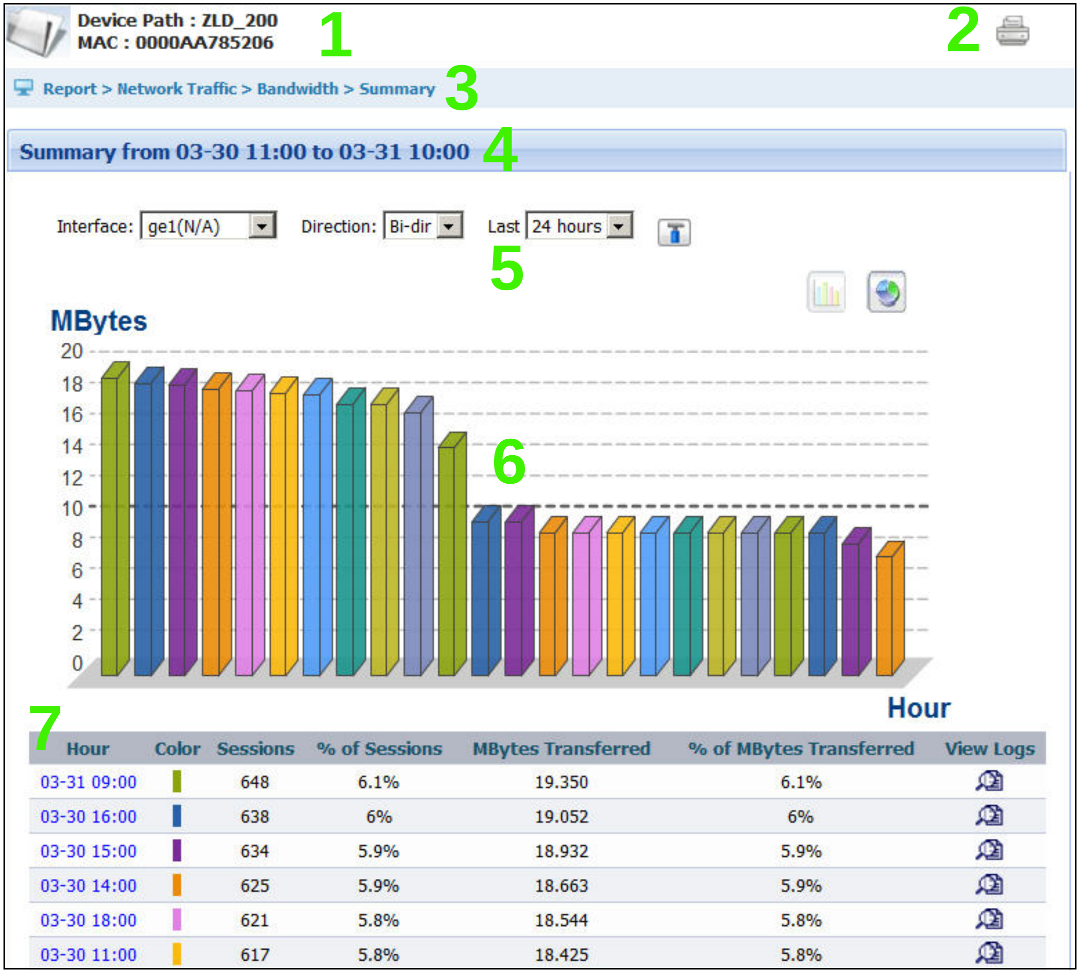
Figure 20 Report and Setting Window Right-Click Menu

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

3.7.2.2 Statistical Report Layout

A typical statistical report is shown in Figure 21.

Figure 21 Typical Statistical Report Layout



Device Path : ZLD_200
MAC : 0000AA785206

Report > Network Traffic > Bandwidth > Summary

Summary from 03-30 11:00 to 03-31 10:00

Interface: ge1(N/A) Direction: Bi-dir Last 24 hours

Hour	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
03-31 09:00	🟩	648	6.1%	19.350	6.1%	🔍
03-30 16:00	🟦	638	6%	19.052	6%	🔍
03-30 15:00	🟪	634	5.9%	18.932	5.9%	🔍
03-30 14:00	🟧	625	5.9%	18.663	5.9%	🔍
03-30 18:00	■	621	5.8%	18.544	5.8%	🔍
03-30 11:00	🟨	617	5.8%	18.425	5.8%	🔍

Each numbered section above is described in the following table.

Table 15 Typical Statistical Report Features

SECTION	DESCRIPTION
1	**Device Path**, **MAC**: These fields display the path you added the ZyXEL device in the Vantage Report and the device's MAC address.
2	**Print** icon: Click this icon to print the current screen.

Table 15 Typical Statistical Report Features

SECTION	DESCRIPTION
3	This field shows the menu items you selected to open this statistical report.
4	This field displays the title of the statistical report. The title includes the date(s) you specified in section 5.
5	**Last**, **Settings** icon: Use one of these fields to specify what historical information is included in the report. • Select how many days, ending (and including today), in the **Last** field. • Click the **Settings** icon, the **Report Display Settings** screen appears. The date range can be up to 30 days long. You can select **custom..** in the **Last** field and then select a specific **Start Date** and **End Date**. When you change any of these fields, the report updates automatically.Both the **Last** and **Settings** fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). They do not reset when you open or close drill-down reports. These fields are not available in drill-down reports because these reports use the same historical information as the main report. See Section 2.3 on page 20 for more information about time in **Report** screens.
6	The graph displays the specified report visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System Setting** > **General Configuration**. See Section 14.1 on page 457. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little. See Section 2.6 on page 22 for more information about the source data used by the statistical report.
7	In the table, • Click on a link to drill down into the report. The current report is replaced by a detailed report for the selected record. The detailed report uses the same historical information you select in #5. • If **DNS Reverse** is enabled in **System Setting** > **General Configuration**, the table displays the domain name, if identifiable, with IP addresses (for example, “www.yahoo.com/ 200.100.20.10”). See Section 14.1 on page 457. • Some reports provide extra information (for example, number of traffic events) in the table. See each report for more information. • Click a view logs icon to display the logs related to the individual record. See Section 2.6 on page 22 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.

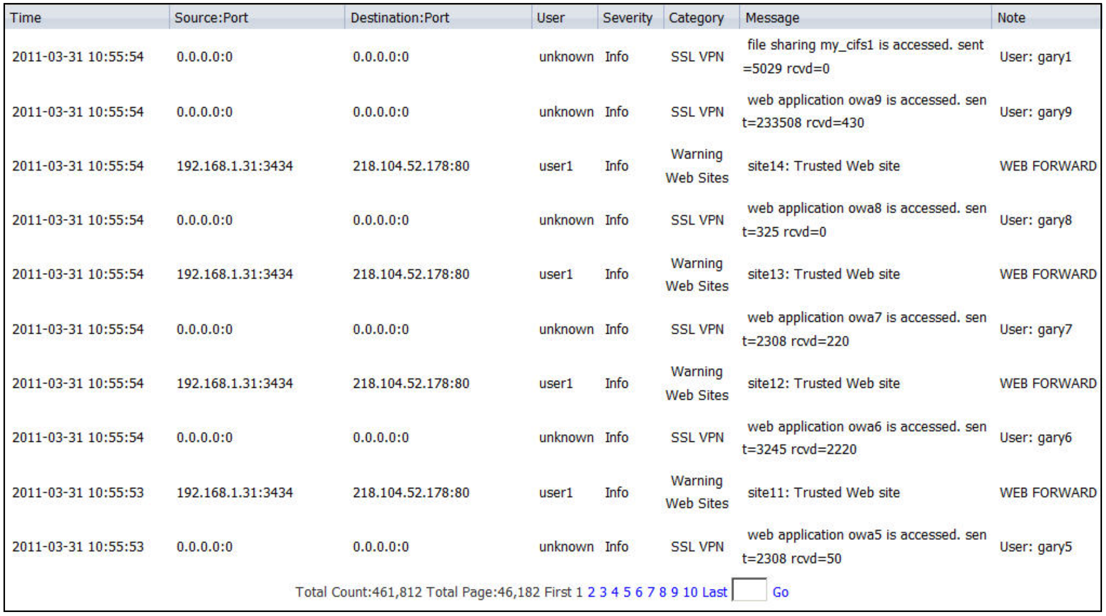
Figure 22 Report and Setting Window Right-Click Menu

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

3.7.3 View Logs

The **Logs** > **Log Viewer** screen displays the logs related to an individual record in a statistical report. See Appendix A on page 491 for information on the logs.

Figure 23 View Logs



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

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

See Table 234 on page 442 for the description of each field in this screen.

PART II

Technical Reference

4

Monitor

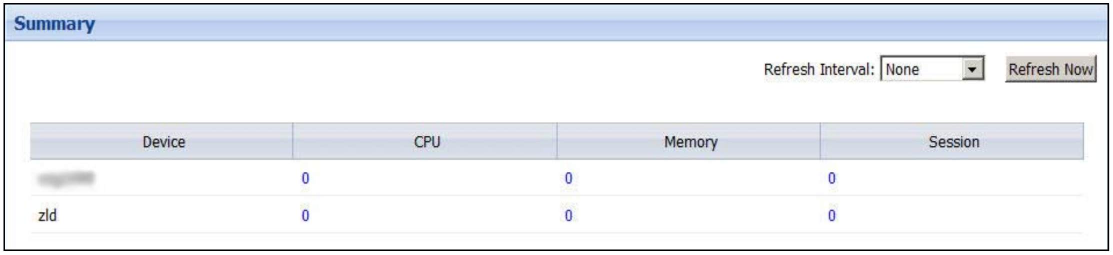
Use monitor screens to check the status of ZyXEL devices. See Section 2.3 on page 20 for a related discussion about time.

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

4.1 Monitor (Folder)

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

Figure 24 Monitor (Folder)



Summary

Refresh Interval: None ▾ Refresh Now

Device	CPU	Memory	Session
[redacted]	0	0	0
zld	0	0	0

Each field is described in the following table.

Table 16 Monitor (Folder)

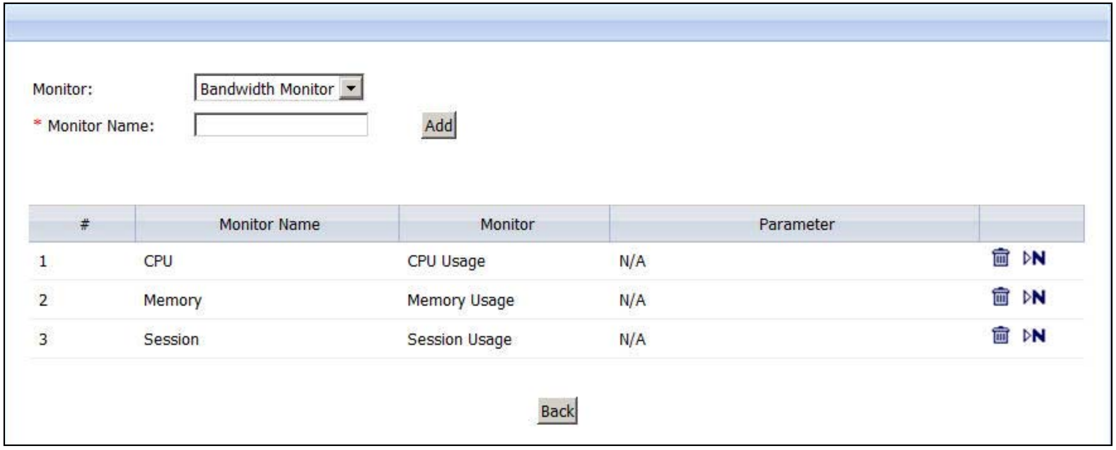
LABEL	DESCRIPTION
Refresh Interval	Select how often (**1 Minute**, **5 Minutes**, **10 Minutes**) the Vantage Report updates the information in this screen. Select **None** to not to update this screen. Click **Refresh Now** to update the screen immediately.
Device	This field displays the name of a device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

4.1.1 Customize the Column Fields

Click a folder and then click the **Setting** ( ) icon at the top-right corner of the screen to open this screen. Use this screen to customize the column fields in the **Monitor (Folder)** screen (see

Figure 24 on page 55). Vantage Report monitors the CPU usage, memory usage and the number of concurrent sessions by default for devices under a folder.

Figure 25 Customize the Column Fields



Monitor: Bandwidth Monitor

* Monitor Name:

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

Each field is described in the following table.

Table 17 Customize the Column Fields

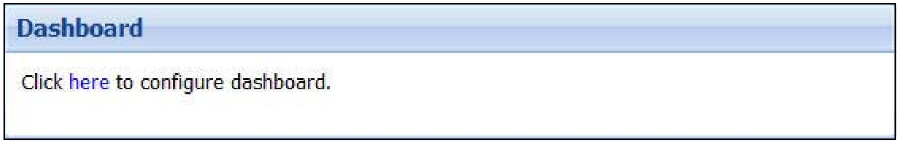
LABEL	DESCRIPTION
Monitor	Select a category to monitor device(s) under the folder.
Port	This field is available when you select **Port Usage** in the **Monitor** field. Select a port to monitor.
Direction	This field is available when you select **Port Usage** or **Interface Usage** in the **Monitor** field. Select transmission (**Tx**), receiving (**Rx**) or both (**Tx+Rx**) for the traffic direction to monitor.
Interface Type	This field is available when you select **Interface Usage** in the **Monitor** field. Select the type of the interface to monitor.
Interface	This field is available when you select **Interface Usage** in the **Monitor** field. The available options in this field may vary depending on the **Interface Type** you select. Select an interface to monitor.
Service	This field is available when you select **Service Monitor** in the **Monitor** field. Select a service type to monitor.
Monitor Name	Type up to 29 alphanumeric characters for the name of the monitor item. Underscore (_) is allowed.
Add	Click this to add the monitor item to the list table below and save the changes to the Vantage Report.
#	This field displays the index number of the monitor item.
Monitor Name	This field displays the name of the monitor item.
Monitor	This field displays the category of the monitor item.
Parameter	This field displays the additional parameters of the monitor item. **N/A** displays if no additional parameters for the monitor item.
Back	Click this to go back to the previous screen.

4.2 Dashboard

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

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

Figure 26 Dashboard Initial View

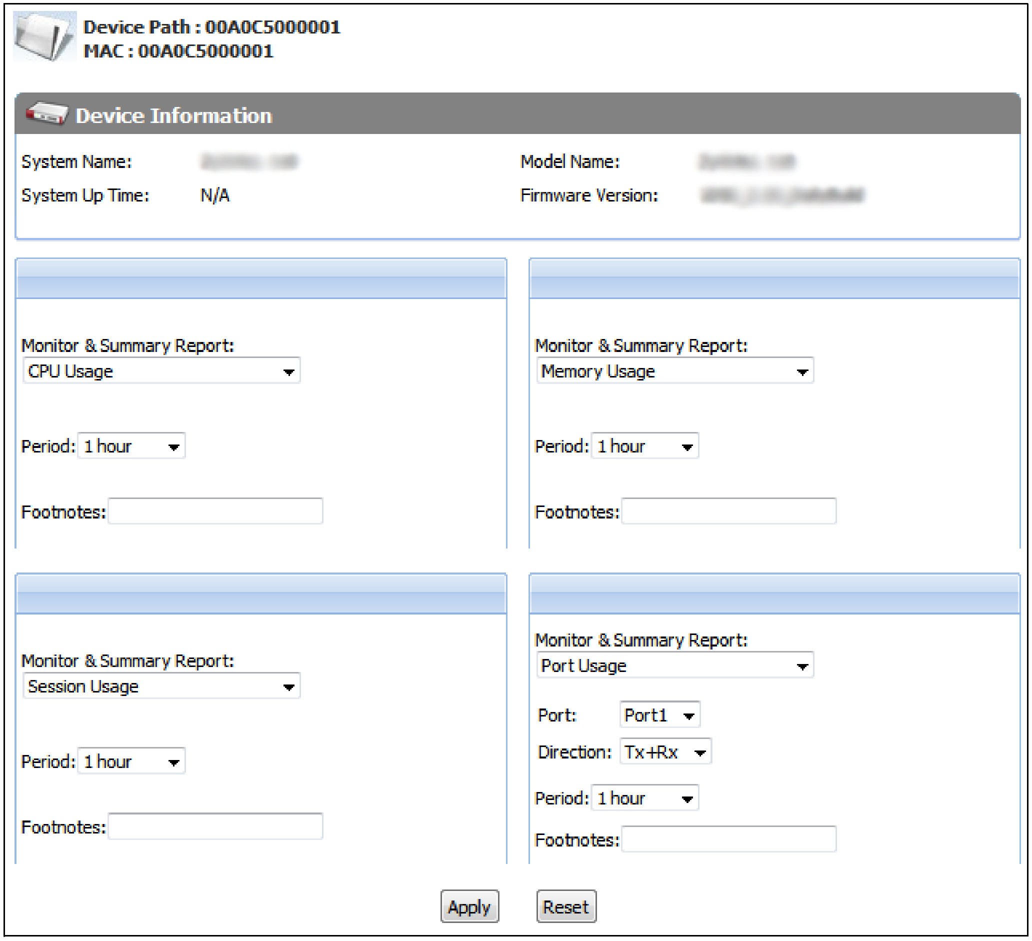


Dashboard

Click here to configure dashboard.

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

Figure 27 Dashboard Configuration



Device Path : 00A0C5000001
MAC : 00A0C5000001

Device Information

System Name: [redacted]
Model Name: [redacted]
System Up Time: N/A
Firmware Version: [redacted]

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

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

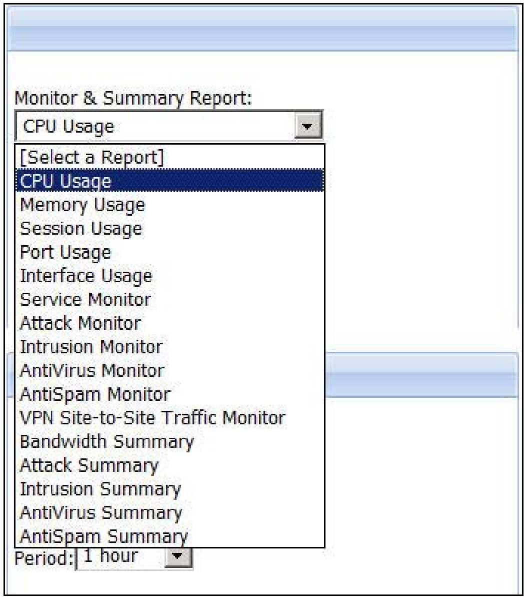
Monitor & Summary Report: Session Usage
Period: 1 hour
Footnotes:

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

Select a monitor or summary report to display for each.

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

Figure 28 Dashboard Select Device and Monitor or Summary



Monitor & Summary Report:

CPU Usage

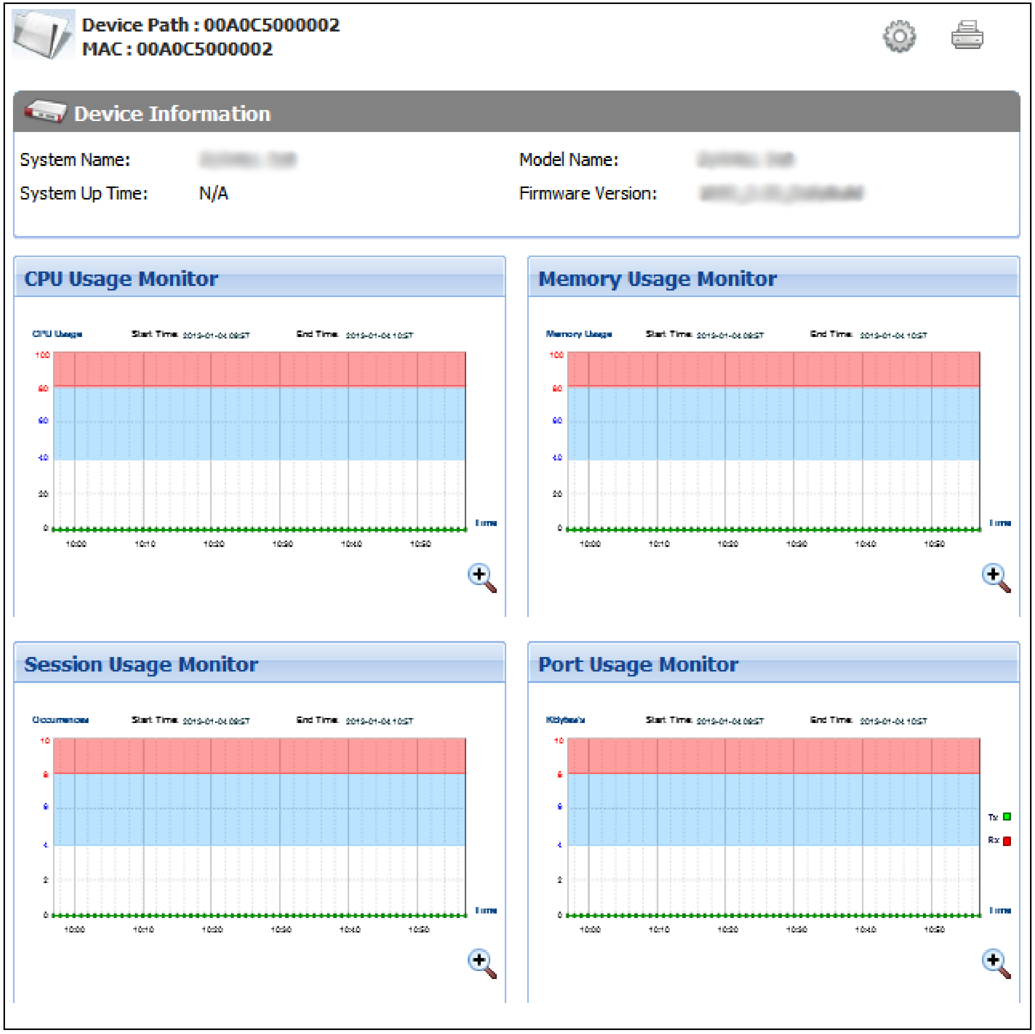
Period: 1 hour

4.3 Dashboard

The dashboard looks as follows when you finish configuring it.

Click the magnifying glass icon at the right bottom of each monitor or report to go to the corresponding monitor screen. The dashboard is available with the full version of Vantage Report. See Section 3.7.1 on page 47 for the field descriptions shown in the screen.

Figure 29 Dashboard Configured



Device Path : 00A0C5000002
MAC : 00A0C5000002

Device Information

System Name:	[redacted]	Model Name:	[redacted]
System Up Time:	N/A	Firmware Version:	[redacted]

CPU Usage Monitor

Memory Usage Monitor

Session Usage Monitor

Port Usage Monitor

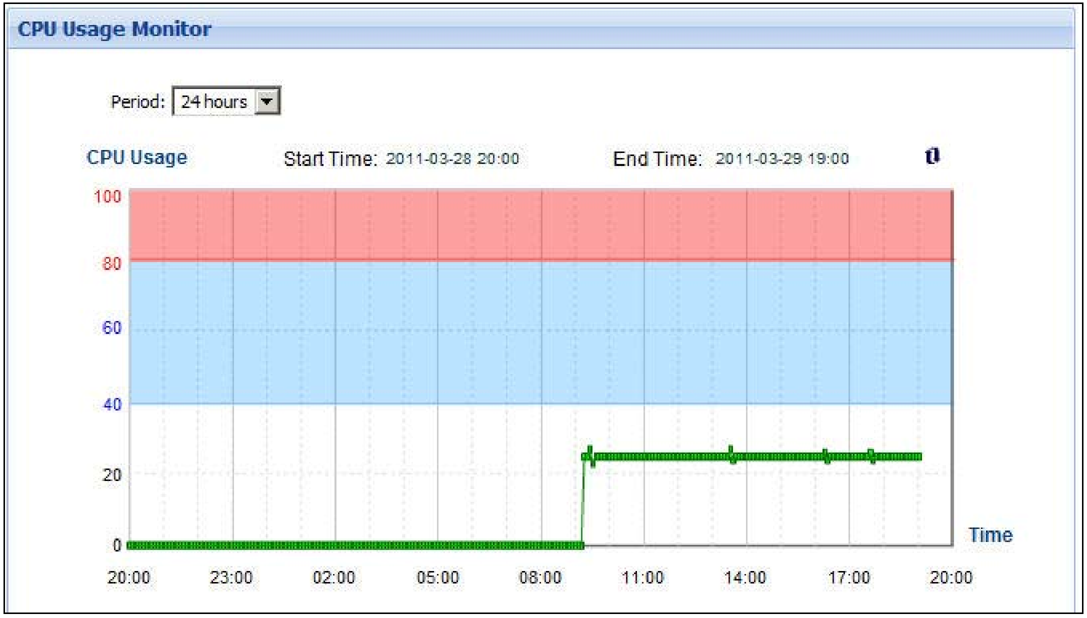
If you want to change a dashboard monitor or report, click the ⚙ icon at the top right corn. See Figure 27 on page 57.

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

4.4 CPU Usage Monitor

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

Figure 30 Monitor > Hardware Status > CPU Usage



CPU Usage Monitor

Period: 24 hours

CPU Usage Start Time: 2011-03-28 20:00 End Time: 2011-03-29 19:00

Each field is described in the following table.

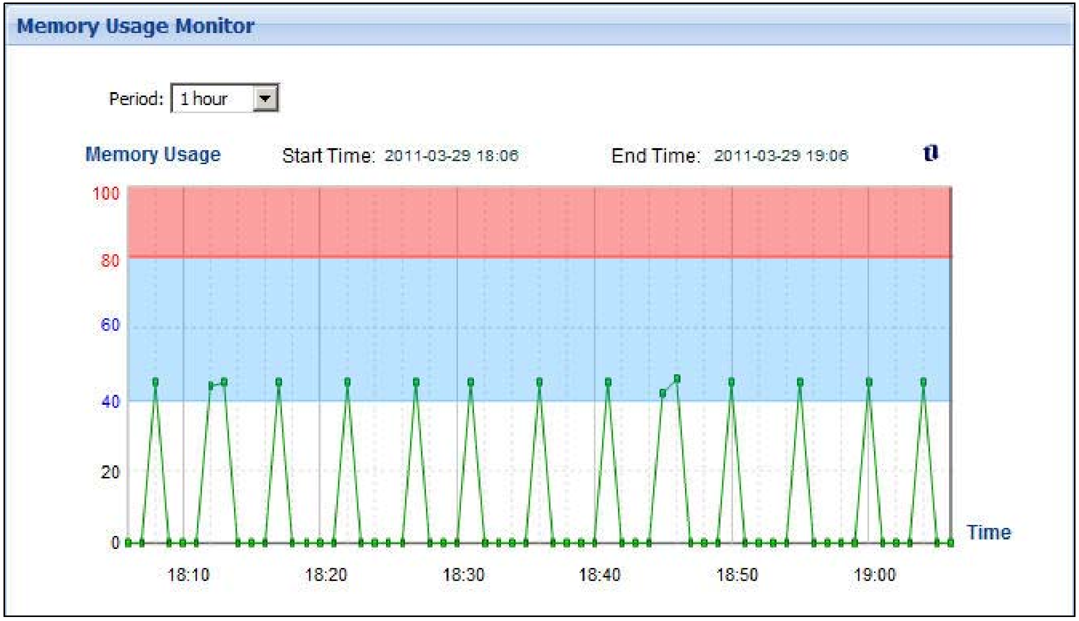
Table 18 Monitor > Hardware Status > CPU Usage

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

4.5 Memory Usage Monitor

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

Figure 31 Monitor > Hardware Status > Memory Usage



Each field is described in the following table.

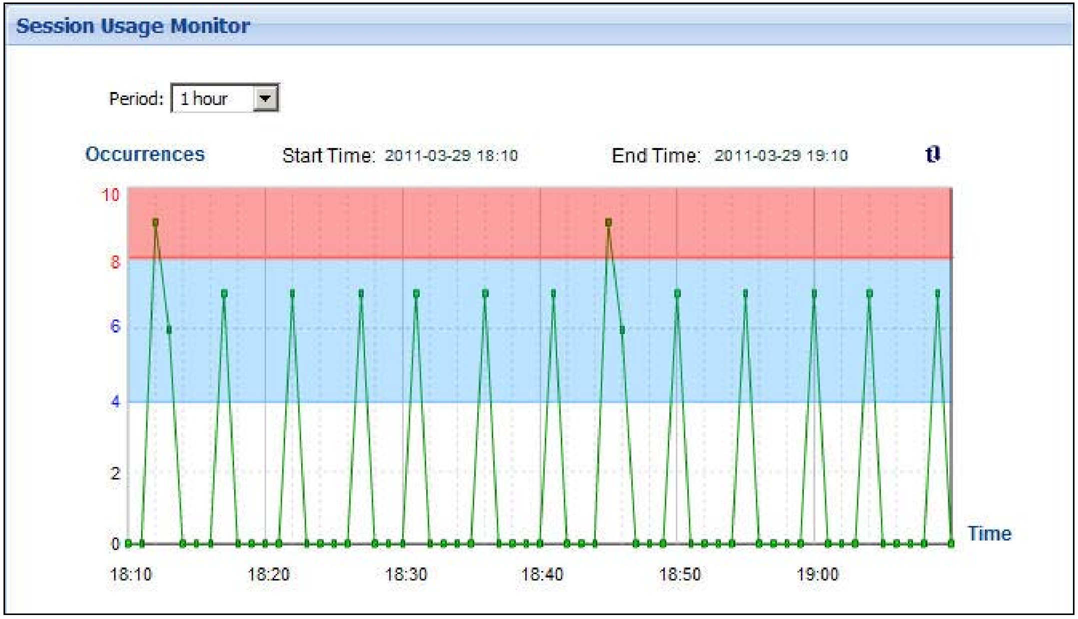
Table 19 Monitor > Hardware Status > Memory Usage

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

4.6 Session Usage Monitor

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

Figure 32 Monitor > Network Traffic > Session Usage



Session Usage Monitor

Period: 1 hour

Start Time: 2011-03-29 18:10

End Time: 2011-03-29 19:10

Each field is described in the following table.

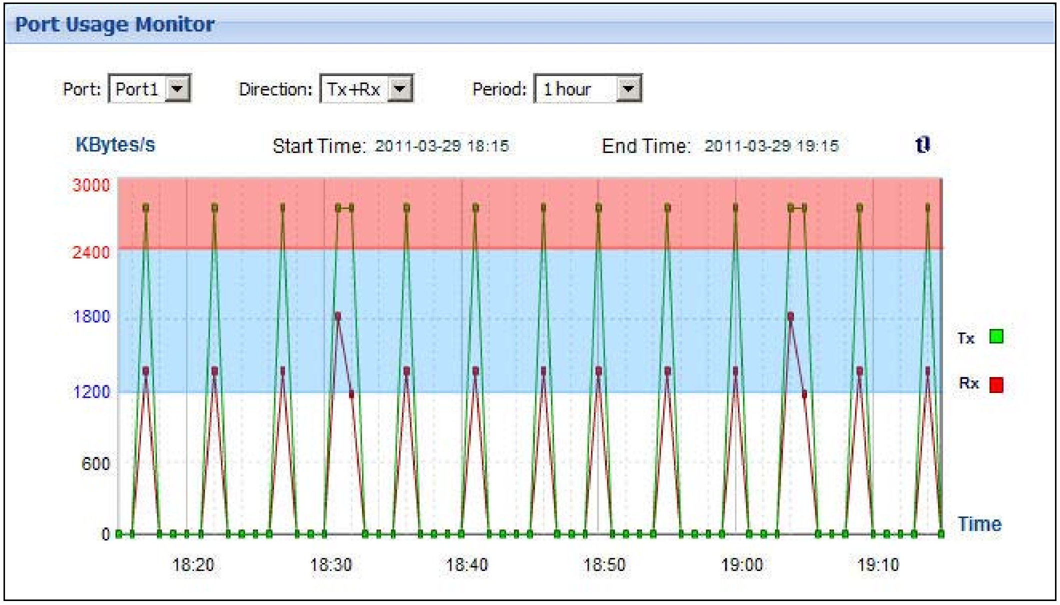
Table 20 Monitor > Network Traffic > Session Usage

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

4.7 Port Usage Monitor

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

Figure 33 Monitor > Network Traffic > Bandwidth > Port Usage



Port Usage Monitor

Port: Port1 Direction: Tx+Rx Period: 1 hour

Start Time: 2011-03-29 18:15 End Time: 2011-03-29 19:15

Each field is described in the following table.

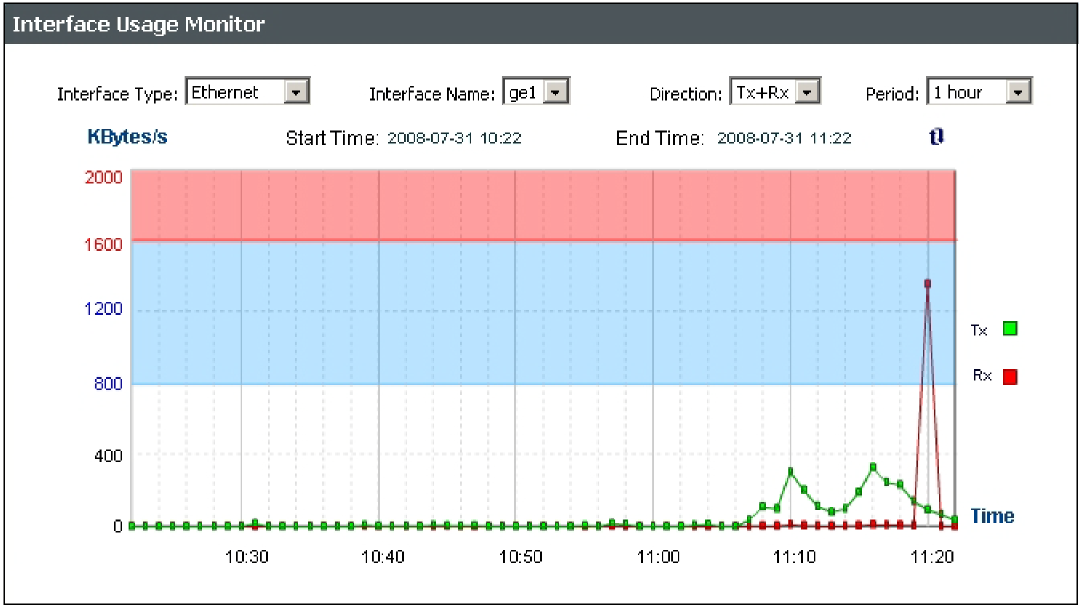
Table 21 Monitor > Network Traffic > Bandwidth > Port Usage

LABEL	DESCRIPTION
Port	Select a port to display the throughput statistics of the corresponding port.
Direction	Select the direction of the traffic for which you want to show throughput statistics in this graph. Select **Tx** to display transmitted traffic throughput statistics and select **Rx** to display received traffic throughput statistics in KBytes per second. Alternatively, select **Tx-Rx** to display both.
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. The Vantage Report automatically calculates the start time depending on the period you selected in the **Period** field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
↻	The **Refresh** icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): the amount of traffic through the selected port. X-axis (horizontal): The X-axis displays a date or time depending on the length of time you choose in the **Period** field.

4.8 Interface Usage Monitor

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

Figure 34 Monitor > Network Traffic > Bandwidth > Interface Usage



Interface Usage Monitor

Interface Type: Ethernet

Interface Name: ge1

Direction: Tx+Rx

Period: 1 hour

Start Time: 2008-07-31 10:22

End Time: 2008-07-31 11:22

Each field is described in the following table.

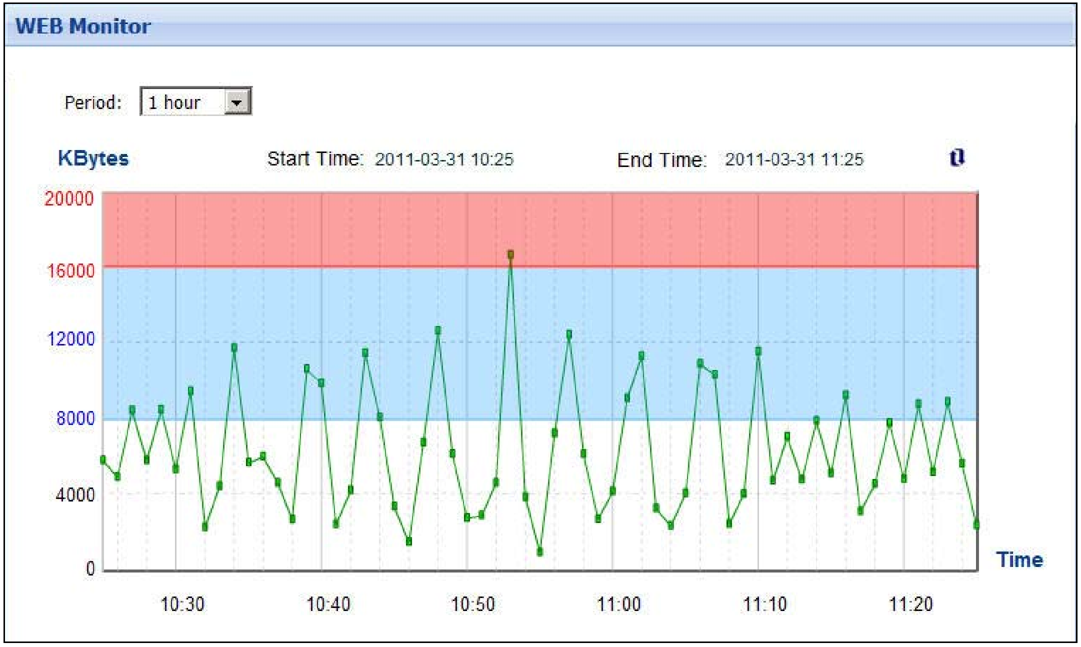
Table 22 Monitor > Network Traffic > Bandwidth > Interface Usage

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

4.9 Web Monitor

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

Figure 35 Monitor > Network Traffic > Web



WEB Monitor

Period: 1 hour

Start Time: 2011-03-31 10:25

End Time: 2011-03-31 11:25

Each field is described in the following table.

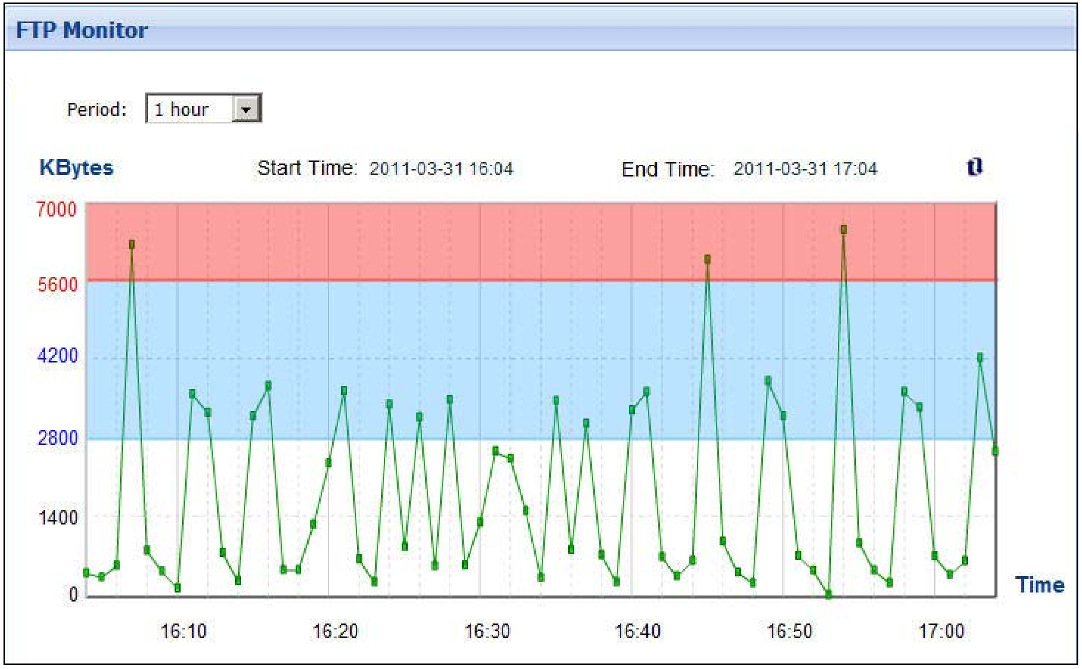
Table 23 Monitor > Network Traffic > Web

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

4.10 FTP Monitor

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

Figure 36 Monitor > Network Traffic > FTP



FTP Monitor

Period: 1 hour

Start Time: 2011-03-31 16:04

End Time: 2011-03-31 17:04

Each field is described in the following table.

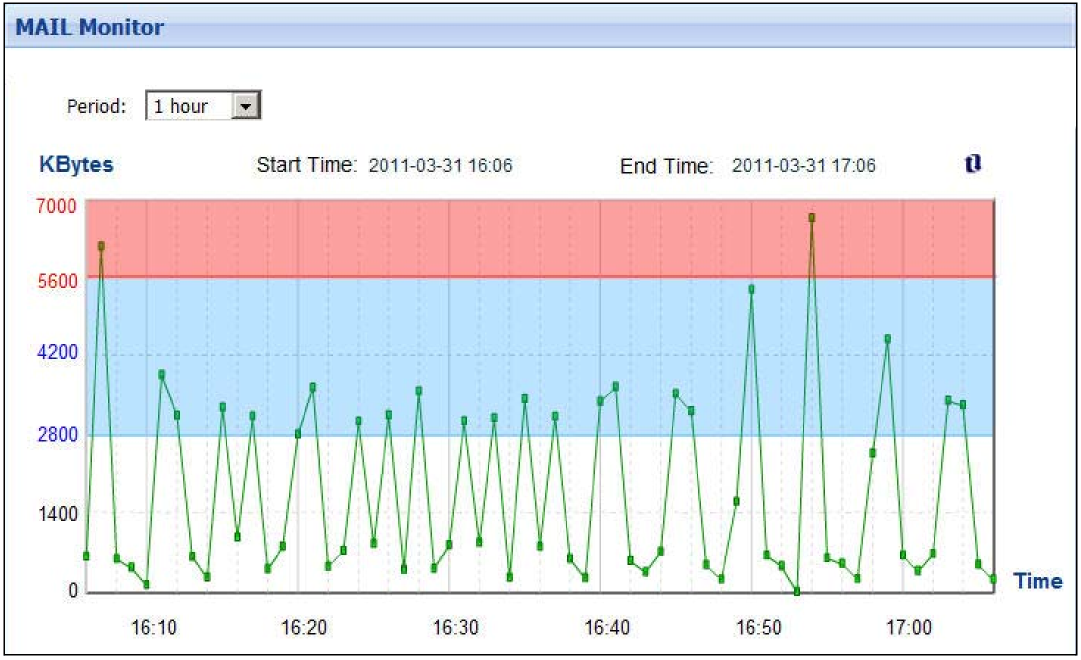
Table 24 Monitor > Network Traffic > FTP

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

4.11 E-Mail Monitor

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

Figure 37 Monitor > Network Traffic > Mail



MAIL Monitor

Period: 1 hour

Start Time: 2011-03-31 16:06

End Time: 2011-03-31 17:06

Each field is described in the following table.

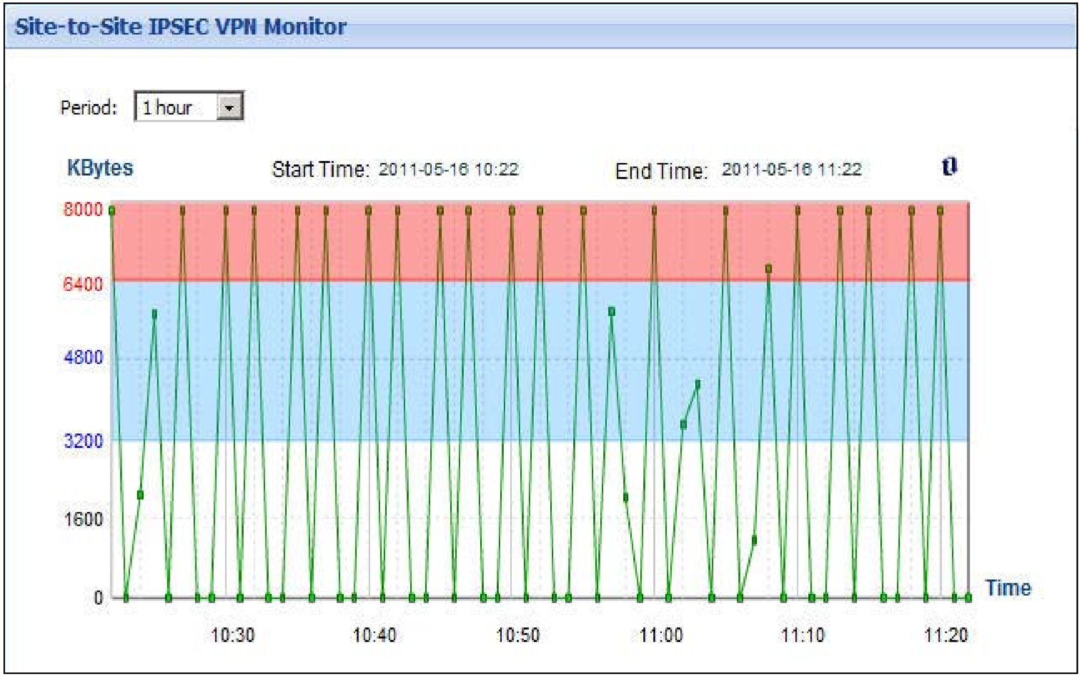
Table 25 Monitor > Network Traffic > Mail

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

4.12 Site to Site (IPSec) VPN Monitor

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

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



Site-to-Site IPSEC VPN Monitor

Period: 1 hour

Start Time: 2011-05-16 10:22

End Time: 2011-05-16 11:22

Each field is described in the following table.

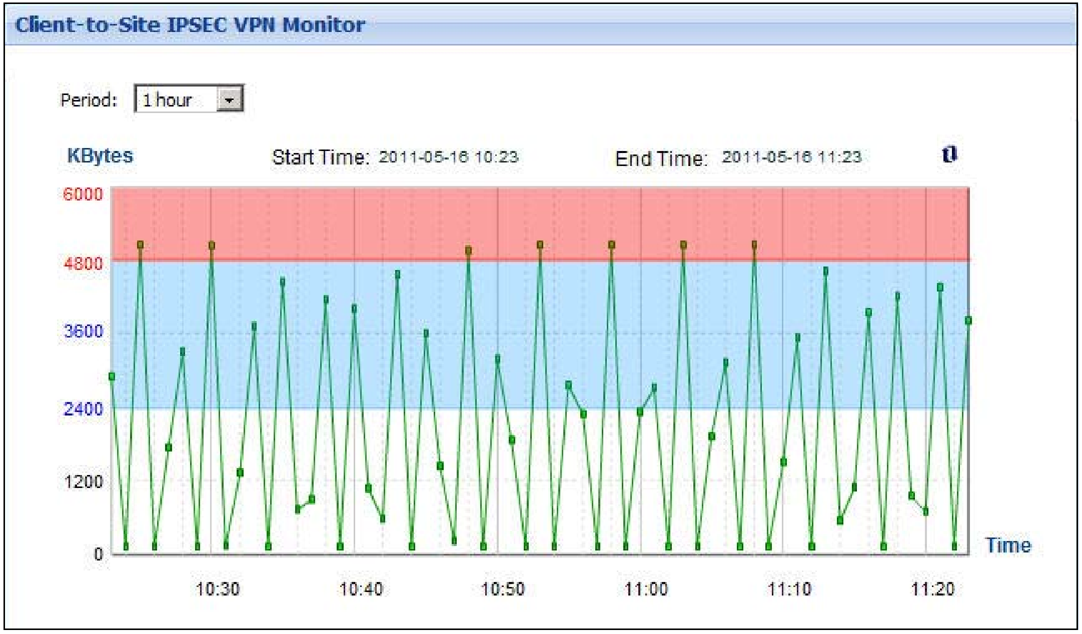
Table 26 Monitor > Secure Remote Access > Site-to-Site(IPSec)

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

4.13 Client to Site (IPSec) VPN Monitor

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

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



Client-to-Site IPSEC VPN Monitor

Period: 1 hour

Start Time: 2011-05-16 10:23

End Time: 2011-05-16 11:23

Each field is described in the following table.

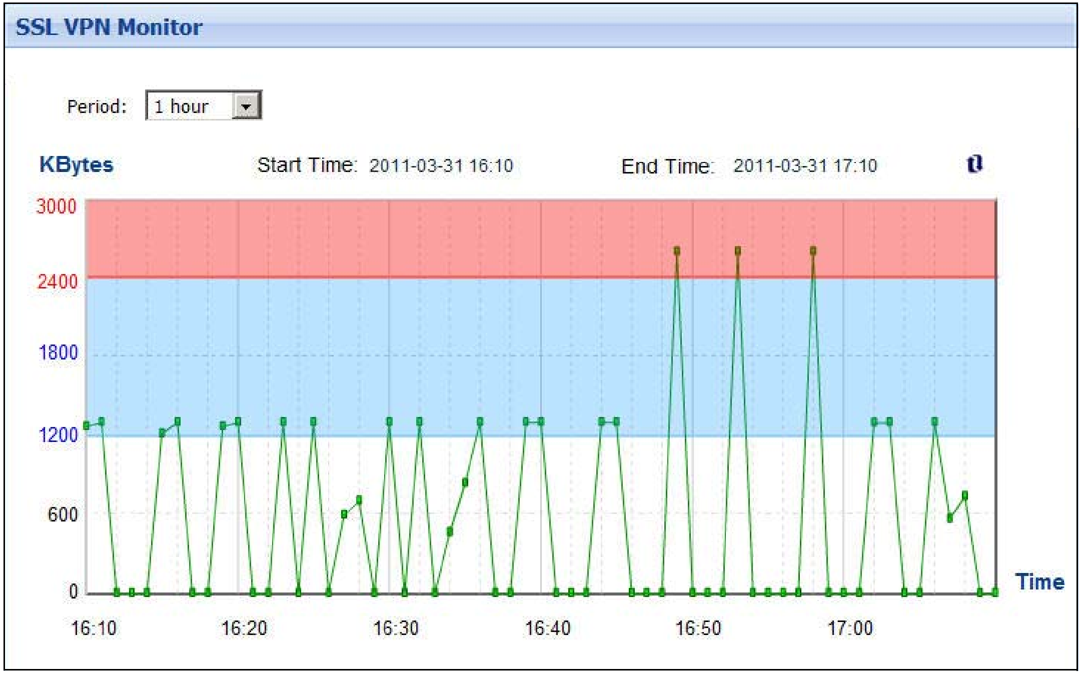
Table 27 Monitor > Secure Remote Access > Client-to-Site(IPSec)

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

4.14 Client to Site (SSL) VPN Monitor

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

Figure 40 Monitor > Secure Remote Access > Client-to-Site(SSL)



Each field is described in the following table.

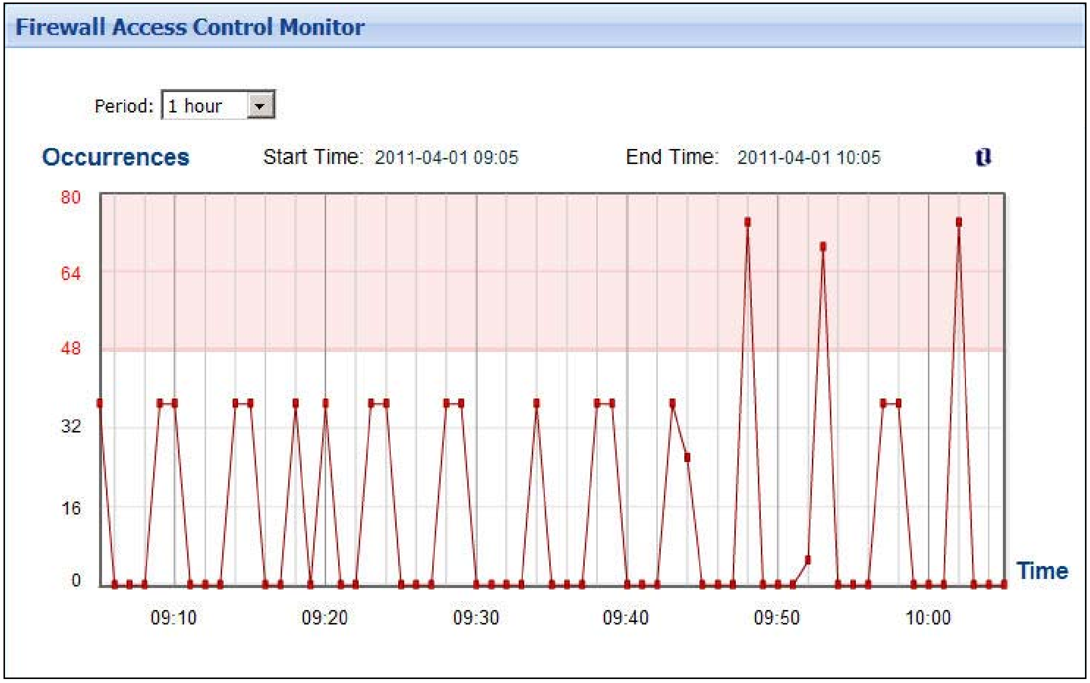
Table 28 Monitor > Secure Remote Access > Client-to-Site(SSL)

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

4.15 Firewall Access Control Monitor

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

Figure 41 Monitor > Network Security > Firewall Access Control



Firewall Access Control Monitor

Period: 1 hour

Occurrences Start Time: 2011-04-01 09:05 End Time: 2011-04-01 10:05

Each field is described in the following table.

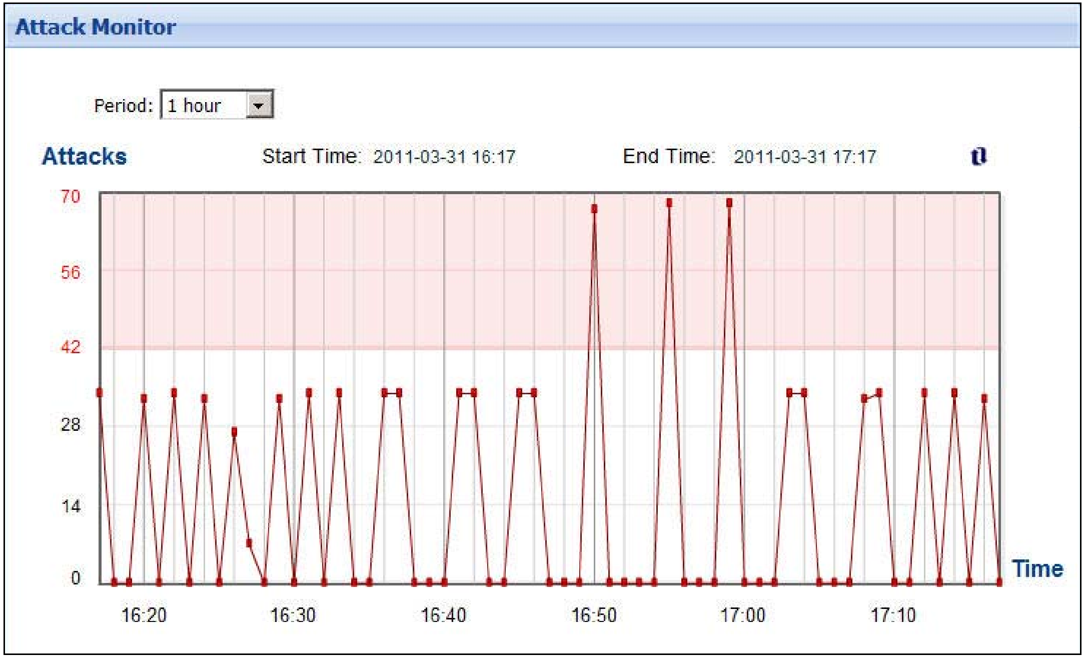
Table 29 Monitor > Network Security > Firewall Access Control

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

4.16 Attack Monitor

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

Figure 42 Monitor > Network Security > Attack



Attack Monitor

Period: 1 hour

Attacks Start Time: 2011-03-31 16:17 End Time: 2011-03-31 17:17

Each field is described in the following table.

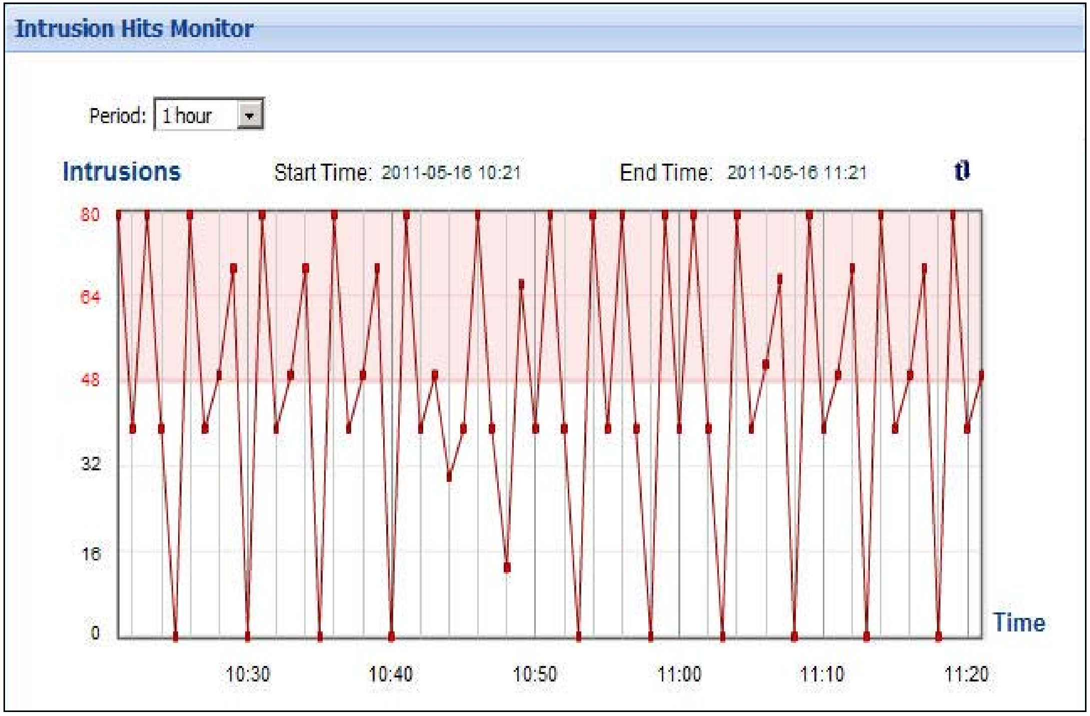
Table 30 Monitor > Network Security > Attack

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

4.17 Intrusion Hits

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

Figure 43 Monitor > Network Security > Intrusion Hits



Intrusion Hits Monitor

Period: 1 hour

Start Time: 2011-05-16 10:21

End Time: 2011-05-16 11:21

Each field is described in the following table.

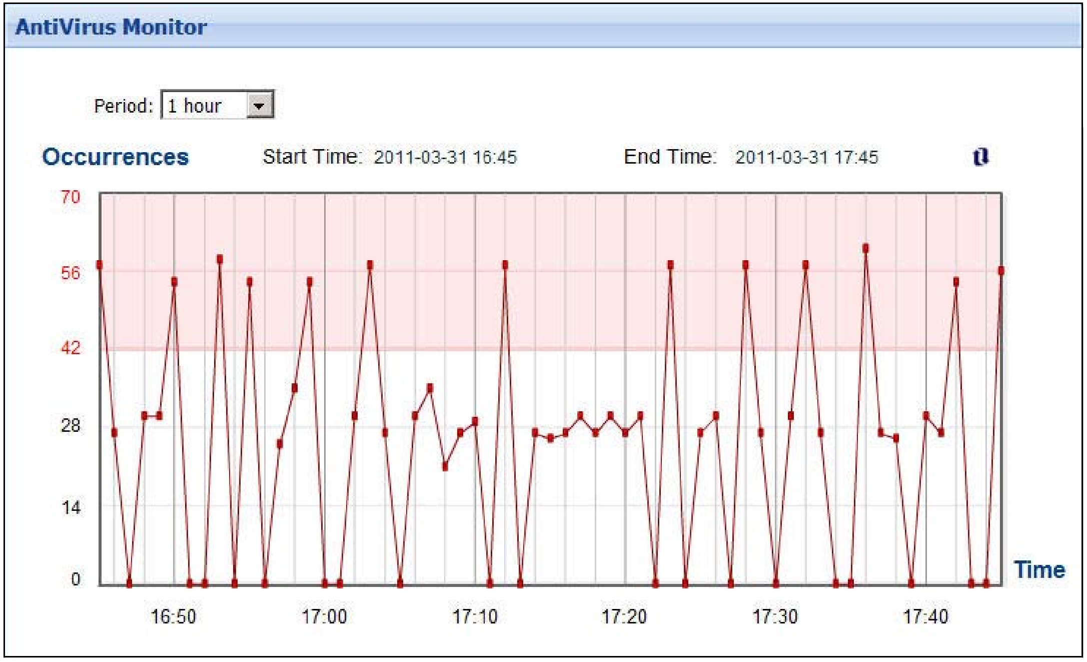
Table 31 Monitor > Network Security > Intrusion Hits

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

4.18 Anti-Virus Monitor

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

Figure 44 Monitor > Network Security > AntiVirus



AntiVirus Monitor

Period: 1 hour

Occurrences Start Time: 2011-03-31 16:45 End Time: 2011-03-31 17:45

Each field is described in the following table.

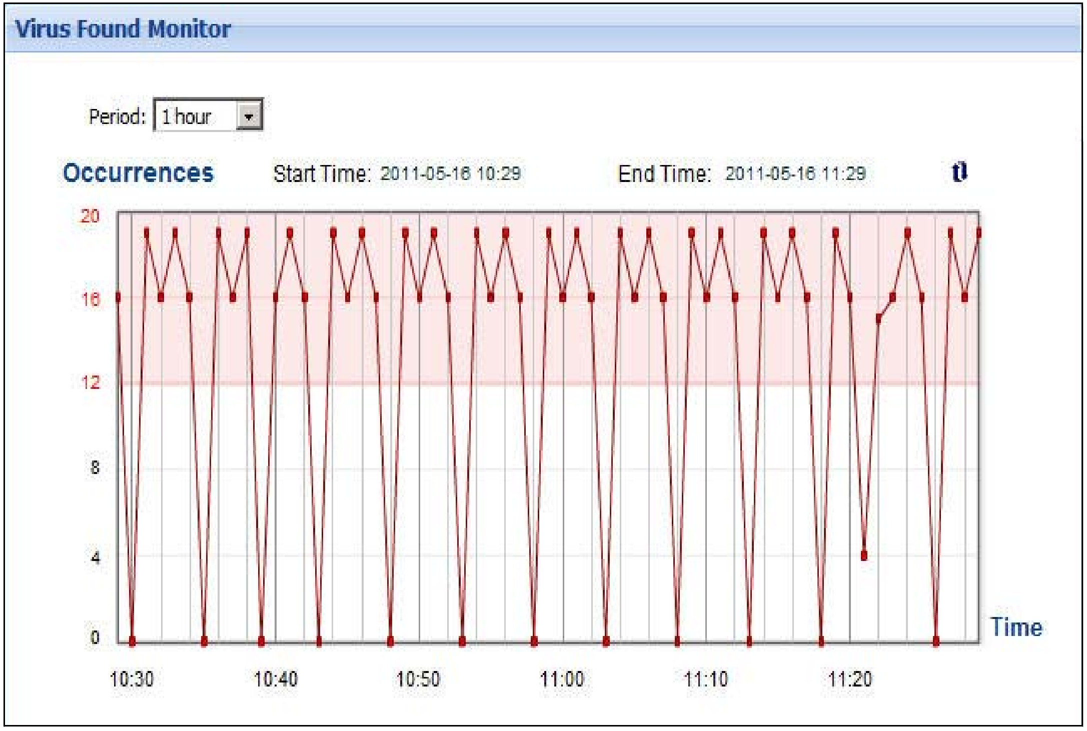
Table 32 Monitor > Network Security > AntiVirus

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

4.19 E-Mail Virus Found Monitor

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

Figure 45 Monitor > E-Mail Security > Virus Found



Virus Found Monitor

Period: 1 hour

Occurrences Start Time: 2011-05-16 10:29 End Time: 2011-05-16 11:29

Each field is described in the following table.

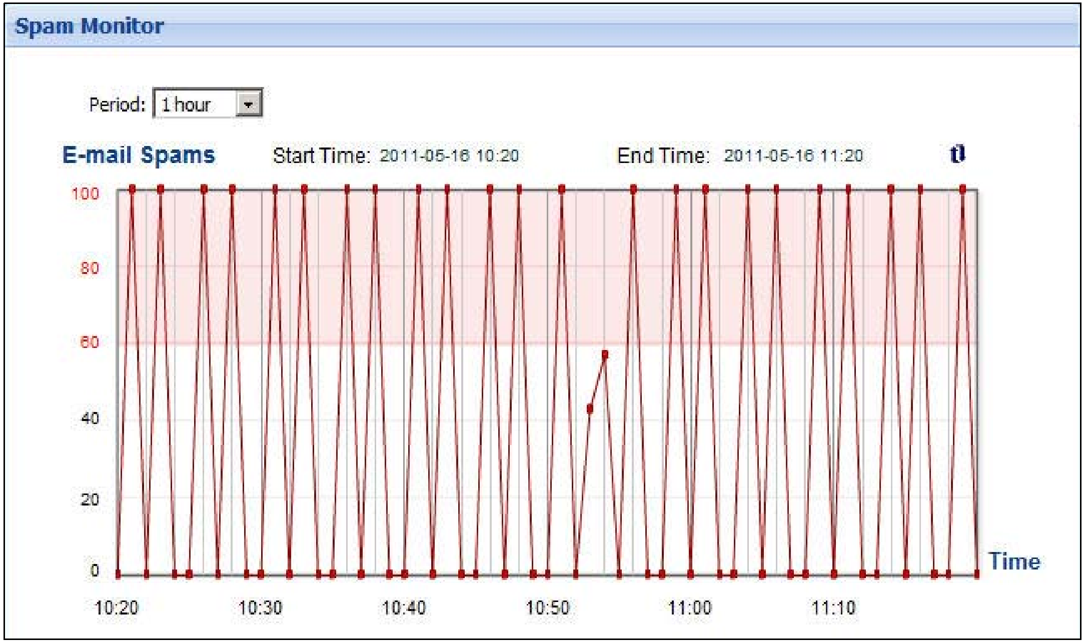
Table 33 Monitor > E-Mail Security > Virus Found

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

4.20 Spam Monitor

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

Figure 46 Monitor > E-Mail Security > Spam



Spam Monitor

Period: 1 hour

E-mail Spams Start Time: 2011-05-16 10:20 End Time: 2011-05-16 11:20

Each field is described in the following table.

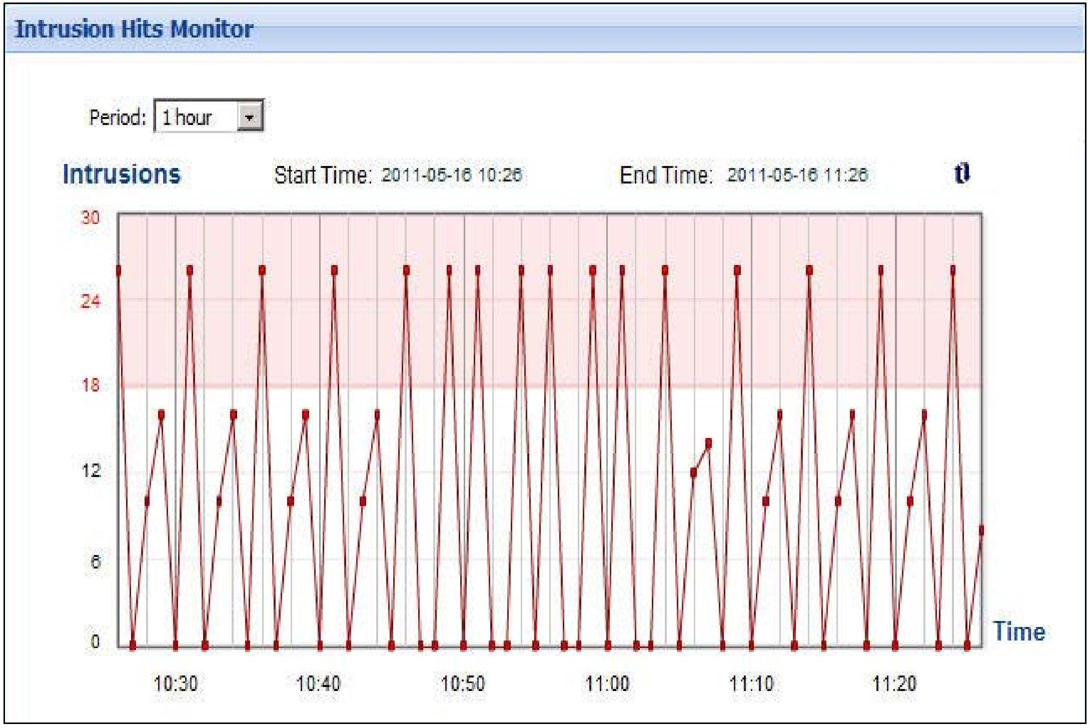
Table 34 Monitor > E-Mail Security > Spam

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

4.21 E-Mail Intrusion Hits Monitor

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

Figure 47 Monitor > E-Mail Security > Intrusion Hits



Each field is described in the following table.

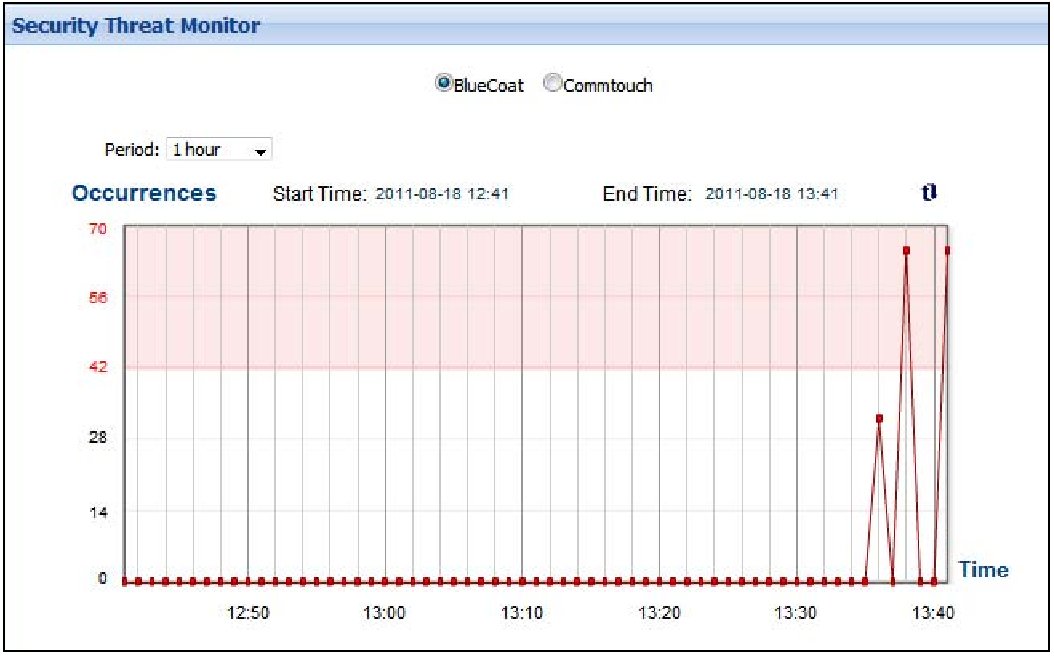
Table 35 Monitor > E-Mail Security > Intrusion Hits

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

4.22 Web Security - Security Threat Monitor

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

Figure 48 Monitor > Web Security > Security Threat



Security Threat Monitor

● BlueCoat ○ Commtouch

Period: 1 hour

Occurrences Start Time: 2011-08-18 12:41 End Time: 2011-08-18 13:41 ↻

Each field is described in the following table.

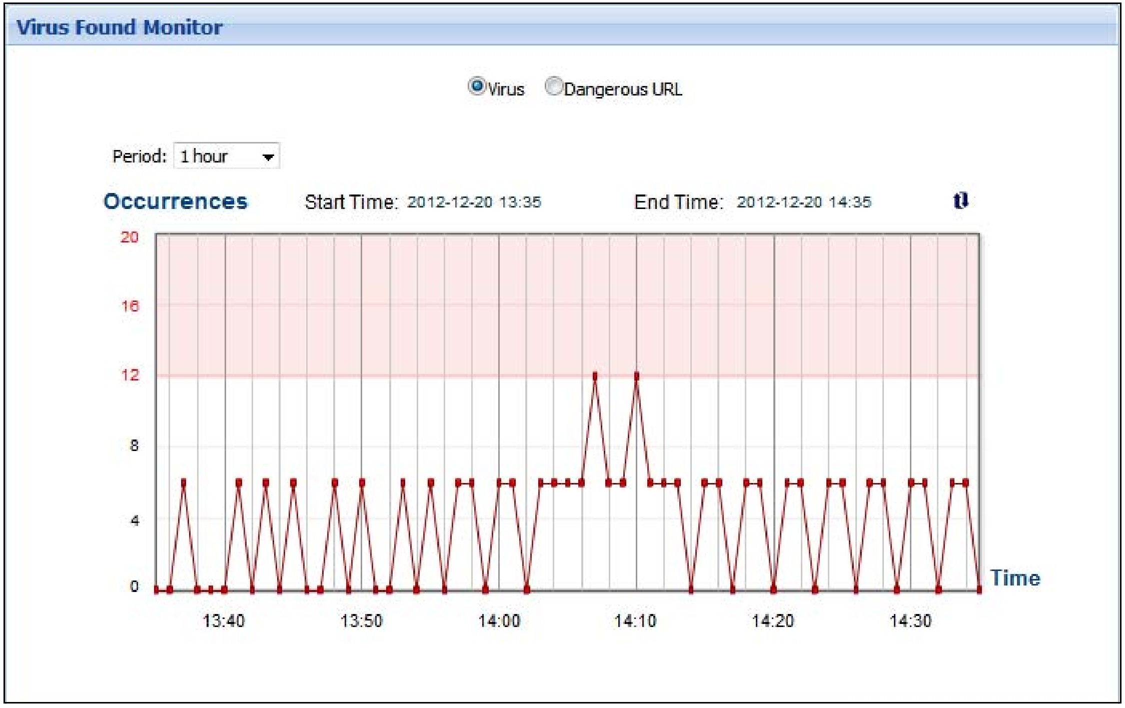
Table 36 Monitor > Web Security > Security Threat

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

4.23 Web Security Virus Found Monitor

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

Figure 49 Monitor > Web Security > Virus Found



Virus Found Monitor

● Virus ○ Dangerous URL

Period: 1 hour

Occurrences Start Time: 2012-12-20 13:35 End Time: 2012-12-20 14:35

Each field is described in the following table.

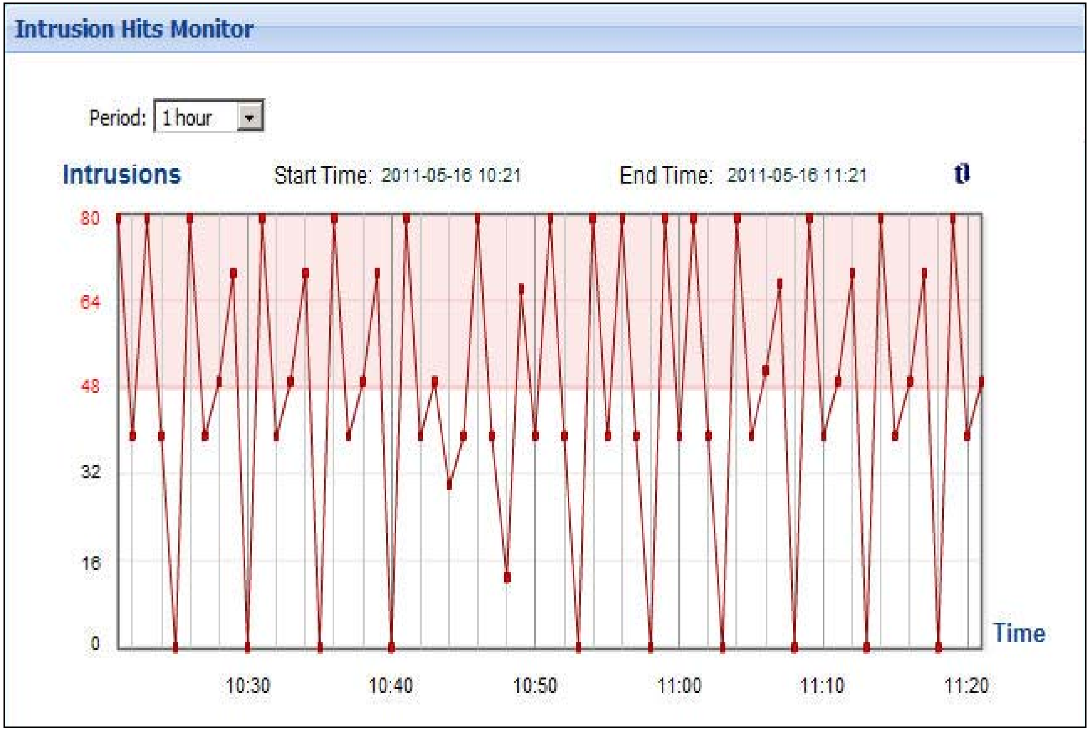
Table 37 Monitor > Web Security > Virus Found

LABEL	DESCRIPTION
Virus	Select this to view the number of virus occurrences prevented by the selected device.
Dangerous URL	A dangerous URL is a web page in which the selected device detected a virus. Select this to view the number of dangerous URLs the device prevented users from accessing.
Period	Select the length of time for which Vantage Report should display statistics.
Start Time	This field displays the date and time of the earliest traffic statistics in the graph. Vantage Report automatically calculates the start time depending on the period you selected in the **Period** field.
End Time	This field displays the date and time of the latest traffic statistics in the graph.
↻	The **Refresh** icon updates the information in the screen.
graph	The graph shows how the status changes over time. Y-axis (vertical): displays the number of virus or virus-infected URL occurrences prevented by the selected device at various times. X-axis (horizontal): displays a date or time depending on the length of time you choose in the **Period** field.

4.24 Web Security Intrusion Hits Monitor

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

Figure 50 Monitor > Web Security > Intrusion Hits



Intrusion Hits Monitor

Period: 1 hour

Intrusions Start Time: 2011-05-16 10:21 End Time: 2011-05-16 11:21

Each field is described in the following table.

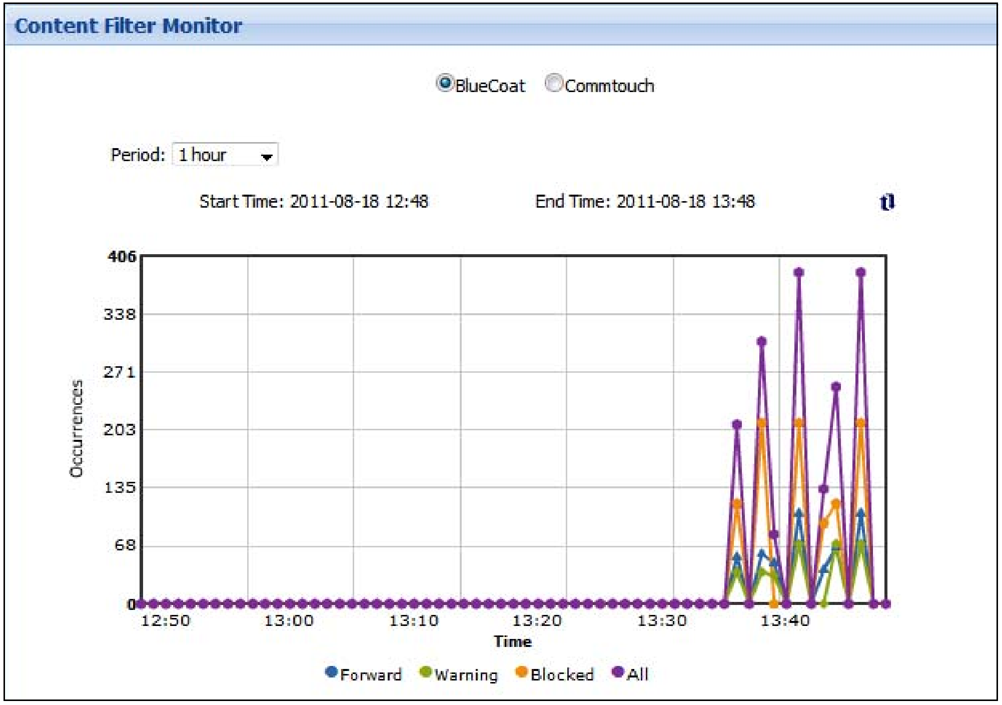
Table 38 Monitor > Web Security > Intrusion Hits

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

4.25 Content Filter Monitor

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

Figure 51 Monitor > Security Policy Enforcement > Content Filter



Content Filter Monitor

● BlueCoat ○ Commtouch

Period: 1 hour

Start Time: 2011-08-18 12:48 End Time: 2011-08-18 13:48

Each field is described in the following table.

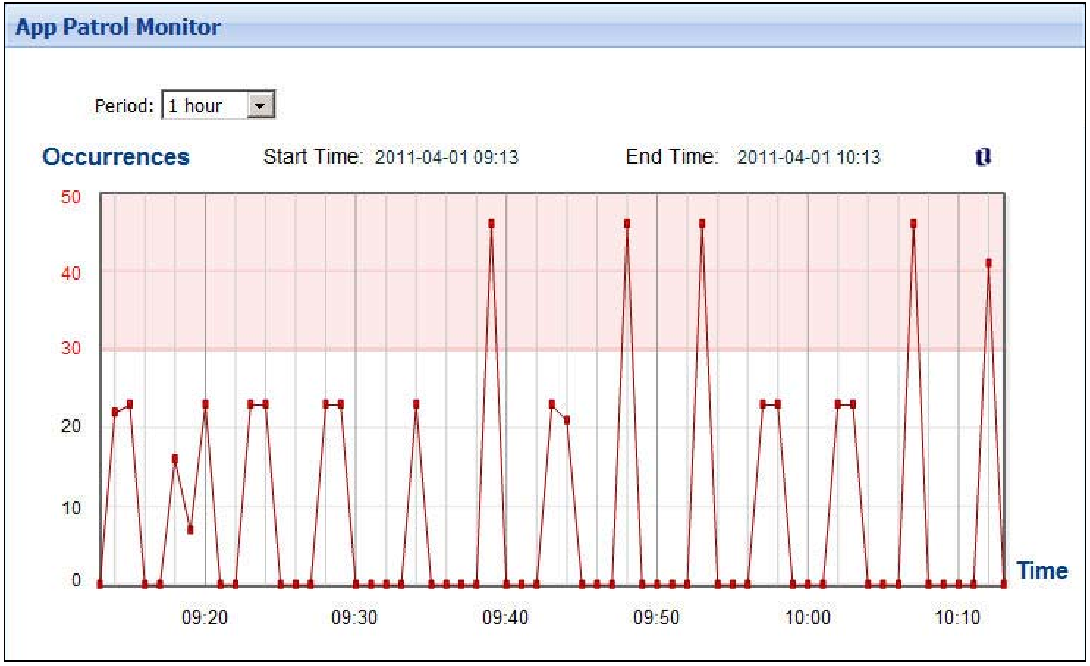
Table 39 Monitor > Security Policy Enforcement > Content Filter

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

4.26 Application Patrol Monitor

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

Figure 52 Monitor > Security Policy Enforcement > App Patrol



App Patrol Monitor

Period: 1 hour

Occurrences Start Time: 2011-04-01 09:13 End Time: 2011-04-01 10:13

Each field is described in the following table.

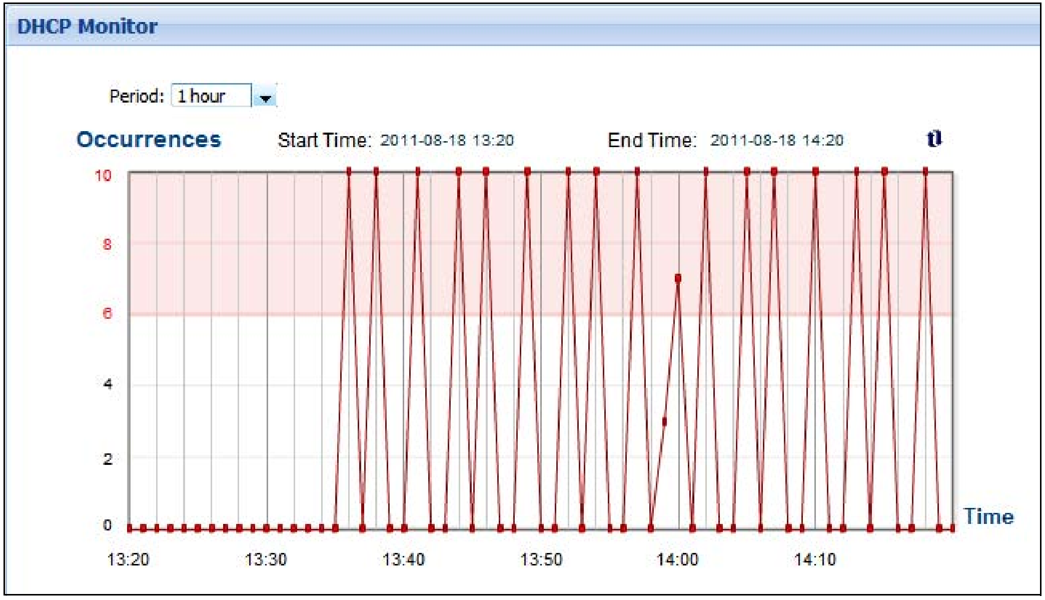
Table 40 Monitor > Security Policy Enforcement > App Patrol

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

4.27 DHCP Leasing Monitor

Click **Monitor** > **Event > DHCP Leasing** to open this screen. Use this screen to monitor the number of DHCP requests over a time period. For a given working day, it should normally appear as many DHCP requests in the morning, and fewer throughout the day. If not (if requests are erratic) it may indicate a virus infection.

Figure 53 Monitor > Event > DHCP Leasing



DHCP Monitor

Period: 1 hour

Start Time: 2011-08-18 13:20

End Time: 2011-08-18 14:20

Each field is described in the following table.

Table 41 Monitor > Event > DHCP Leasing

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

Network Traffic

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

5.1 Bandwidth

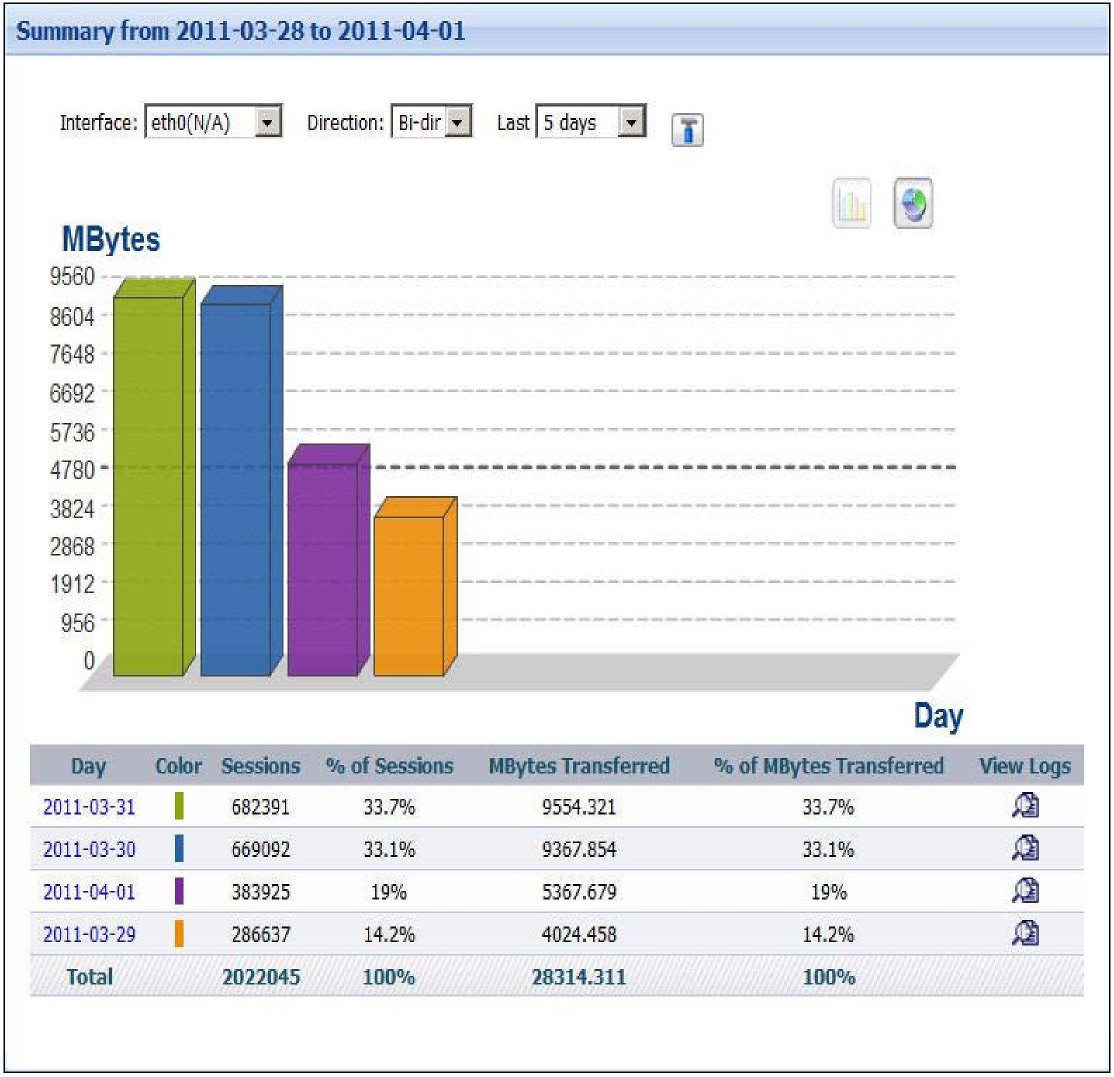
These reports look at how much traffic was handled by ZyXEL devices, who used the most bandwidth in a ZyXEL device, and which protocols were used. You can also look at traffic in various directions.

5.1.1 Bandwidth Summary

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

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

Figure 54 Report > Network Traffic > Bandwidth > Summary



Summary from 2011-03-28 to 2011-04-01

Interface: eth0(N/A) Direction: Bi-dir Last 5 days

Day	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
2011-03-31	🟩	682391	33.7%	9554.321	33.7%	
2011-03-30	🟦	669092	33.1%	9367.854	33.1%	
2011-04-01	🟪	383925	19%	5367.679	19%	
2011-03-29	🟧	286637	14.2%	4024.458	14.2%	
Total		2022045	100%	28314.311	100%	

Each field is described in the following table.

Table 42 Report > Network Traffic > Bandwidth > Summary

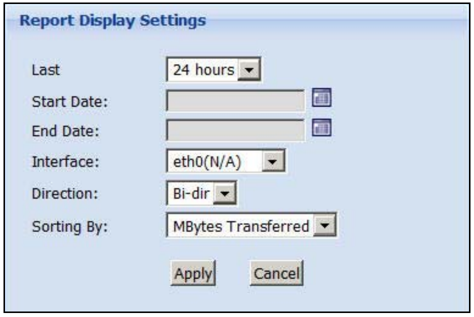
LABEL	DESCRIPTION
Interface	Select the logical interface for which you want to view bandwidth usage. This field is not available with all models.
Direction	Select which kind of traffic, by direction, you want to look at. **Bi-dir** - all traffic, regardless of direction **Rx** - all traffic received on the device **Tx** - all traffic sent from the device For models where no **Interface** field displays, there are options for traffic going to and from specific device interfaces. In addition, the following options may appear. **All** - all traffic, regardless of direction **INBOUND** - all traffic routed from the WAN **OUTBOUND** - all traffic routed to the WAN
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields or **Last** to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Interface: eth0(N/A) Direction: Bi-dir Sorting By: MBytes Transferred Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. You can display the report sorting by the **MBytes Transferred**, **Sessions** or **Date/Time** fields selected from the **Sorting By** field. These fields reset to their default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 42 Report > Network Traffic > Bandwidth > Summary

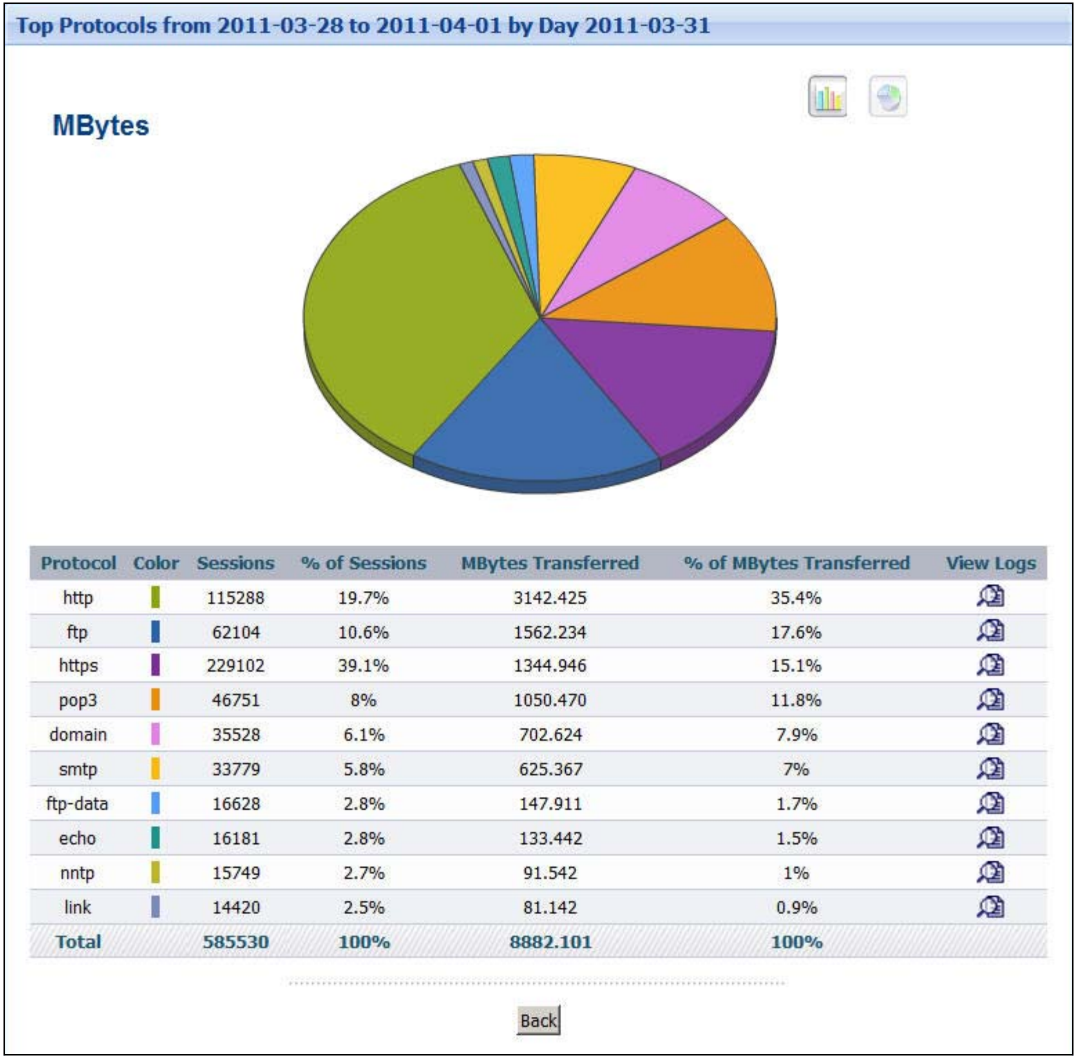
LABEL	DESCRIPTION
Hour (Day)	This field displays the time intervals sorting by the amount of traffic transmitted in the period accordingly. If you select one day of historical information or less (in the **Last** or **Settings** field) and it is in the last seven days (today is day one), the time interval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

5.1.2 Bandwidth Summary Drill-Down

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

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

Figure 55 Report > Network Traffic > Bandwidth > Summary > Drill-Down



Top Protocols from 2011-03-28 to 2011-04-01 by Day 2011-03-31

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
http	🟩	115288	19.7%	3142.425	35.4%	🔍
ftp	🟦	62104	10.6%	1562.234	17.6%	🔍
https	🟪	229102	39.1%	1344.946	15.1%	🔍
pop3	🟧	46751	8%	1050.470	11.8%	🔍
domain	🟪	35528	6.1%	702.624	7.9%	🔍
smtp	🟨	33779	5.8%	625.367	7%	🔍
ftp-data	🟦	16628	2.8%	147.911	1.7%	🔍
echo	🟩	16181	2.8%	133.442	1.5%	🔍
nntp	🟨	15749	2.7%	91.542	1%	🔍
link	🟦	14420	2.5%	81.142	0.9%	🔍
Total		**585530**	**100%**	**8882.101**	**100%**	

Each field is described in the following table.

Table 43 Report > Network Traffic > Bandwidth > Summary > Drill-Down

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

Table 43 Report > Network Traffic > Bandwidth > Summary > Drill-Down

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

5.1.3 Bandwidth Top Protocols

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

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

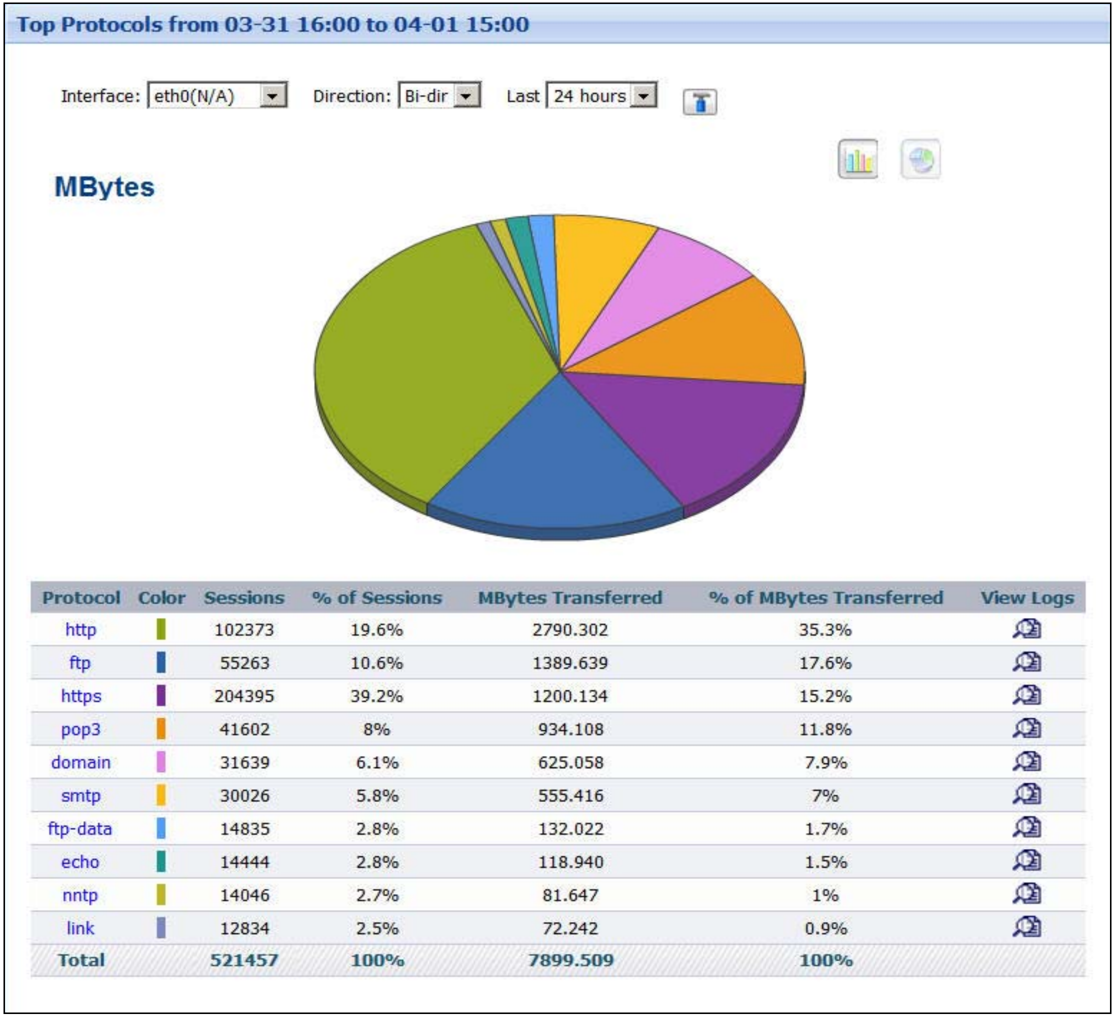


Figure 56 Report > Network Traffic > Bandwidth > Top Protocols

Top Protocols from 03-31 16:00 to 04-01 15:00

Interface: eth0(N/A) Direction: Bi-dir Last 24 hours

MBytes

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
http	🟩	102373	19.6%	2790.302	35.3%	🔍
ftp	🟦	55263	10.6%	1389.639	17.6%	🔍
https	🟪	204395	39.2%	1200.134	15.2%	🔍
pop3	🟧	41602	8%	934.108	11.8%	🔍
domain	🟪	31639	6.1%	625.058	7.9%	🔍
smtp	🟨	30026	5.8%	555.416	7%	🔍
ftp-data	🟦	14835	2.8%	132.022	1.7%	🔍
echo	🟩	14444	2.8%	118.940	1.5%	🔍
nntp	🟨	14046	2.7%	81.647	1%	🔍
link	🟦	12834	2.5%	72.242	0.9%	🔍
Total		521457	100%	7899.509	100%	

Each field is described in the following table.

Table 44 Report > Network Traffic > Bandwidth > Top Protocols

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

Table 44 Report > Network Traffic > Bandwidth > Top Protocols

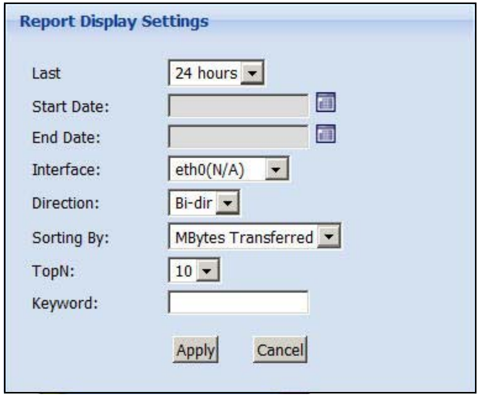
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields or **Last** to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 24 hours Start Date: End Date: Interface: eth0(N/A) Direction: Bi-dir Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Protocol** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the top services generating traffic through the selected device, sorted by the amount of traffic for each one. If the number of services is less than the maximum number of records displayed in this table, every service is displayed. These services may be different than the ones you manage in the **Service Settings** screen. Click on a service to look at the top sources of traffic for the selected service.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service.

Table 44 Report > Network Traffic > Bandwidth > Top Protocols

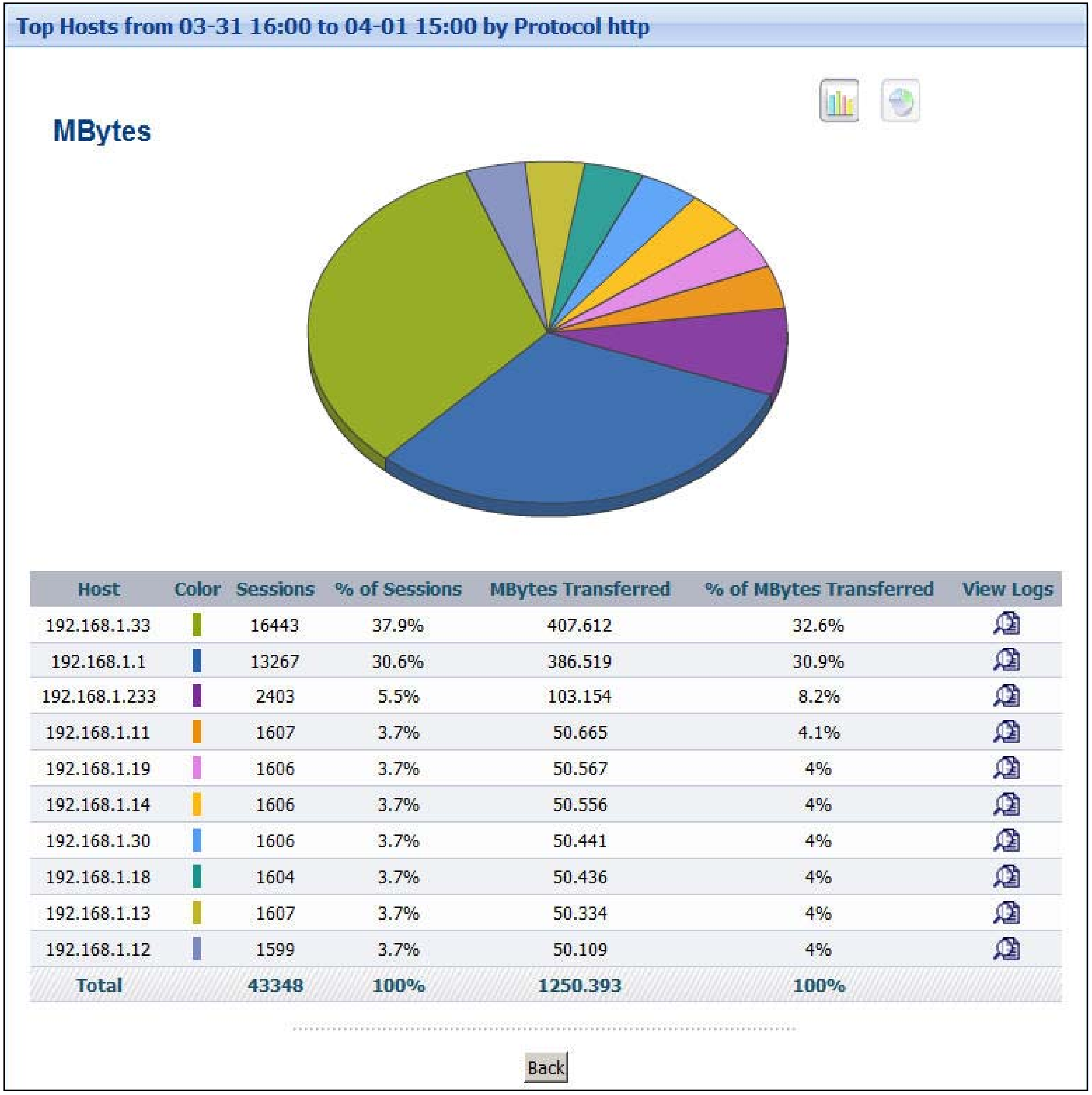
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each service's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each service generated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

5.1.4 Bandwidth Top Protocols Drill-Down

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

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

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



Top Hosts from 03-31 16:00 to 04-01 15:00 by Protocol http

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	🟩	16443	37.9%	407.612	32.6%	🔍
192.168.1.1	🟦	13267	30.6%	386.519	30.9%	🔍
192.168.1.233	🟪	2403	5.5%	103.154	8.2%	🔍
192.168.1.11	🟧	1607	3.7%	50.665	4.1%	🔍
192.168.1.19	🟪	1606	3.7%	50.567	4%	🔍
192.168.1.14	🟨	1606	3.7%	50.556	4%	🔍
192.168.1.30	🟦	1606	3.7%	50.441	4%	🔍
192.168.1.18	🟩	1604	3.7%	50.436	4%	🔍
192.168.1.13	🟨	1607	3.7%	50.334	4%	🔍
192.168.1.12	🟦	1599	3.7%	50.109	4%	🔍
Total		43348	100%	1250.393	100%	

Each field is described in the following table.

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

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

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

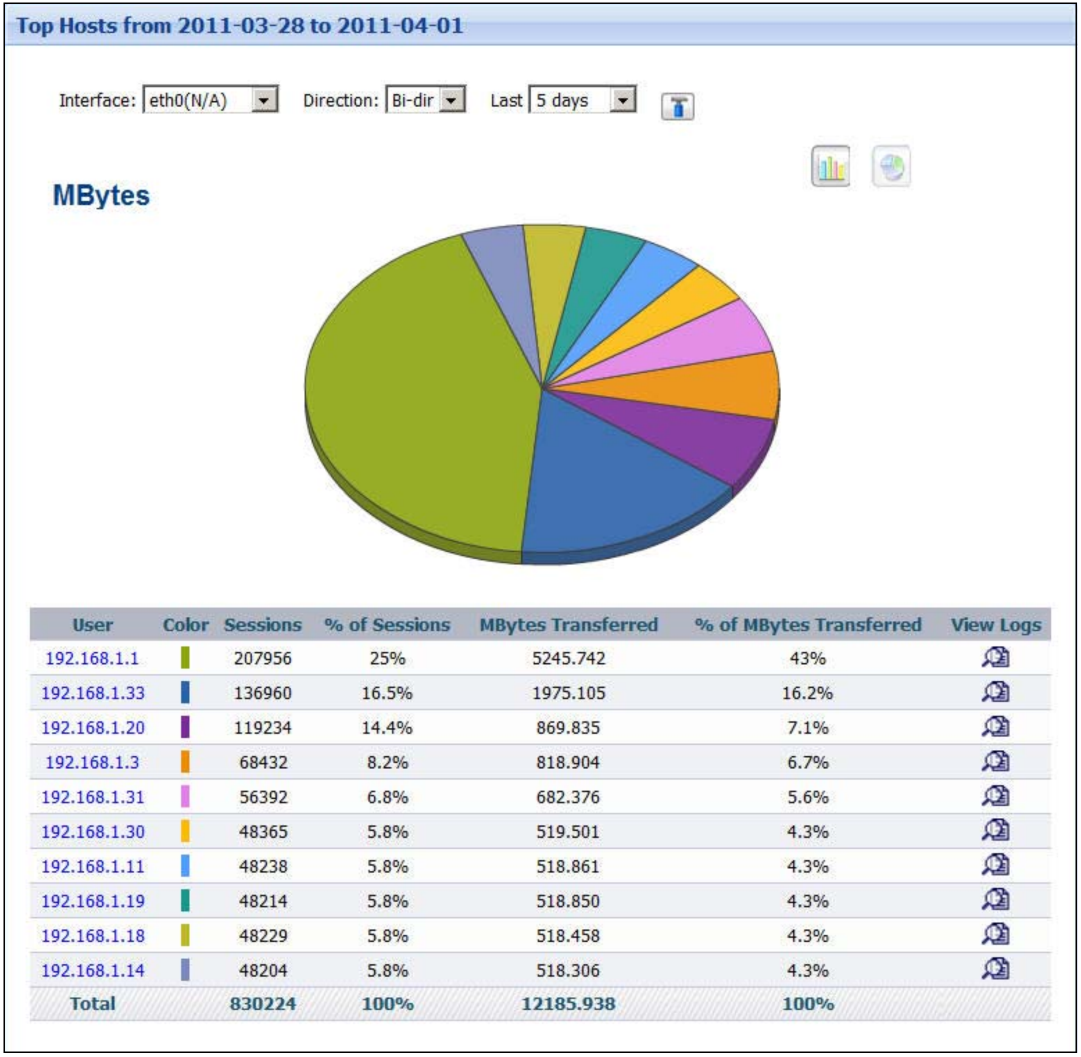
LABEL	DESCRIPTION
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events each source generated using the selected service.
% of Sessions	This field displays what percentage of the selected service's total number of traffic events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

5.1.5 Top Bandwidth Hosts

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

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

Figure 58 Report > Network Traffic > Bandwidth > Top Hosts



Top Hosts from 2011-03-28 to 2011-04-01

Interface: eth0(N/A) Direction: Bi-dir Last 5 days

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.1	■	207956	25%	5245.742	43%	🔍
192.168.1.33	■	136960	16.5%	1975.105	16.2%	🔍
192.168.1.20	■	119234	14.4%	869.835	7.1%	🔍
192.168.1.3	■	68432	8.2%	818.904	6.7%	🔍
192.168.1.31	■	56392	6.8%	682.376	5.6%	🔍
192.168.1.30	■	48365	5.8%	519.501	4.3%	🔍
192.168.1.11	■	48238	5.8%	518.861	4.3%	🔍
192.168.1.19	■	48214	5.8%	518.850	4.3%	🔍
192.168.1.18	■	48229	5.8%	518.458	4.3%	🔍
192.168.1.14	■	48204	5.8%	518.306	4.3%	🔍
Total		830224	100%	12185.938	100%	

Each field is described in the following table.

Table 46 Report > Network Traffic > Bandwidth > Top Hosts

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

Table 46 Report > Network Traffic > Bandwidth > Top Hosts

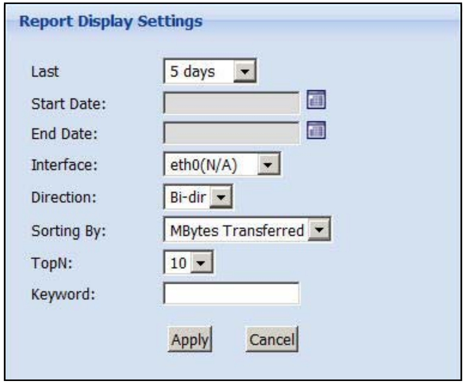
LABEL	DESCRIPTION
Settings	Use these fields or **Last** to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 5 days Start Date: End Date: Interface: eth0(N/A) Direction: Bi-dir Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top services by amount of traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each source generated through the selected device.
% of MBytes Transferred	This field displays what percentage each record's amount of traffic makes out of the total amount of traffic that matches the settings you displayed in this report.

Table 46 Report > Network Traffic > Bandwidth > Top Hosts

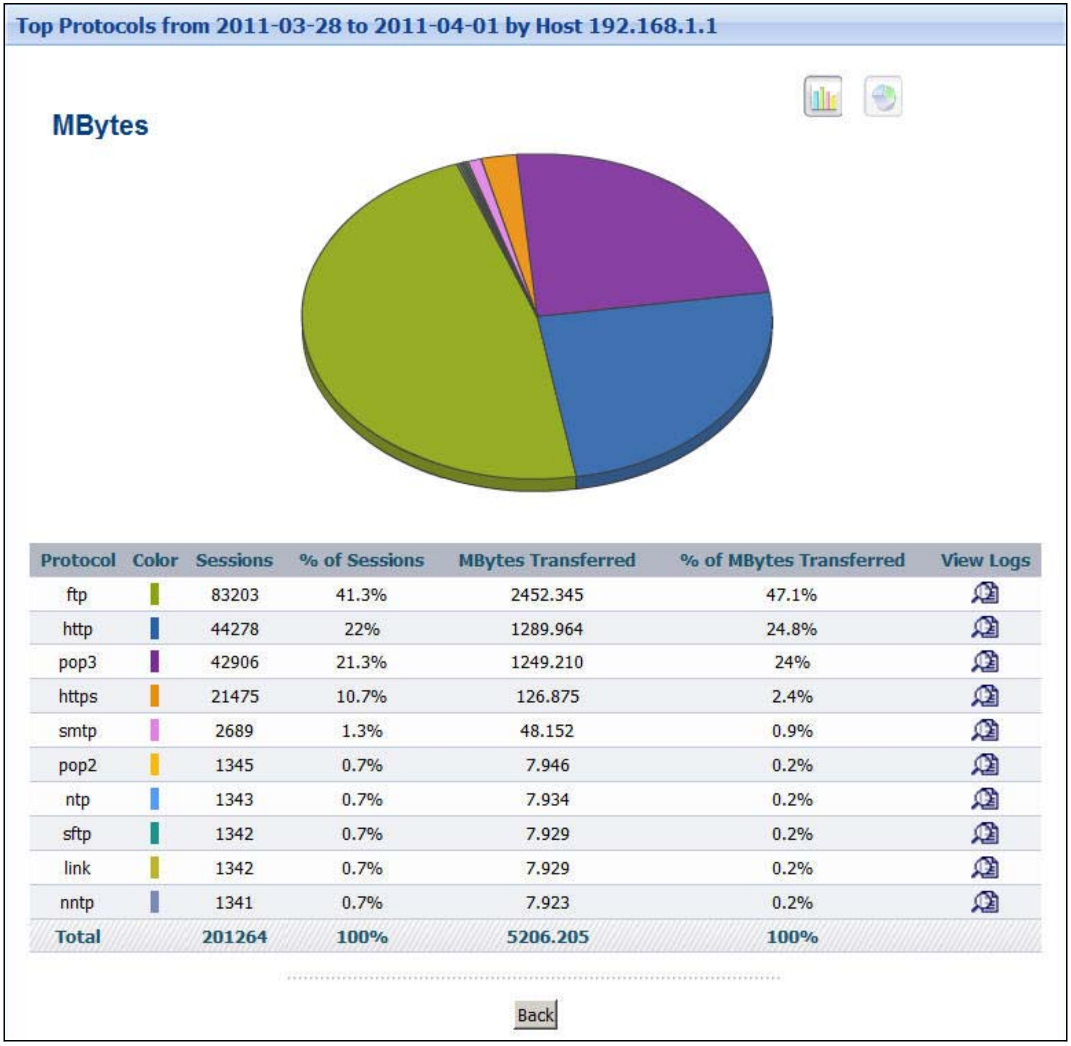
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

5.1.6 Top Bandwidth Hosts Drill-Down

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

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

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



Top Protocols from 2011-03-28 to 2011-04-01 by Host 192.168.1.1

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
ftp	■	83203	41.3%	2452.345	47.1%	🔍
http	■	44278	22%	1289.964	24.8%	🔍
pop3	■	42906	21.3%	1249.210	24%	🔍
https	■	21475	10.7%	126.875	2.4%	🔍
smtp	■	2689	1.3%	48.152	0.9%	🔍
pop2	■	1345	0.7%	7.946	0.2%	🔍
ntp	■	1343	0.7%	7.934	0.2%	🔍
sftp	■	1342	0.7%	7.929	0.2%	🔍
link	■	1342	0.7%	7.929	0.2%	🔍
nntp	■	1341	0.7%	7.923	0.2%	🔍
Total		201264	100%	5206.205	100%	

Each field is described in the following table.

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

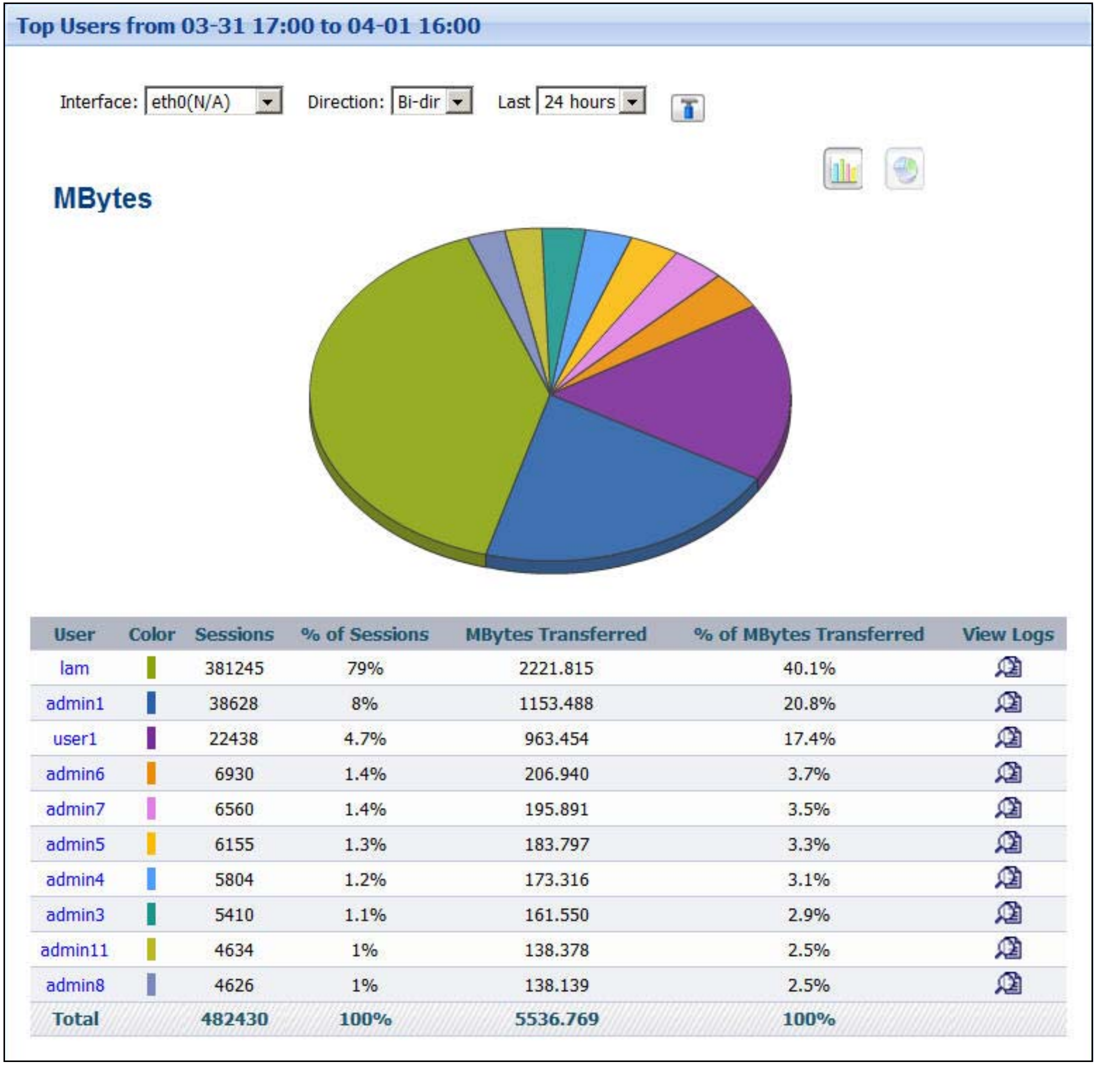
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.1.7 Top Bandwidth Users

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

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

Figure 60 Report > Network Traffic > Bandwidth > Top Users



Top Users from 03-31 17:00 to 04-01 16:00

Interface: eth0(N/A) Direction: Bi-dir Last 24 hours

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
lam	🟩	381245	79%	2221.815	40.1%	🔍
admin1	🟦	38628	8%	1153.488	20.8%	🔍
user1	🟪	22438	4.7%	963.454	17.4%	🔍
admin6	🟧	6930	1.4%	206.940	3.7%	🔍
admin7	🟪	6560	1.4%	195.891	3.5%	🔍
admin5	🟨	6155	1.3%	183.797	3.3%	🔍
admin4	🟦	5804	1.2%	173.316	3.1%	🔍
admin3	🟩	5410	1.1%	161.550	2.9%	🔍
admin11	🟨	4634	1%	138.378	2.5%	🔍
admin8	🟦	4626	1%	138.139	2.5%	🔍
Total		482430	100%	5536.769	100%	

Each field is described in the following table.

Table 48 Report > Network Traffic > Bandwidth > Top Users

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

Table 48 Report > Network Traffic > Bandwidth > Top Users

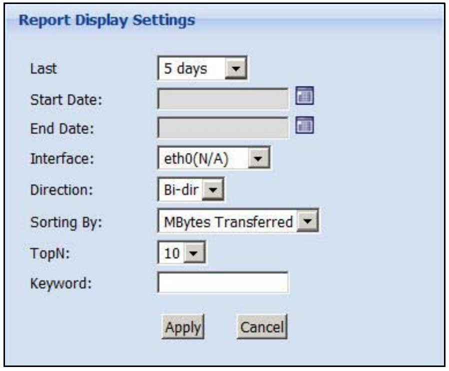
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 5 days Start Date: End Date: Interface: eth0(N/A) Direction: Bi-dir Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users with the most traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click a user name to look at the top services by amount of traffic for the selected user.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.

Table 48 Report > Network Traffic > Bandwidth > Top Users

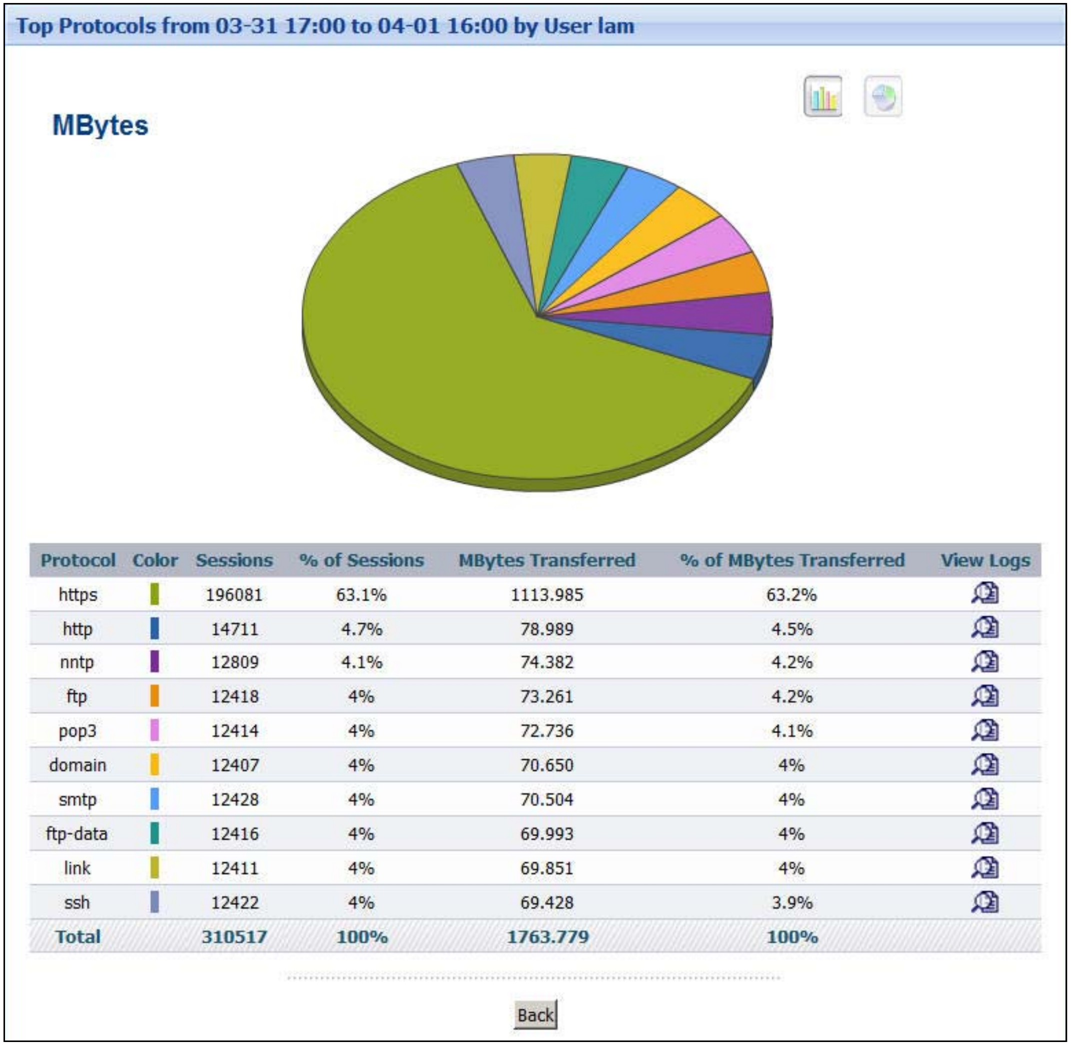
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) each user generated through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

5.1.8 Top Bandwidth Users Drill-Down

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

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

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



Top Protocols from 03-31 17:00 to 04-01 16:00 by User lam

MBytes

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
https	🟩	196081	63.1%	1113.985	63.2%	🔍
http	🟦	14711	4.7%	78.989	4.5%	🔍
nntp	🟪	12809	4.1%	74.382	4.2%	🔍
ftp	🟧	12418	4%	73.261	4.2%	🔍
pop3	🟪	12414	4%	72.736	4.1%	🔍
domain	🟨	12407	4%	70.650	4%	🔍
smtp	🟦	12428	4%	70.504	4%	🔍
ftp-data	🟩	12416	4%	69.993	4%	🔍
link	🟨	12411	4%	69.851	4%	🔍
ssh	🟦	12422	4%	69.428	3.9%	🔍
Total		310517	100%	1763.779	100%	

Each field is described in the following table.

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

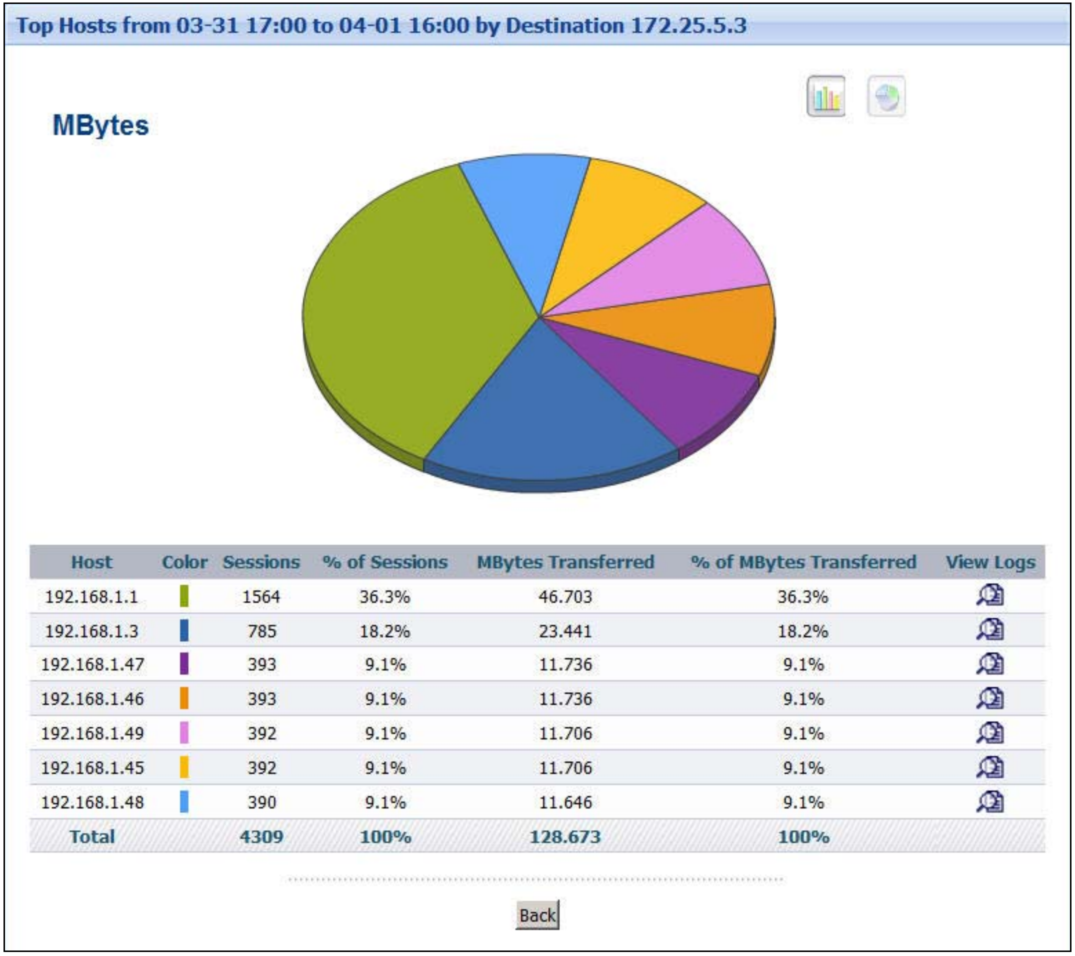
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.1.9 Top Bandwidth Destinations

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

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

Figure 62 Report > Network Traffic > Bandwidth > Top Destinations



Top Hosts from 03-31 17:00 to 04-01 16:00 by Destination 172.25.5.3

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.1	■	1564	36.3%	46.703	36.3%	
192.168.1.3	■	785	18.2%	23.441	18.2%	
192.168.1.47	■	393	9.1%	11.736	9.1%	
192.168.1.46	■	393	9.1%	11.736	9.1%	
192.168.1.49	■	392	9.1%	11.706	9.1%	
192.168.1.45	■	392	9.1%	11.706	9.1%	
192.168.1.48	■	390	9.1%	11.646	9.1%	
Total		4309	100%	128.673	100%	

Each field is described in the following table.

Table 50 Report > Network Traffic > Bandwidth > Top Destinations

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

Table 50 Report > Network Traffic > Bandwidth > Top Destinations

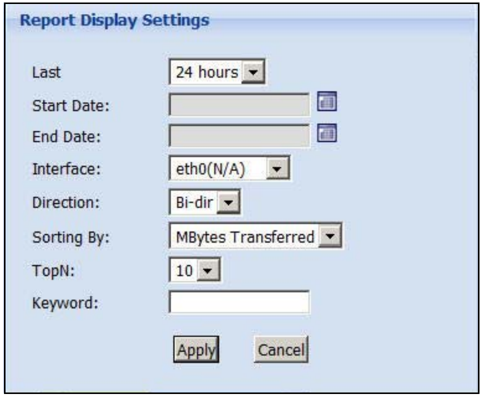
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Interface: eth0(N/A) Direction: Bi-dir Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Interface** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the destinations to which the selected device sent the most traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a destination to look at the top sources of web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.

Table 50 Report > Network Traffic > Bandwidth > Top Destinations

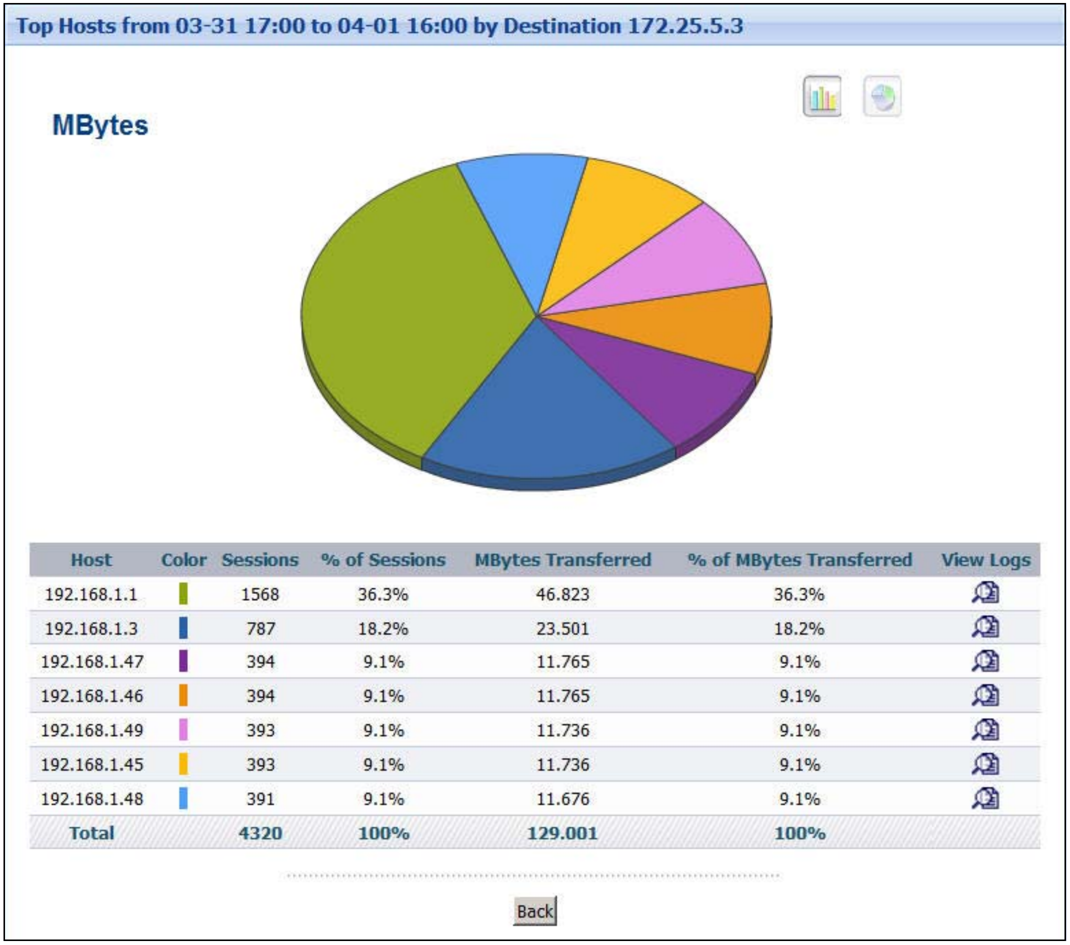
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes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

5.1.10 Top Bandwidth Destinations Drill-Down

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

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

Figure 63 Report > Network Traffic > Bandwidth > Top Destinations > Drill-Down



Top Hosts from 03-31 17:00 to 04-01 16:00 by Destination 172.25.5.3

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.1	🟩	1568	36.3%	46.823	36.3%	🔍
192.168.1.3	🟦	787	18.2%	23.501	18.2%	🔍
192.168.1.47	🟪	394	9.1%	11.765	9.1%	🔍
192.168.1.46	🟧	394	9.1%	11.765	9.1%	🔍
192.168.1.49	■	393	9.1%	11.736	9.1%	🔍
192.168.1.45	🟨	393	9.1%	11.736	9.1%	🔍
192.168.1.48	🟦	391	9.1%	11.676	9.1%	🔍
Total		4320	100%	129.001	100%	

Each field is described in the following table.

Table 51 Report > Network Traffic > Bandwidth > Top Destinations > Drill-Down

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

5.2 Web Traffic

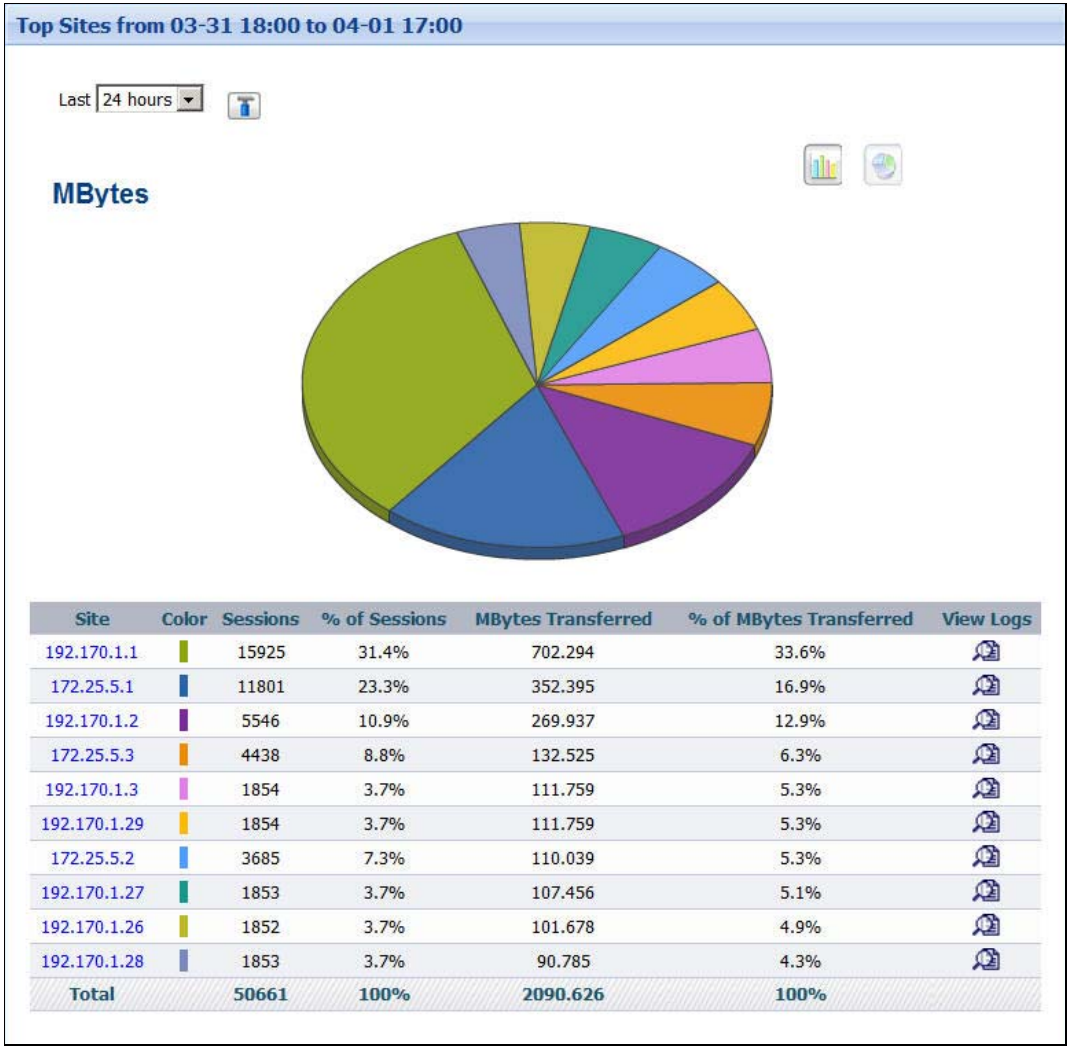
These reports look at the top destinations and sources of web traffic.

5.2.1 Top Web Sites

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

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

Figure 64 Report > Network Traffic > WEB > Top Sites



Top Sites from 03-31 18:00 to 04-01 17:00

Last 24 hours

MBytes

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.1	■	15925	31.4%	702.294	33.6%	🔍
172.25.5.1	■	11801	23.3%	352.395	16.9%	🔍
192.170.1.2	■	5546	10.9%	269.937	12.9%	🔍
172.25.5.3	■	4438	8.8%	132.525	6.3%	🔍
192.170.1.3	■	1854	3.7%	111.759	5.3%	🔍
192.170.1.29	■	1854	3.7%	111.759	5.3%	🔍
172.25.5.2	■	3685	7.3%	110.039	5.3%	🔍
192.170.1.27	■	1853	3.7%	107.456	5.1%	🔍
192.170.1.26	■	1852	3.7%	101.678	4.9%	🔍
192.170.1.28	■	1853	3.7%	90.785	4.3%	🔍
Total		50661	100%	2090.626	100%	

Each field is described in the following table.

Table 52 Report > Network Traffic > WEB > Top Sites

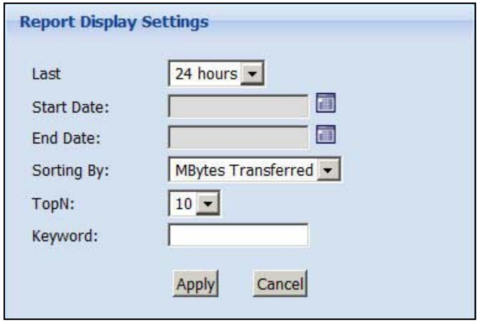
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top sources of web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.

Table 52 Report > Network Traffic > WEB > Top Sites

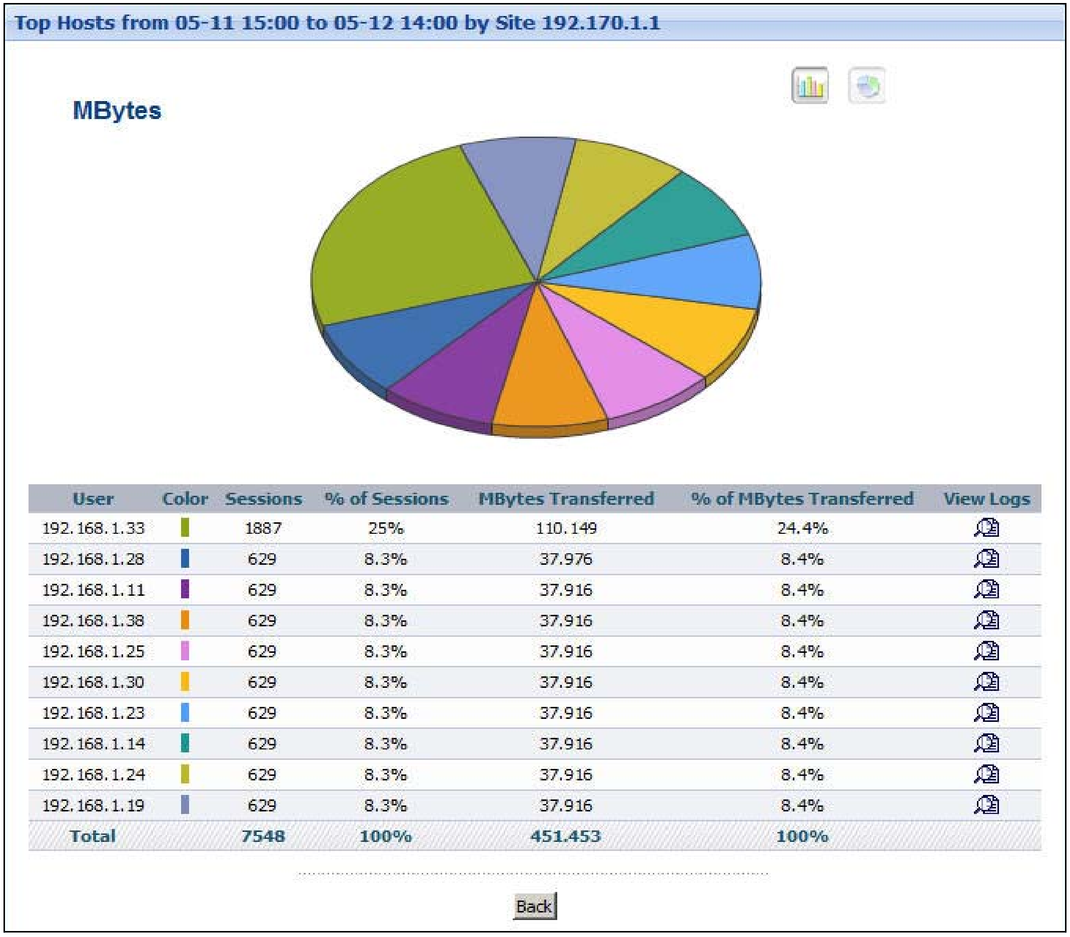
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled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

5.2.2 Top Web Sites Drill-Down

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

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

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



Top Hosts from 05-11 15:00 to 05-12 14:00 by Site 192.170.1.1

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	■	1887	25%	110.149	24.4%	🔍
192.168.1.28	■	629	8.3%	37.976	8.4%	🔍
192.168.1.11	■	629	8.3%	37.916	8.4%	🔍
192.168.1.38	■	629	8.3%	37.916	8.4%	🔍
192.168.1.25	■	629	8.3%	37.916	8.4%	🔍
192.168.1.30	■	629	8.3%	37.916	8.4%	🔍
192.168.1.23	■	629	8.3%	37.916	8.4%	🔍
192.168.1.14	■	629	8.3%	37.916	8.4%	🔍
192.168.1.24	■	629	8.3%	37.916	8.4%	🔍
192.168.1.19	■	629	8.3%	37.916	8.4%	🔍
Total		7548	100%	451.453	100%	

Each field is described in the following table.

Table 53 Report > Traffic > WEB > Top Sites > Drill-Down

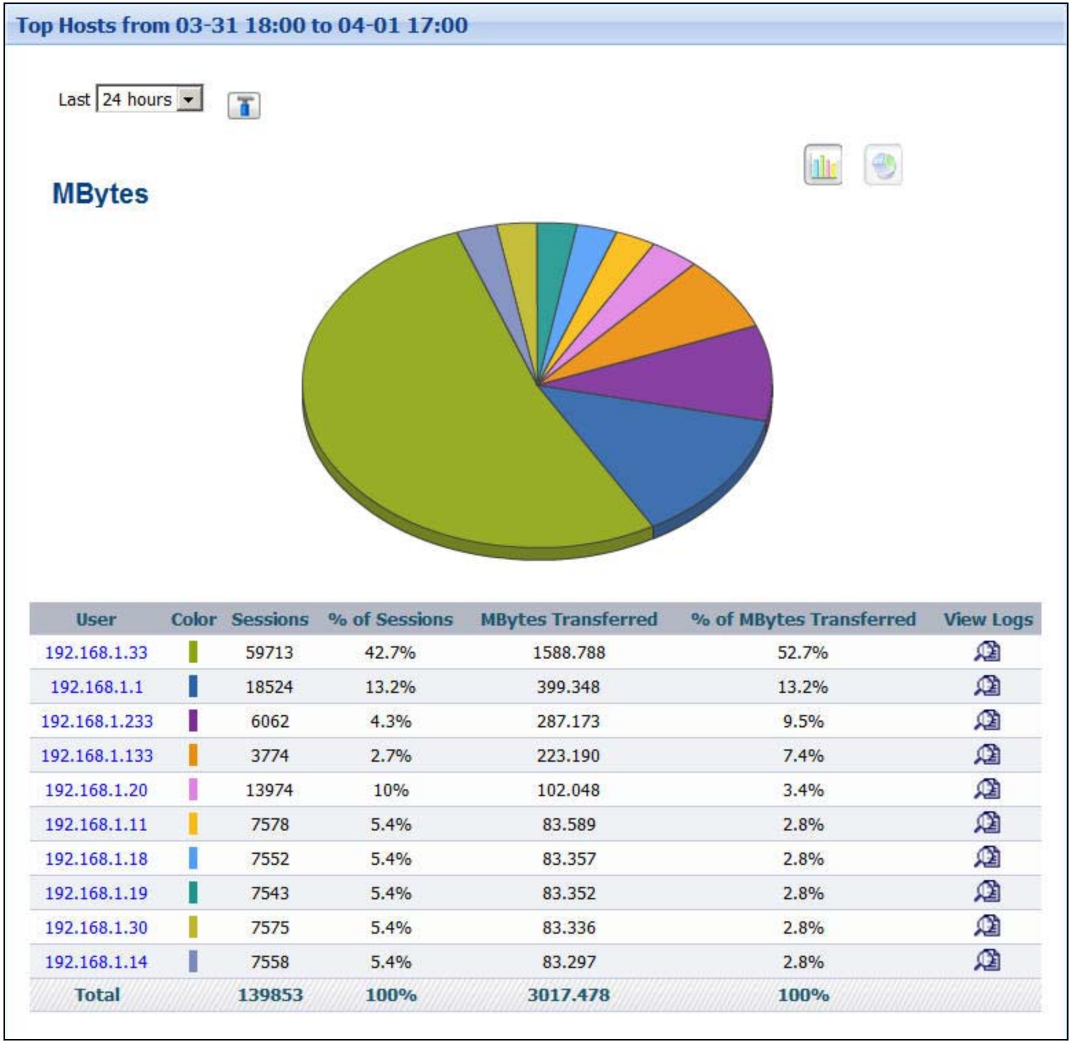
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.2.3 Top Web Hosts

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

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

Figure 66 Report > Network Traffic > WEB > Top Hosts



Top Hosts from 03-31 18:00 to 04-01 17:00

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	■	59713	42.7%	1588.788	52.7%	🔍
192.168.1.1	■	18524	13.2%	399.348	13.2%	🔍
192.168.1.233	■	6062	4.3%	287.173	9.5%	🔍
192.168.1.133	■	3774	2.7%	223.190	7.4%	🔍
192.168.1.20	■	13974	10%	102.048	3.4%	🔍
192.168.1.11	■	7578	5.4%	83.589	2.8%	🔍
192.168.1.18	■	7552	5.4%	83.357	2.8%	🔍
192.168.1.19	■	7543	5.4%	83.352	2.8%	🔍
192.168.1.30	■	7575	5.4%	83.336	2.8%	🔍
192.168.1.14	■	7558	5.4%	83.297	2.8%	🔍
Total		139853	100%	3017.478	100%	

Each field is described in the following table.

Table 54 Report > Network Traffic > WEB > Top Hosts

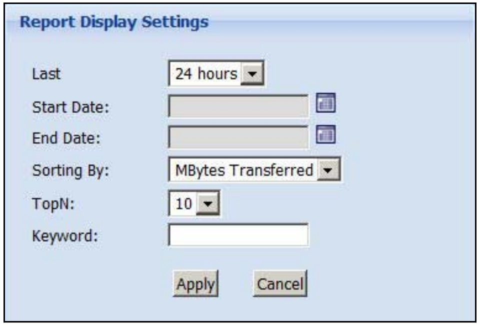
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of web traffic events for each source.

Table 54 Report > Network Traffic > WEB > Top Hosts

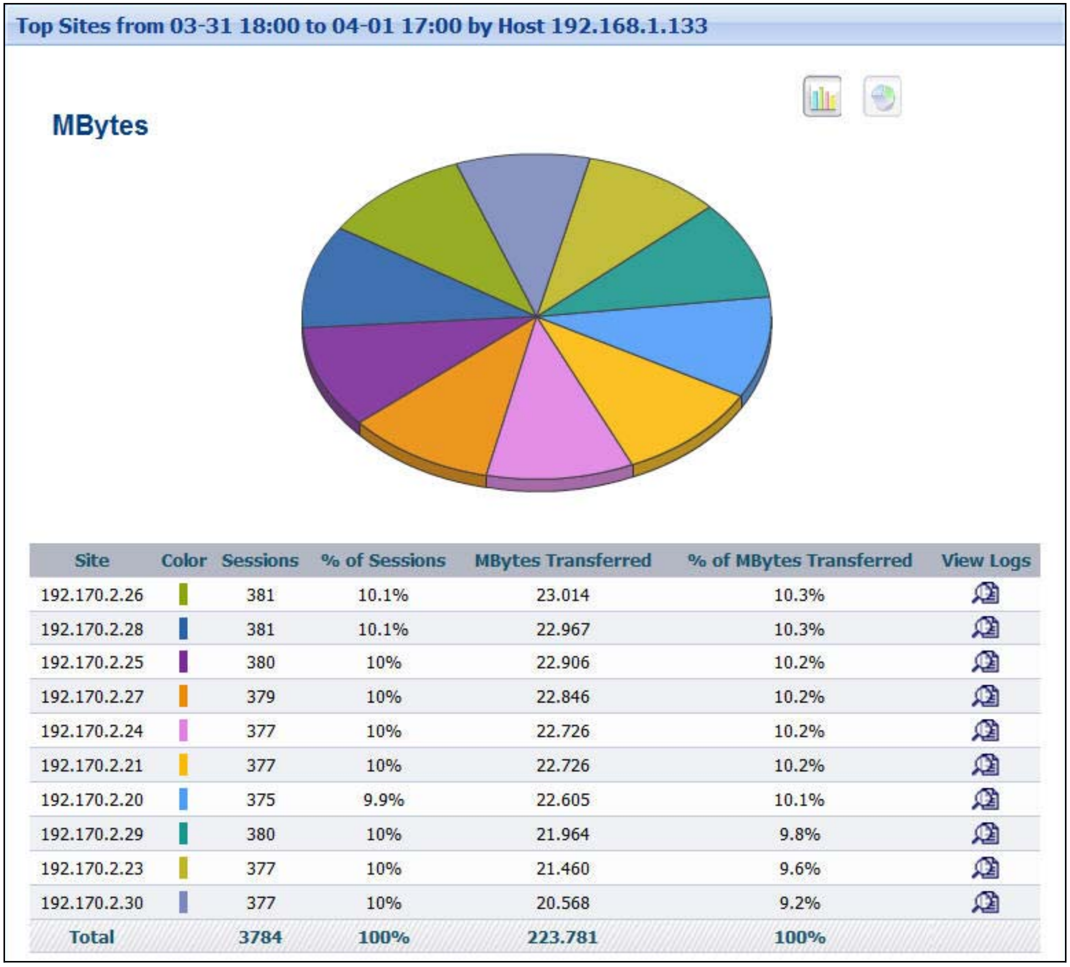
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of web traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled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

5.2.4 Top Web Hosts Drill-Down

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

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

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



Top Sites from 03-31 18:00 to 04-01 17:00 by Host 192.168.1.133

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.2.26	■	381	10.1%	23.014	10.3%	🔍
192.170.2.28	■	381	10.1%	22.967	10.3%	🔍
192.170.2.25	■	380	10%	22.906	10.2%	🔍
192.170.2.27	■	379	10%	22.846	10.2%	🔍
192.170.2.24	■	377	10%	22.726	10.2%	🔍
192.170.2.21	■	377	10%	22.726	10.2%	🔍
192.170.2.20	■	375	9.9%	22.605	10.1%	🔍
192.170.2.29	■	380	10%	21.964	9.8%	🔍
192.170.2.23	■	377	10%	21.460	9.6%	🔍
192.170.2.30	■	377	10%	20.568	9.2%	🔍
Total		3784	100%	223.781	100%	

Each field is described in the following table.

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

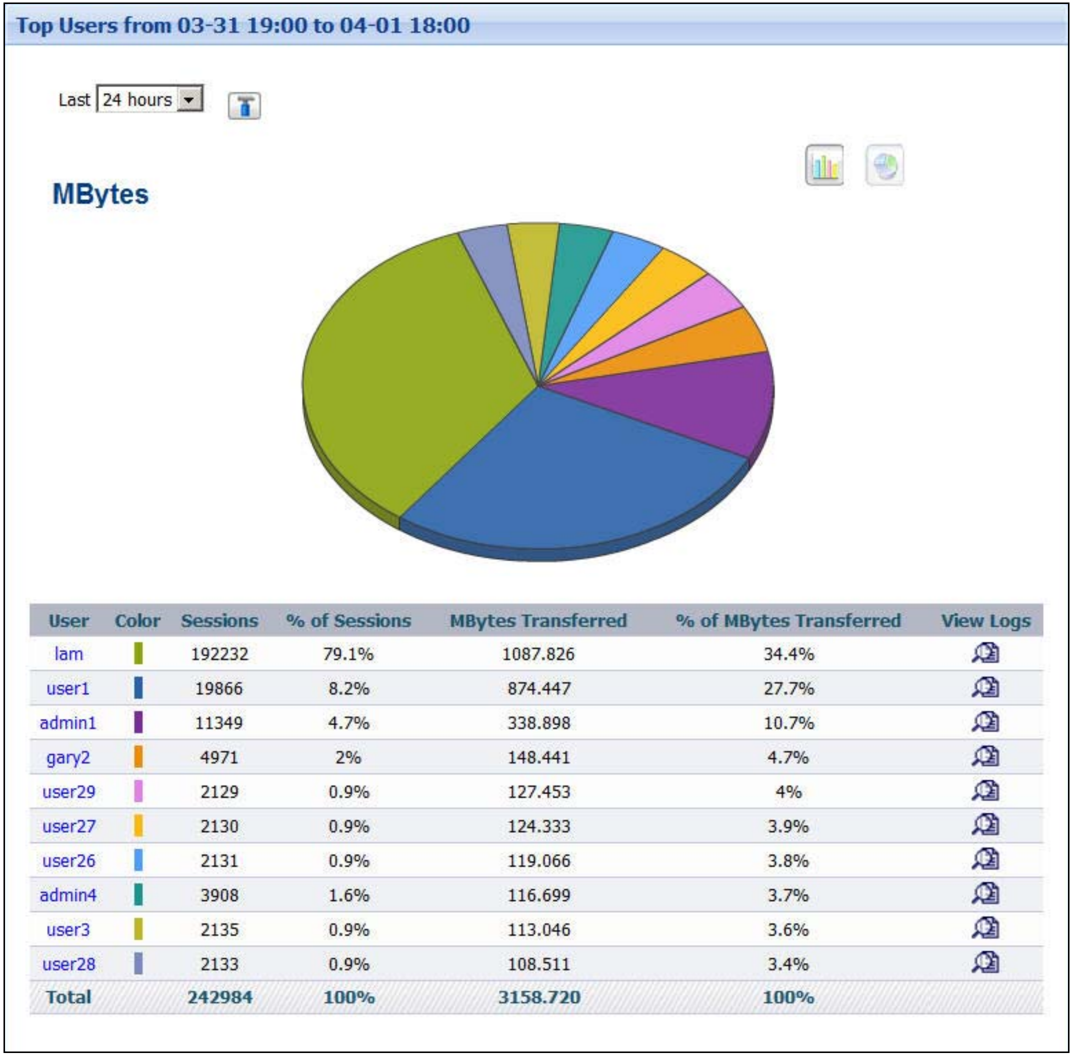
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.2.5 Top Web Users

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

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

Figure 68 Report > Network Traffic > WEB > Top Users



Top Users from 03-31 19:00 to 04-01 18:00

Last 24 hours

MBytes

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
lam	▮	192232	79.1%	1087.826	34.4%	🔍
user1	▮	19866	8.2%	874.447	27.7%	🔍
admin1	▮	11349	4.7%	338.898	10.7%	🔍
gary2	▮	4971	2%	148.441	4.7%	🔍
user29	▮	2129	0.9%	127.453	4%	🔍
user27	▮	2130	0.9%	124.333	3.9%	🔍
user26	▮	2131	0.9%	119.066	3.8%	🔍
admin4	▮	3908	1.6%	116.699	3.7%	🔍
user3	▮	2135	0.9%	113.046	3.6%	🔍
user28	▮	2133	0.9%	108.511	3.4%	🔍
Total		242984	100%	3158.720	100%	

Each field is described in the following table.

Table 56 Report > Network Traffic > WEB > Top Users

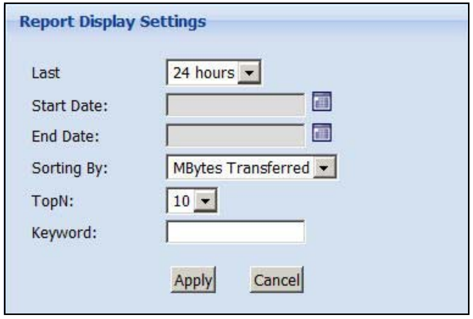
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that send the most web traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 56 Report > Network Traffic > WEB > Top Users

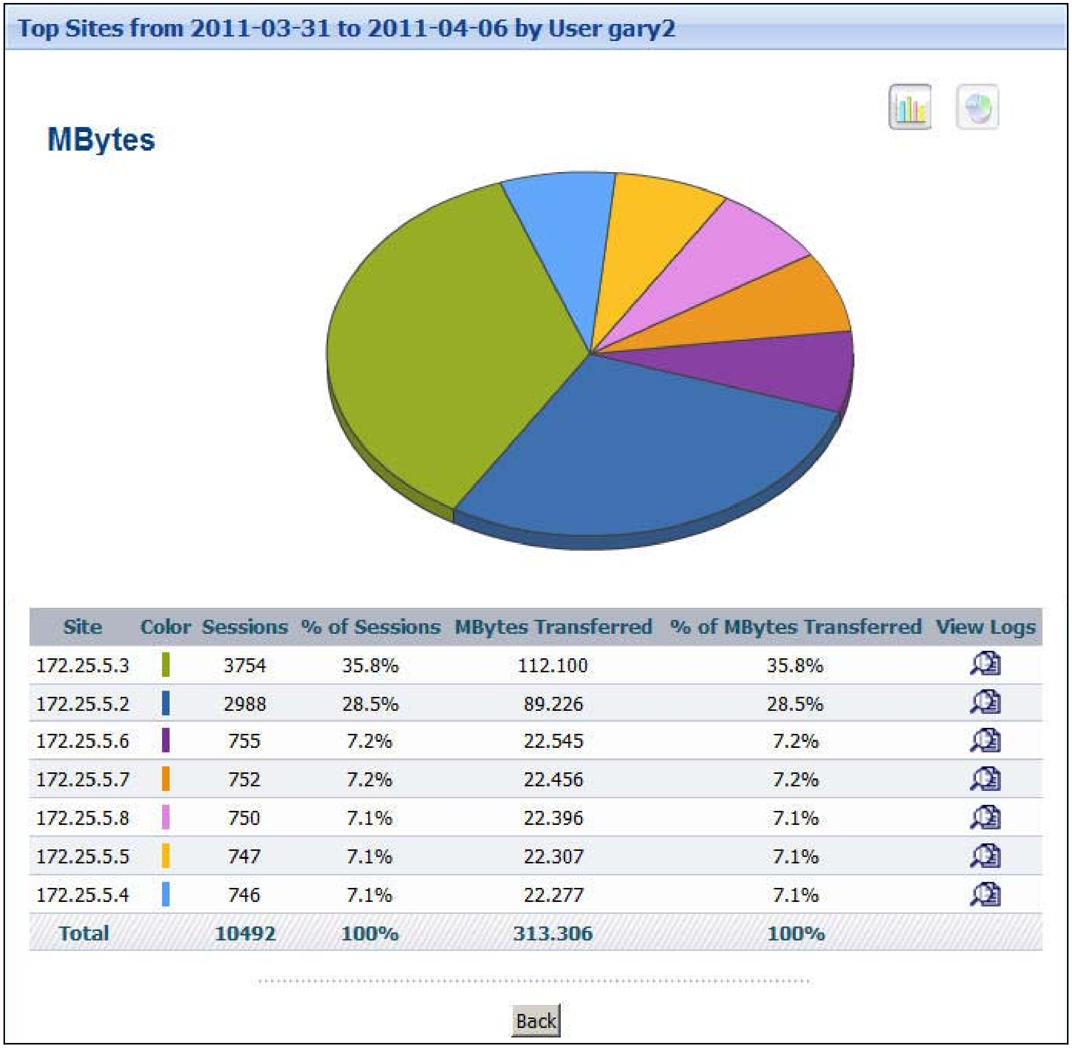
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage each user’s traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click 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 **Report > Network Traffic > WEB** > **Top Users** to open this screen.

Figure 69 Report > Network Traffic > WEB > Top Users > Drill-Down



Top Sites from 2011-03-31 to 2011-04-06 by User gary2

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.3	▮	3754	35.8%	112.100	35.8%	🔍
172.25.5.2	▮	2988	28.5%	89.226	28.5%	🔍
172.25.5.6	▮	755	7.2%	22.545	7.2%	🔍
172.25.5.7	▮	752	7.2%	22.456	7.2%	🔍
172.25.5.8	▮	750	7.1%	22.396	7.1%	🔍
172.25.5.5	▮	747	7.1%	22.307	7.1%	🔍
172.25.5.4	▮	746	7.1%	22.277	7.1%	🔍
Total		10492	100%	313.306	100%	

Each field is described in the following table.

Table 57 Report > Network Traffic > WEB > Top Users > Drill-Down

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

5.3 FTP Traffic

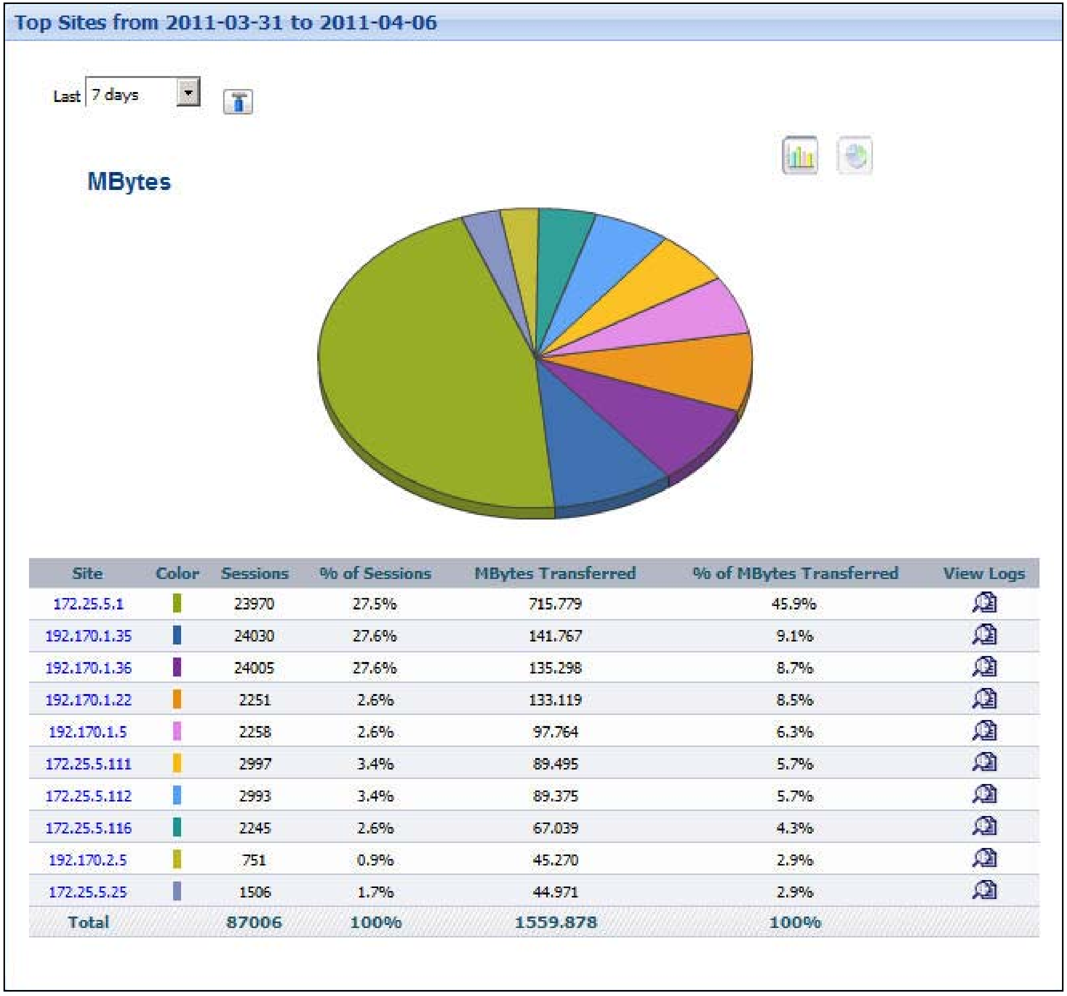
These reports look at the top destinations and sources of FTP traffic.

5.3.1 Top FTP Sites

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

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

Figure 70 Report > Network Traffic > FTP > Top Sites



Top Sites from 2011-03-31 to 2011-04-06

Last 7 days

MBytes

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	🟩	23970	27.5%	715.779	45.9%	
192.170.1.35	🟦	24030	27.6%	141.767	9.1%	
192.170.1.36	🟪	24005	27.6%	135.298	8.7%	
192.170.1.22	🟧	2251	2.6%	133.119	8.5%	
192.170.1.5	🟪	2258	2.6%	97.764	6.3%	
172.25.5.111	🟨	2997	3.4%	89.495	5.7%	
172.25.5.112	🟦	2993	3.4%	89.375	5.7%	
172.25.5.116	🟩	2245	2.6%	67.039	4.3%	
192.170.2.5	🟨	751	0.9%	45.270	2.9%	
172.25.5.25	🟦	1506	1.7%	44.971	2.9%	
Total		87006	100%	1559.878	100%	

Each field is described in the following table.

Table 58 Report > Network Traffic > FTP > Top Sites

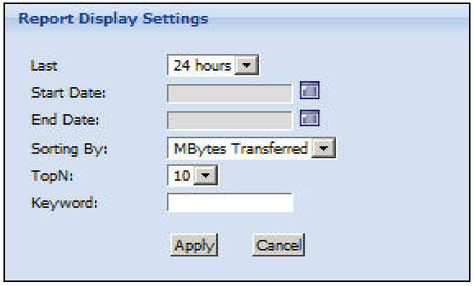
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a destination to look at the top sources of FTP traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 58 Report > Network Traffic > FTP > Top Sites

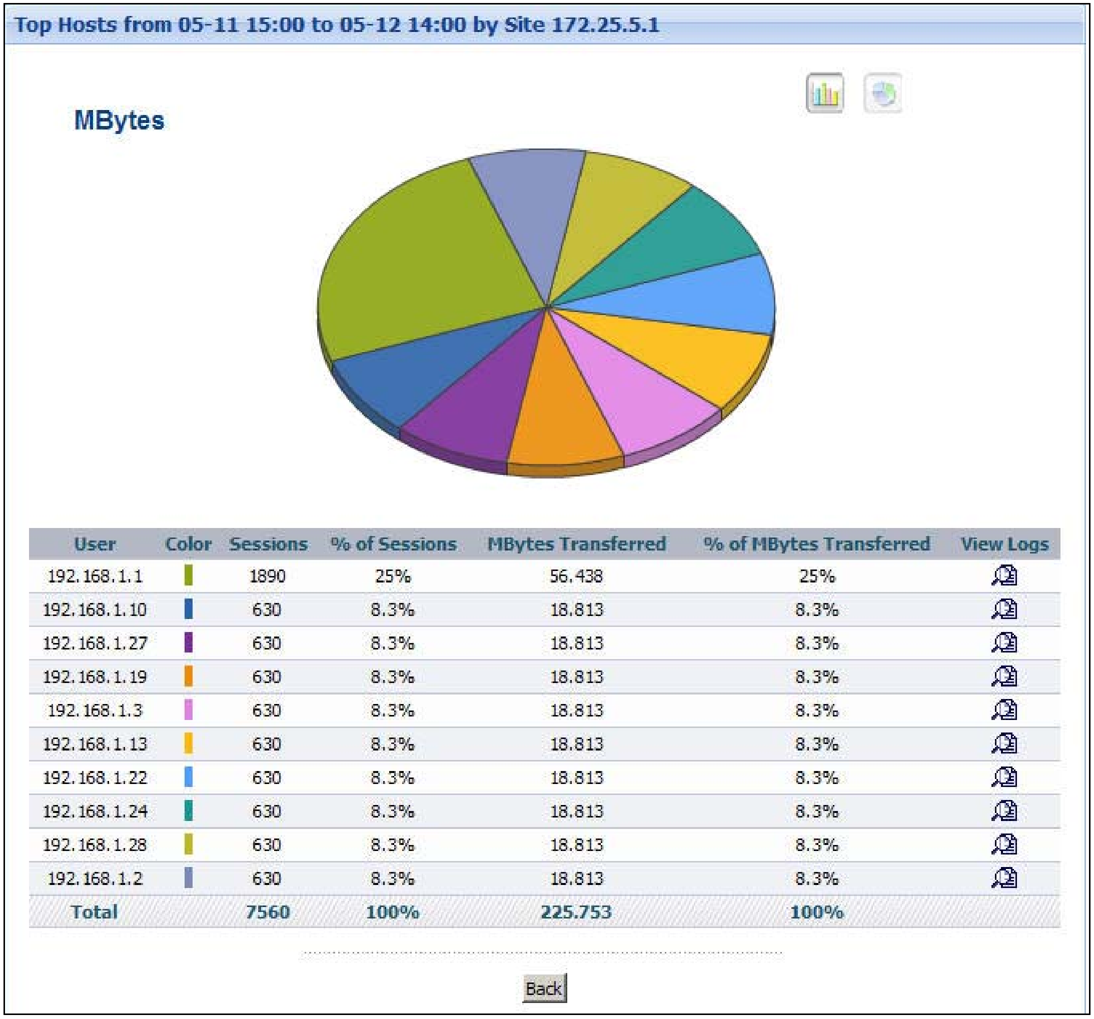
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination's traffic makes out of the total traffic that matches the settings you displayed in this report.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

5.3.2 Top FTP Sites Drill-Down

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

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

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



Top Hosts from 05-11 15:00 to 05-12 14:00 by Site 172.25.5.1

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.1	🟩	1890	25%	56.438	25%	🔍
192.168.1.10	🟦	630	8.3%	18.813	8.3%	🔍
192.168.1.27	🟪	630	8.3%	18.813	8.3%	🔍
192.168.1.19	🟧	630	8.3%	18.813	8.3%	🔍
192.168.1.3	🟪	630	8.3%	18.813	8.3%	🔍
192.168.1.13	🟨	630	8.3%	18.813	8.3%	🔍
192.168.1.22	🟦	630	8.3%	18.813	8.3%	🔍
192.168.1.24	🟩	630	8.3%	18.813	8.3%	🔍
192.168.1.28	🟨	630	8.3%	18.813	8.3%	🔍
192.168.1.2	🟦	630	8.3%	18.813	8.3%	🔍
Total		7560	100%	225.753	100%	

Each field is described in the following table.

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

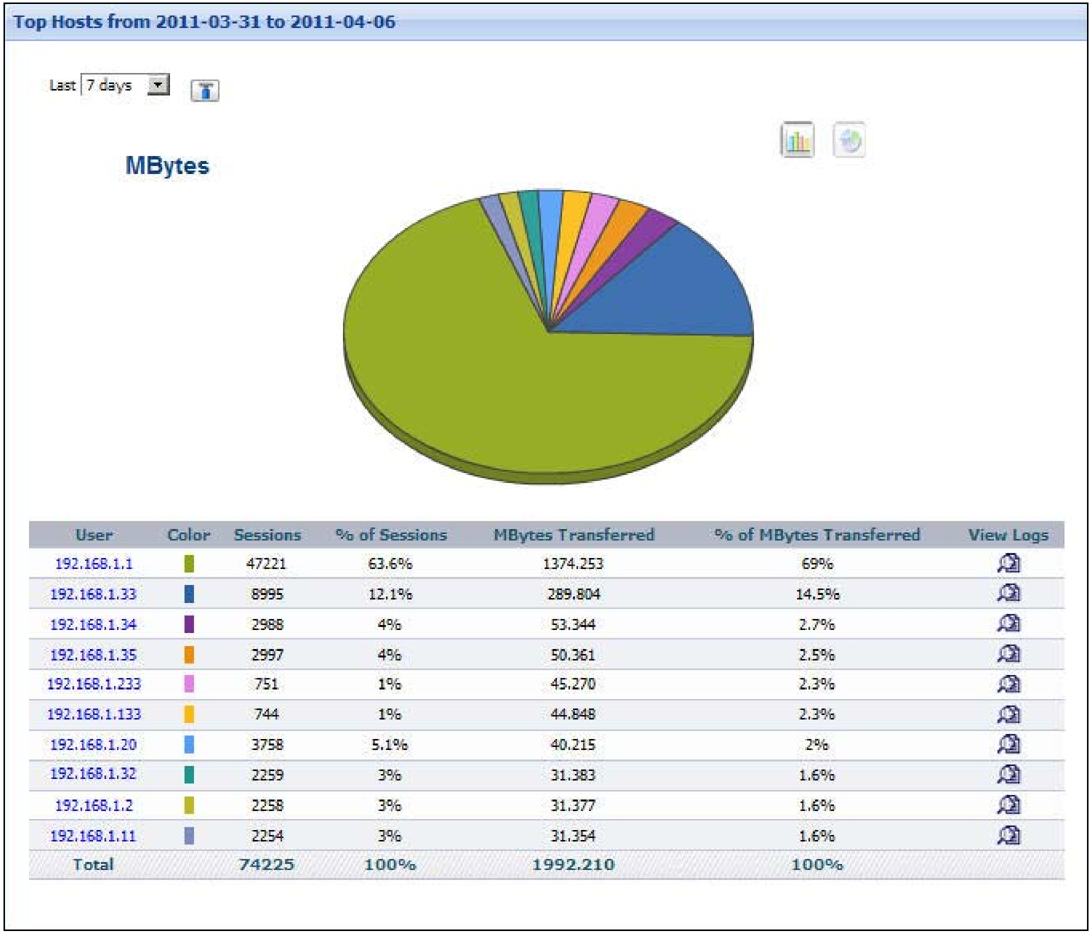
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.3.3 Top FTP Hosts

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

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

Figure 72 Report > Network Traffic > FTP > Top Hosts



Top Hosts from 2011-03-31 to 2011-04-06

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.1	🟩	47221	63.6%	1374.253	69%	
192.168.1.33	🟦	8995	12.1%	289.804	14.5%	
192.168.1.34	🟪	2988	4%	53.344	2.7%	
192.168.1.35	🟧	2997	4%	50.361	2.5%	
192.168.1.233	🟪	751	1%	45.270	2.3%	
192.168.1.133	🟨	744	1%	44.848	2.3%	
192.168.1.20	🟦	3758	5.1%	40.215	2%	
192.168.1.32	🟩	2259	3%	31.383	1.6%	
192.168.1.2	🟨	2258	3%	31.377	1.6%	
192.168.1.11	🟦	2254	3%	31.354	1.6%	
Total		74225	100%	1992.210	100%	

Each field is described in the following table.

Table 60 Report > Network Traffic > FTP > Top Hosts

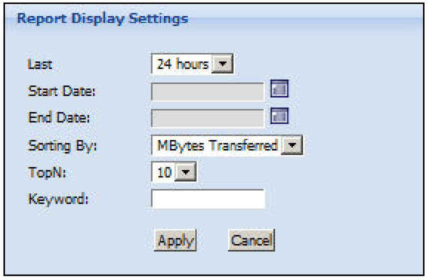
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of FTP traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 60 Report > Network Traffic > FTP > Top Hosts

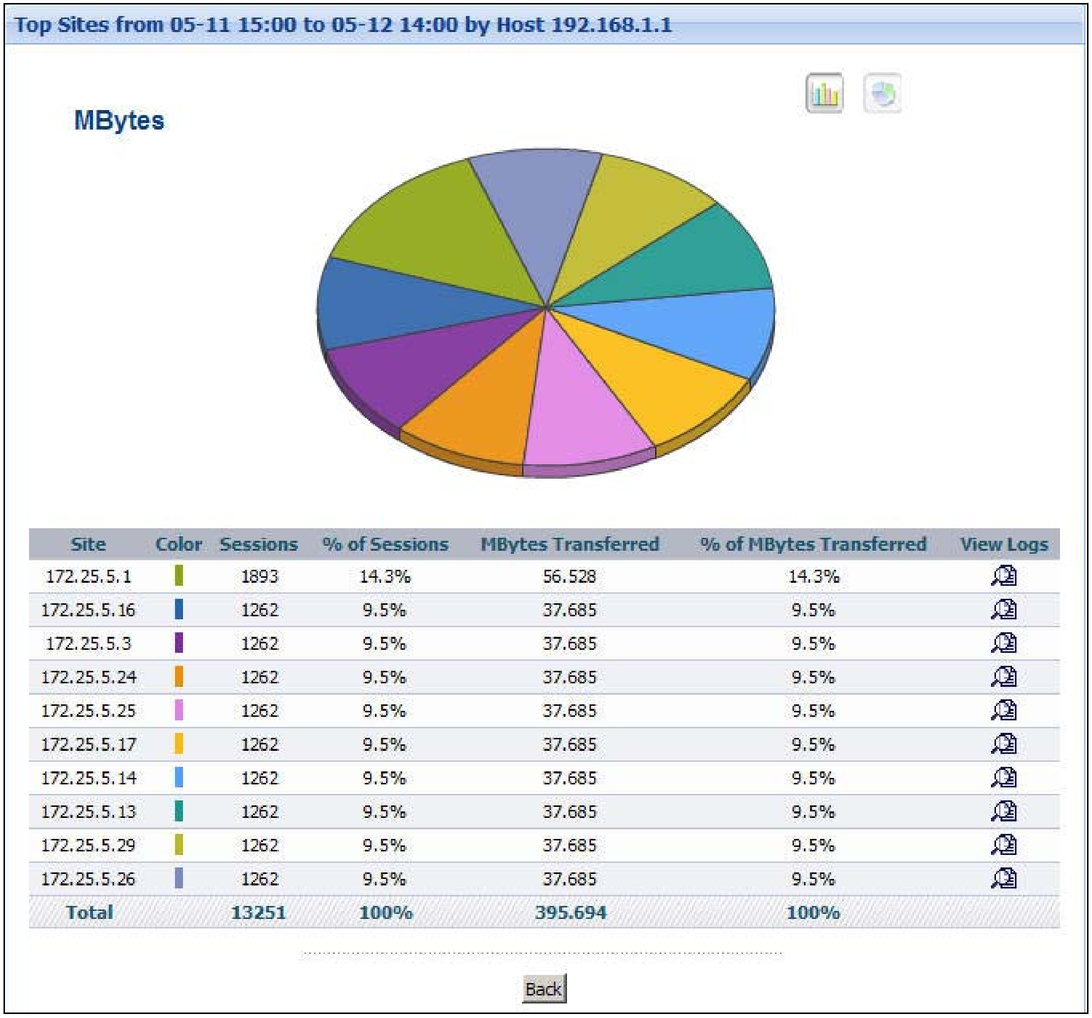
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source’s traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	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 **Report > Network Traffic > FTP** > **Top Hosts** to open this screen.

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



Top Sites from 05-11 15:00 to 05-12 14:00 by Host 192.168.1.1

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	🟩	1893	14.3%	56.528	14.3%	🔍
172.25.5.16	🟦	1262	9.5%	37.685	9.5%	🔍
172.25.5.3	🟪	1262	9.5%	37.685	9.5%	🔍
172.25.5.24	🟧	1262	9.5%	37.685	9.5%	🔍
172.25.5.25	🟪	1262	9.5%	37.685	9.5%	🔍
172.25.5.17	🟨	1262	9.5%	37.685	9.5%	🔍
172.25.5.14	🟦	1262	9.5%	37.685	9.5%	🔍
172.25.5.13	🟩	1262	9.5%	37.685	9.5%	🔍
172.25.5.29	🟨	1262	9.5%	37.685	9.5%	🔍
172.25.5.26	🟦	1262	9.5%	37.685	9.5%	🔍
Total		13251	100%	395.694	100%	

Each field is described in the following table.

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

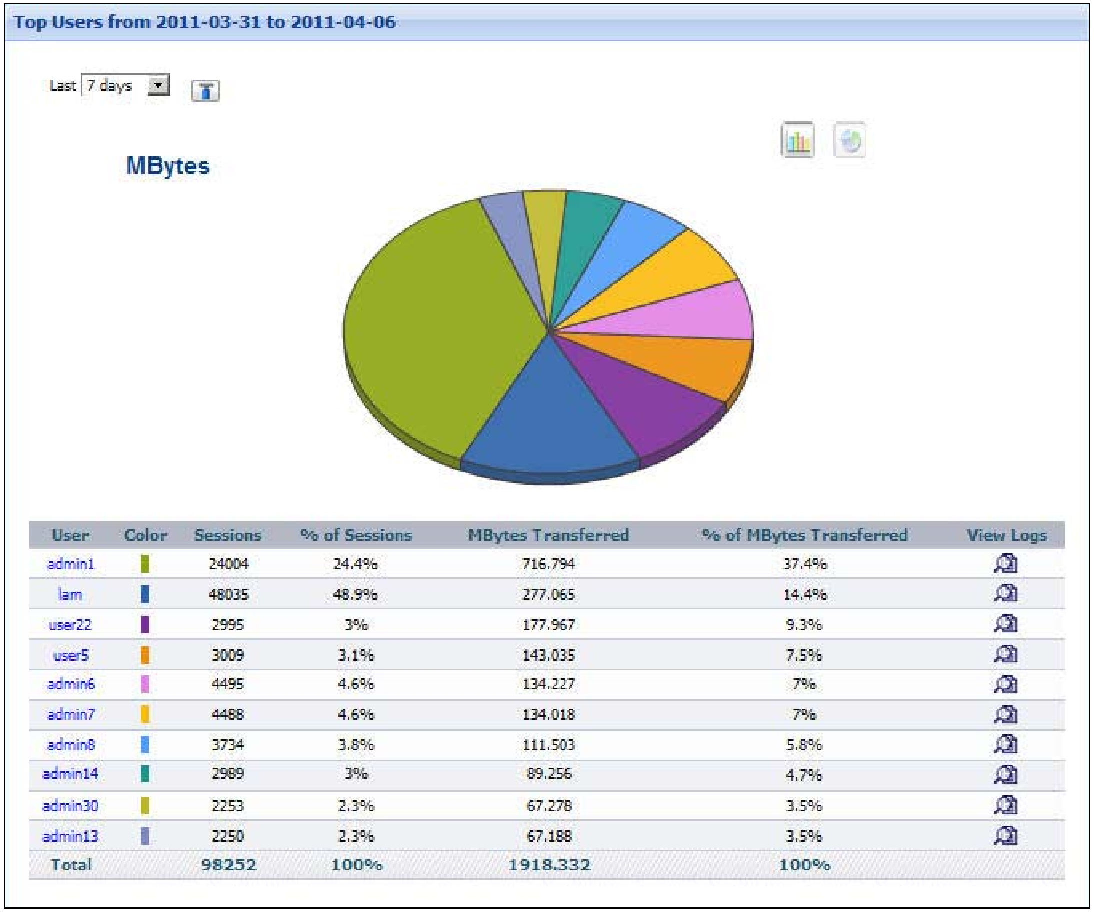
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.3.5 Top FTP Users

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

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

Figure 74 Report > Network Traffic > FTP > Top Users



Top Users from 2011-03-31 to 2011-04-06

Last 7 days

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
admin1	■	24004	24.4%	716.794	37.4%	🔍
lam	■	48035	48.9%	277.065	14.4%	🔍
user22	■	2995	3%	177.967	9.3%	🔍
user5	■	3009	3.1%	143.035	7.5%	🔍
admin6	■	4495	4.6%	134.227	7%	🔍
admin7	■	4488	4.6%	134.018	7%	🔍
admin8	■	3734	3.8%	111.503	5.8%	🔍
admin14	■	2989	3%	89.256	4.7%	🔍
admin30	■	2253	2.3%	67.278	3.5%	🔍
admin13	■	2250	2.3%	67.188	3.5%	🔍
Total		98252	100%	1918.332	100%	

Each field is described in the following table.

Table 62 Report > Network Traffic > FTP > Top Users

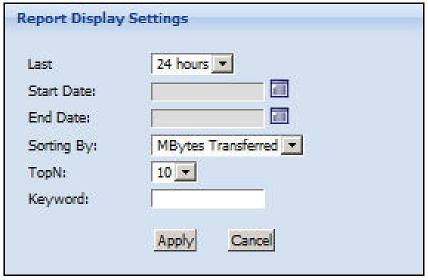
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that sent the most FTP traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click a user name to look at the top destinations of FTP traffic for the selected user.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.

Table 62 Report > Network Traffic > FTP > Top Users

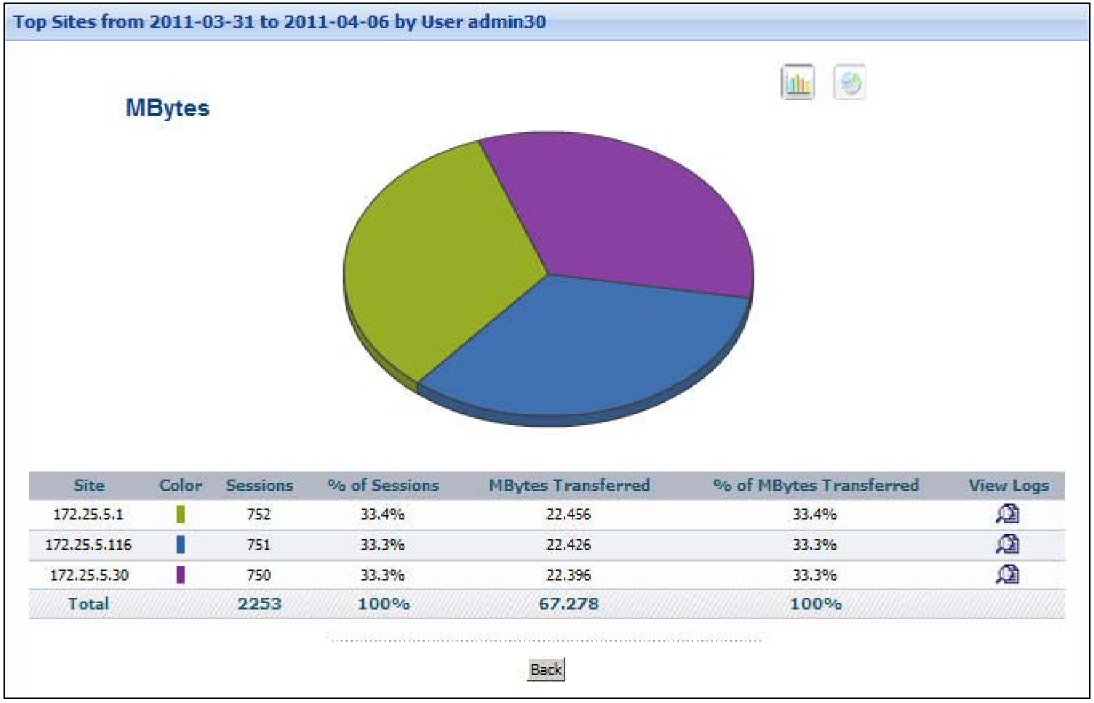
LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources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

5.3.6 Top FTP Users Drill-Down

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

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

Figure 75 Report > Network Traffic > FTP > Top Users > Drill-Down



Top Sites from 2011-03-31 to 2011-04-06 by User admin30

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	🟩	752	33.4%	22.456	33.4%	🔍
172.25.5.116	🟦	751	33.3%	22.426	33.3%	🔍
172.25.5.30	🟪	750	33.3%	22.396	33.3%	🔍
Total		2253	100%	67.278	100%	

Each field is described in the following table.

Table 63 Report > Network Traffic > FTP > Top Users > Drill-Down

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

Table 63 Report > Network Traffic > FTP > Top Users > Drill-Down

LABEL	DESCRIPTION
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events from the selected 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 user is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
View Logs	Click this icon to see the logs that go with the record.
Back	Click this to return to the main report.

5.4 Mail Traffic

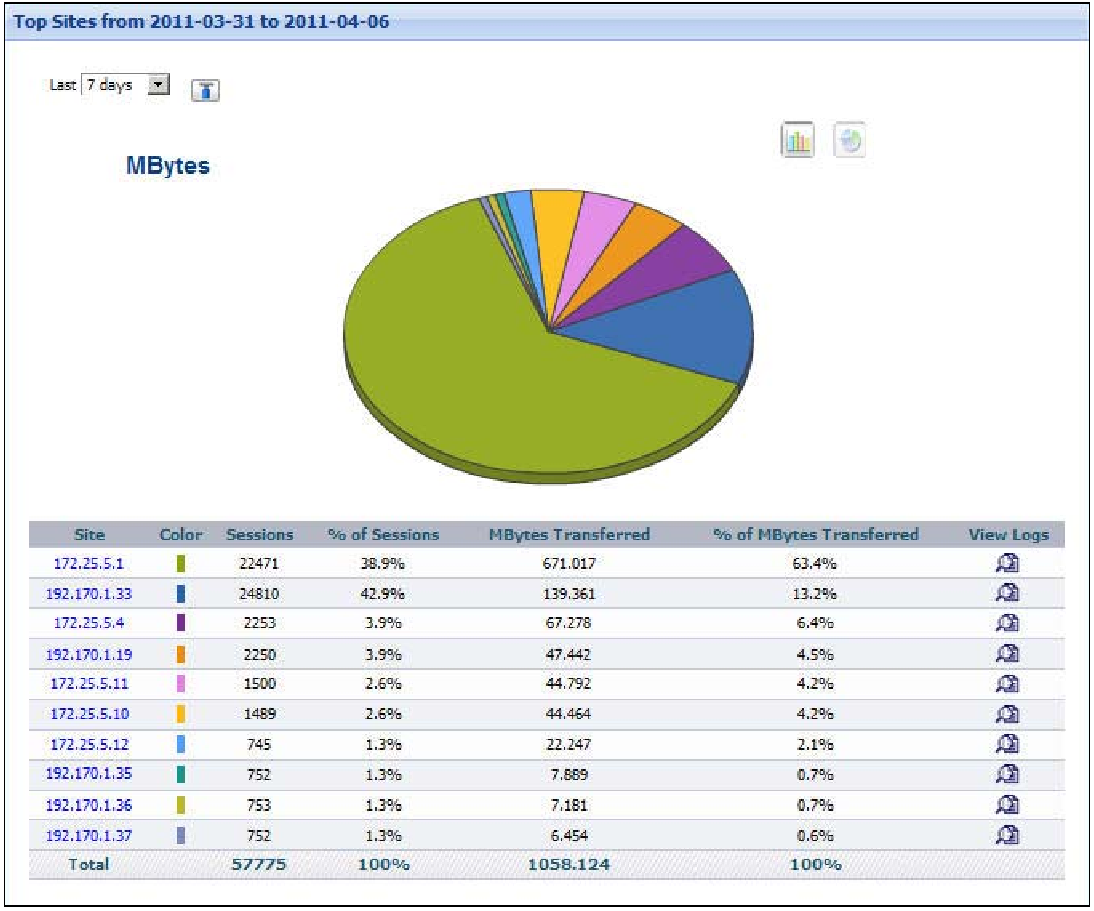
These reports look at the top destinations and sources of mail traffic.

5.4.1 Top Mail Sites

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

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

Figure 76 Report > Network Traffic > MAIL > Top Sites



Top Sites from 2011-03-31 to 2011-04-06

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	🟩	22471	38.9%	671.017	63.4%	🔍
192.170.1.33	🟦	24810	42.9%	139.361	13.2%	🔍
172.25.5.4	🟪	2253	3.9%	67.278	6.4%	🔍
192.170.1.19	🟧	2250	3.9%	47.442	4.5%	🔍
172.25.5.11	🟪	1500	2.6%	44.792	4.2%	🔍
172.25.5.10	🟨	1489	2.6%	44.464	4.2%	🔍
172.25.5.12	🟦	745	1.3%	22.247	2.1%	🔍
192.170.1.35	🟩	752	1.3%	7.889	0.7%	🔍
192.170.1.36	🟨	753	1.3%	7.181	0.7%	🔍
192.170.1.37	⬜	752	1.3%	6.454	0.6%	🔍
Total		57775	100%	1058.124	100%	

Each field is described in the following table.

Table 64 Report > Traffic > MAIL > Top Sites

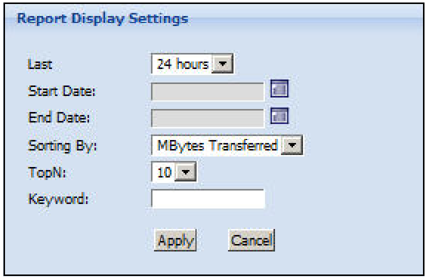
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a destination to look at the top sources of mail traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 64 Report > Traffic > MAIL > Top Sites

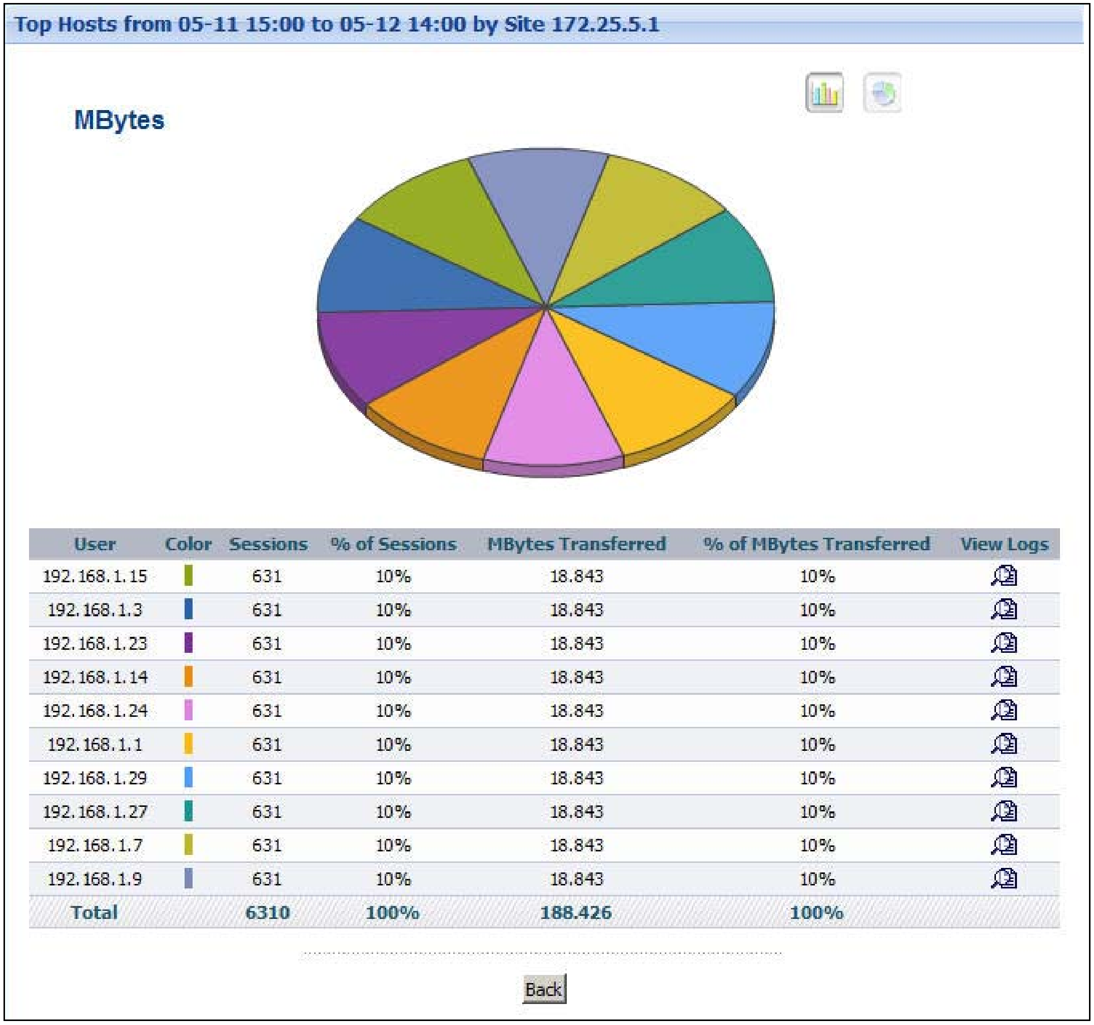
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage each destination's traffic makes out of the total traffic that matches the settings you displayed in this report.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

5.4.2 Top Mail Sites Drill-Down

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

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

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



Top Hosts from 05-11 15:00 to 05-12 14:00 by Site 172.25.5.1

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.15	🟩	631	10%	18.843	10%	🔍
192.168.1.3	🟦	631	10%	18.843	10%	🔍
192.168.1.23	🟪	631	10%	18.843	10%	🔍
192.168.1.14	🟧	631	10%	18.843	10%	🔍
192.168.1.24	🟪	631	10%	18.843	10%	🔍
192.168.1.1	🟨	631	10%	18.843	10%	🔍
192.168.1.29	🟦	631	10%	18.843	10%	🔍
192.168.1.27	🟩	631	10%	18.843	10%	🔍
192.168.1.7	🟨	631	10%	18.843	10%	🔍
192.168.1.9	🟦	631	10%	18.843	10%	🔍
Total		6310	100%	188.426	100%	

Each field is described in the following table.

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

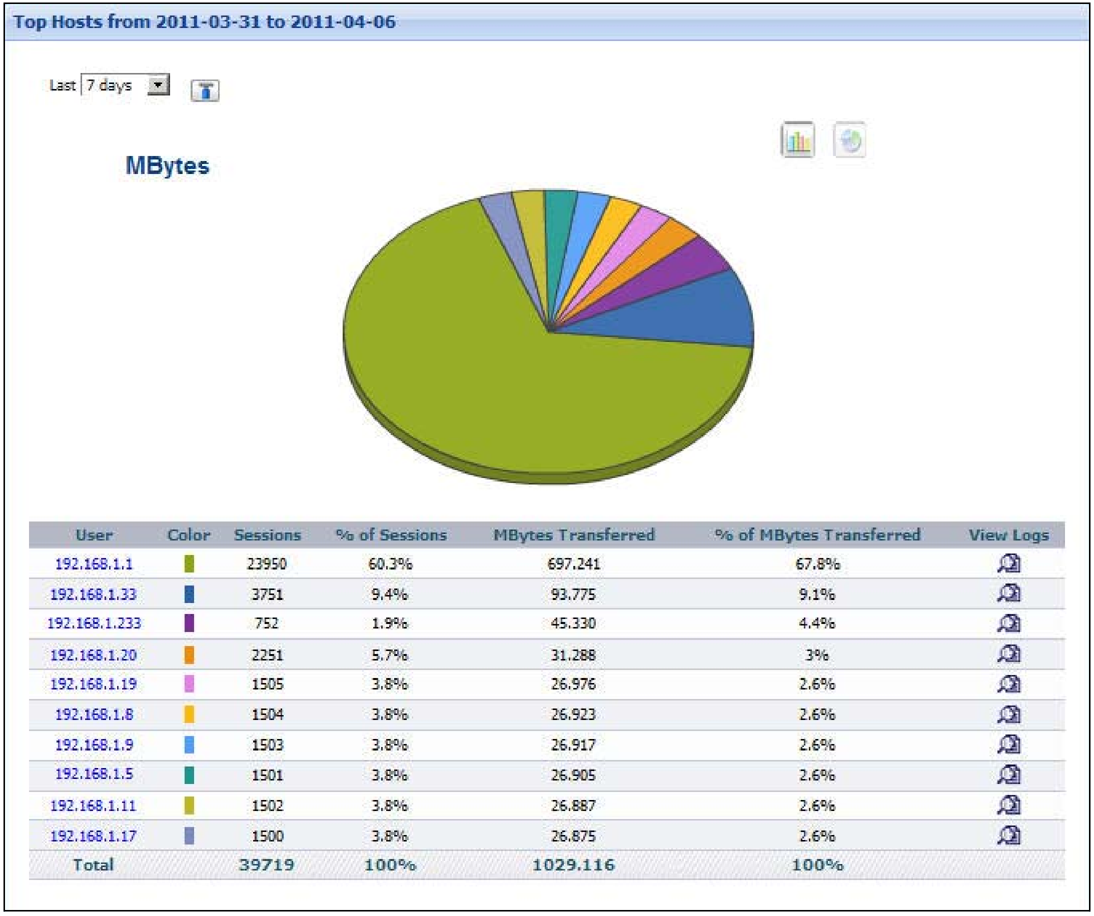
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.4.3 Top Mail Hosts

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

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

Figure 78 Report > Network Traffic > MAIL > Top Hosts



Top Hosts from 2011-03-31 to 2011-04-06

Last 7 days

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.1	■	23950	60.3%	697.241	67.8%	🔍
192.168.1.33	■	3751	9.4%	93.775	9.1%	🔍
192.168.1.233	■	752	1.9%	45.330	4.4%	🔍
192.168.1.20	■	2251	5.7%	31.288	3%	🔍
192.168.1.19	■	1505	3.8%	26.976	2.6%	🔍
192.168.1.8	■	1504	3.8%	26.923	2.6%	🔍
192.168.1.9	■	1503	3.8%	26.917	2.6%	🔍
192.168.1.5	■	1501	3.8%	26.905	2.6%	🔍
192.168.1.11	■	1502	3.8%	26.887	2.6%	🔍
192.168.1.17	■	1500	3.8%	26.875	2.6%	🔍
Total		39719	100%	1029.116	100%	

Each field is described in the following table.

Table 66 Report > Network Traffic > MAIL > Top Hosts

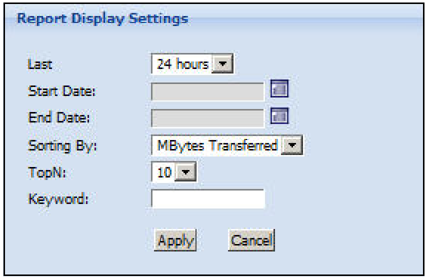
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of mail traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

Table 66 Report > Network Traffic > MAIL > Top Hosts

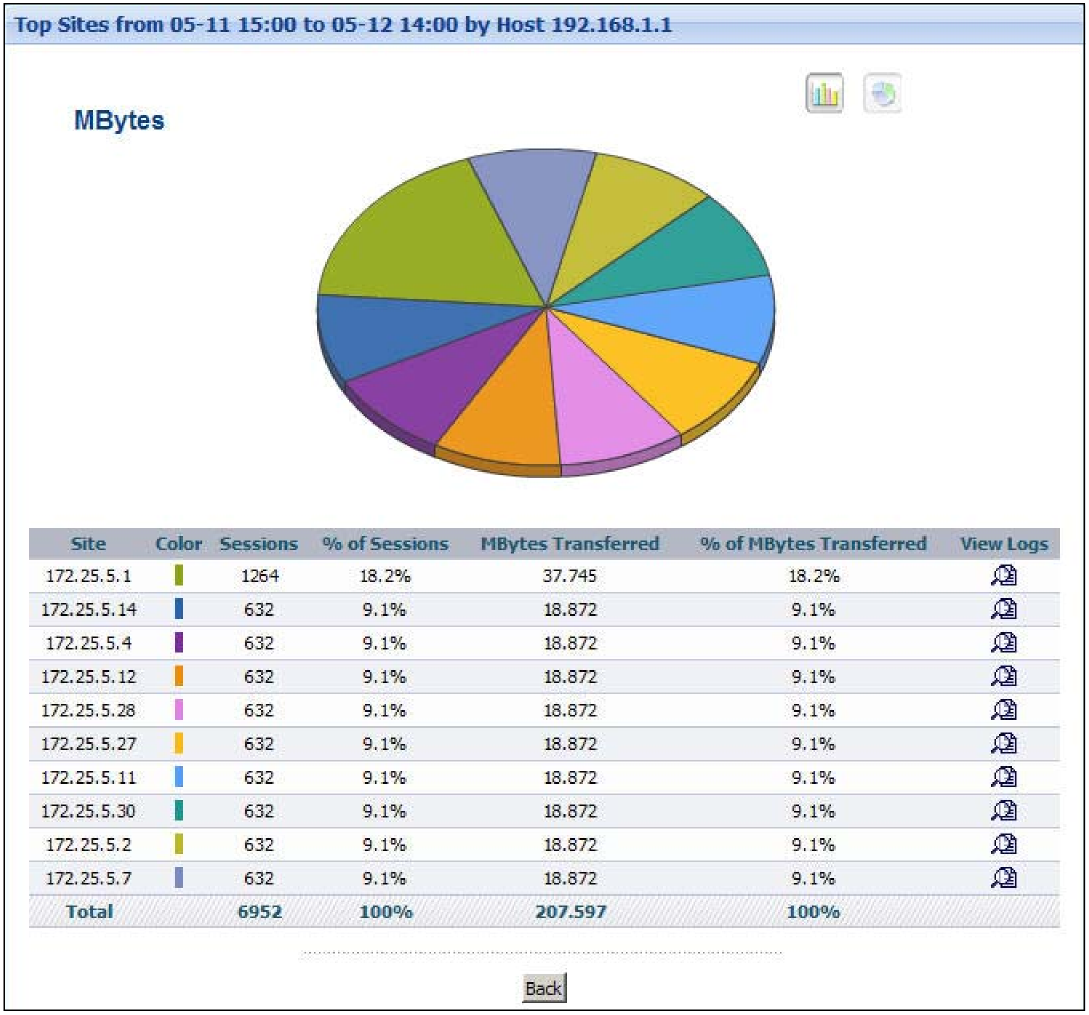
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each source.
% of MBytes Transferred	This field displays what percentage each source's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	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 **Report > Network Traffic > MAIL** > **Top Hosts** to open this screen.

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



Top Sites from 05-11 15:00 to 05-12 14:00 by Host 192.168.1.1

MBytes

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	🟩	1264	18.2%	37.745	18.2%	🔍
172.25.5.14	🟦	632	9.1%	18.872	9.1%	🔍
172.25.5.4	🟪	632	9.1%	18.872	9.1%	🔍
172.25.5.12	🟧	632	9.1%	18.872	9.1%	🔍
172.25.5.28	🟪	632	9.1%	18.872	9.1%	🔍
172.25.5.27	🟨	632	9.1%	18.872	9.1%	🔍
172.25.5.11	🟦	632	9.1%	18.872	9.1%	🔍
172.25.5.30	🟩	632	9.1%	18.872	9.1%	🔍
172.25.5.2	🟨	632	9.1%	18.872	9.1%	🔍
172.25.5.7	🟦	632	9.1%	18.872	9.1%	🔍
Total		6952	100%	207.597	100%	

Each field is described in the following table.

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

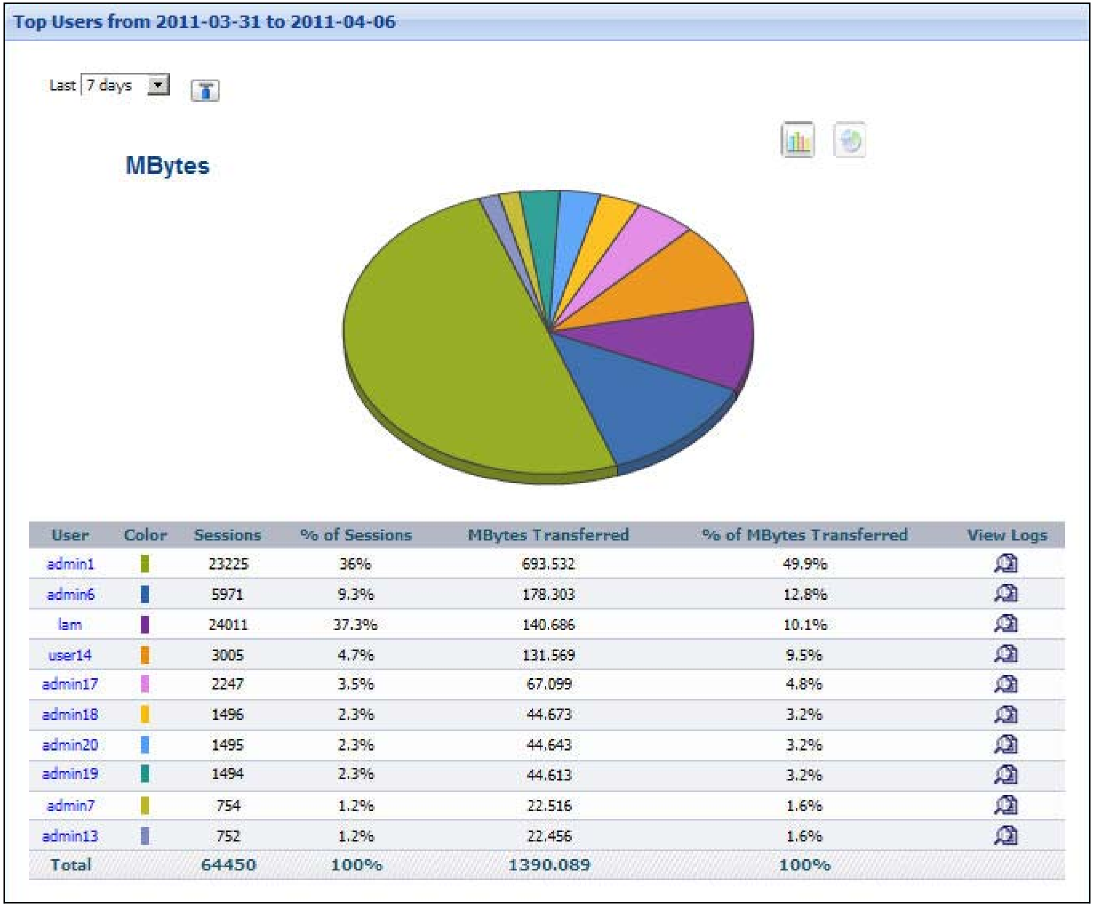
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.4.5 Top Mail Users

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

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

Figure 80 Report > Network Traffic > MAIL > Top Users



Top Users from 2011-03-31 to 2011-04-06

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
admin1	🟩	23225	36%	693.532	49.9%	🔍
admin6	🟦	5971	9.3%	178.303	12.8%	🔍
lam	🟪	24011	37.3%	140.686	10.1%	🔍
user14	🟧	3005	4.7%	131.569	9.5%	🔍
admin17	🟪	2247	3.5%	67.099	4.8%	🔍
admin18	🟨	1496	2.3%	44.673	3.2%	🔍
admin20	🟦	1495	2.3%	44.643	3.2%	🔍
admin19	🟩	1494	2.3%	44.613	3.2%	🔍
admin7	🟨	754	1.2%	22.516	1.6%	🔍
admin13	🟦	752	1.2%	22.456	1.6%	🔍
Total		64450	100%	1390.089	100%	

Each field is described in the following table.

Table 68 Report > Network Traffic > MAIL > Top Users

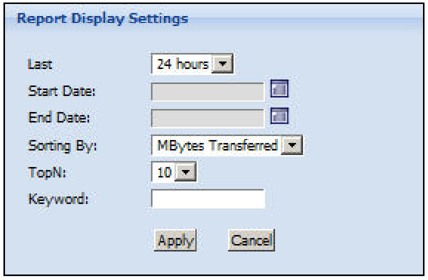
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that send the most mail traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of mail traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.

Table 68 Report > Network Traffic > MAIL > Top Users

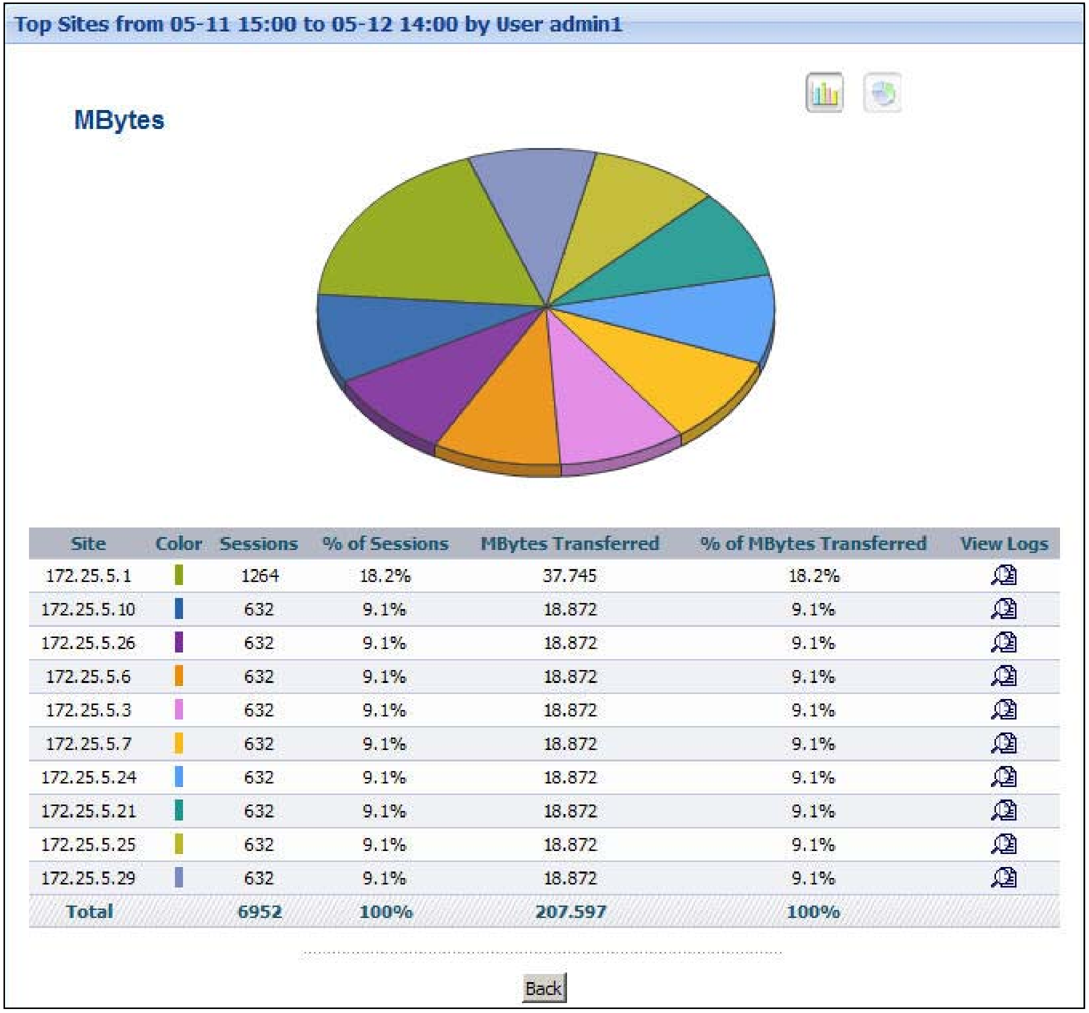
LABEL	DESCRIPTION
% of MBytes Transferred	This field displays what percentage each user's traffic makes out of the total traffic that matches the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources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

5.4.6 Top Mail Users Drill-Down

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

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

Figure 81 Report > Network Traffic > MAIL > Top Users > Drill-Down



Top Sites from 05-11 15:00 to 05-12 14:00 by User admin1

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	■	1264	18.2%	37.745	18.2%	🔍
172.25.5.10	■	632	9.1%	18.872	9.1%	🔍
172.25.5.26	■	632	9.1%	18.872	9.1%	🔍
172.25.5.6	■	632	9.1%	18.872	9.1%	🔍
172.25.5.3	■	632	9.1%	18.872	9.1%	🔍
172.25.5.7	■	632	9.1%	18.872	9.1%	🔍
172.25.5.24	■	632	9.1%	18.872	9.1%	🔍
172.25.5.21	■	632	9.1%	18.872	9.1%	🔍
172.25.5.25	■	632	9.1%	18.872	9.1%	🔍
172.25.5.29	■	632	9.1%	18.872	9.1%	🔍
Total		6952	100%	207.597	100%	

Each field is described in the following table.

Table 69 Report > Network Traffic > MAIL > Top Users > Drill-Down

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

5.5 Other Traffic

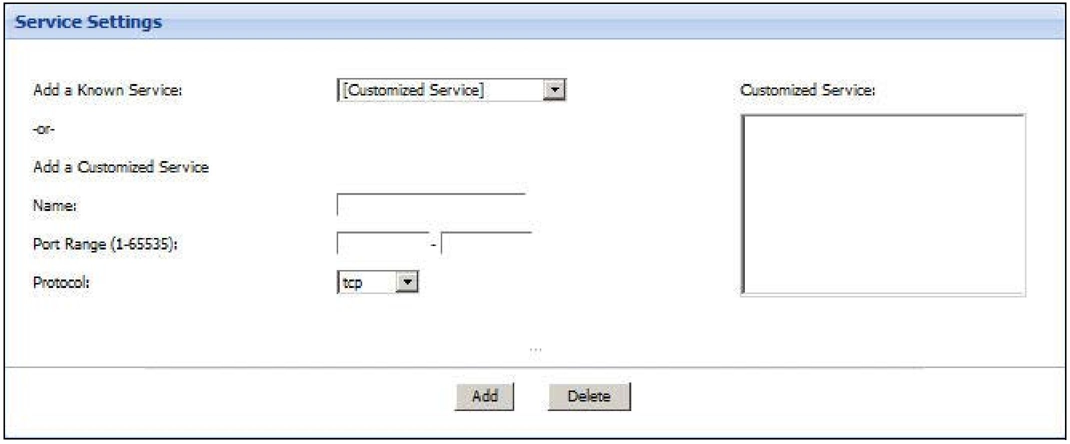
These reports look at the top sources and destinations of any kind of traffic.

5.5.1 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 82 Report > Network Traffic > Customization > Customization (Service Settings)



Service Settings

Add a Known Service: [Customized Service]

-or-

Add a Customized Service

Name:

Port Range (1-65535): -

Protocol: tcp

Customized Service:

Each field is described in the following table.

Table 70 Report > Network Traffic > Customization > Customization (Service Settings)

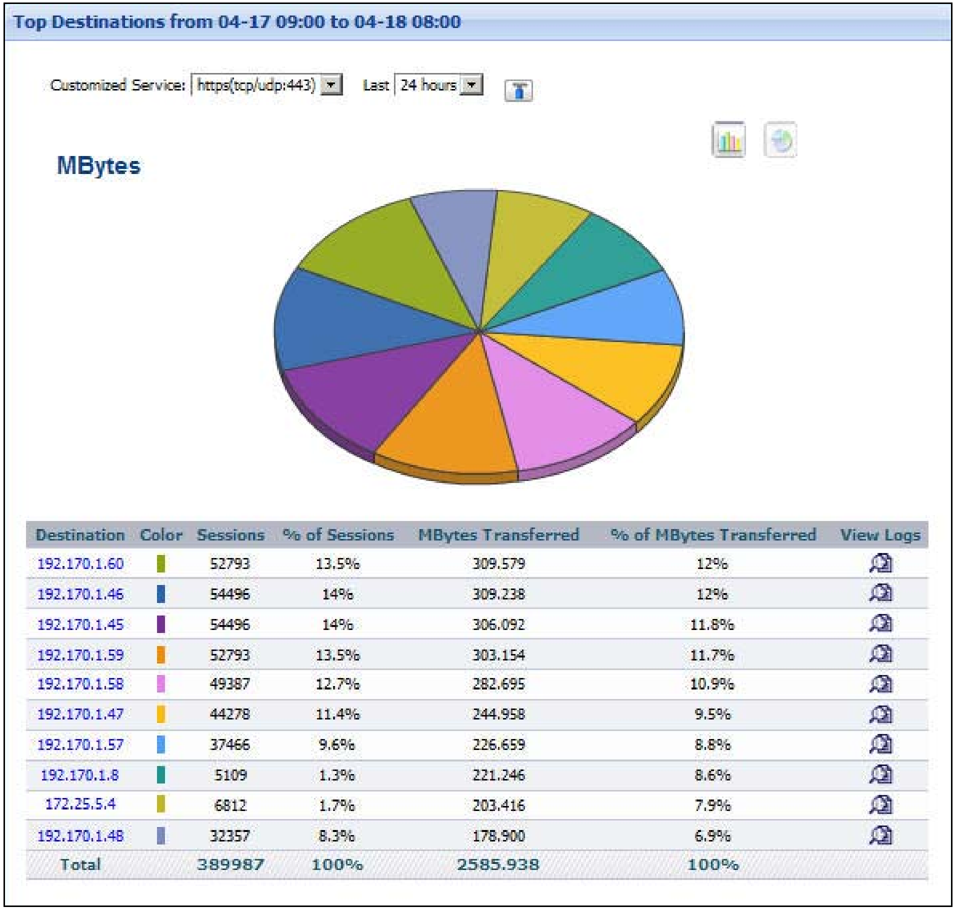
LABEL	DESCRIPTION
Add a Known Service	Use this drop-down box to add a service to the **Customized Service** drop-down box. • Select a pre-defined service from the drop-down list box, and click the **Add** button; or • Select **[Customized Service]**, fill in the **Add a Customized Service** section,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

5.5.2 Top Destinations of Other Traffic

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

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

Figure 83 Report > Network Traffic > Customization > Top Destinations



Top Destinations from 04-17 09:00 to 04-18 08:00

Customized Service: https(tcp/udp:443) Last 24 hours

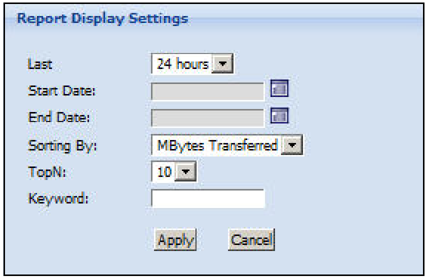
Destination	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.60	■	52793	13.5%	309.579	12%	🔍
192.170.1.46	■	54496	14%	309.238	12%	🔍
192.170.1.45	■	54496	14%	306.092	11.8%	🔍
192.170.1.59	■	52793	13.5%	303.154	11.7%	🔍
192.170.1.58	■	49387	12.7%	282.695	10.9%	🔍
192.170.1.47	■	44278	11.4%	244.958	9.5%	🔍
192.170.1.57	■	37466	9.6%	226.659	8.8%	🔍
192.170.1.8	■	5109	1.3%	221.246	8.6%	🔍
172.25.5.4	■	6812	1.7%	203.416	7.9%	🔍
192.170.1.48	■	32357	8.3%	178.900	6.9%	🔍
Total		389987	100%	2585.938	100%	

Each field is described in the following table.

Table 71 Report > Network Traffic > Customization > Top Destinations

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

Table 71 Report > Network Traffic > Customization > Top Destinations

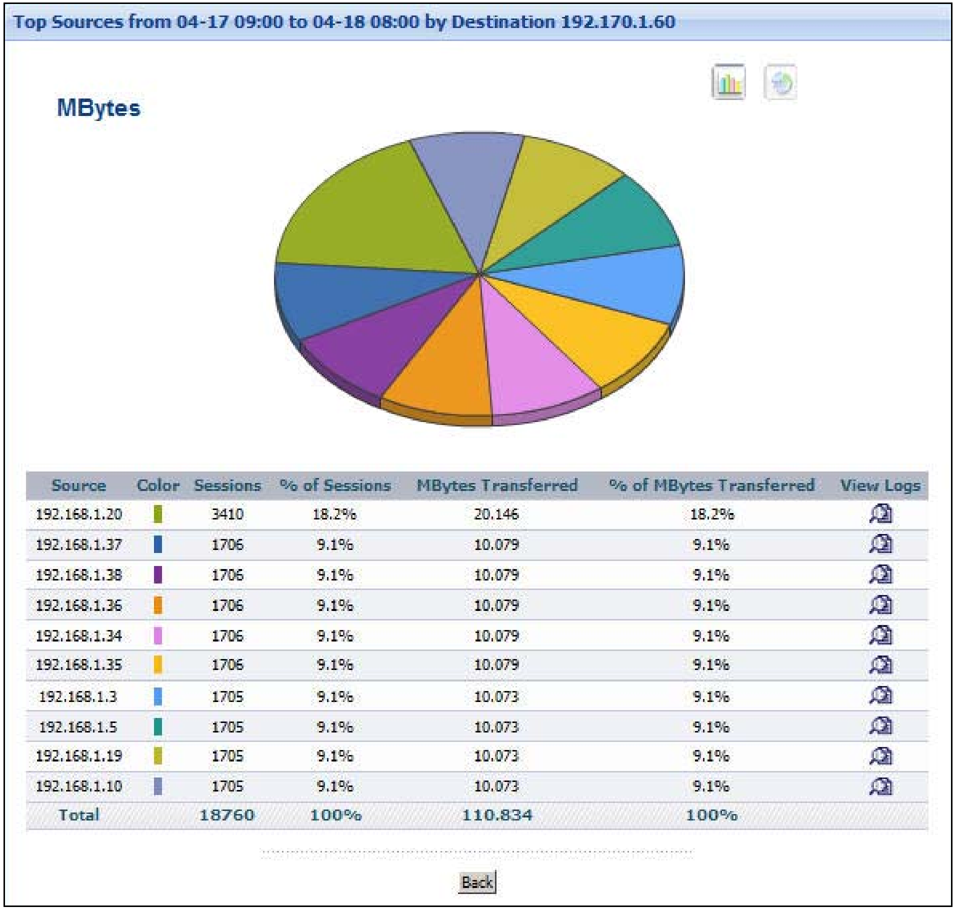
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the top sources of the selected service's traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
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.

5.5.3 Top Destinations of Other Traffic Drill-Down

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

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

Figure 84 Report > Network Traffic > Customization > Top Destinations > Drill-Down



Top Sources from 04-17 09:00 to 04-18 08:00 by Destination 192.170.1.60

Source	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.20	■	3410	18.2%	20.146	18.2%	🔍
192.168.1.37	■	1706	9.1%	10.079	9.1%	🔍
192.168.1.38	■	1706	9.1%	10.079	9.1%	🔍
192.168.1.36	■	1706	9.1%	10.079	9.1%	🔍
192.168.1.34	■	1706	9.1%	10.079	9.1%	🔍
192.168.1.35	■	1706	9.1%	10.079	9.1%	🔍
192.168.1.3	■	1705	9.1%	10.073	9.1%	🔍
192.168.1.5	■	1705	9.1%	10.073	9.1%	🔍
192.168.1.19	■	1705	9.1%	10.073	9.1%	🔍
192.168.1.10	■	1705	9.1%	10.073	9.1%	🔍
Total		18760	100%	110.834	100%	

Each field is described in the following table.

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

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

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

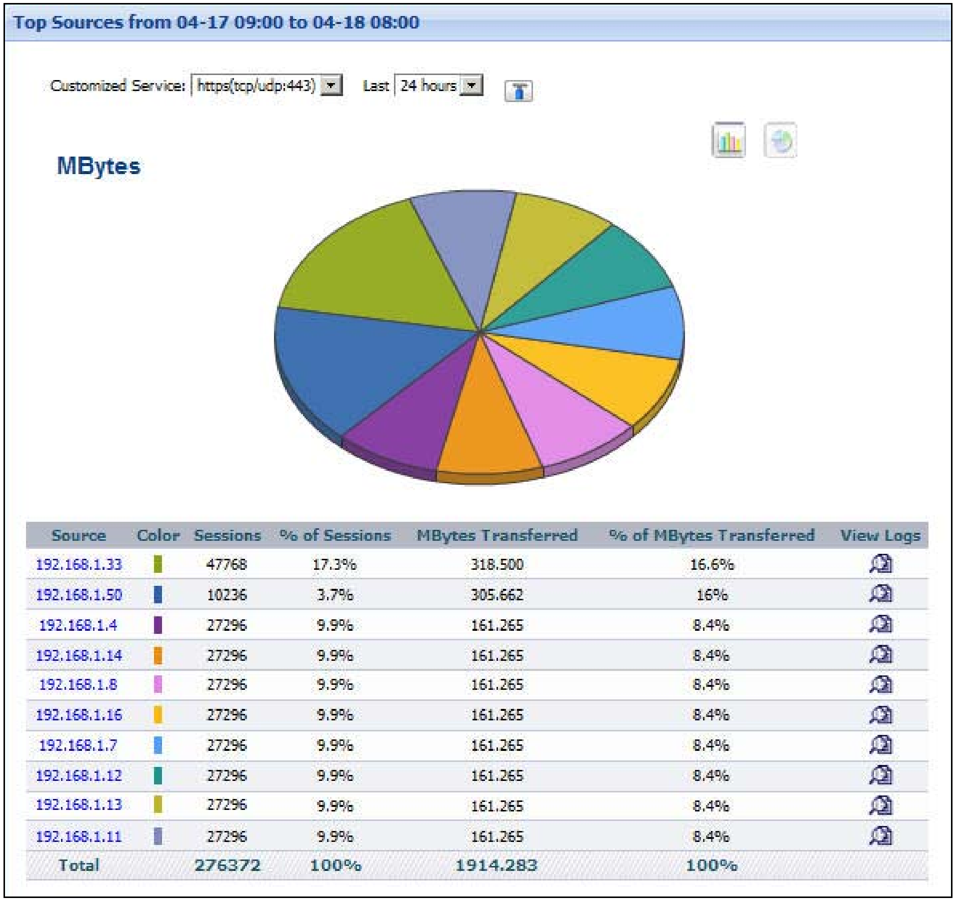
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events from each source to the selected destination.
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events for the selected destination.
MBytes Transferred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

5.5.4 Top Sources of Other Traffic

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

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

Figure 85 Report > Network Traffic > Customization > Top Sources



Top Sources from 04-17 09:00 to 04-18 08:00

Customized Service: https(tcp/udp:443) Last 24 hours

Source	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	■	47768	17.3%	318.500	16.6%	🔍
192.168.1.50	■	10236	3.7%	305.662	16%	🔍
192.168.1.4	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.14	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.8	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.16	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.7	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.12	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.13	■	27296	9.9%	161.265	8.4%	🔍
192.168.1.11	■	27296	9.9%	161.265	8.4%	🔍
Total		276372	100%	1914.283	100%	

Each field is described in the following table.

Table 73 Report > Network Traffic > Customization > Top Sources

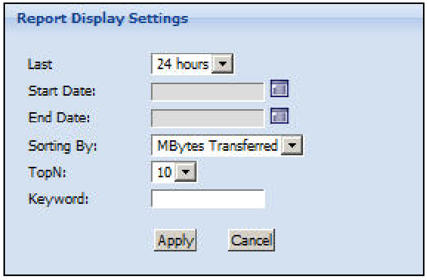
LABEL	DESCRIPTION
Customized Service	Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the **Service Settings** screen.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top senders of the selected service's traffic in the selected device, sorted by the amount of traffic for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of the selected service's traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Sessions	This field displays the number of traffic events for each source.

Table 73 Report > Network Traffic > Customization > Top Sources

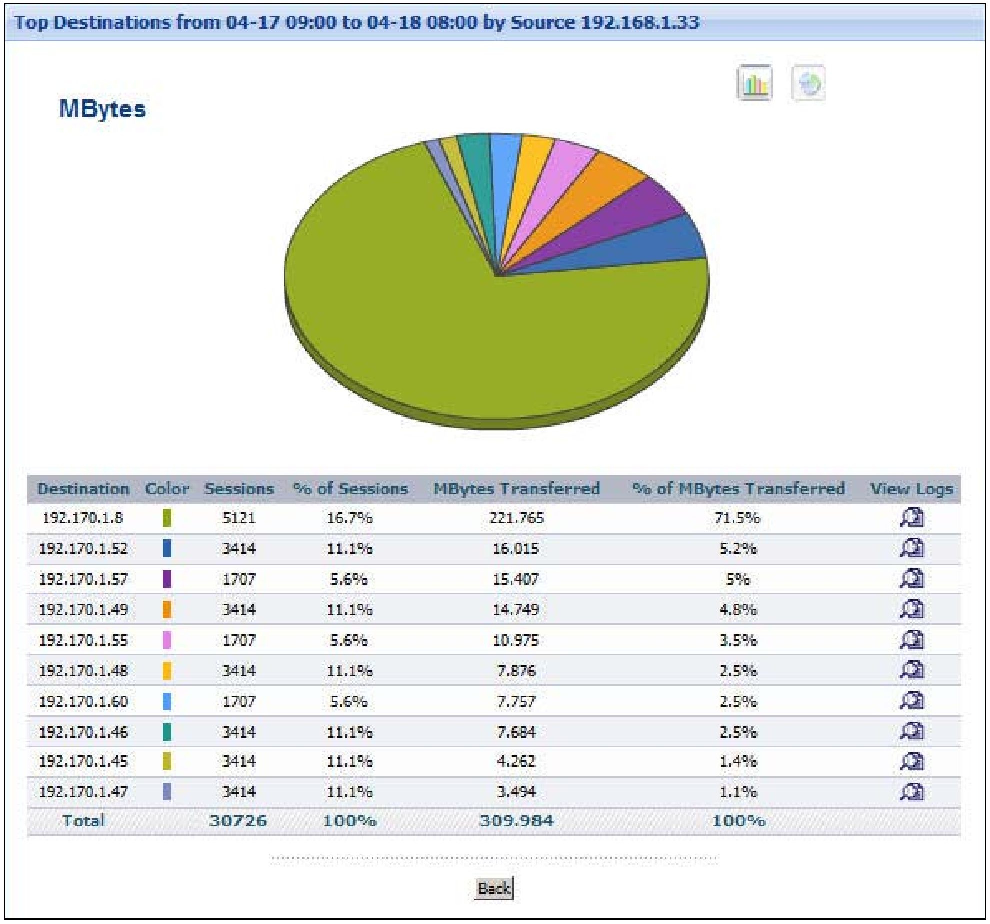
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each source's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for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

5.5.5 Top Sources of Other Traffic Drill-Down

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

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

Figure 86 Report > Network Traffic > Customization > Top Sources > Drill-Down



Top Destinations from 04-17 09:00 to 04-18 08:00 by Source 192.168.1.33

Destination	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.8	🟩	5121	16.7%	221.765	71.5%	🔍
192.170.1.52	🟦	3414	11.1%	16.015	5.2%	🔍
192.170.1.57	🟪	1707	5.6%	15.407	5%	🔍
192.170.1.49	🟧	3414	11.1%	14.749	4.8%	🔍
192.170.1.55	🟪	1707	5.6%	10.975	3.5%	🔍
192.170.1.48	🟨	3414	11.1%	7.876	2.5%	🔍
192.170.1.60	🟦	1707	5.6%	7.757	2.5%	🔍
192.170.1.46	🟩	3414	11.1%	7.684	2.5%	🔍
192.170.1.45	🟨	3414	11.1%	4.262	1.4%	🔍
192.170.1.47	🟦	3414	11.1%	3.494	1.1%	🔍
Total		30726	100%	309.984	100%	

Each field is described in the following table.

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

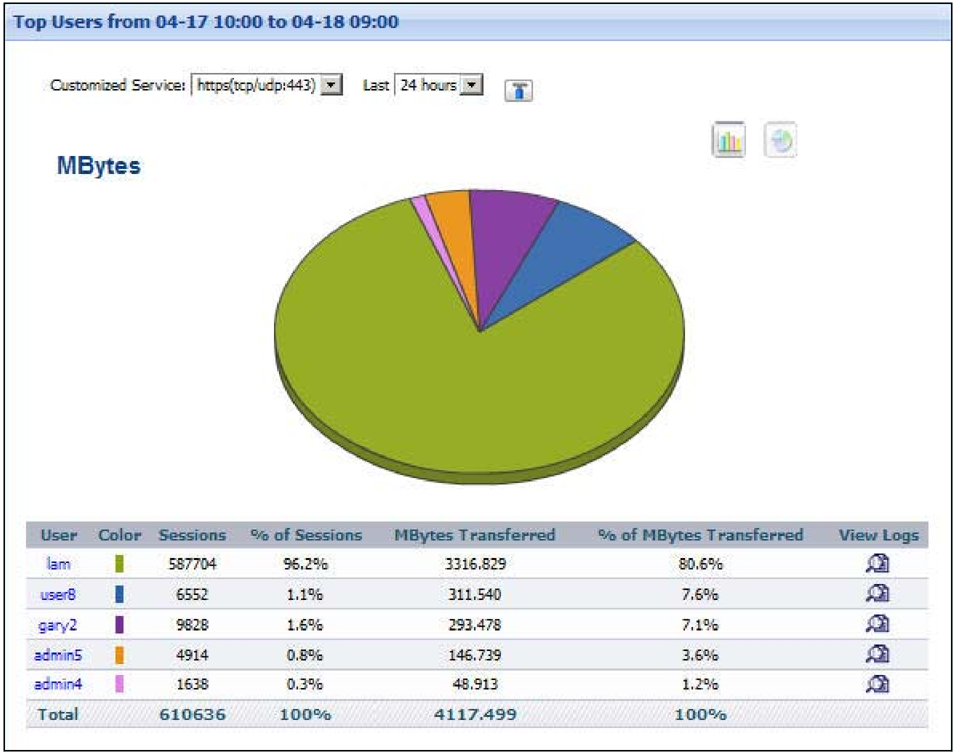
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

5.5.6 Top Other Traffic Users

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

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

Figure 87 Report > Network Traffic > Customization > Top Users



Top Users from 04-17 10:00 to 04-18 09:00

Customized Service: https(tcp/udp:443) Last 24 hours

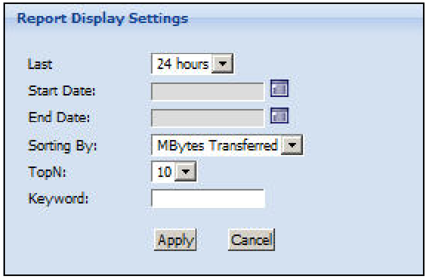
User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
lam	🟩	587704	96.2%	3316.829	80.6%	🔍
user8	🟦	6552	1.1%	311.540	7.6%	🔍
gary2	🟪	9828	1.6%	293.478	7.1%	🔍
admin5	🟧	4914	0.8%	146.739	3.6%	🔍
admin4	🟪	1638	0.3%	48.913	1.2%	🔍
Total		610636	100%	4117.499	100%	

Each field is described in the following table.

Table 75 Report > Network Traffic > Customization > Top Users

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

Table 75 Report > Network Traffic > Customization > Top Users

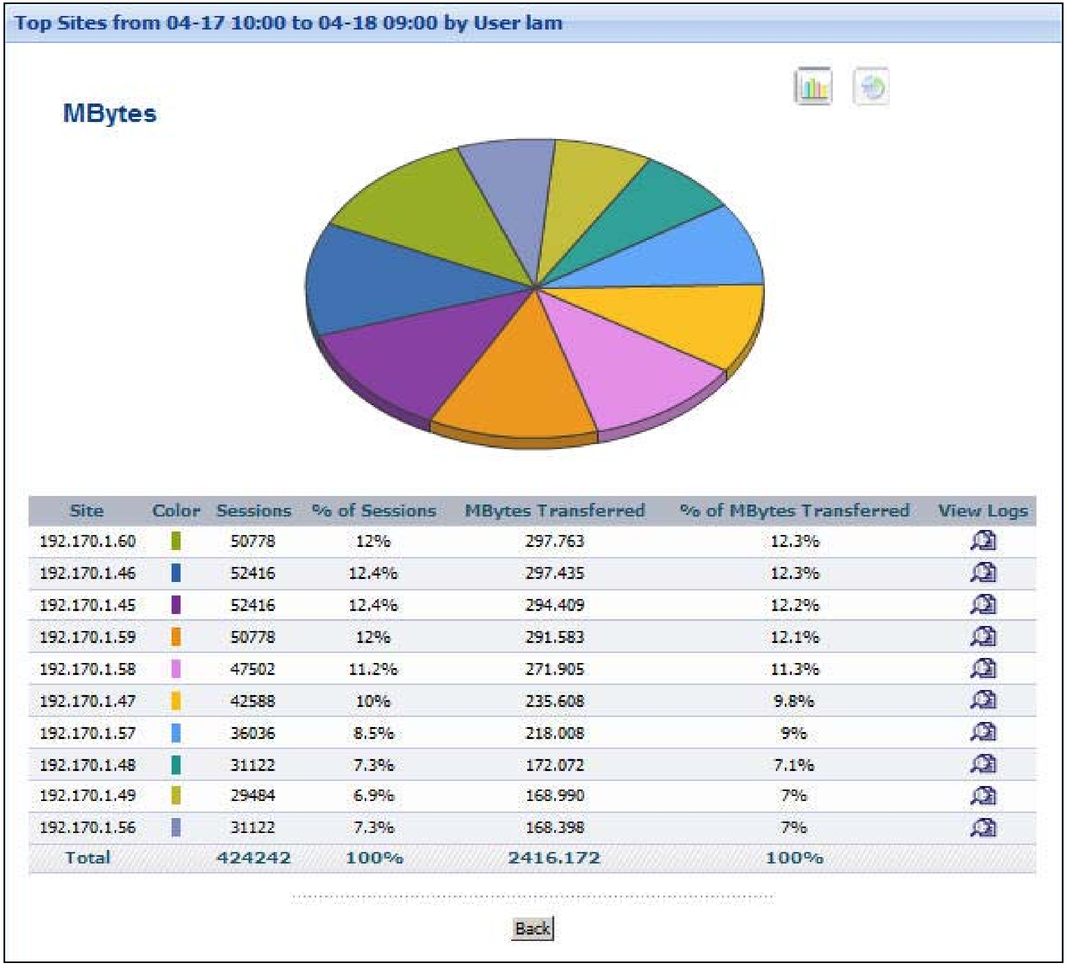
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: Enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users that sent the most of the selected service’s traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of the selected service’s traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user’s number of traffic events makes out of the total number of traffic events for the time range of the report.
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.

5.5.7 Top Users of Other Traffic Drill-Down

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

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

Figure 88 Report > Network Traffic > Customization > Top Users > Drill-Down



Top Sites from 04-17 10:00 to 04-18 09:00 by User lam

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.60	🟩	50778	12%	297.763	12.3%	🔍
192.170.1.46	🟦	52416	12.4%	297.435	12.3%	🔍
192.170.1.45	🟪	52416	12.4%	294.409	12.2%	🔍
192.170.1.59	🟧	50778	12%	291.583	12.1%	🔍
192.170.1.58	🟪	47502	11.2%	271.905	11.3%	🔍
192.170.1.47	🟨	42588	10%	235.608	9.8%	🔍
192.170.1.57	🟦	36036	8.5%	218.008	9%	🔍
192.170.1.48	🟩	31122	7.3%	172.072	7.1%	🔍
192.170.1.49	🟨	29484	6.9%	168.990	7%	🔍
192.170.1.56	🟪	31122	7.3%	168.398	7%	🔍
Total		424242	100%	2416.172	100%	

Each field is described in the following table.

Table 76 Report > Network Traffic > Customization > Top Users > Drill-Down

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

Secure Remote Access

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

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

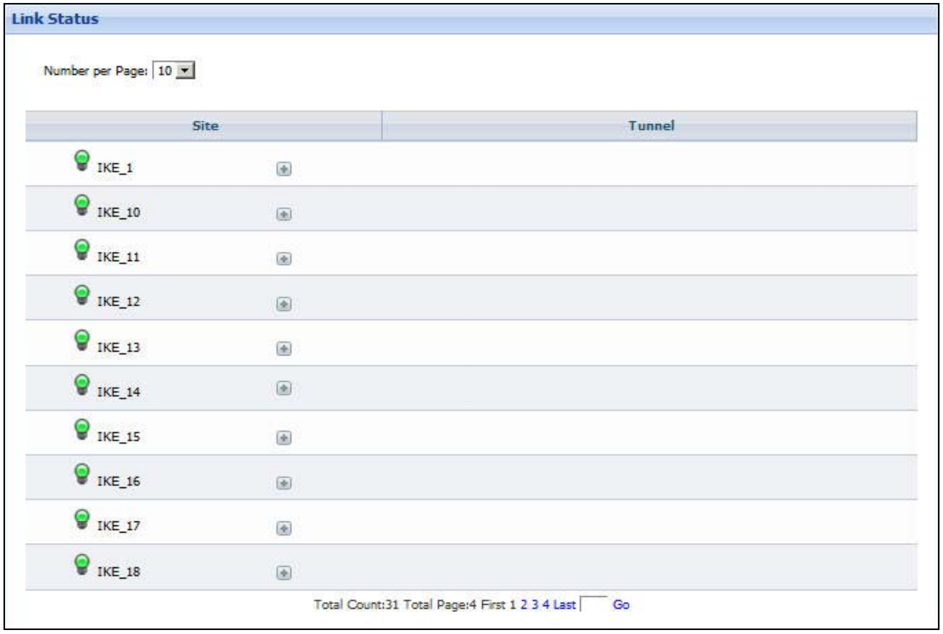
Note: To look at Secure Remote Access usage reports, each ZyXEL device must record forwarded IPSec Secure Remote Access traffic in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **IPSec** is enabled.

6.1.1 Secure Remote Access Link Status

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

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

Figure 89 Report > Secure Remote Access > Site-to-Site (IPSec) > Link Status



Link Status

Number per Page: 10

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

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

Each field is described in the following table.

Table 77 Report > Secure Remote Access > Site-to-Site (IPSec) > Link Status

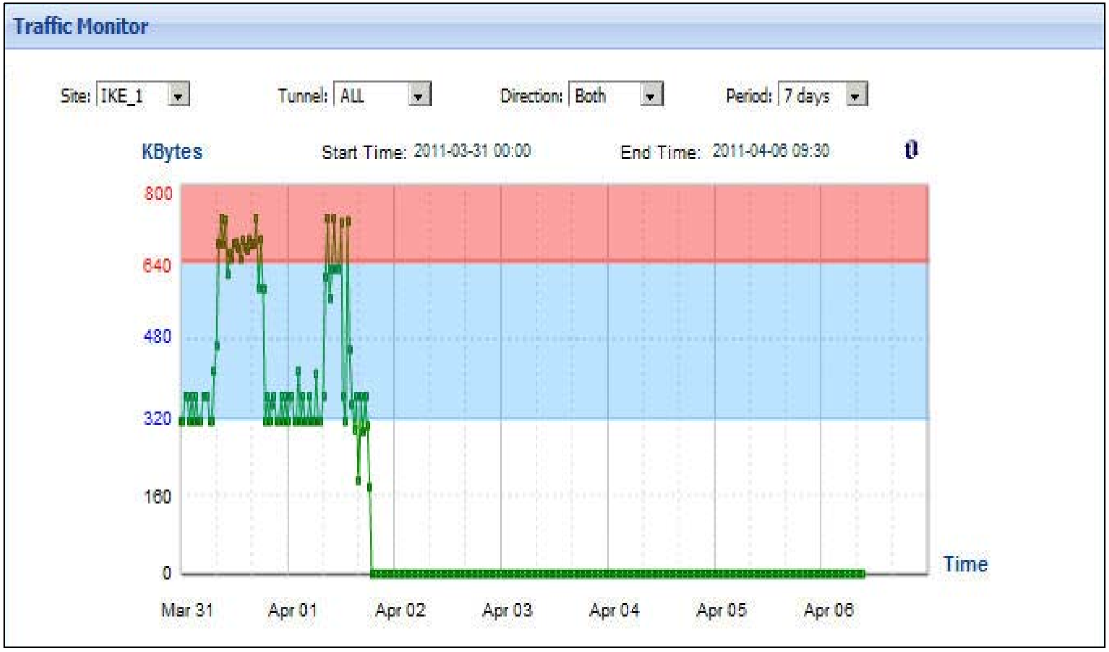
LABEL	DESCRIPTION
Site	This column displays the names of peer IPSec routers. Each IPSec router is identified by the name of the phase 1 IKE SA (also known as the gateway policy). A site's status icon is green when all of the configured Secure Remote Access tunnels between the device and the peer IPSec router are connected. A site's status icon is yellow when some of the configured Secure Remote Access tunnels between the device and the peer IPSec router are connected. A site's status icon is red when none of the configured Secure Remote Access tunnels between the device and the peer IPSec router are connected.
Tunnel	This column displays the names of the device's Secure Remote Access tunnels. A tunnel's status icon is green when the Secure Remote Access tunnel is connected. A tunnel's status icon is red when the Secure Remote Access tunnel is not connected.
Total Count	This field displays how many sites are recorded.
Total Page	This field displays how many screens it takes to display all the sites.
First .. Last	Click **First**, **Last**, or a specific page number to look at the sites on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click **Go**.

6.1.2 Secure Remote Access Traffic Monitor

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

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

Figure 90 Report > Secure Remote Access > Site-to-Site (IPSec) > Traffic Monitor



Traffic Monitor

Site: IKE_1 Tunnel: ALL Direction: Both Period: 7 days

Start Time: 2011-03-31 00:00 End Time: 2011-04-06 09:30

Each field is described in the following table.

Table 78 Report > Secure Remote Access > Site-to-Site (IPSec) > Traffic Monitor

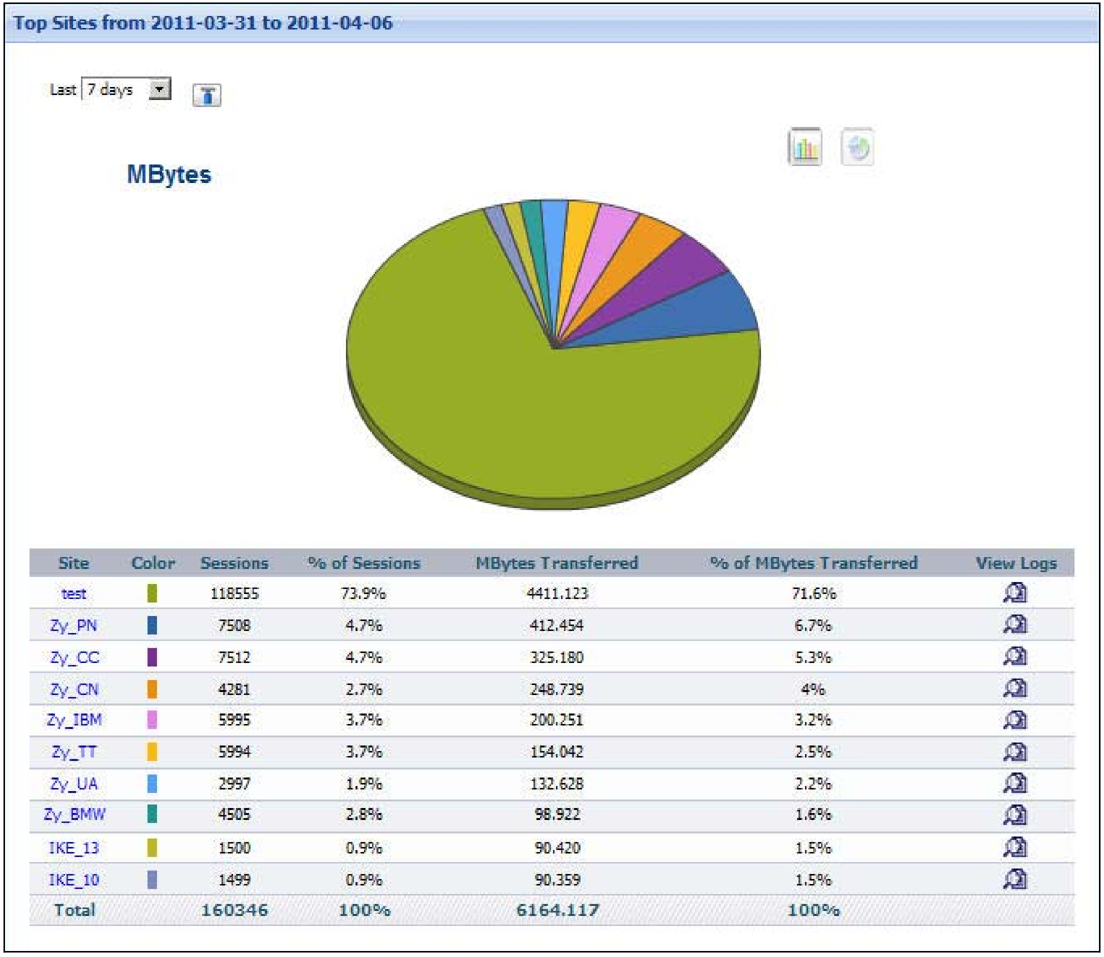
LABEL	DESCRIPTION
Site	Select a peer IPSec router.
Tunnel	Select a Secure Remote Access tunnel. Select **All** to display the total traffic for the device’s Secure Remote Access tunnels with the selected site.
Direction	Select which direction of traffic, you want to view statistics. **Both** - all Secure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

6.1.3 Top Secure Remote Access Sites

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

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

Figure 91 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Sites



Top Sites from 2011-03-31 to 2011-04-06

Last 7 days

MBytes

Site	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
test	🟩	118555	73.9%	4411.123	71.6%	🔍
Zy_PN	🟦	7508	4.7%	412.454	6.7%	🔍
Zy_CC	🟪	7512	4.7%	325.180	5.3%	🔍
Zy_CN	🟧	4281	2.7%	248.739	4%	🔍
Zy_IBM	🟪	5995	3.7%	200.251	3.2%	🔍
Zy_TT	🟨	5994	3.7%	154.042	2.5%	🔍
Zy_UA	🟦	2997	1.9%	132.628	2.2%	🔍
Zy_BMW	🟩	4505	2.8%	98.922	1.6%	🔍
IKE_13	🟨	1500	0.9%	90.420	1.5%	🔍
IKE_10	🟦	1499	0.9%	90.359	1.5%	🔍
Total		160346	100%	6164.117	100%	

Each field is described in the following table.

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

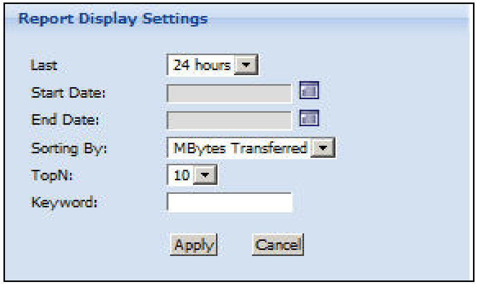
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the peer IPSec routers with the most Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of peer IPSec routers is less than the maximum number of records displayed in this table, every peer IPSec router is displayed. Each peer IPSec router is identified by the name of the phase 1 IKE SA (also known as the gateway policy). Click on a name to look at the top sources of Secure Remote Access traffic for the selected site.
Color	This field displays what color represents each site in the graph.
Sessions	This field displays the number of traffic events for each site.
% of Sessions	This field displays what percentage each site's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.

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

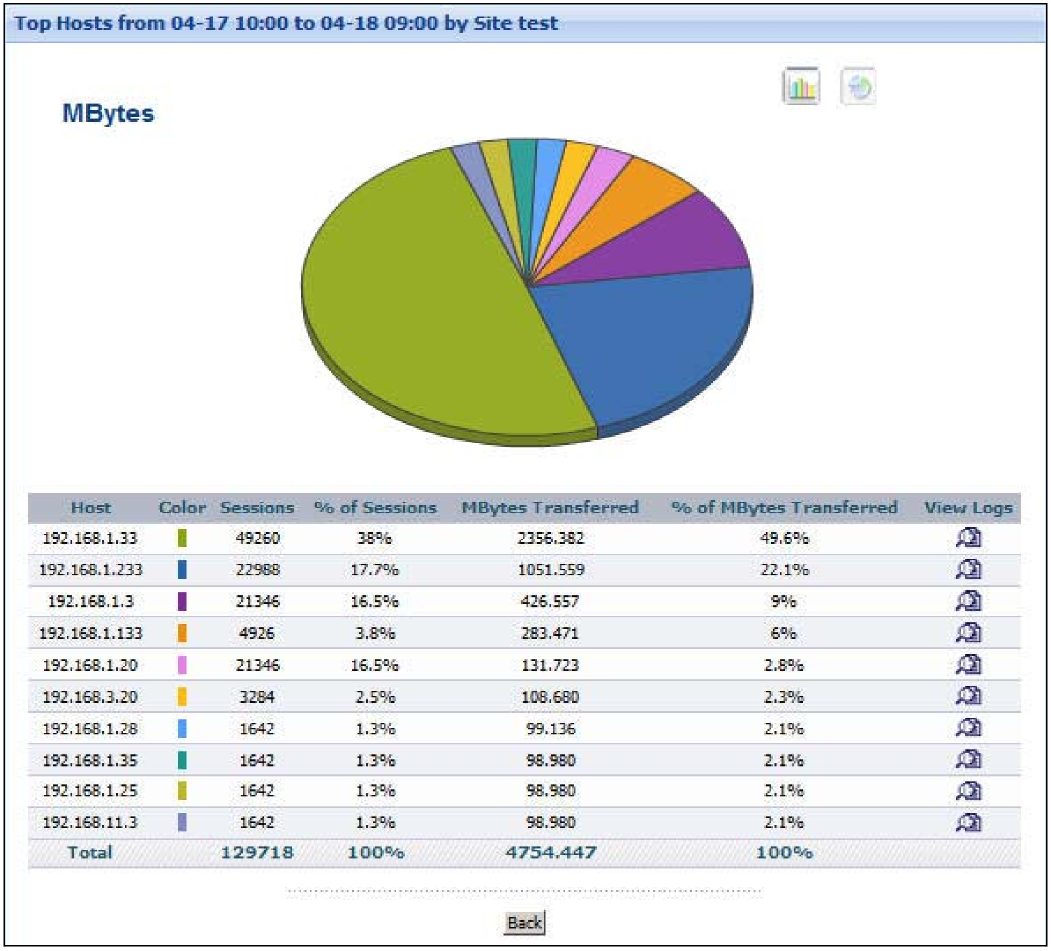
LABEL	DESCRIPTION
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each site.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each site.
View Logs	Click this icon to see the logs that go with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

6.1.4 Top Secure Remote Access Sites Drill-Down

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

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

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



Top Hosts from 04-17 10:00 to 04-18 09:00 by Site test

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	🟩	49260	38%	2356.382	49.6%	🔍
192.168.1.233	🟦	22988	17.7%	1051.559	22.1%	🔍
192.168.1.3	🟪	21346	16.5%	426.557	9%	🔍
192.168.1.133	🟧	4926	3.8%	283.471	6%	🔍
192.168.1.20	🟪	21346	16.5%	131.723	2.8%	🔍
192.168.3.20	🟨	3284	2.5%	108.680	2.3%	🔍
192.168.1.28	🟦	1642	1.3%	99.136	2.1%	🔍
192.168.1.35	🟩	1642	1.3%	98.980	2.1%	🔍
192.168.1.25	🟨	1642	1.3%	98.980	2.1%	🔍
192.168.11.3	🟪	1642	1.3%	98.980	2.1%	🔍
Total		129718	100%	4754.447	100%	

Back

Each field is described in the following table.

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

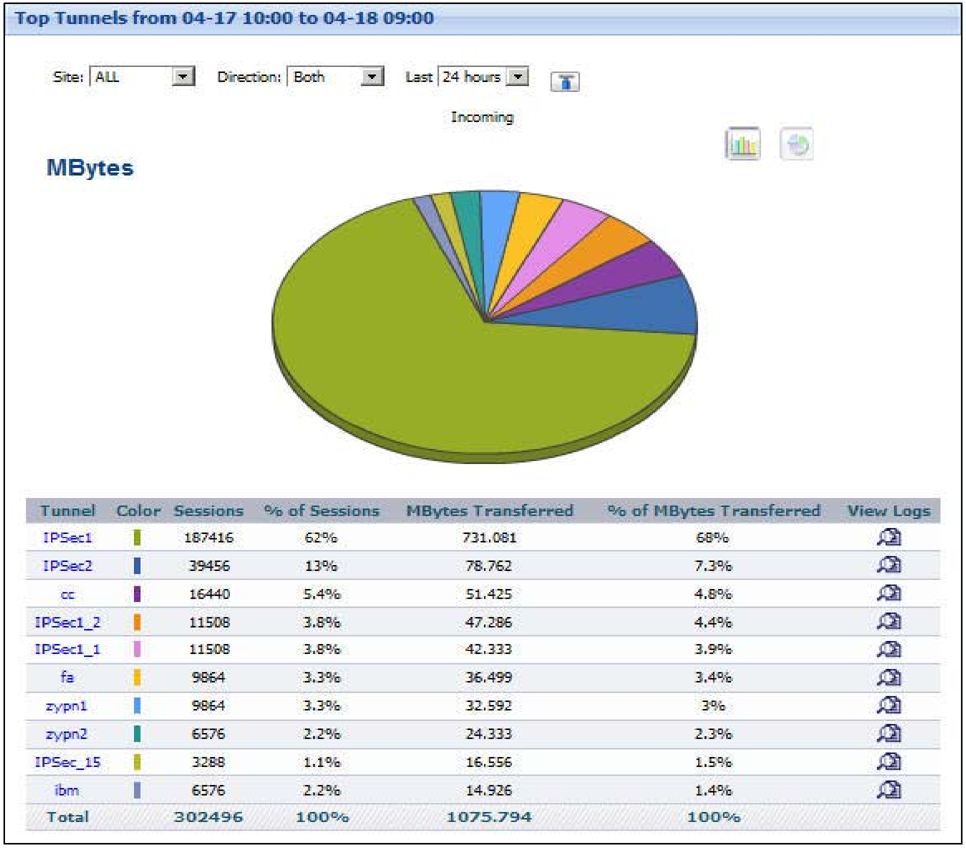
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.1.5 Top Secure Remote Access Tunnels

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

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

Figure 93 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Tunnels



Top Tunnels from 04-17 10:00 to 04-18 09:00

Site: ALL Direction: Both Last 24 hours

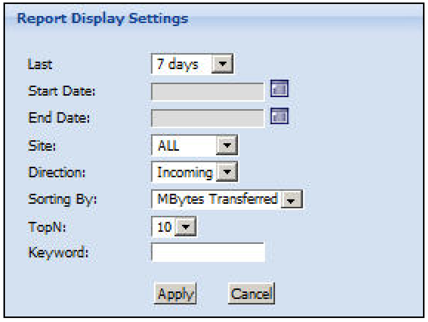
Tunnel	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
IPSec1	▮	187416	62%	731.081	68%	🔍
IPSec2	▮	39456	13%	78.762	7.3%	🔍
cc	▮	16440	5.4%	51.425	4.8%	🔍
IPSec1_2	▮	11508	3.8%	47.286	4.4%	🔍
IPSec1_1	▮	11508	3.8%	42.333	3.9%	🔍
fa	▮	9864	3.3%	36.499	3.4%	🔍
zypn1	▮	9864	3.3%	32.592	3%	🔍
zypn2	▮	6576	2.2%	24.333	2.3%	🔍
IPSec_15	▮	3288	1.1%	16.556	1.5%	🔍
ibm	▮	6576	2.2%	14.926	1.4%	🔍
Total		302496	100%	1075.794	100%	

Each field is described in the following table.

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

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

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

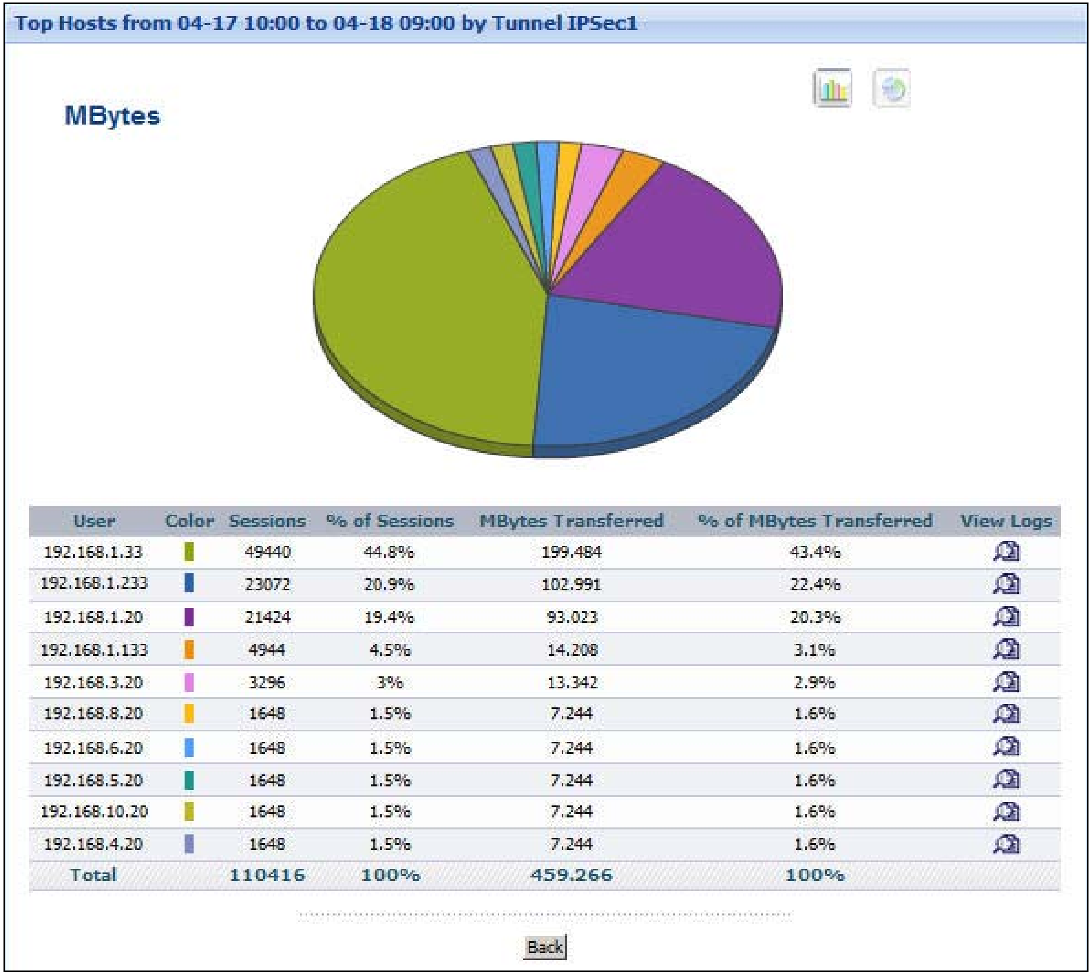
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Site: ALL Direction: Incoming Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Site** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Tunnel** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Tunnel	This field displays the phase 2 IPSec tunnels with the most Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of tunnels is less than the maximum number of records displayed in this table, every tunnel is displayed. Each tunnel is identified by the name of the phase 2 IPSec SA (also known as the network policy). Click on a name to look at the top sources of Secure Remote Access traffic for the selected tunnel.
Color	This field displays what color represents each tunnel in the graph.
Sessions	This field displays the number of traffic events for each tunnel.
% of Sessions	This field displays what percentage each tunnel’s number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each tunnel.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each tunnel.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.1.6 Top Secure Remote Access Tunnels Drill-Down

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

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

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



Top Hosts from 04-17 10:00 to 04-18 09:00 by Tunnel IPSec1

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	■	49440	44.8%	199.484	43.4%	🔍
192.168.1.233	■	23072	20.9%	102.991	22.4%	🔍
192.168.1.20	■	21424	19.4%	93.023	20.3%	🔍
192.168.1.133	■	4944	4.5%	14.208	3.1%	🔍
192.168.3.20	■	3296	3%	13.342	2.9%	🔍
192.168.8.20	■	1648	1.5%	7.244	1.6%	🔍
192.168.6.20	■	1648	1.5%	7.244	1.6%	🔍
192.168.5.20	■	1648	1.5%	7.244	1.6%	🔍
192.168.10.20	■	1648	1.5%	7.244	1.6%	🔍
192.168.4.20	■	1648	1.5%	7.244	1.6%	🔍
Total		110416	100%	459.266	100%	

Each field is described in the following table.

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

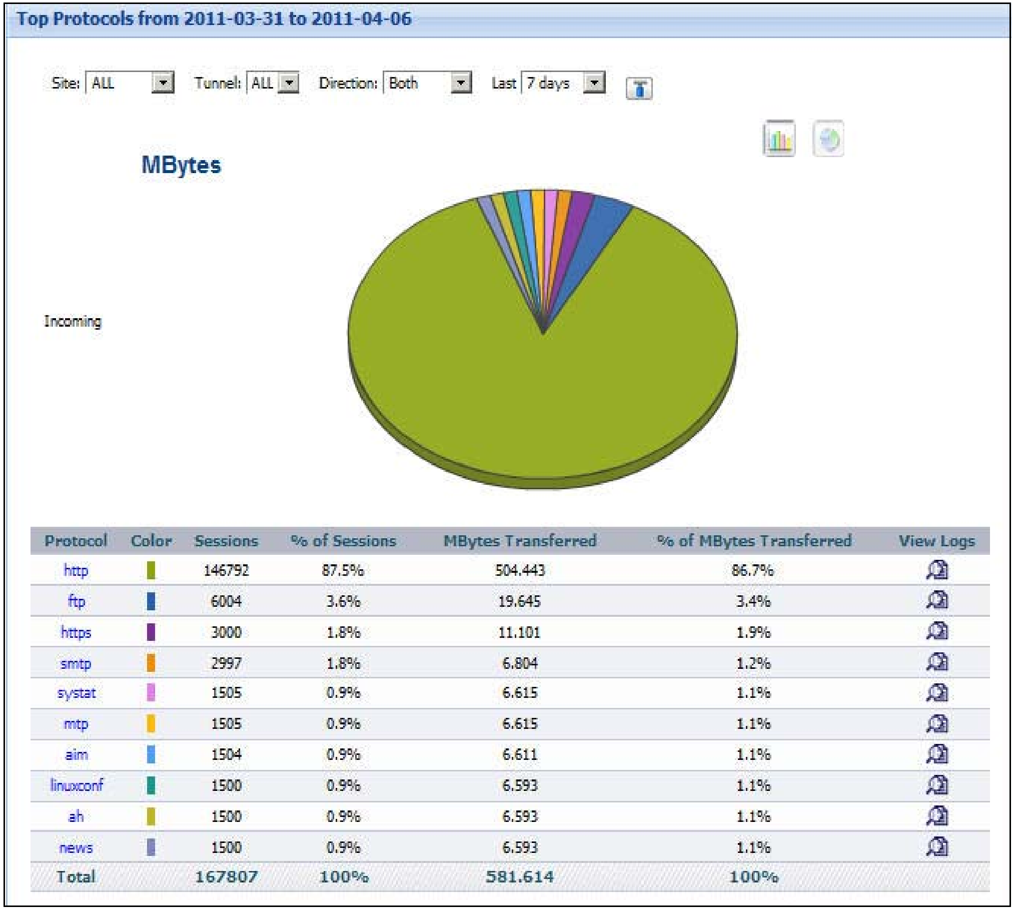
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.1.7 Top Secure Remote Access Protocols

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

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

Figure 95 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Protocols



Top Protocols from 2011-03-31 to 2011-04-06

Site: ALL Tunnel: ALL Direction: Both Last 7 days

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
http	■	146792	87.5%	504.443	86.7%	🔍
ftp	■	6004	3.6%	19.645	3.4%	🔍
https	■	3000	1.8%	11.101	1.9%	🔍
smtp	■	2997	1.8%	6.804	1.2%	🔍
systat	■	1505	0.9%	6.615	1.1%	🔍
mtp	■	1505	0.9%	6.615	1.1%	🔍
aim	■	1504	0.9%	6.611	1.1%	🔍
linuxconf	■	1500	0.9%	6.593	1.1%	🔍
ah	■	1500	0.9%	6.593	1.1%	🔍
news	■	1500	0.9%	6.593	1.1%	🔍
Total		167807	100%	581.614	100%	

Each field is described in the following table.

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

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

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

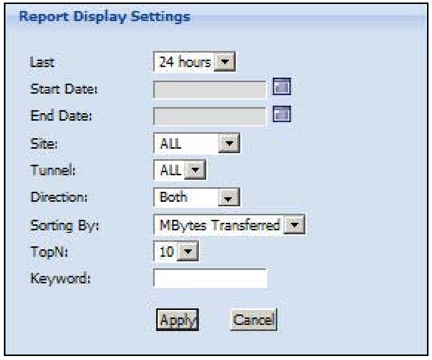
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Site: ALL Tunnel: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Protocol** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most used by Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through Secure Remote Access.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.

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

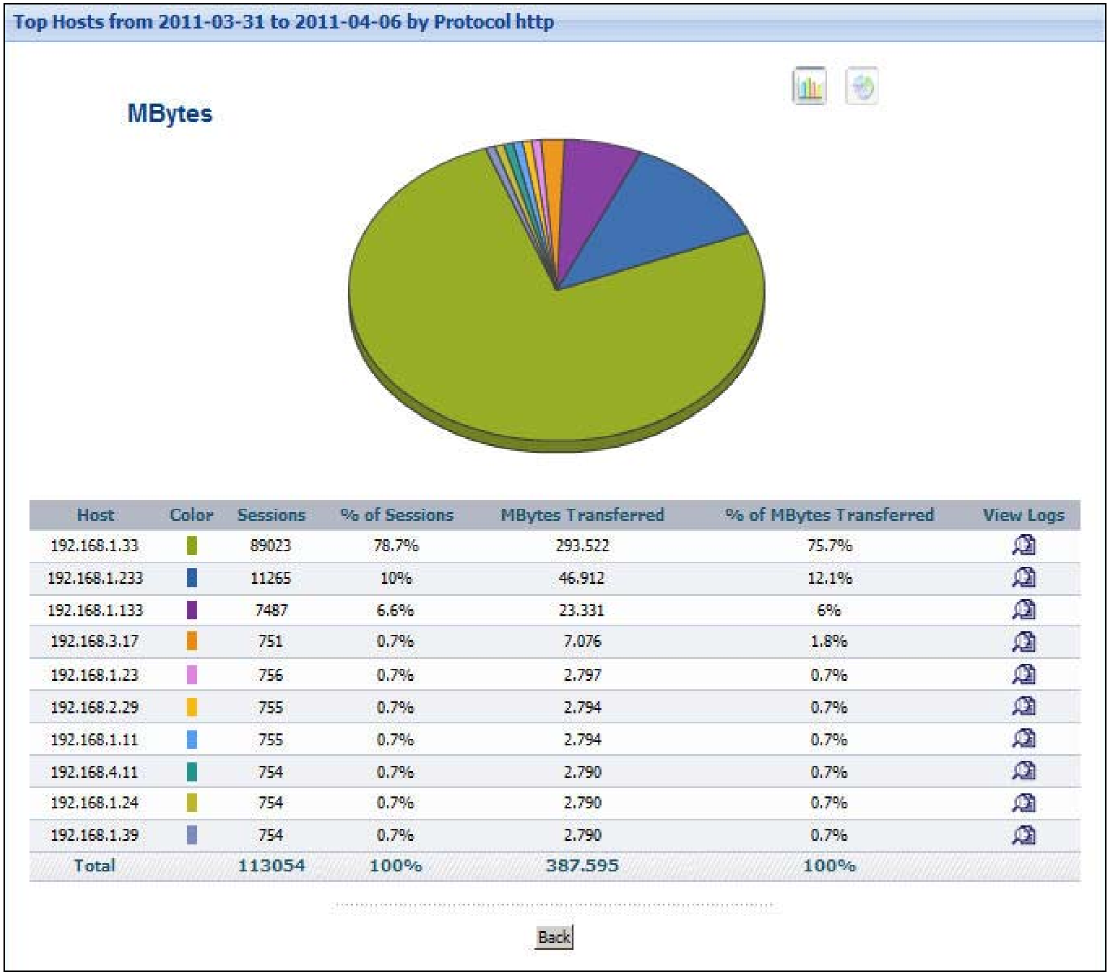
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled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

6.1.8 Top Secure Remote Access Protocols Drill-Down

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

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

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



Top Hosts from 2011-03-31 to 2011-04-06 by Protocol http

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	🟩	89023	78.7%	293.522	75.7%	🔍
192.168.1.233	🟦	11265	10%	46.912	12.1%	🔍
192.168.1.133	🟪	7487	6.6%	23.331	6%	🔍
192.168.3.17	🟧	751	0.7%	7.076	1.8%	🔍
192.168.1.23	🟪	756	0.7%	2.797	0.7%	🔍
192.168.2.29	🟨	755	0.7%	2.794	0.7%	🔍
192.168.1.11	🟦	755	0.7%	2.794	0.7%	🔍
192.168.4.11	🟩	754	0.7%	2.790	0.7%	🔍
192.168.1.24	🟨	754	0.7%	2.790	0.7%	🔍
192.168.1.39	🟦	754	0.7%	2.790	0.7%	🔍
Total		113054	100%	387.595	100%	

Each field is described in the following table.

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

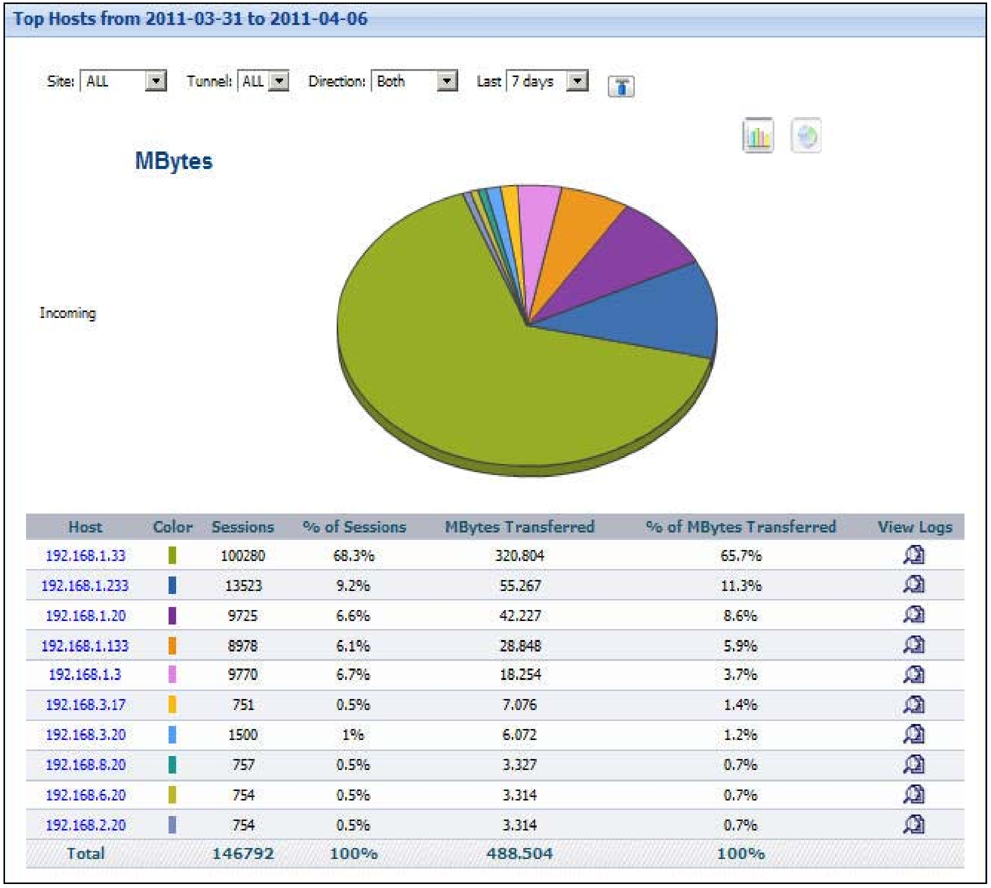
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.1.9 Top Secure Remote Access Hosts

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

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

Figure 97 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Hosts



Top Hosts from 2011-03-31 to 2011-04-06

Site: ALL Tunnel: ALL Direction: Both Last 7 days

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.33	■	100280	68.3%	320.804	65.7%	🔍
192.168.1.233	■	13523	9.2%	55.267	11.3%	🔍
192.168.1.20	■	9725	6.6%	42.227	8.6%	🔍
192.168.1.133	■	8978	6.1%	28.848	5.9%	🔍
192.168.1.3	■	9770	6.7%	18.254	3.7%	🔍
192.168.3.17	■	751	0.5%	7.076	1.4%	🔍
192.168.3.20	■	1500	1%	6.072	1.2%	🔍
192.168.8.20	■	757	0.5%	3.327	0.7%	🔍
192.168.6.20	■	754	0.5%	3.314	0.7%	🔍
192.168.2.20	■	754	0.5%	3.314	0.7%	🔍
Total		146792	100%	488.504	100%	

Each field is described in the following table.

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

LABEL	DESCRIPTION
Site	Select a peer IPSec router. Select **All** to display the device’s Secure Remote Access tunnels with the most traffic, regardless of which peer IPSec router they use. This field is not available with all models.
Tunnel	Select a Secure Remote Access tunnel. Select **All** to display the total traffic for the device’s Secure Remote Access tunnels with the selected site (or all sites). This field is not available with all models.
Direction	Select which direction of traffic, you want to view statistics. This field is not available with all models. **Both** - all Secure Remote Access traffic the devices sent or received. **Incoming** - all traffic the devices received through Secure Remote Access tunnel. **Outgoing** - all traffic the devices sent out through Secure Remote Access tunnel.

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

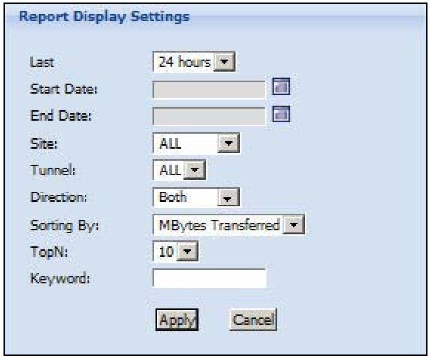
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Site: ALL Tunnel: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top senders or receivers of Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of hosts is less than the maximum number of records displayed in this table, every host is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a host to look at the top protocols of Secure Remote Access traffic for the selected host.
Color	This field displays what color represents each host in the graph.

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

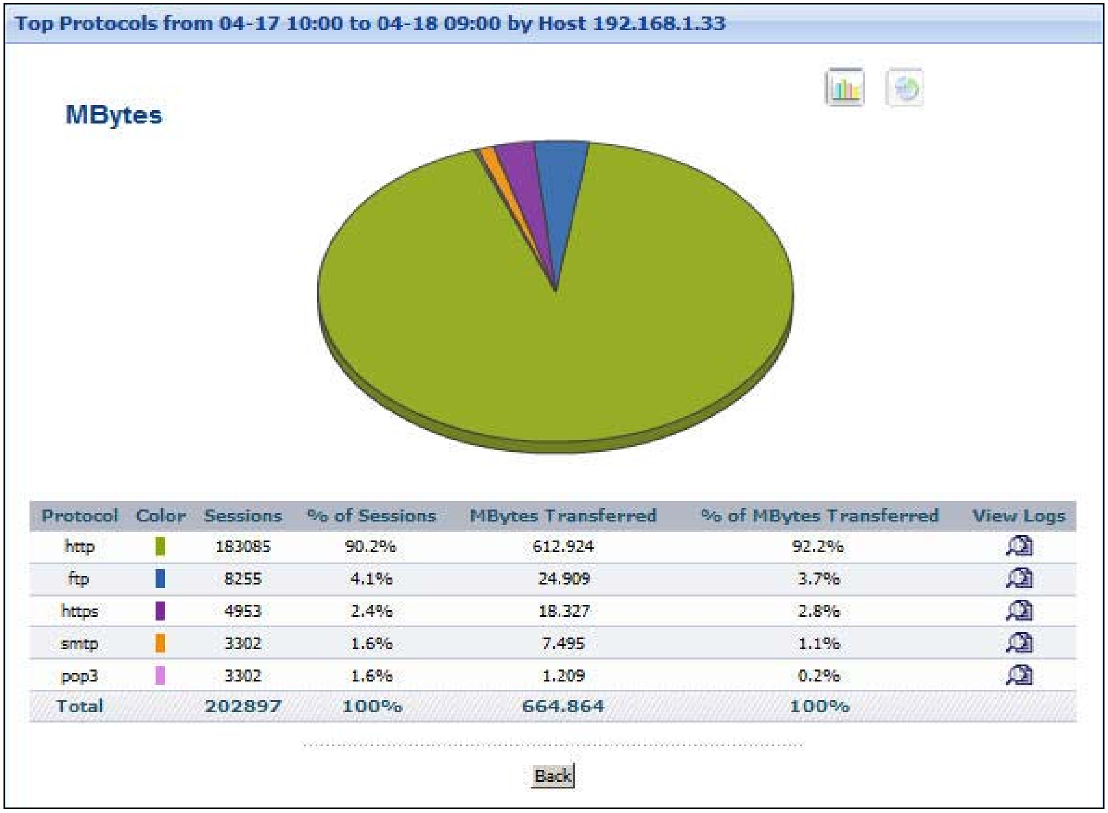
LABEL	DESCRIPTION
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This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

6.1.10 Top Secure Remote Access Hosts Drill-Down

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

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

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



Top Protocols from 04-17 10:00 to 04-18 09:00 by Host 192.168.1.33

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
http	🟩	183085	90.2%	612.924	92.2%	🔍
ftp	🟦	8255	4.1%	24.909	3.7%	🔍
https	🟪	4953	2.4%	18.327	2.8%	🔍
smtp	🟧	3302	1.6%	7.495	1.1%	🔍
pop3	🟪	3302	1.6%	1.209	0.2%	🔍
Total		202897	100%	664.864	100%	

Each field is described in the following table.

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

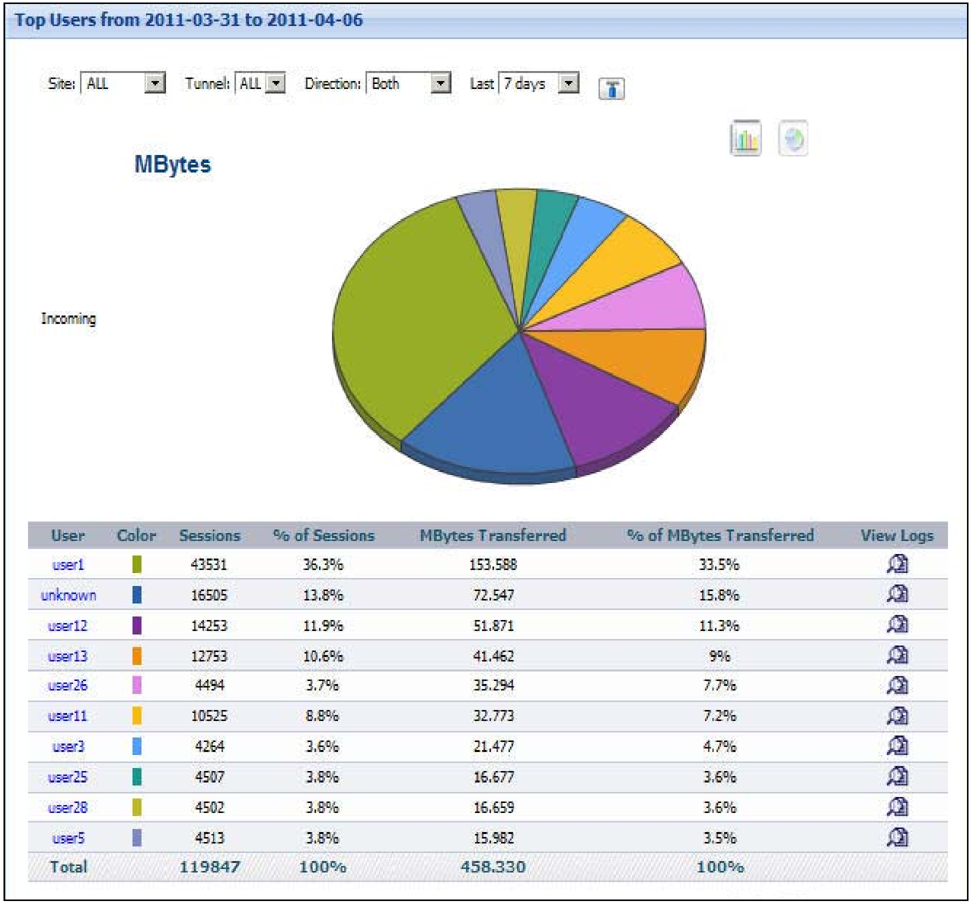
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.1.11 Top Secure Remote Access Users

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

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

Figure 99 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Users



Top Users from 2011-03-31 to 2011-04-06

Site: ALL Tunnel: ALL Direction: Both Last 7 days

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
user1	🟩	43531	36.3%	153.588	33.5%	🔍
unknown	🟦	16505	13.8%	72.547	15.8%	🔍
user12	🟪	14253	11.9%	51.871	11.3%	🔍
user13	🟧	12753	10.6%	41.462	9%	🔍
user26	🟪	4494	3.7%	35.294	7.7%	🔍
user11	🟨	10525	8.8%	32.773	7.2%	🔍
user3	🟦	4264	3.6%	21.477	4.7%	🔍
user25	🟩	4507	3.8%	16.677	3.6%	🔍
user28	🟨	4502	3.8%	16.659	3.6%	🔍
user5	🟦	4513	3.8%	15.982	3.5%	🔍
Total		119847	100%	458.330	100%	

Each field is described in the following table.

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

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

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

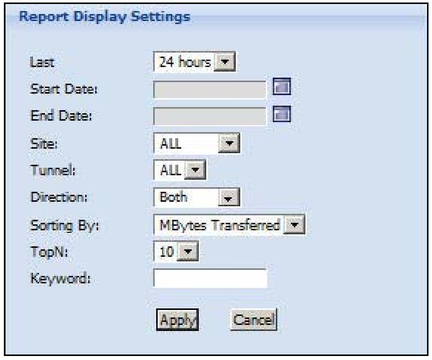
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Site: ALL Tunnel: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top senders or receivers of Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user to look at where the user sent the most Secure Remote Access traffic.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.

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

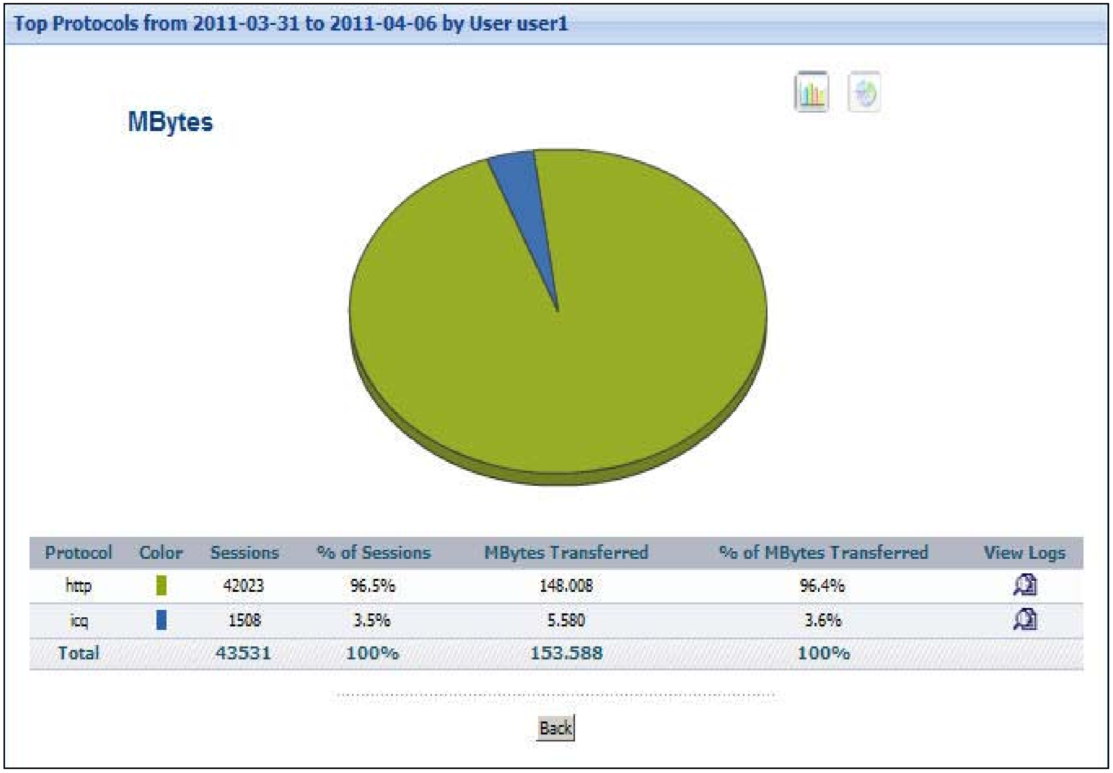
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for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

6.1.12 Top Secure Remote Access Users Drill-Down

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

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

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



Top Protocols from 2011-03-31 to 2011-04-06 by User user1

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
http	🟩	42023	96.5%	148.008	96.4%	🔍
icq	🟦	1508	3.5%	5.580	3.6%	🔍
Total		43531	100%	153.588	100%	

Each field is described in the following table.

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

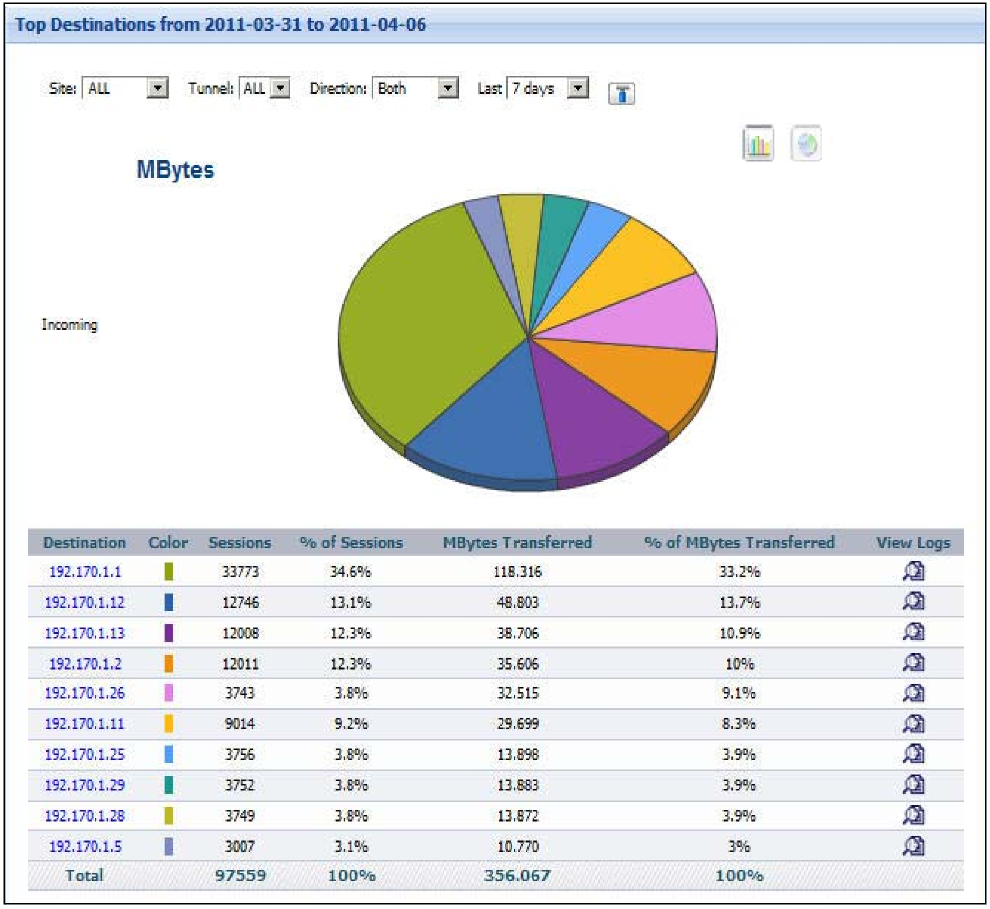
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.1.13 Top Secure Remote Access Destinations

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

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

Figure 101 Report > Secure Remote Access > Site-to-Site (IPSec) > Top Destinations



Top Destinations from 2011-03-31 to 2011-04-06

Site: ALL Tunnel: ALL Direction: Both Last 7 days

Destination	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.1	🟩	33773	34.6%	118.316	33.2%	🔍
192.170.1.12	🟦	12746	13.1%	48.803	13.7%	🔍
192.170.1.13	🟪	12008	12.3%	38.706	10.9%	🔍
192.170.1.2	🟧	12011	12.3%	35.606	10%	🔍
192.170.1.26	🟪	3743	3.8%	32.515	9.1%	🔍
192.170.1.11	🟨	9014	9.2%	29.699	8.3%	🔍
192.170.1.25	🟦	3756	3.8%	13.898	3.9%	🔍
192.170.1.29	🟩	3752	3.8%	13.883	3.9%	🔍
192.170.1.28	🟨	3749	3.8%	13.872	3.9%	🔍
192.170.1.5	🟦	3007	3.1%	10.770	3%	🔍
Total		97559	100%	356.067	100%	

Each field is described in the following table.

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

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

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

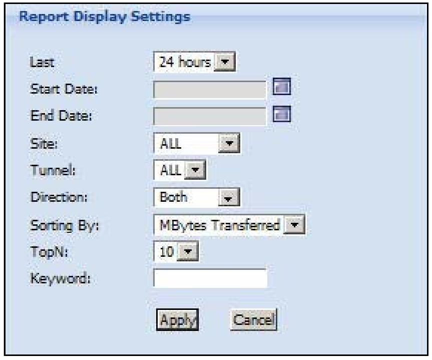
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 24 hours Start Date: End Date: Site: ALL Tunnel: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Site**, **Tunnel** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the where the device sent the most Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the sender hosts that sent the most Secure Remote Access traffic to the selected host.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.

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

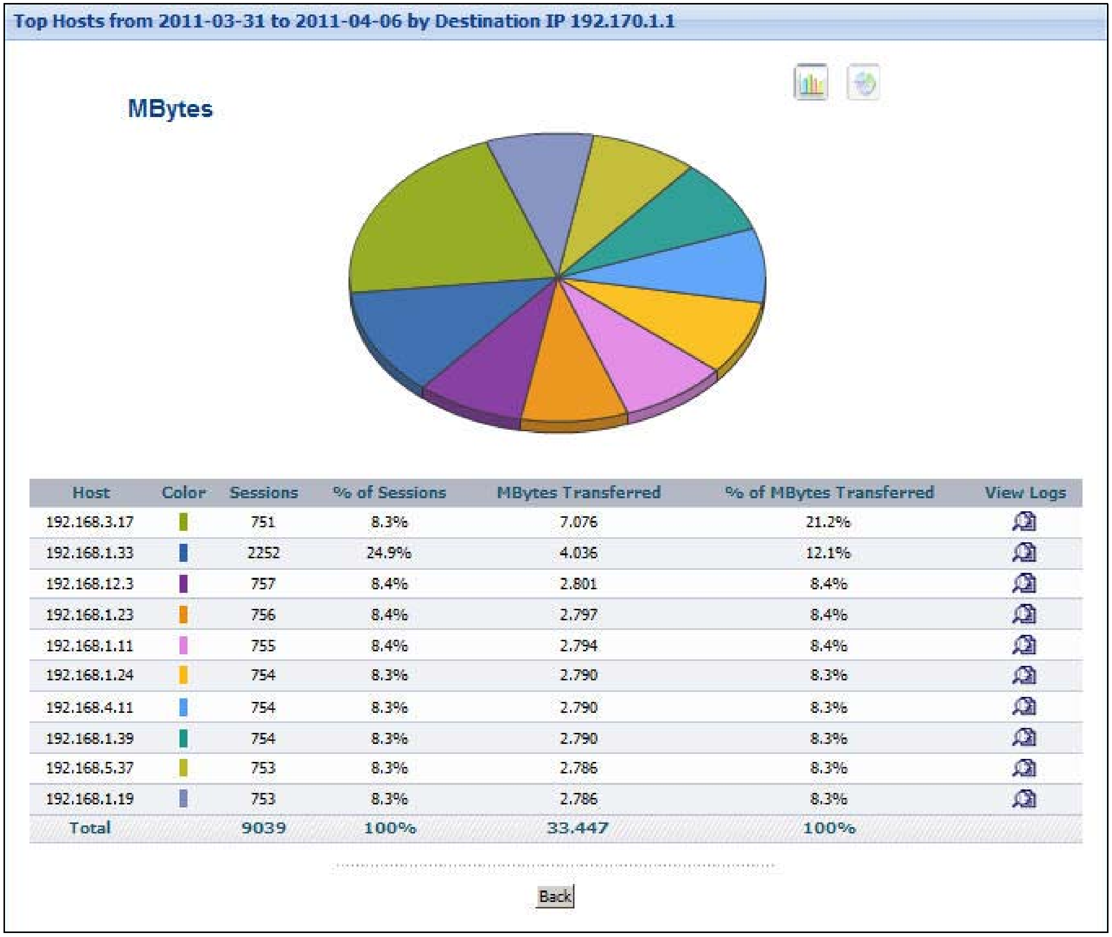
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled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

6.1.14 Top Secure Remote Access Destinations Drill-Down

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

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

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



Top Hosts from 2011-03-31 to 2011-04-06 by Destination IP 192.170.1.1

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.3.17	🟩	751	8.3%	7.076	21.2%	🔍
192.168.1.33	🟦	2252	24.9%	4.036	12.1%	🔍
192.168.12.3	🟪	757	8.4%	2.801	8.4%	🔍
192.168.1.23	🟧	756	8.4%	2.797	8.4%	🔍
192.168.1.11	🟪	755	8.4%	2.794	8.4%	🔍
192.168.1.24	🟨	754	8.3%	2.790	8.3%	🔍
192.168.4.11	🟦	754	8.3%	2.790	8.3%	🔍
192.168.1.39	🟩	754	8.3%	2.790	8.3%	🔍
192.168.5.37	🟨	753	8.3%	2.786	8.3%	🔍
192.168.1.19	🟪	753	8.3%	2.786	8.3%	🔍
Total		9039	100%	33.447	100%	

Each field is described in the following table.

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

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

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

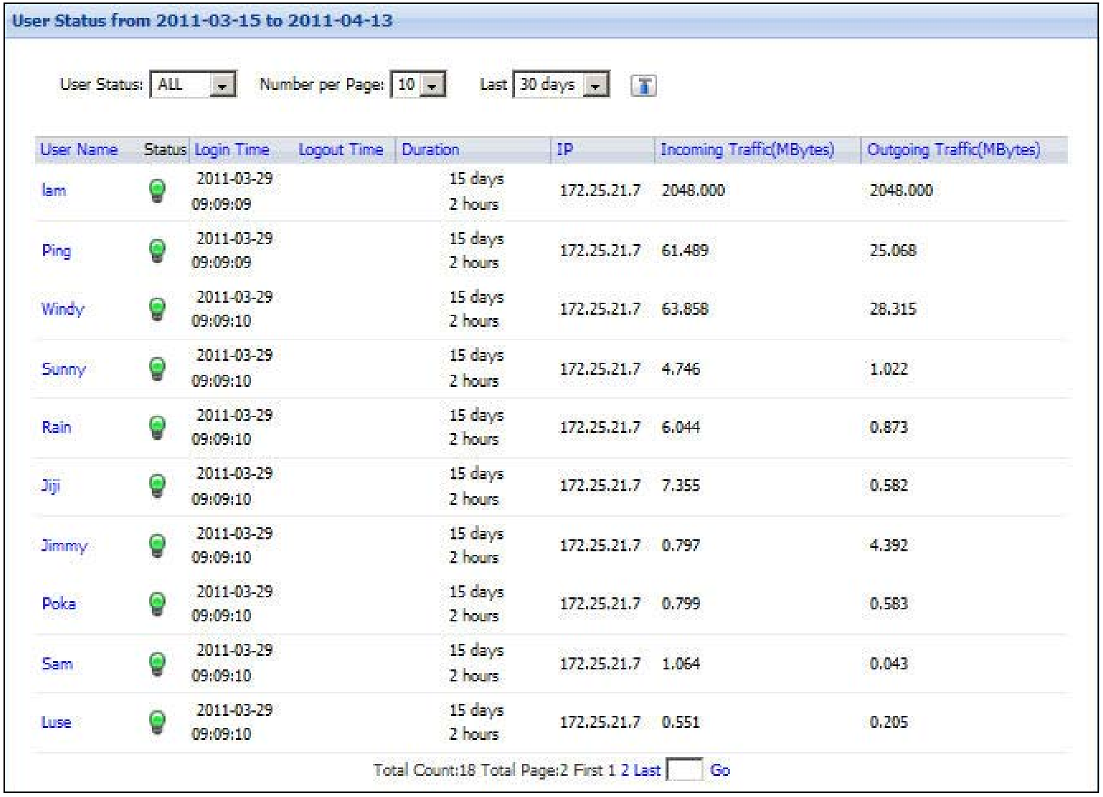
Secure Remote Access tunnels with the remote gateway set as any are called dynamic tunnels (only the remote device can initiate a dynamic IPSec Secure Remote Access tunnel). Devices can use xauth to authenticate remote users (by username and password) when they try to initiate a dynamic Secure Remote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

6.2.1 Secure Remote Access User Status

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

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

Figure 103 Report > Secure Remote Access > Client-to-Site (IPSec) > User Status



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

User Status: ALL   Number per Page: 10   Last 30 days

User Name	Status	Login Time	Logout Time	Duration	IP	Incoming Traffic(MBytes)	Outgoing Traffic(MBytes)
lam	●	2011-03-29 09:09:09		15 days 2 hours	172.25.21.7	2048.000	2048.000
Ping	●	2011-03-29 09:09:09		15 days 2 hours	172.25.21.7	61.489	25.068
Windy	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	63.858	28.315
Sunny	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	4.746	1.022
Rain	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	6.044	0.873
Jiji	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	7.355	0.582
Jimmy	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	0.797	4.392
Poka	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	0.799	0.583
Sam	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	1.064	0.043
Luse	●	2011-03-29 09:09:10		15 days 2 hours	172.25.21.7	0.551	0.205

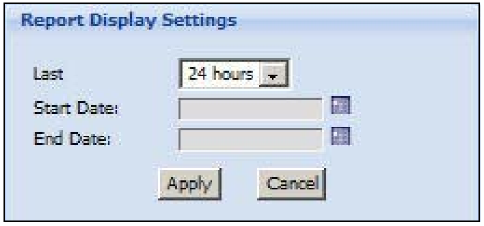
Total Count:18 Total Page:2 First 1 2 Last Go

Each field is described in the following table.

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

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

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

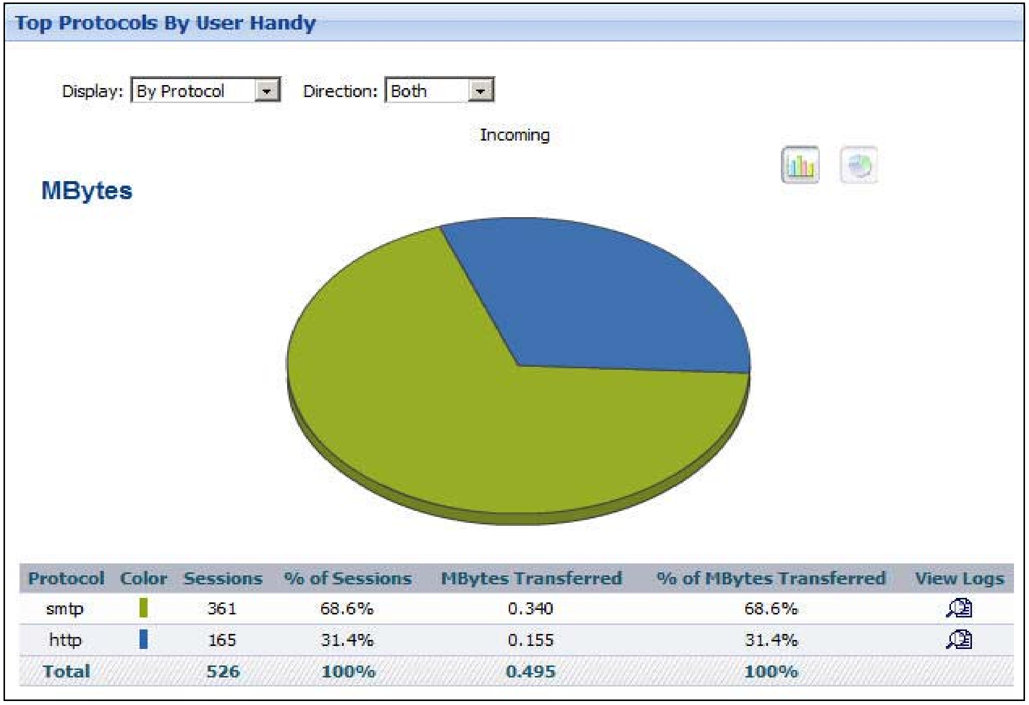
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 24 hours Start Date: End Date: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
User Name	This field displays the top remote access senders or receivers of Secure Remote Access traffic in the selected device. Click the title of this column to sort the list of users in alphabetical or reverse-alphabetical order. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Status	This column displays the current status of users who have logged in. A user’s status icon is green when the user is currently connected. A user’s status icon is red when the user has already logged out.
Login Time	This column displays when the remote access user last logged in. Click the title of this column to sort the list of users by the time they last logged in.
Logout Time	This column displays when the remote access user last logged out. The field is empty if the remote access user is still logged in. Click the title of this column to sort the list of users by the time they last logged out.
Duration	This field displays current length (duration) of the login if the remote access user is still logged in. Click the title of this column to sort the list of users by how long they have been logged in.
IP	This field displays the user's IP address. Click the title of this column to sort the list of users by IP address.
Incoming Traffic (MBytes)	This field displays the amount of traffic received by the user through the device. Click the title of this column to sort the list of users by the amount of traffic routed through the device.
Outgoing Traffic (MBytes)	This field displays the amount of traffic sent by the user through the device. Click the title of this column to sort the list of users by the amount of traffic routed from the device.
Total	This entry displays the total number of users on each page of the report.

6.2.2 Secure Remote Access User Status Drill-Down

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

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

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



Top Protocols By User Handy

Display: By Protocol

Direction: Both

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
smtp	🟩	361	68.6%	0.340	68.6%	
http	🟦	165	31.4%	0.155	31.4%	
Total		526	100%	0.495	100%	

Each field is described in the following table.

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

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

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

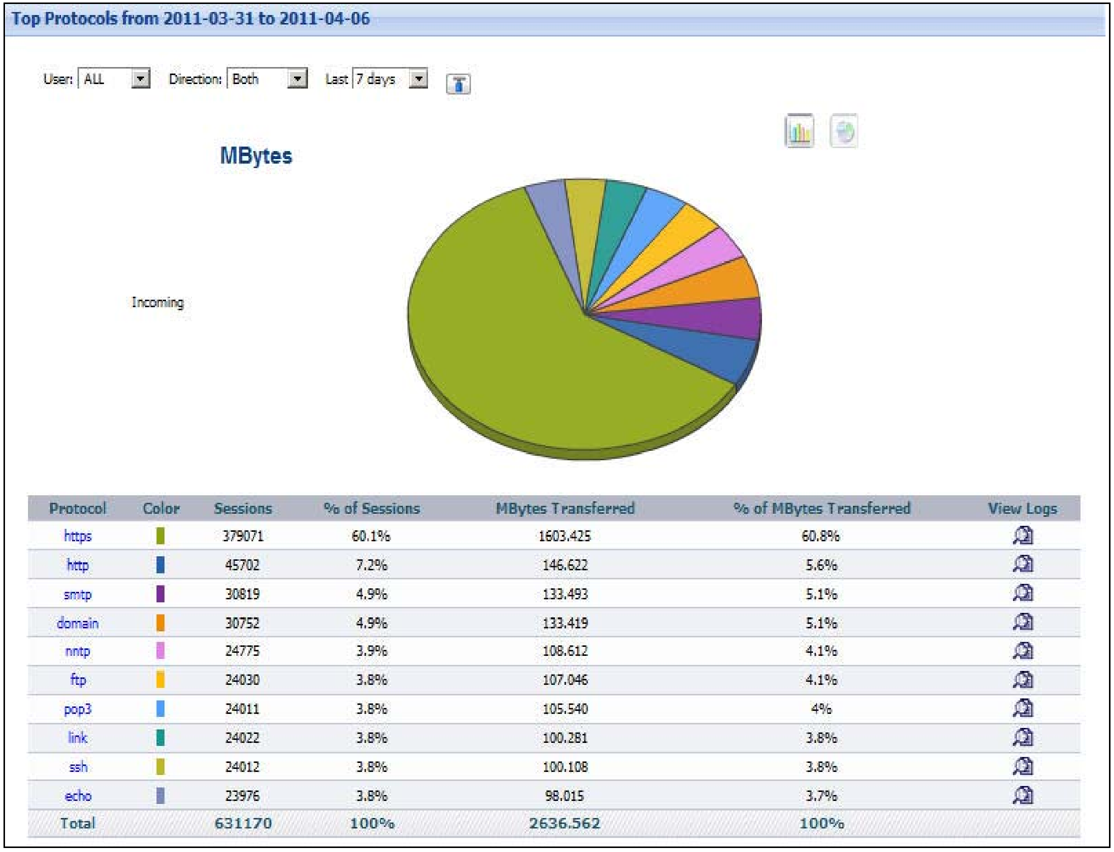
LABEL	DESCRIPTION
Protocol	This field displays the services most used by the selected user, sorted by the amount of traffic for each one. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the **TopN** setting in **Settings**. Each protocol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

6.2.3 Top Secure Remote Access Protocols

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

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

Figure 105 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Protocols



Top Protocols from 2011-03-31 to 2011-04-06

User: ALL Direction: Both Last 7 days

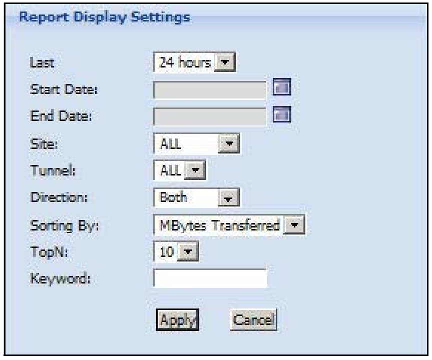
Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
https	🟩	379071	60.1%	1603.425	60.8%	🔍
http	🟦	45702	7.2%	146.622	5.6%	🔍
smtp	🟪	30819	4.9%	133.493	5.1%	🔍
domain	🟧	30752	4.9%	133.419	5.1%	🔍
nntp	🟪	24775	3.9%	108.612	4.1%	🔍
ftp	🟨	24030	3.8%	107.046	4.1%	🔍
pop3	🟦	24011	3.8%	105.540	4%	🔍
link	🟩	24022	3.8%	100.281	3.8%	🔍
ssh	🟨	24012	3.8%	100.108	3.8%	🔍
echo	▨	23976	3.8%	98.015	3.7%	🔍
Total		631170	100%	2636.562	100%	

Each field is described in the following table.

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

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

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

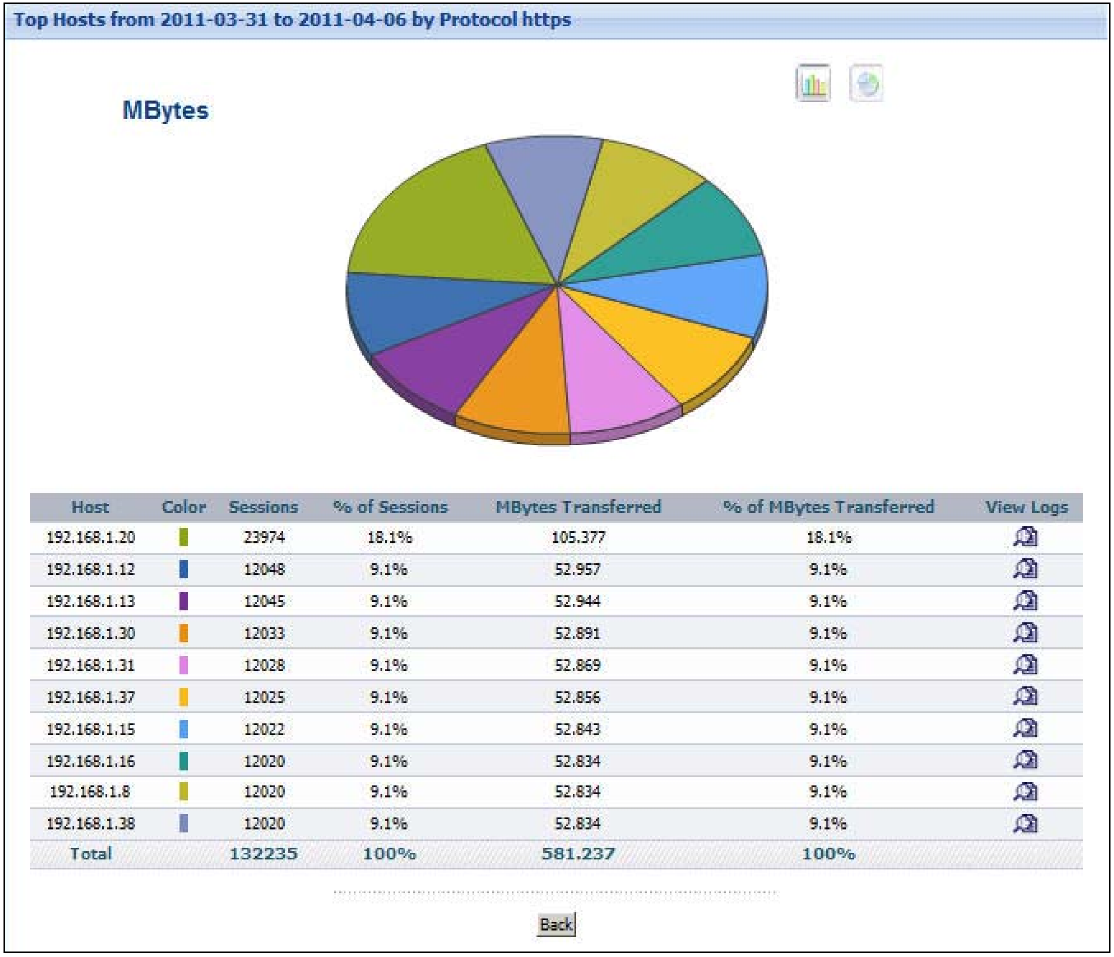
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: Site: ALL Tunnel: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Protocol** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most used by remote access Secure Remote Access traffic in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through Secure Remote Access.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

6.2.4 Top Secure Remote Access Protocols Drill-Down

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

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

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



Top Hosts from 2011-03-31 to 2011-04-06 by Protocol https

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.20	■	23974	18.1%	105.377	18.1%	🔍
192.168.1.12	■	12048	9.1%	52.957	9.1%	🔍
192.168.1.13	■	12045	9.1%	52.944	9.1%	🔍
192.168.1.30	■	12033	9.1%	52.891	9.1%	🔍
192.168.1.31	■	12028	9.1%	52.869	9.1%	🔍
192.168.1.37	■	12025	9.1%	52.856	9.1%	🔍
192.168.1.15	■	12022	9.1%	52.843	9.1%	🔍
192.168.1.16	■	12020	9.1%	52.834	9.1%	🔍
192.168.1.8	■	12020	9.1%	52.834	9.1%	🔍
192.168.1.38	■	12020	9.1%	52.834	9.1%	🔍
Total		132235	100%	581.237	100%	

Each field is described in the following table.

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

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

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

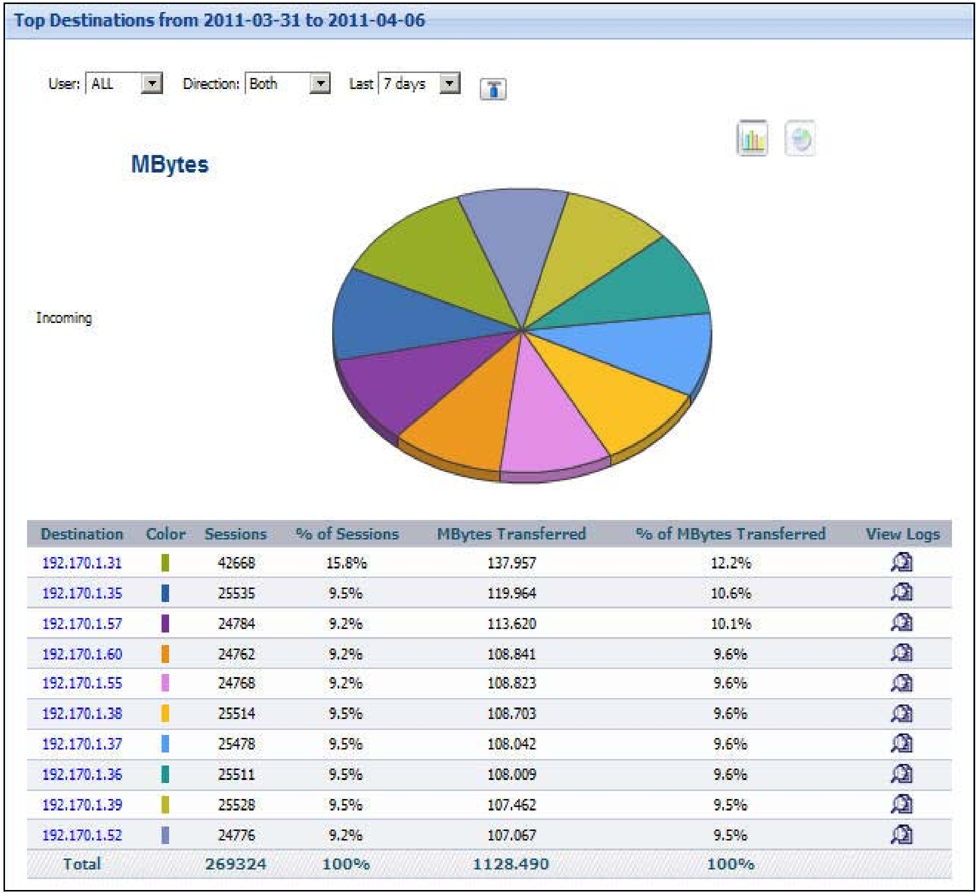
LABEL	DESCRIPTION
Color	This field displays what color represents each host in the graph.
Sessions	This field displays the number of traffic events for each host.
% of Sessions	This field displays what percentage each host's number of traffic events makes out of the total number of traffic events for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

6.2.5 Top Secure Remote Access Destinations

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

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

Figure 107 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Destinations



Top Destinations from 2011-03-31 to 2011-04-06

User: ALL Direction: Both Last 7 days

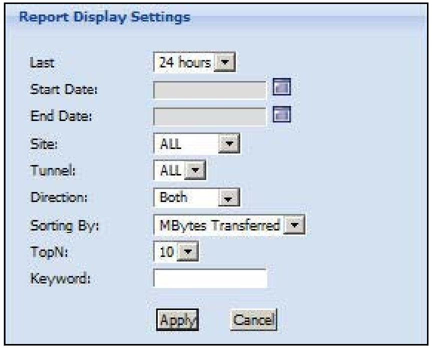
Destination	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.170.1.31	■	42668	15.8%	137.957	12.2%	🔍
192.170.1.35	■	25535	9.5%	119.964	10.6%	🔍
192.170.1.57	■	24784	9.2%	113.620	10.1%	🔍
192.170.1.60	■	24762	9.2%	108.841	9.6%	🔍
192.170.1.55	■	24768	9.2%	108.823	9.6%	🔍
192.170.1.38	■	25514	9.5%	108.703	9.6%	🔍
192.170.1.37	■	25478	9.5%	108.042	9.6%	🔍
192.170.1.36	■	25511	9.5%	108.009	9.6%	🔍
192.170.1.39	■	25528	9.5%	107.462	9.5%	🔍
192.170.1.52	■	24776	9.2%	107.067	9.5%	🔍
Total		269324	100%	1128.490	100%	

Each field is described in the following table.

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

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

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

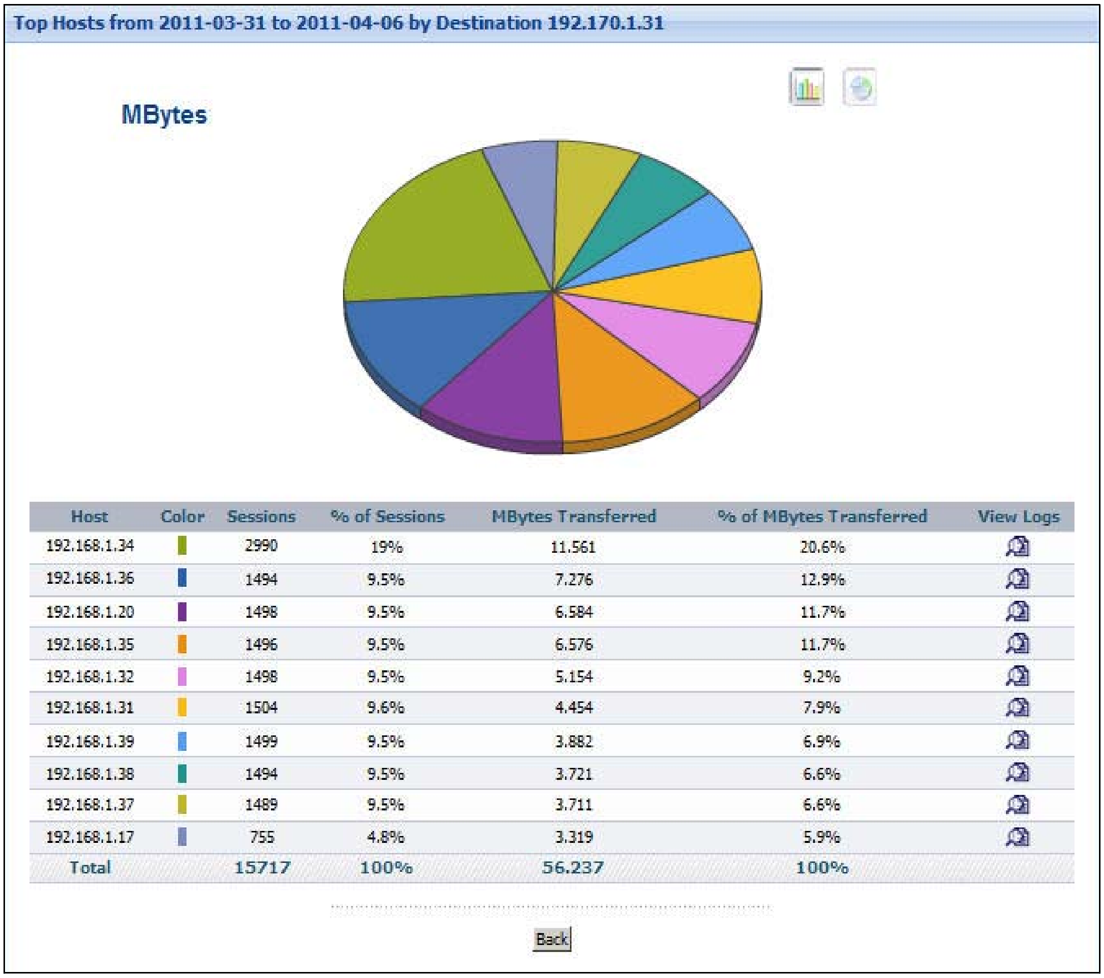
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 24 hours Start Date: End Date: Site: ALL Tunnel: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the IP addresses to which the selected device sent the most remote access Secure Remote Access traffic, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. Click on a destination to look at the sender hosts that send the most Secure Remote Access traffic to the selected host.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.2.6 Top Secure Remote Access Destinations Drill-Down

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

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

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



Top Hosts from 2011-03-31 to 2011-04-06 by Destination 192.170.1.31

Host	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
192.168.1.34	■	2990	19%	11.561	20.6%	🔍
192.168.1.36	■	1494	9.5%	7.276	12.9%	🔍
192.168.1.20	■	1498	9.5%	6.584	11.7%	🔍
192.168.1.35	■	1496	9.5%	6.576	11.7%	🔍
192.168.1.32	■	1498	9.5%	5.154	9.2%	🔍
192.168.1.31	■	1504	9.6%	4.454	7.9%	🔍
192.168.1.39	■	1499	9.5%	3.882	6.9%	🔍
192.168.1.38	■	1494	9.5%	3.721	6.6%	🔍
192.168.1.37	■	1489	9.5%	3.711	6.6%	🔍
192.168.1.17	■	755	4.8%	3.319	5.9%	🔍
Total		15717	100%	56.237	100%	

Each field is described in the following table.

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

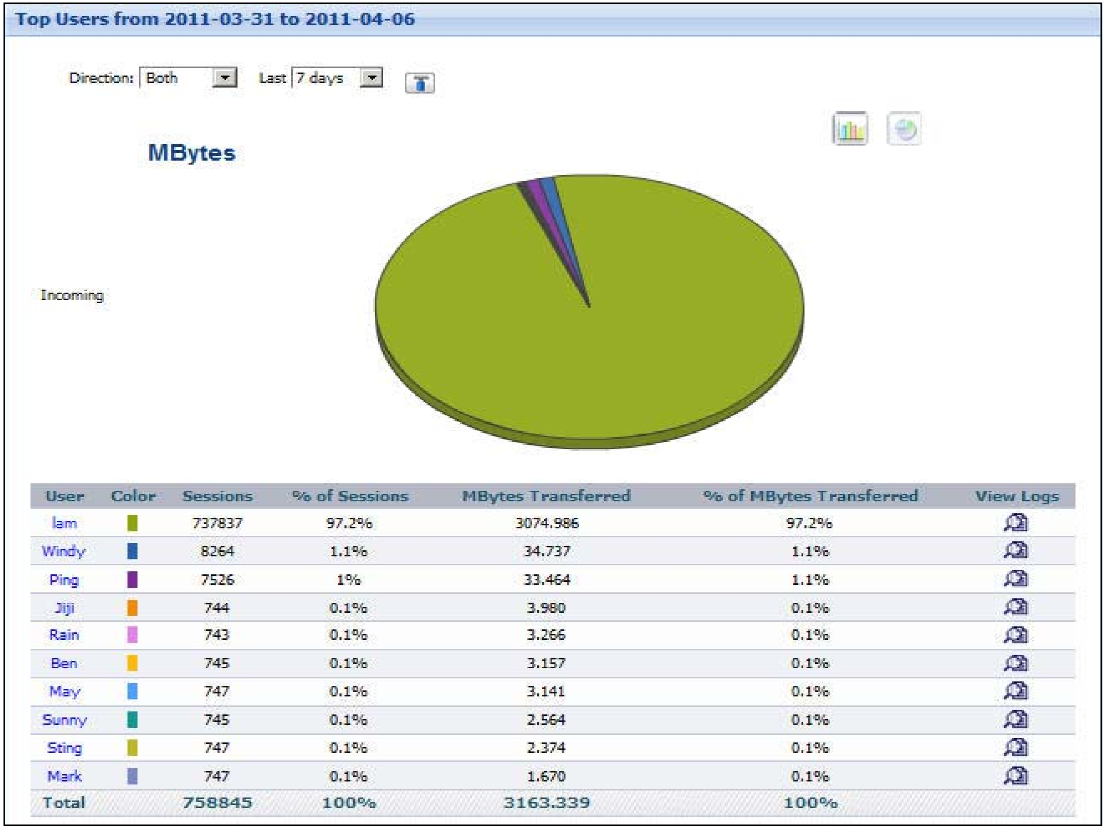
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.2.7 Secure Remote Access Top Users

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

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

Figure 109 Report > Secure Remote Access > Client-to-Site (IPSec) > Top Users



Top Users from 2011-03-31 to 2011-04-06

Direction: Both Last 7 days

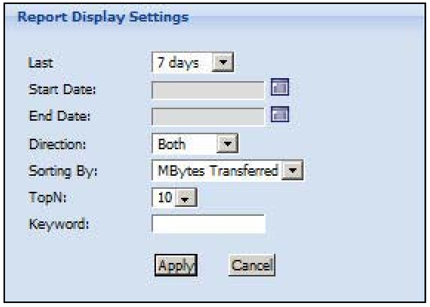
User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
Iam	🟩	737837	97.2%	3074.986	97.2%	🔍
Windy	🟦	8264	1.1%	34.737	1.1%	🔍
Ping	🟪	7526	1%	33.464	1.1%	🔍
Jiji	🟧	744	0.1%	3.980	0.1%	🔍
Rain	🟪	743	0.1%	3.266	0.1%	🔍
Ben	🟨	745	0.1%	3.157	0.1%	🔍
May	🟦	747	0.1%	3.141	0.1%	🔍
Sunny	🟩	745	0.1%	2.564	0.1%	🔍
Sting	🟨	747	0.1%	2.374	0.1%	🔍
Mark	🟪	747	0.1%	1.670	0.1%	🔍
Total		758845	100%	3163.339	100%	

Each field is described in the following table.

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

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

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

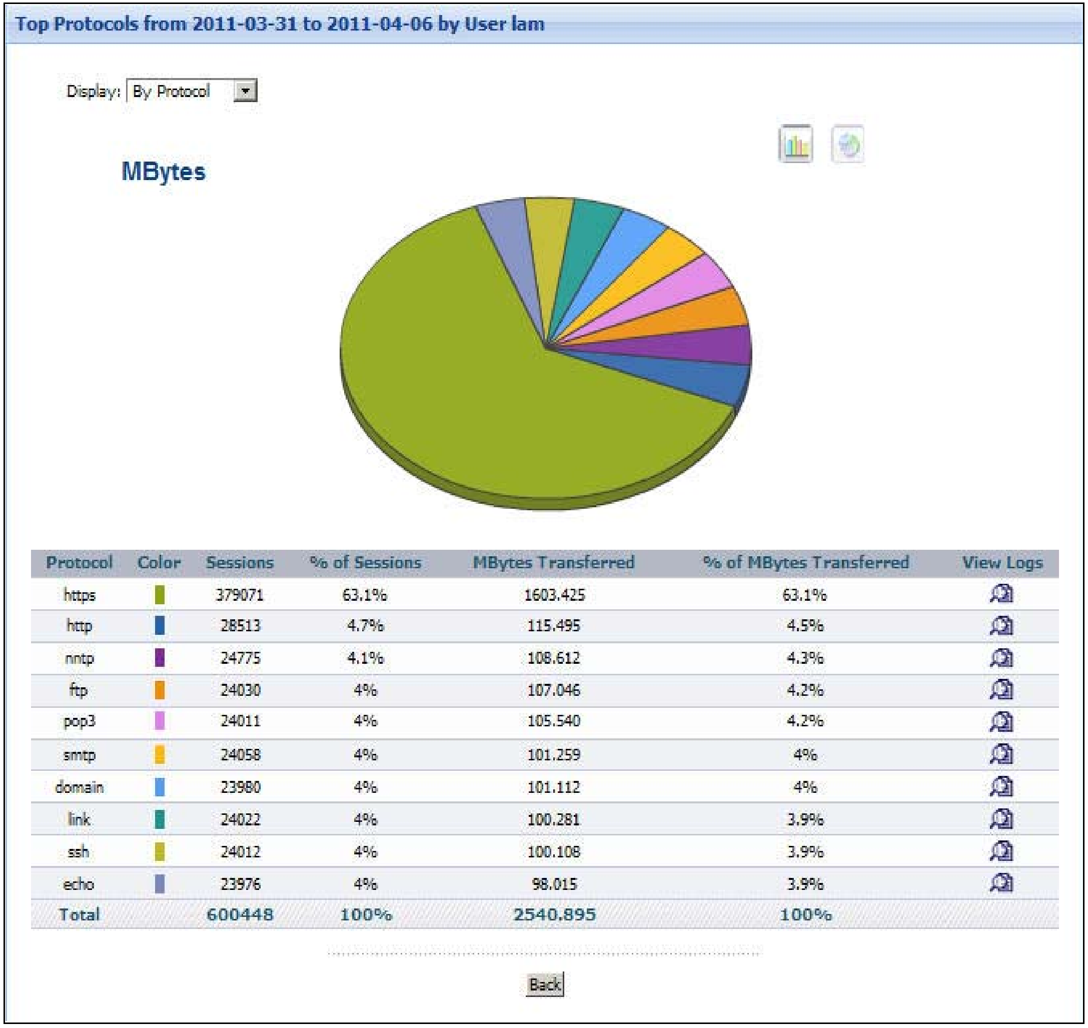
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the **Settings** icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Direction** field is the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most remote access Secure Remote Access traffic. Click on a user to look at the services of Secure Remote Access traffic sent or received the most by the selected user.
Color	This field displays what color represents each destination in the graph.
Sessions	This field displays the number of traffic events for each destination.
% of Sessions	This field displays what percentage each destination's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each destination.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

6.2.8 Secure Remote Access Top Users Drill-Down

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

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

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



Top Protocols from 2011-03-31 to 2011-04-06 by User lam

Display: By Protocol

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
https	🟩	379071	63.1%	1603.425	63.1%	🔍
http	🟦	28513	4.7%	115.495	4.5%	🔍
nntp	🟪	24775	4.1%	108.612	4.3%	🔍
ftp	🟧	24030	4%	107.046	4.2%	🔍
pop3	🟪	24011	4%	105.540	4.2%	🔍
smtp	🟨	24058	4%	101.259	4%	🔍
domain	🟦	23980	4%	101.112	4%	🔍
link	🟩	24022	4%	100.281	3.9%	🔍
ssh	🟨	24012	4%	100.108	3.9%	🔍
echo	🟦	23976	4%	98.015	3.9%	🔍
Total		600448	100%	2540.895	100%	

Each field is described in the following table.

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

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

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

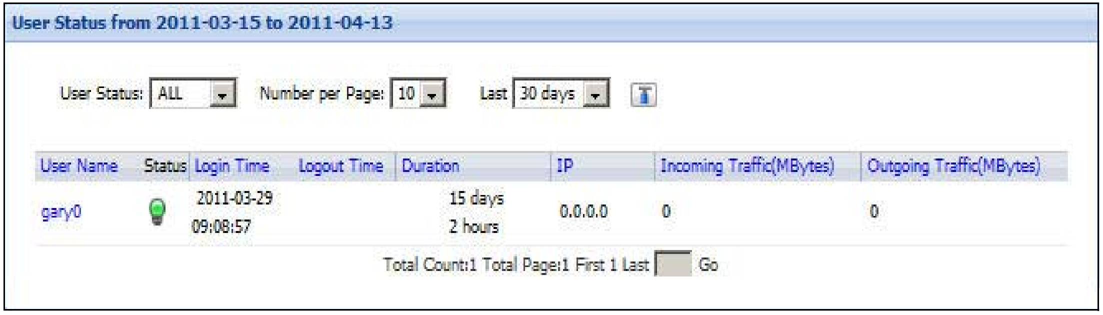
SSL Secure Remote Access tunnels are HTTPS connections via the ZyXEL devices. Only remote hosts can initiate SSL Secure Remote Access tunnels. Devices authenticates remote users (by username and password) when they try to initiate a SSL Secure Remote Access tunnel. The Secure Remote Access remote access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

6.3.1 Secure Remote Access User Status

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

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

Figure 111 Report > Secure Remote Access > Client-to-Site (SSL) > User Status



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

User Status: ALL　Number per Page: 10　Last 30 days

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

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

Each field is described in the following table.

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

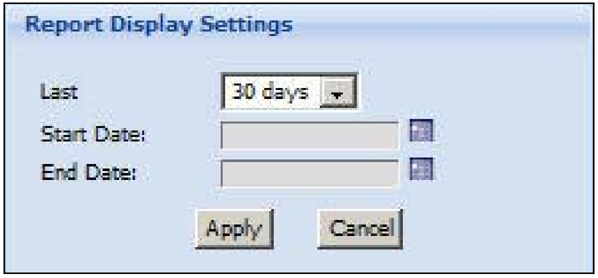
LABEL	DESCRIPTION
User Status	Select which status of users, you want to view statistics. **ALL** - to display for both connected and disconnected users. **Online** - to display information for connected users. **Offline** - to display information for disconnected users.
Last	Use this field or **Settings**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

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

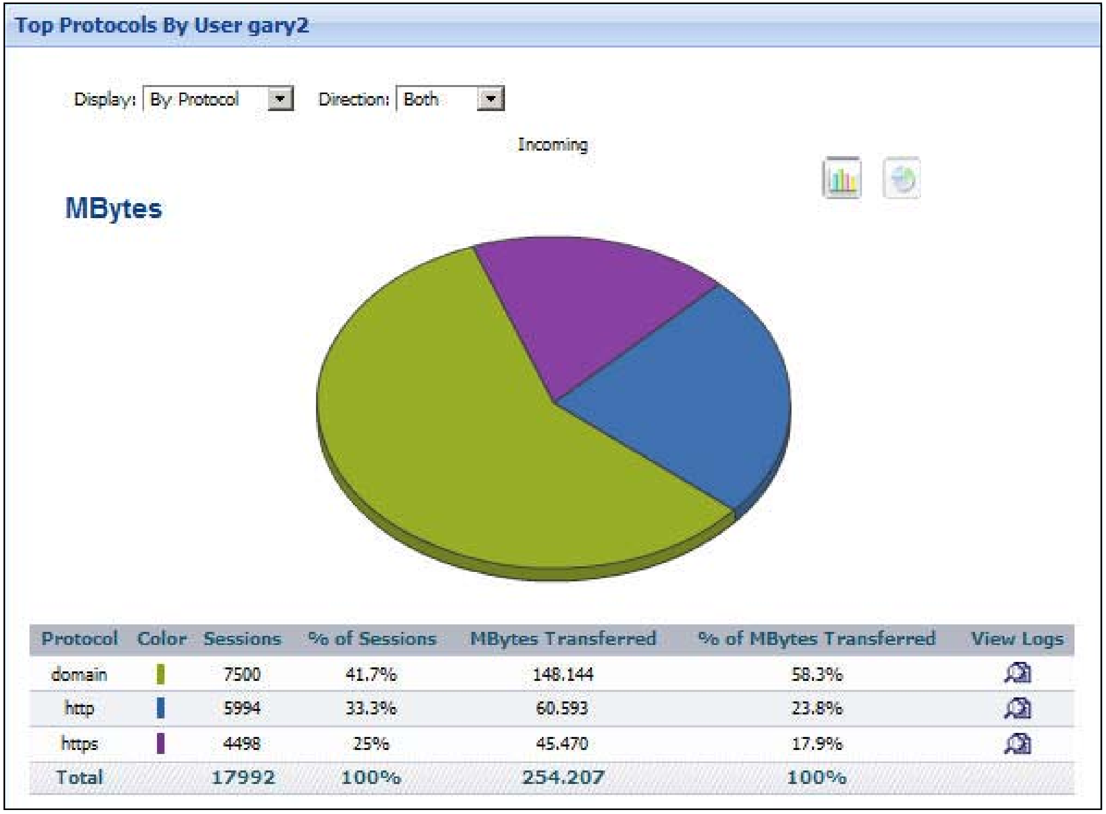
LABEL	DESCRIPTION
Status	This column displays the current status of users who have logged in. A user’s status icon is green when the user is currently connected. A user’s status icon is red when the user has already logged out.
Login Time	This column displays when the remote access user last logged in.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

6.3.2 Secure Remote Access User Status Drill-Down

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

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

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



Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
domain	🟩	7500	41.7%	148.144	58.3%	🔍
http	🟦	5994	33.3%	60.593	23.8%	🔍
https	🟪	4498	25%	45.470	17.9%	🔍
Total		17992	100%	254.207	100%	

Each field is described in the following table.

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

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

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

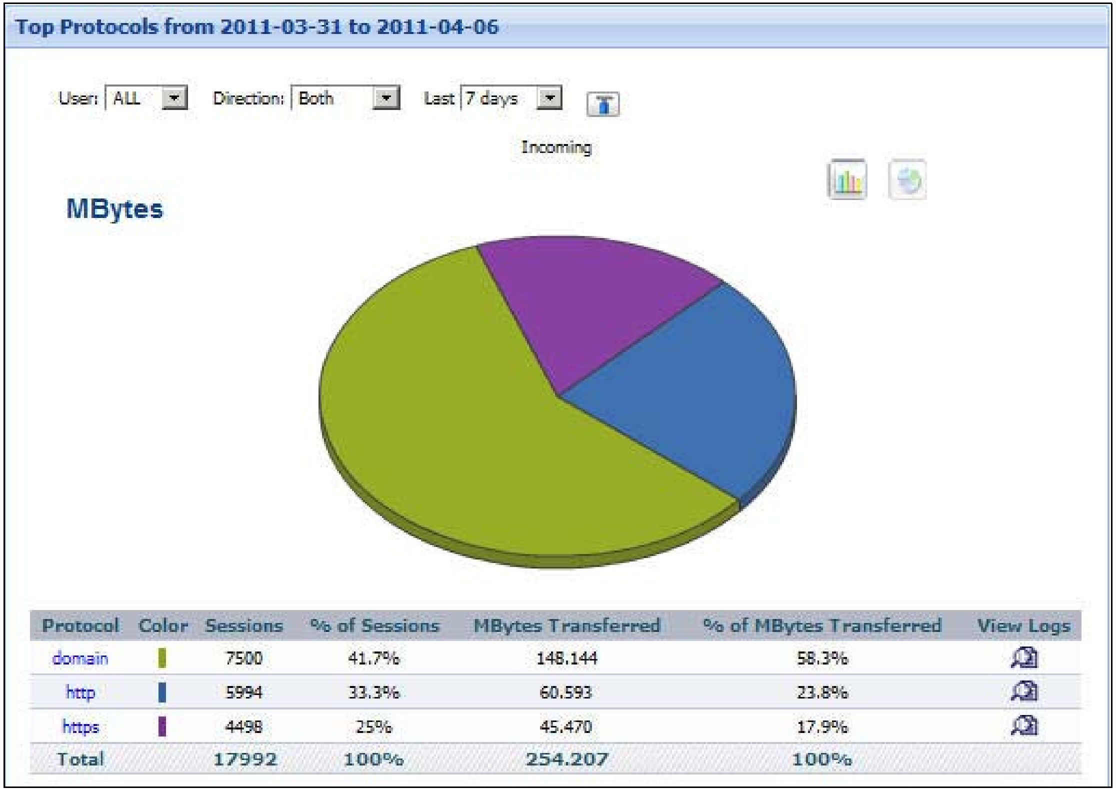
LABEL	DESCRIPTION
Protocol	This field displays the services most used by the selected user, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name.
Color	This field displays what color represents each service in the graph.
Sessions	This field displays the number of traffic events for each service.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events for the selected user.
MBytes Transferred	This field displays how much traffic (in megabytes) went through Secure Remote Access for each service.
% of MBytes Transferred	This field displays what percentage of the selected Secure Remote Access traffic was for each service.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the service above. The entry is just for top 10 services for the selected user.
Back	Click this to return to the main report.

6.3.3 Top Secure Remote Access Protocols

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

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

Figure 113 Report > Secure Remote Access > Client-to-Site (SSL) > Top Protocols



Top Protocols from 2011-03-31 to 2011-04-06

User: ALL Direction: Both Last 7 days

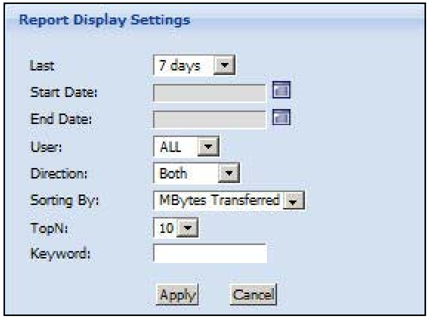
Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
domain	🟩	7500	41.7%	148.144	58.3%	
http	🟦	5994	33.3%	60.593	23.8%	
https	🟪	4498	25%	45.470	17.9%	
Total		17992	100%	254.207	100%	

Each field is described in the following table.

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

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

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

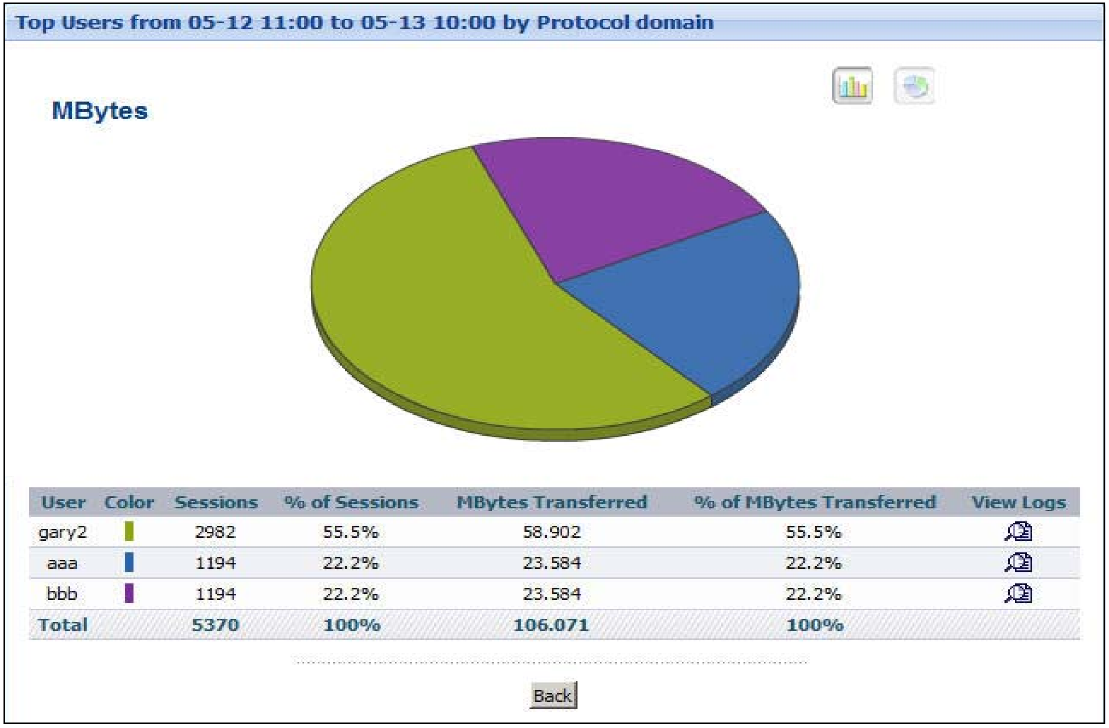
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: User: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Protocol** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Protocol	This field displays the services most transferred through SSL Secure Remote Access tunnel in the selected device, sorted by the amount of traffic for each one. If the number of protocols is less than the maximum number of records displayed in this table, every protocol is displayed. Each protocol is identified by its name. Click on a protocol to look at the top senders or receivers of the service through Secure Remote Access.
Color	This field displays what color represents each protocol in the graph.
Sessions	This field displays the number of traffic events for each protocol.
% of Sessions	This field displays what percentage each protocol's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each protocol.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each protocol.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

6.3.4 Top Secure Remote Access Protocols Drill-Down

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

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

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



Top Users from 05-12 11:00 to 05-13 10:00 by Protocol domain

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
gary2	🟩	2982	55.5%	58.902	55.5%	
aaa	🟦	1194	22.2%	23.584	22.2%	
bbb	🟪	1194	22.2%	23.584	22.2%	
Total		5370	100%	106.071	100%	

Each field is described in the following table.

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

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

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

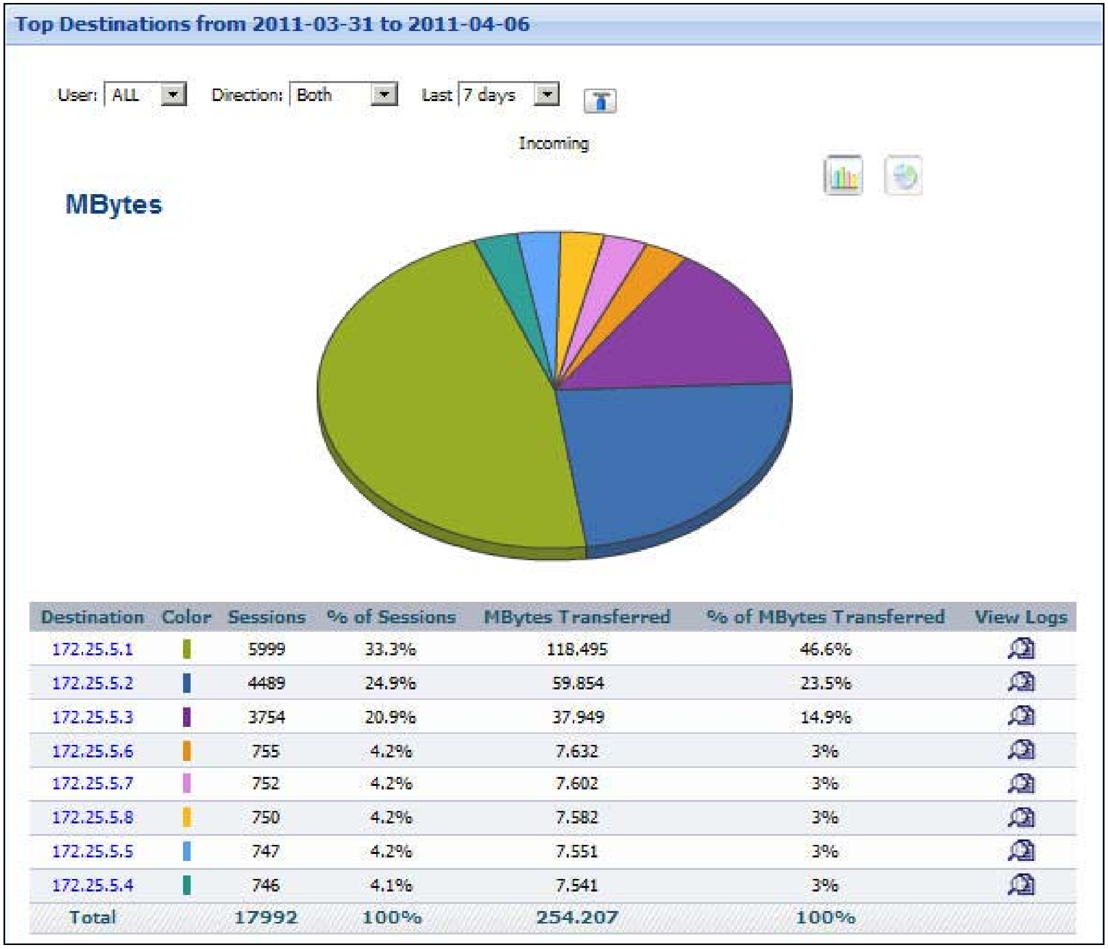
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the **TopN** setting in **Settings**.
Back	Click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

6.3.5 Top Secure Remote Access Destinations

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

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

Figure 115 Report > Secure Remote Access > Client-to-Site (SSL) > Top Destinations



Top Destinations from 2011-03-31 to 2011-04-06

User: ALL Direction: Both Last 7 days

Destination	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
172.25.5.1	▮	5999	33.3%	118.495	46.6%	🔍
172.25.5.2	▮	4489	24.9%	59.854	23.5%	🔍
172.25.5.3	▮	3754	20.9%	37.949	14.9%	🔍
172.25.5.6	▮	755	4.2%	7.632	3%	🔍
172.25.5.7	▮	752	4.2%	7.602	3%	🔍
172.25.5.8	▮	750	4.2%	7.582	3%	🔍
172.25.5.5	▮	747	4.2%	7.551	3%	🔍
172.25.5.4	▮	746	4.1%	7.541	3%	🔍
Total		17992	100%	254.207	100%	

Each field is described in the following table.

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

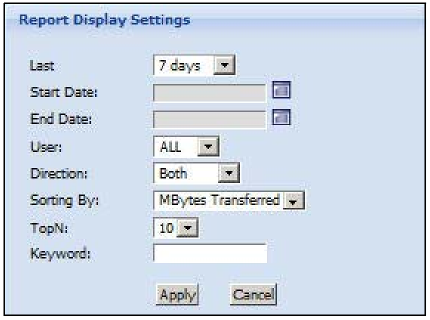
LABEL	DESCRIPTION
User	Select a remote access user. Select **ALL** to display the destinations with the most traffic sent through the remote access Secure Remote Access tunnels.
Direction	Select which direction of traffic, you want to view statistics. **Both** - all Secure Remote Access traffic the devices sent or received. **Incoming** - all traffic the devices received through Secure Remote Access tunnel. **Outgoing** - all traffic the devices sent out through Secure Remote Access tunnel.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: User: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

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

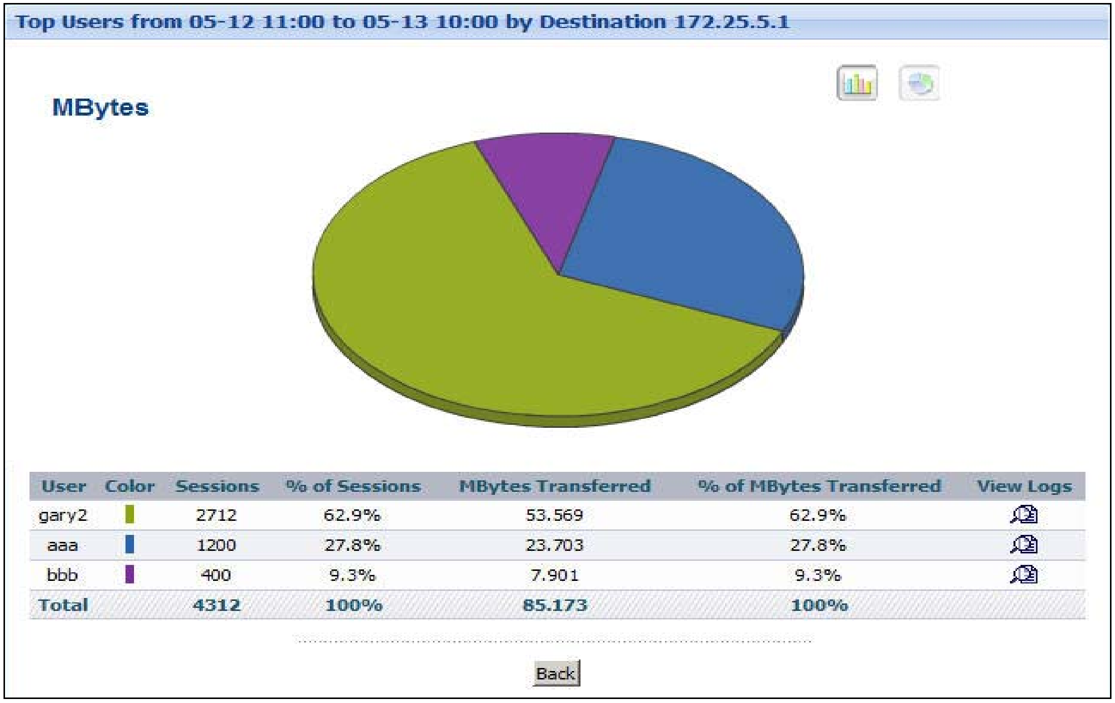
LABEL	DESCRIPTION
Destination	This field displays where the remote user sent the most Secure Remote Access traffic, sorted by the amount of traffic for each destination. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each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

6.3.6 Top Secure Remote Access Destinations Drill-Down

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

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

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



Top Users from 05-12 11:00 to 05-13 10:00 by Destination 172.25.5.1

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
gary2	🟩	2712	62.9%	53.569	62.9%	🔍
aaa	🟦	1200	27.8%	23.703	27.8%	🔍
bbb	🟪	400	9.3%	7.901	9.3%	🔍
Total		4312	100%	85.173	100%	

Each field is described in the following table.

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

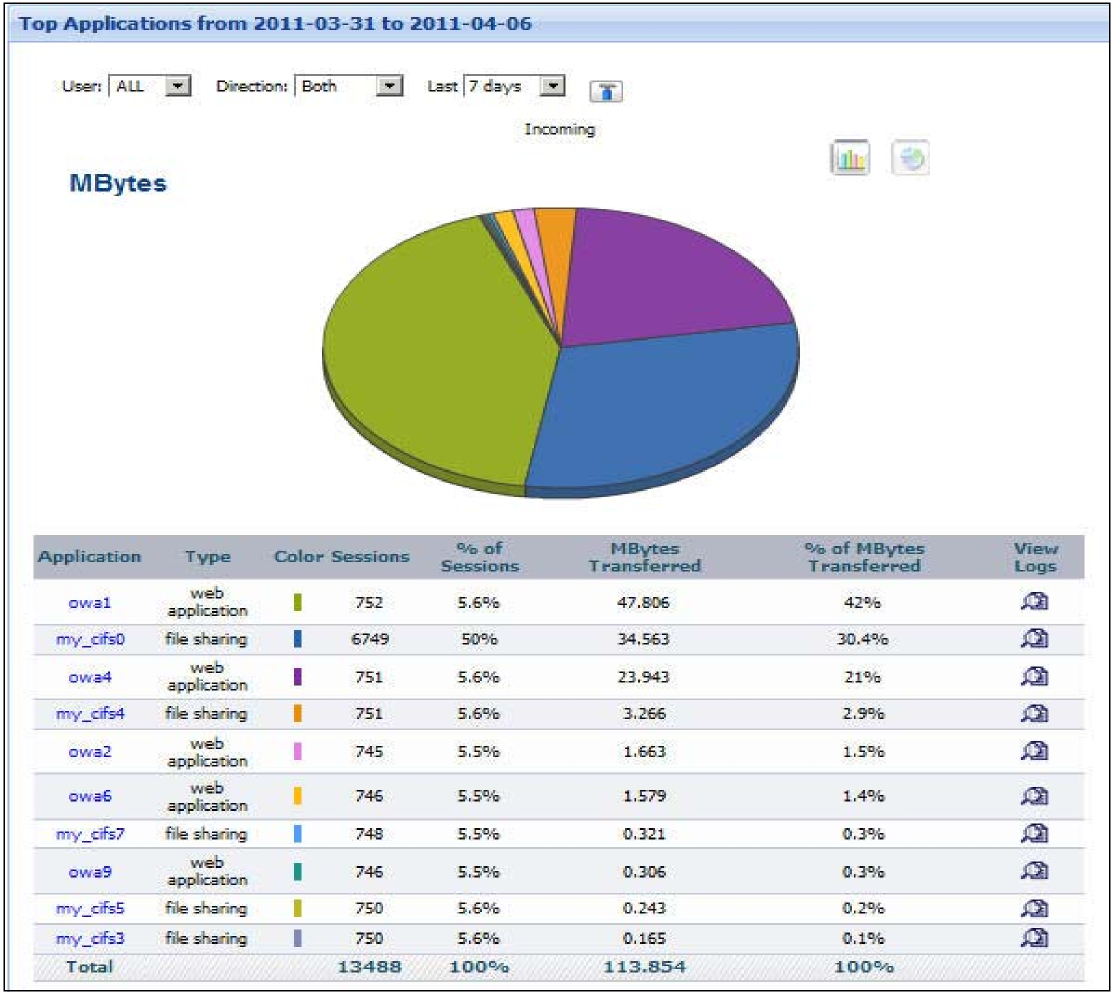
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.3.7 Top Secure Remote Access Applications

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

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

Figure 117 Report > Secure Remote Access > Client-to-Site (SSL) > Top Applications



Top Applications from 2011-03-31 to 2011-04-06

User: ALL Direction: Both Last 7 days

Incoming

MBytes

Application	Type	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
owa1	web application	■	752	5.6%	47.806	42%	🔍
my_cifs0	file sharing	■	6749	50%	34.563	30.4%	🔍
owa4	web application	■	751	5.6%	23.943	21%	🔍
my_cifs4	file sharing	■	751	5.6%	3.266	2.9%	🔍
owa2	web application	■	745	5.5%	1.663	1.5%	🔍
owa6	web application	■	746	5.5%	1.579	1.4%	🔍
my_cifs7	file sharing	■	748	5.5%	0.321	0.3%	🔍
owa9	web application	■	746	5.5%	0.306	0.3%	🔍
my_cifs5	file sharing	■	750	5.6%	0.243	0.2%	🔍
my_cifs3	file sharing	■	750	5.6%	0.165	0.1%	🔍
Total			13488	100%	113.854	100%	

Each field is described in the following table.

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

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

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

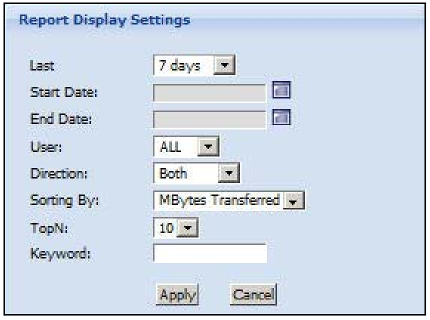
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: User: ALL Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **User** and **Direction** fields are the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Application** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the internal services the remote users access the most through SSL Secure Remote Access, sorted by the amount of traffic for each one. If the number of applications is less than the maximum number of records displayed in this table, every application is displayed. Each application is identified by its name. Click on an application to look at the top remote user’s hosts of Secure Remote Access traffic for the selected application.
Type	This field displays what kind of service the internal server provides.
Color	This field displays what color represents each application in the graph.
Sessions	This field displays the number of traffic events for each application.

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

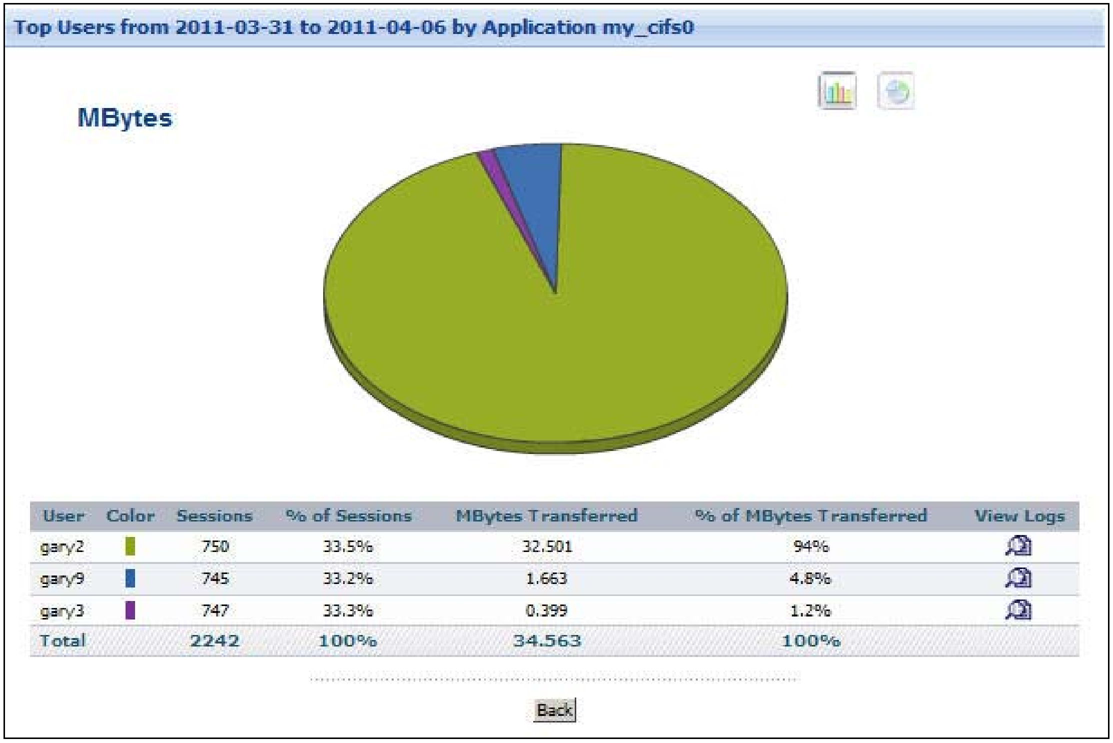
LABEL	DESCRIPTION
% of Sessions	This field displays what percentage each application's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled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

6.3.8 Top Secure Remote Access Applications Drill-Down

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

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

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



Top Users from 2011-03-31 to 2011-04-06 by Application my_cifs0

User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
gary2	🟩	750	33.5%	32.501	94%	🔍
gary9	🟦	745	33.2%	1.663	4.8%	🔍
gary3	🟪	747	33.3%	0.399	1.2%	🔍
Total		2242	100%	34.563	100%	

Each field is described in the following table.

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

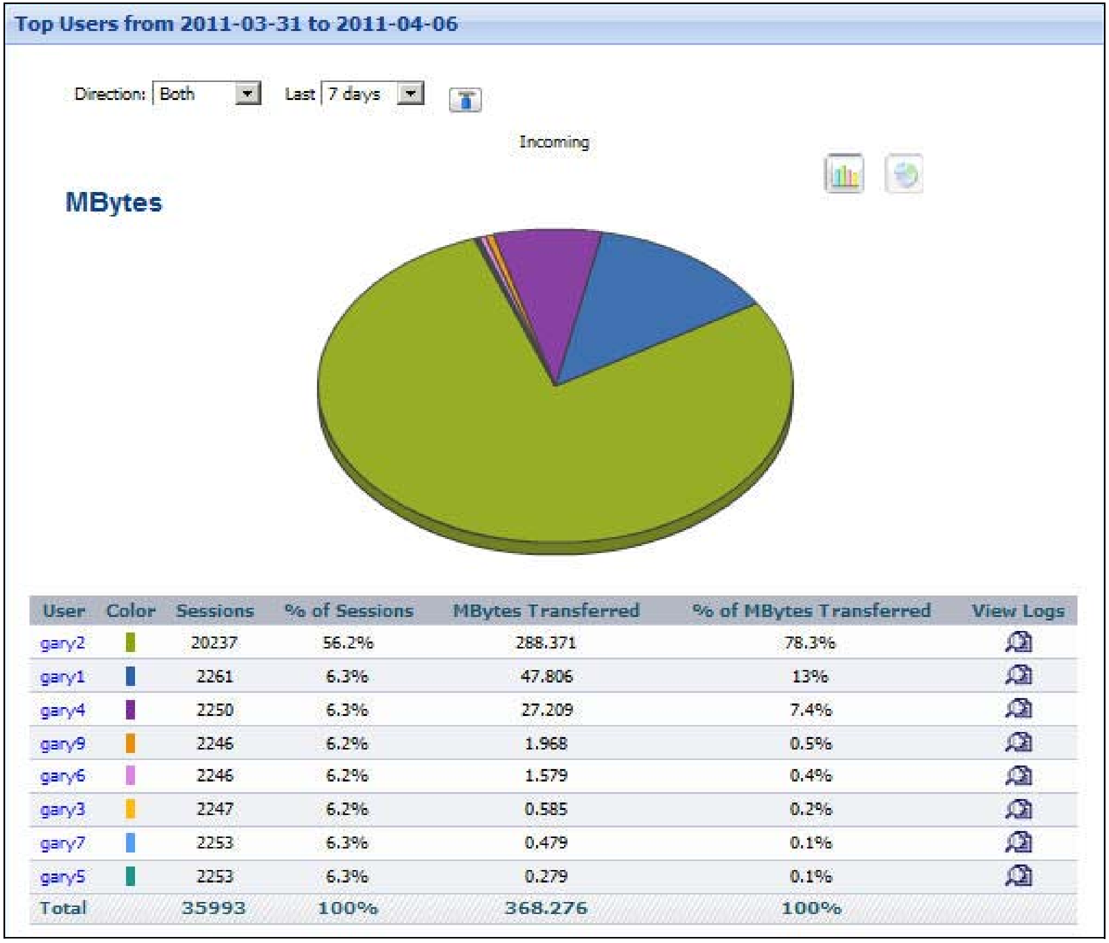
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

6.3.9 Secure Remote Access Top Users

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

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

Figure 119 Report > Secure Remote Access > Client-to-Site (SSL) > Top Users



Top Users from 2011-03-31 to 2011-04-06

Direction: Both

Last 7 days

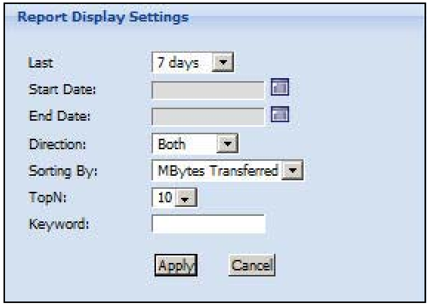
User	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
gary2	🟩	20237	56.2%	288.371	78.3%	🔍
gary1	🟦	2261	6.3%	47.806	13%	🔍
gary4	🟪	2250	6.3%	27.209	7.4%	🔍
gary9	🟧	2246	6.2%	1.968	0.5%	🔍
gary6	🟪	2246	6.2%	1.579	0.4%	🔍
gary3	🟨	2247	6.2%	0.585	0.2%	🔍
gary7	🟦	2253	6.3%	0.479	0.1%	🔍
gary5	🟩	2253	6.3%	0.279	0.1%	🔍
Total		35993	100%	368.276	100%	

Each field is described in the following table.

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

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

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

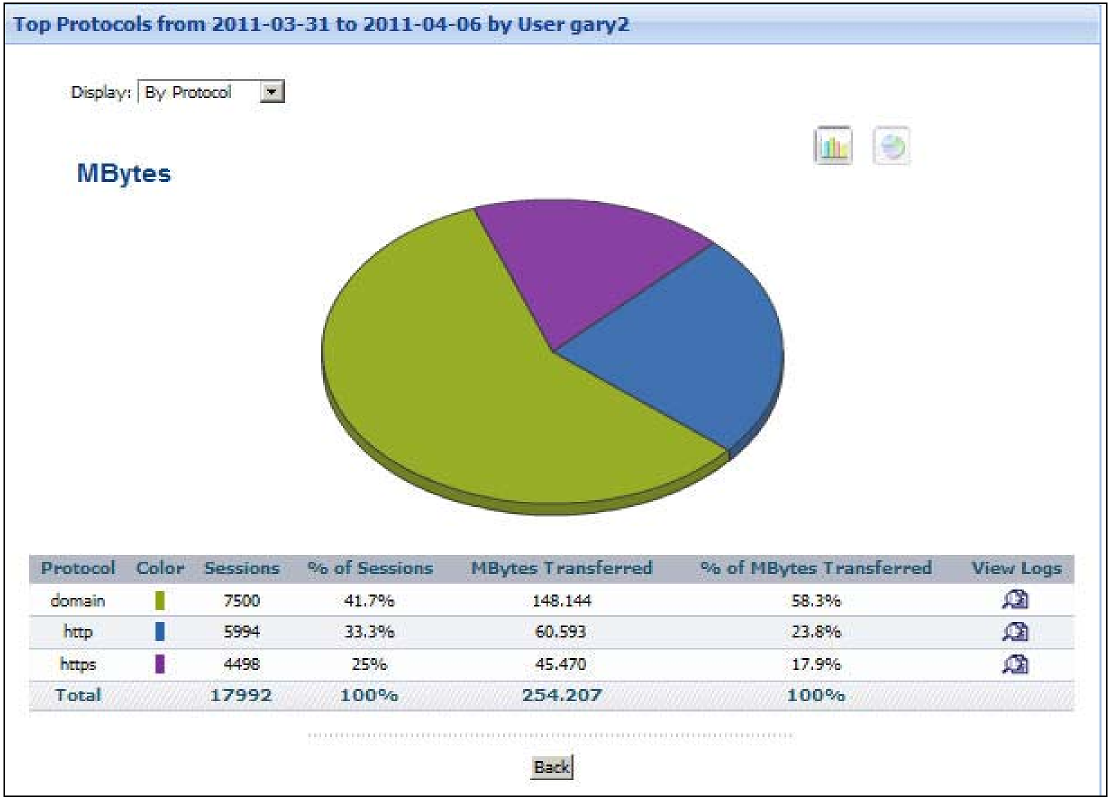
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Direction: Both Sorting By: MBytes Transferred TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. The **Direction** field is the same as in the main screen. Select **MBytes Transferred** to sort the records by the amount of traffic. Select **Sessions** to sort by the number of sessions. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). The fields do not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users who sent the most Secure Remote Access traffic. Click on a user to look at the services of Secure Remote Access traffic sent or received the most by the selected user.
Color	This field displays what color represents each user in the graph.
Sessions	This field displays the number of traffic events for each user.
% of Sessions	This field displays what percentage each user's number of traffic events makes out of the total number of traffic events that match the settings you displayed in this report.
MBytes Transferred	This field displays how much traffic (in megabytes) the device handled for each user.
% of MBytes Transferred	This field displays what percentage of Secure Remote Access traffic the device handled for each user.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above. By default, only the top 10 services are displayed. You can change the number of services to be displayed through the **TopN** setting in **Settings**.

6.3.10 Secure Remote Access Top Users Drill-Down

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

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

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



Top Protocols from 2011-03-31 to 2011-04-06 by User gary2

Display: By Protocol

Protocol	Color	Sessions	% of Sessions	MBytes Transferred	% of MBytes Transferred	View Logs
domain	🟩	7500	41.7%	148.144	58.3%	🔍
http	🟦	5994	33.3%	60.593	23.8%	🔍
https	🟪	4498	25%	45.470	17.9%	🔍
Total		17992	100%	254.207	100%	

Each field is described in the following table.

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

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

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

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

6.4 Xauth

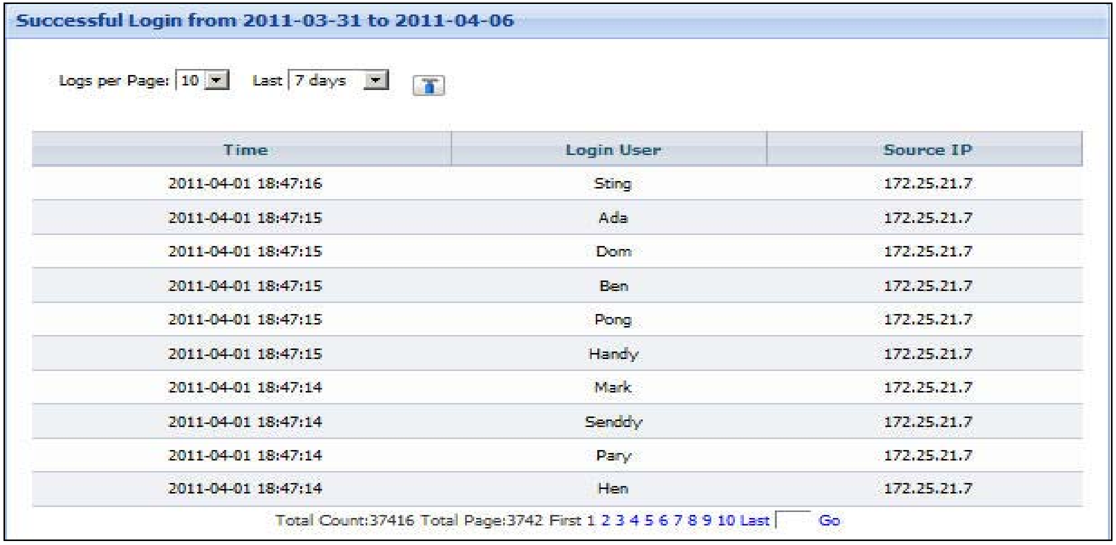
Devices can use xauth to authenticate remote users (by username and password) when they try to initiate a dynamic IPSec Secure Remote Access tunnel. Use these screens to display records of successful and unsuccessful logins to the device's IPSec Secure Remote Access tunnels.

6.4.1 Secure Remote Access Successful Login

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

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

Figure 121 Report > Secure Remote Access > Xauth> Successful Login



Successful Login from 2011-03-31 to 2011-04-06

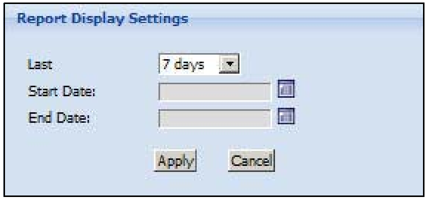
Logs per Page: 10 Last 7 days

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

Total Count:37416 Total Page:3742 First 1 2 3 4 5 6 7 8 9 10 Last Go

Each field is described in the following table.

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

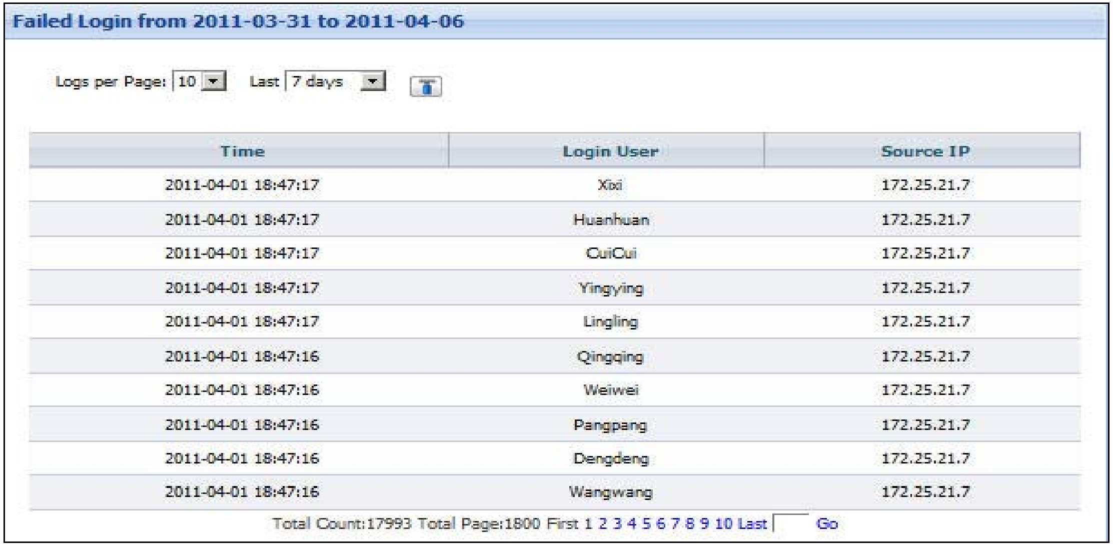
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen.
Time	This column displays when the user last logged in. The entries are sorted in chronological order.
Login User	This field displays the user name of a user that logged into one of the device's Secure Remote Access tunnels. Each user is identified by user name.
Source IP	This is the IP address from which the user logged into one of the device's Secure Remote Access tunnels.
Total	This entry displays the total number of users on the current page of the report. If you want to see a different page of the report, type the number of the page in the field.

6.4.2 Secure Remote Access Failed Login

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

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

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



Failed Login from 2011-03-31 to 2011-04-06

Logs per Page: 10 Last 7 days

Time	Login User	Source IP
2011-04-01 18:47:17	Xixi	172.25.21.7
2011-04-01 18:47:17	Huanhuan	172.25.21.7
2011-04-01 18:47:17	CuiCui	172.25.21.7
2011-04-01 18:47:17	Yingying	172.25.21.7
2011-04-01 18:47:17	Lingling	172.25.21.7
2011-04-01 18:47:16	Qingqing	172.25.21.7
2011-04-01 18:47:16	Weiwei	172.25.21.7
2011-04-01 18:47:16	Pangpang	172.25.21.7
2011-04-01 18:47:16	Dengdeng	172.25.21.7
2011-04-01 18:47:16	Wangwang	172.25.21.7

Total Count:17993 Total Page:1800 First 1 2 3 4 5 6 7 8 9 10 Last Go

Each field is described in the following table.

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

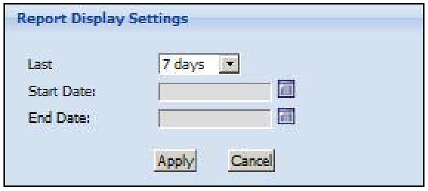
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). The field does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen.
Time	This column displays when the user last failed to log in. The entries are sorted in chronological order.
Login User	This field displays the user name of a user that failed to log into one of the device's Secure Remote Access tunnels. Each user is identified by user name.

Table 110 Report > Secure Remote Access > 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 Secure Remote Access tunnels.
Total	This entry displays the total number of users on the current page of the report. If you want to see a different page of the report, type the number of the page in the field.

Network Security

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

7.1 Firewall Access Control

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

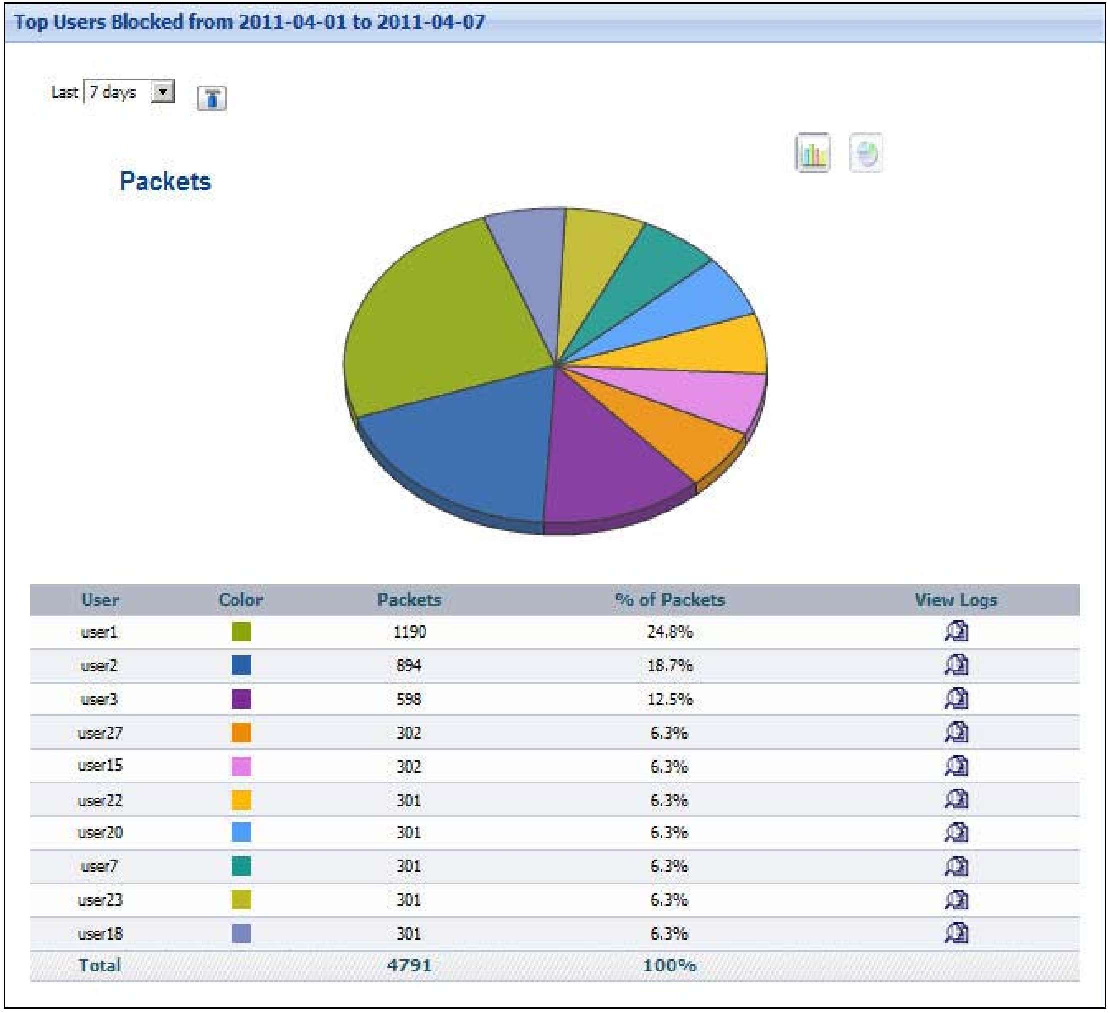
Note: To look at firewall access control reports, each ZyXEL device must record blocked packets and users in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Access Control** is enabled.

7.1.1 Top Users Blocked

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

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

Figure 123 Report > Network Security > Firewall Access Control > Top Users Blocked



Top Users Blocked from 2011-04-01 to 2011-04-07

Last 7 days

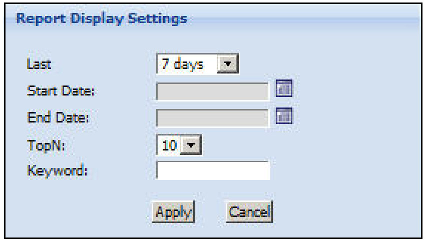
User	Color	Packets	% of Packets	View Logs
user1	🟩	1190	24.8%	🔍
user2	🟦	894	18.7%	🔍
user3	🟪	598	12.5%	🔍
user27	🟧	302	6.3%	🔍
user15	🟪	302	6.3%	🔍
user22	🟨	301	6.3%	🔍
user20	🟦	301	6.3%	🔍
user7	🟩	301	6.3%	🔍
user23	🟨	301	6.3%	🔍
user18	🟪	301	6.3%	🔍
Total		4791	100%	

Each field is described in the following table.

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

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 111 Report > Network Security > 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.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System > General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users from which the selected device blocked the most traffic, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Packets	This field displays the number of packets the device blocked from each user.
% of Packets	This field displays what percentage each user's number of blocked packets makes out of the total number of blocked packets that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

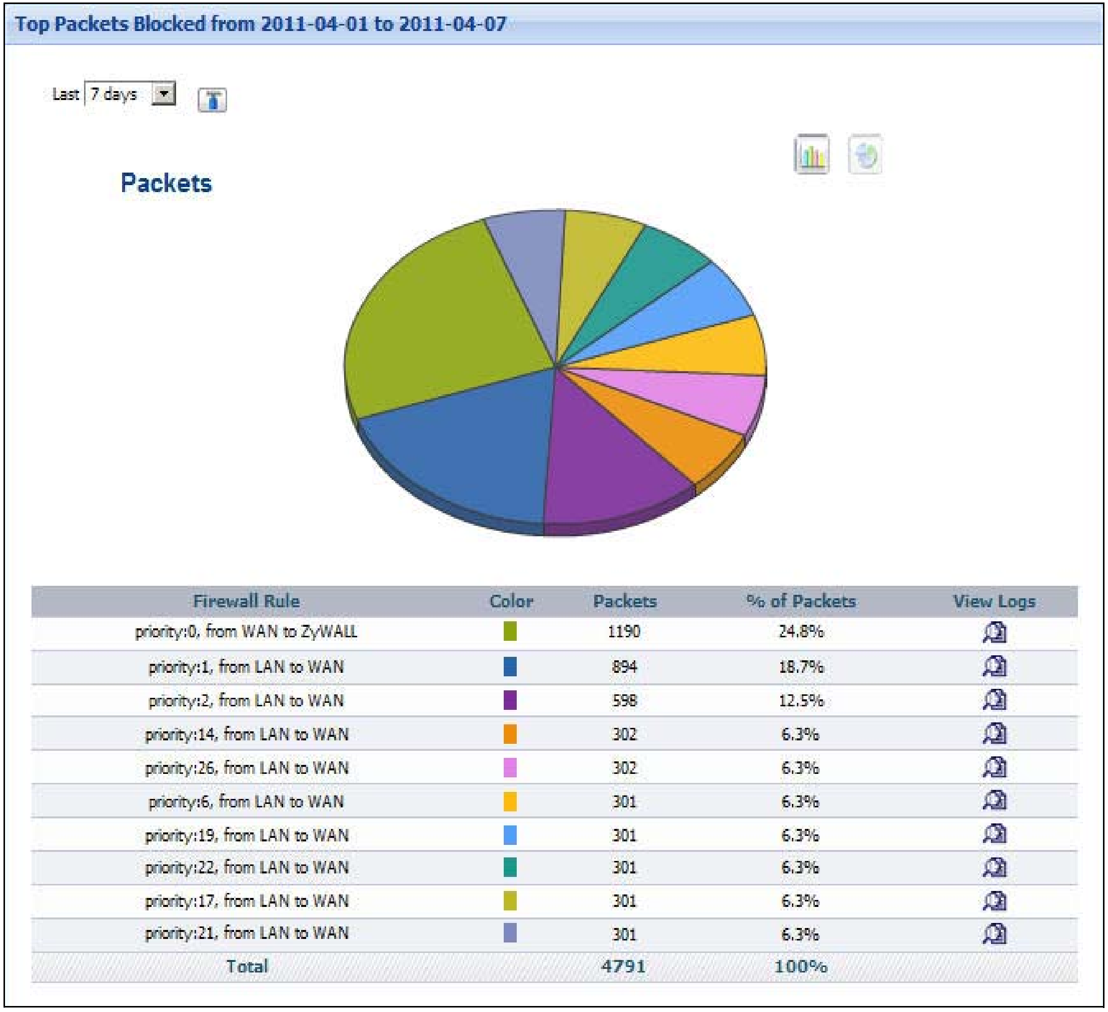
7.1.2 Top Packets Blocked

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

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

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

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



Top Packets Blocked from 2011-04-01 to 2011-04-07

Last: 7 days

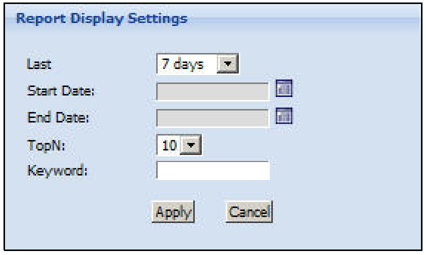
Firewall Rule	Color	Packets	% of Packets	View Logs
priority:0, from WAN to ZyWALL	🟩	1190	24.8%	🔍
priority:1, from LAN to WAN	🟦	894	18.7%	🔍
priority:2, from LAN to WAN	🟪	598	12.5%	🔍
priority:14, from LAN to WAN	🟧	302	6.3%	🔍
priority:26, from LAN to WAN	🟪	302	6.3%	🔍
priority:6, from LAN to WAN	🟨	301	6.3%	🔍
priority:19, from LAN to WAN	🟦	301	6.3%	🔍
priority:22, from LAN to WAN	🟩	301	6.3%	🔍
priority:17, from LAN to WAN	🟨	301	6.3%	🔍
priority:21, from LAN to WAN	🟦	301	6.3%	🔍
Total		4791	100%	

Each field is described in the following table.

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

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 112 Report > Network Security > 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.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Firewall Rule** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Firewall Rule	This field displays the name of the firewall rule on the selected device that blocked packets, sorted by the number of packets for each one. Each firewall rule is identified by priority in the firewall rule list and the traffic direction to which it applies.
Color	This field displays what color represents each firewall rule in the graph.
Packets	This field displays the number of packets the firewall rule blocked from each user.
% of Packets	This field displays what percentage each firewall rule's number of blocked packets makes out of the total number of blocked packets that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the firewall rules above.

7.2 Attack

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

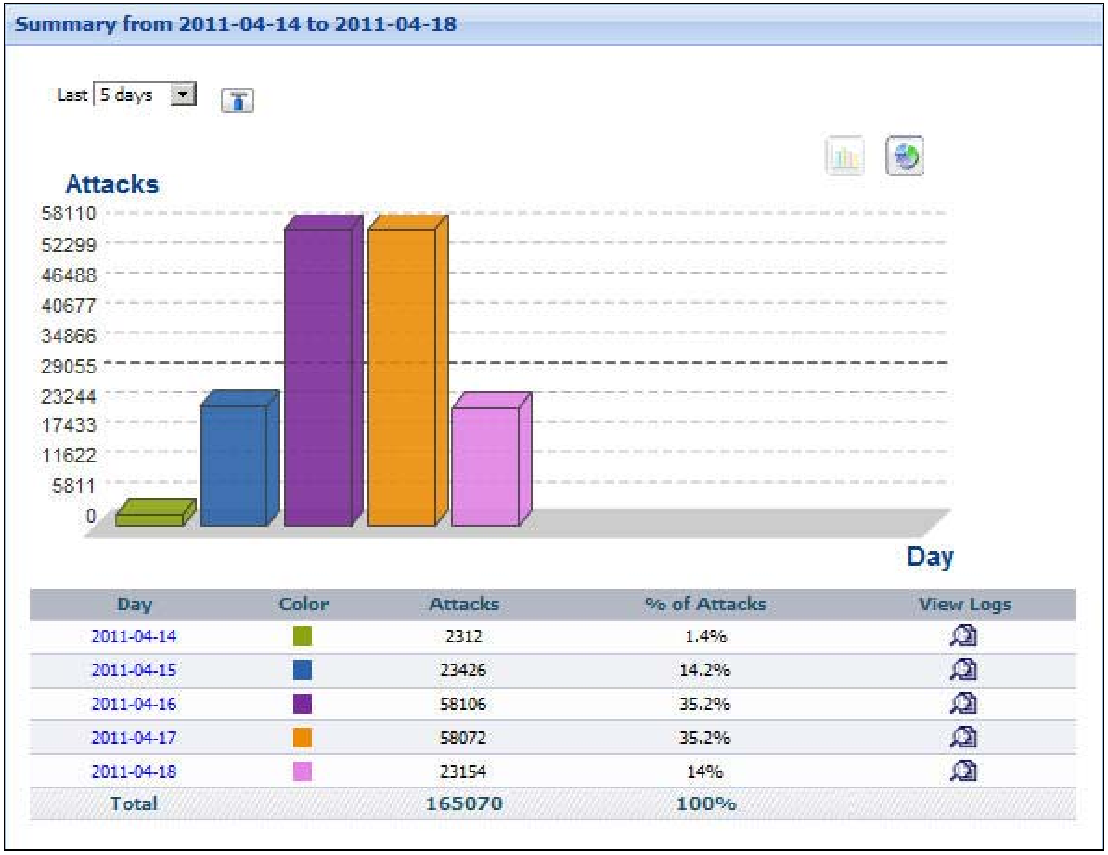
7.2.1 Attack Summary

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

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

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

Figure 125 Report > Network Security > Attack > Summary



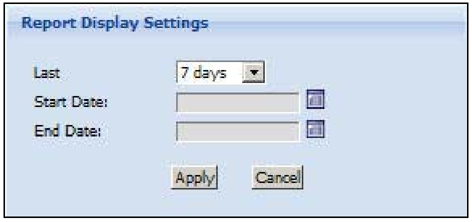
Summary from 2011-04-14 to 2011-04-18

Last 5 days

Day	Color	Attacks	% of Attacks	View Logs
2011-04-14	🟩	2312	1.4%	
2011-04-15	🟦	23426	14.2%	
2011-04-16	🟪	58106	35.2%	
2011-04-17	🟧	58072	35.2%	
2011-04-18	■	23154	14%	
Total		165070	100%	

Each field is described in the following table.

Table 113 Report > Network Security > Attack > Summary

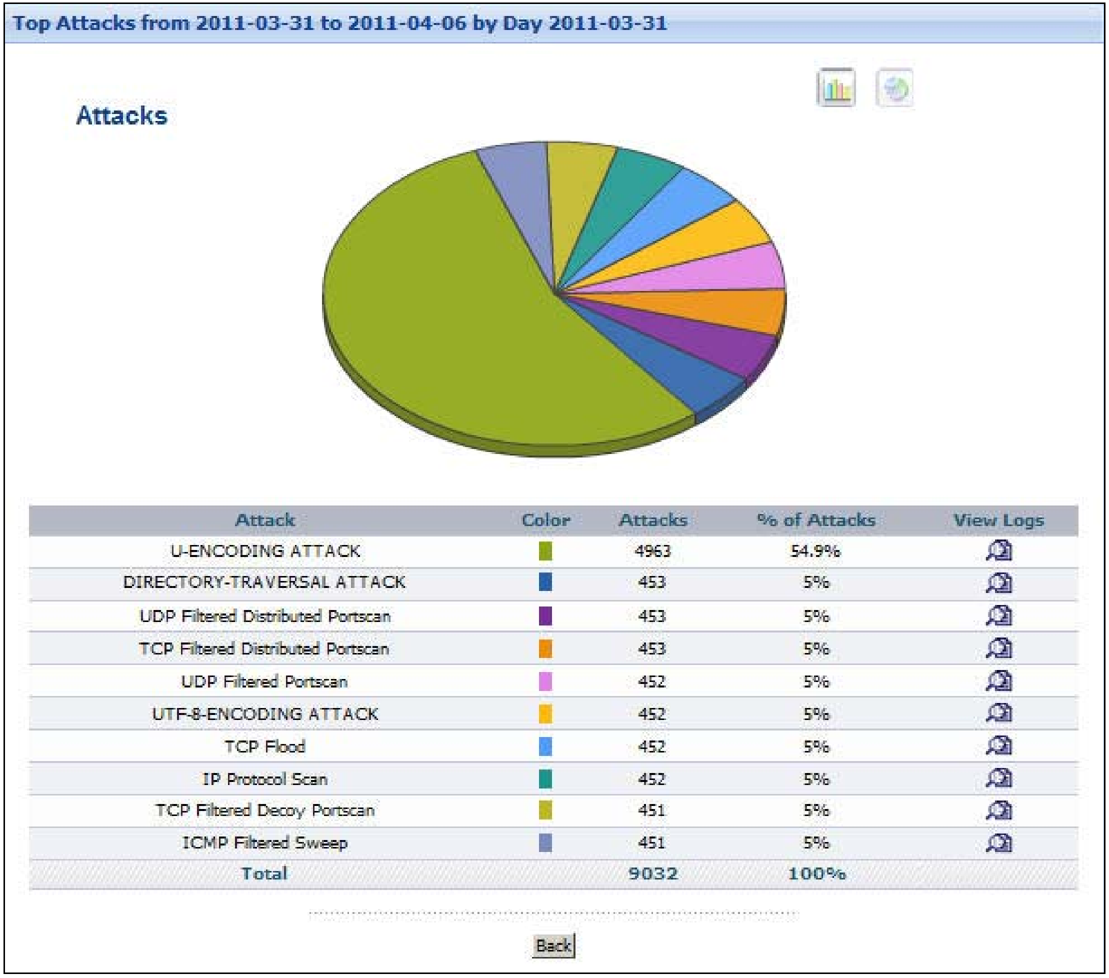
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top categories of attacks in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attacks	This field displays the number of DoS attacks in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.2.2 Attack Summary Drill-Down

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

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

Figure 126 Report > Network Security > Attack > Summary > Drill-Down



Top Attacks from 2011-03-31 to 2011-04-06 by Day 2011-03-31

Attacks

Attack	Color	Attacks	% of Attacks	View Logs
U-ENCODING ATTACK	🟩	4963	54.9%	🔍
DIRECTORY-TRAVERSAL ATTACK	🟦	453	5%	🔍
UDP Filtered Distributed Portscan	🟪	453	5%	🔍
TCP Filtered Distributed Portscan	🟧	453	5%	🔍
UDP Filtered Portscan	🟪	452	5%	🔍
UTF-8-ENCODING ATTACK	🟨	452	5%	🔍
TCP Flood	🟦	452	5%	🔍
IP Protocol Scan	🟩	452	5%	🔍
TCP Filtered Decoy Portscan	🟨	451	5%	🔍
ICMP Filtered Sweep	🟦	451	5%	🔍
Total		9032	100%	

Each field is described in the following table.

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

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

Table 114 Report > Network Security > 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.

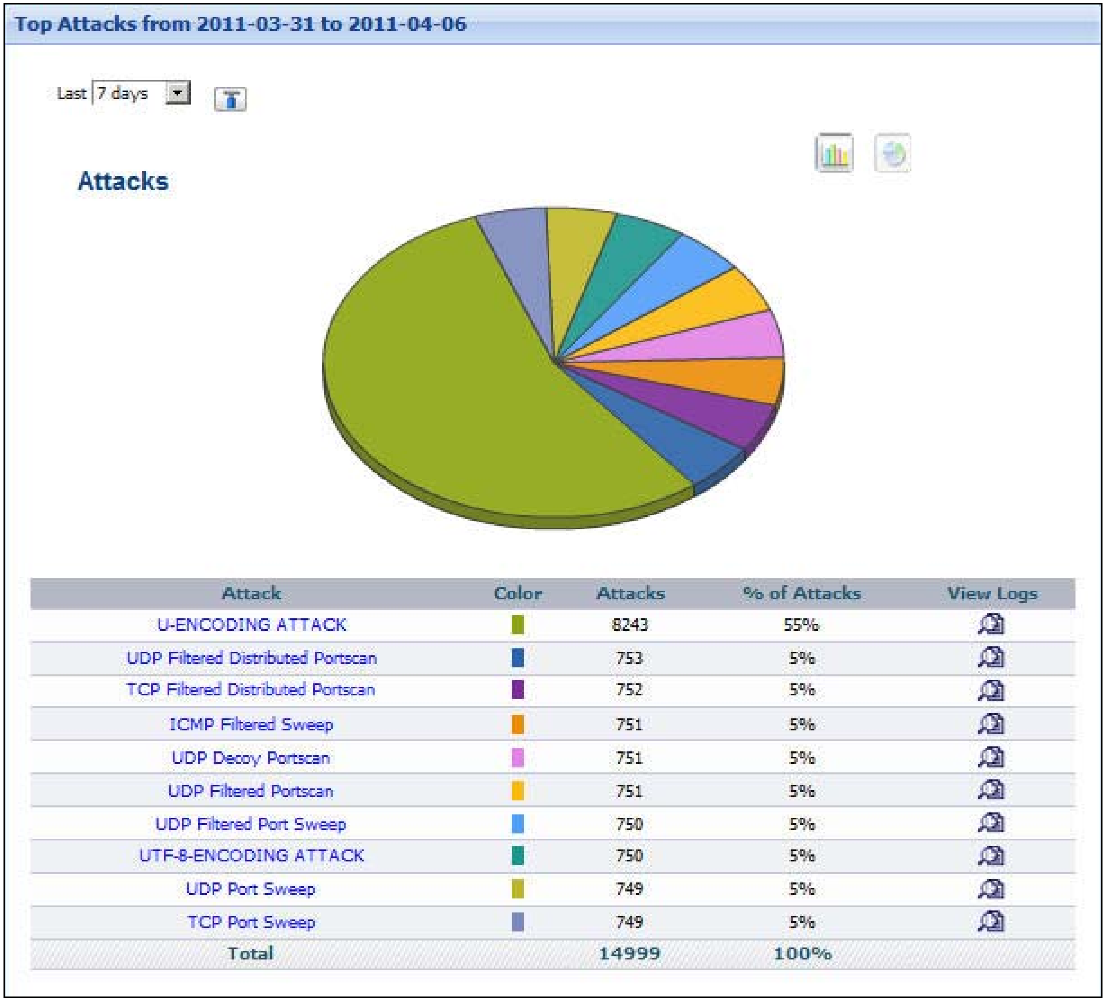
7.2.3 Top Attacks

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

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

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

Figure 127 Report > Network Security > Attack > Top Attacks

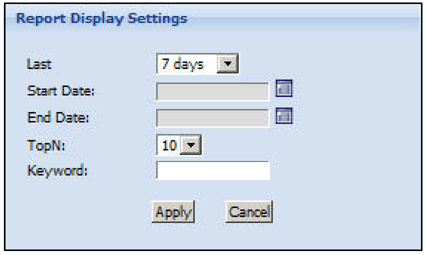


Top Attacks from 2011-03-31 to 2011-04-06

Attack	Color	Attacks	% of Attacks	View Logs
U-ENCODING ATTACK	🟩	8243	55%	🔍
UDP Filtered Distributed Portscan	🟦	753	5%	🔍
TCP Filtered Distributed Portscan	🟪	752	5%	🔍
ICMP Filtered Sweep	🟧	751	5%	🔍
UDP Decoy Portscan	🟪	751	5%	🔍
UDP Filtered Portscan	🟨	751	5%	🔍
UDP Filtered Port Sweep	🟦	750	5%	🔍
UTF-8-ENCODING ATTACK	🟩	750	5%	🔍
UDP Port Sweep	🟨	749	5%	🔍
TCP Port Sweep	🟦	749	5%	🔍
Total		14999	100%	

Each field is described in the following table.

Table 115 Report > Network Security > Attack > Top Attacks

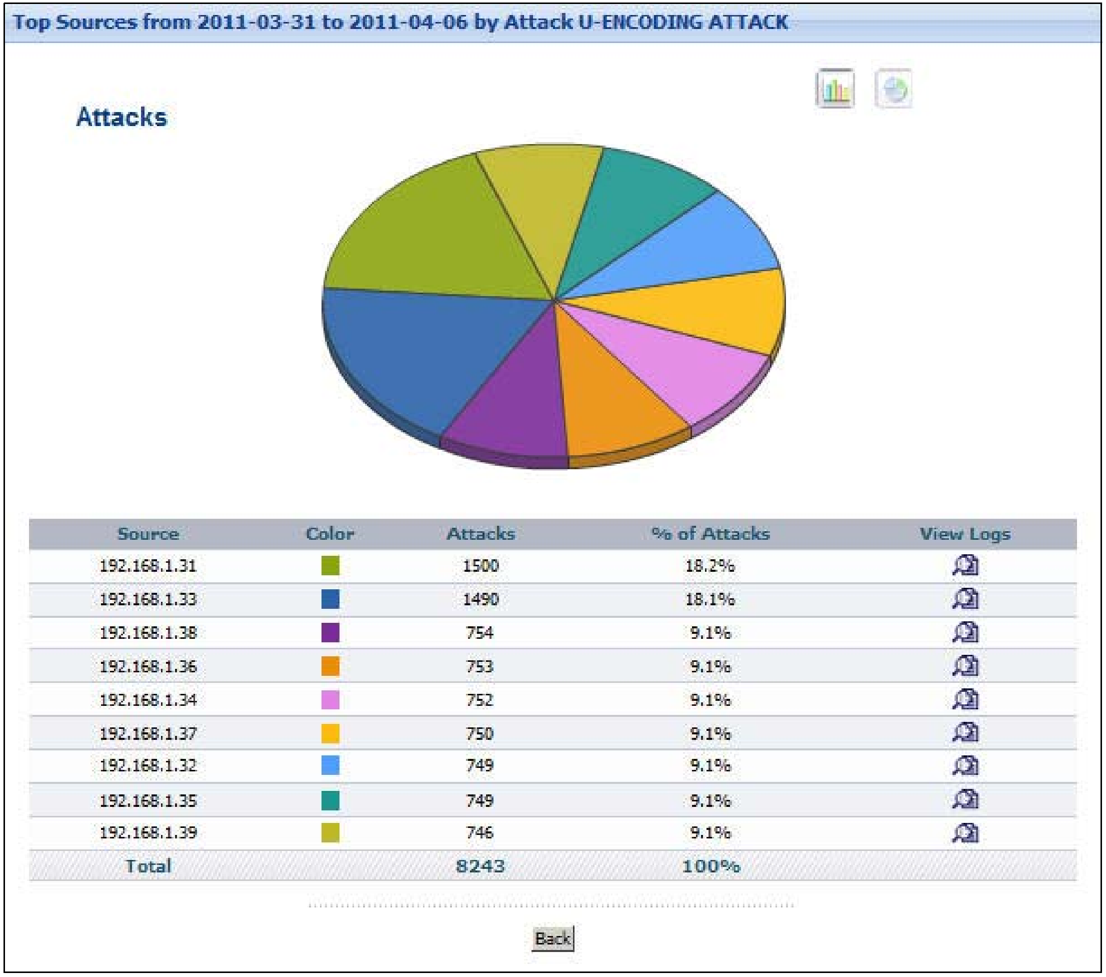
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Attack** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System > General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Attack	This field displays the top categories of DoS attacks in the selected time interval, sorted by the number of attacks by each one.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks from each category occurred in the selected time interval.
% of Attacks	This field displays what percentage of all DoS attacks in the selected time interval comes from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above. If the number of categories in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.

7.2.4 Top Attacks Drill-Down

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

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

Figure 128 Report > Network Security > Attack > Top Attacks > Drill-Down



Top Sources from 2011-03-31 to 2011-04-06 by Attack U-ENCODING ATTACK

Attacks

Source	Color	Attacks	% of Attacks	View Logs
192.168.1.31	🟩	1500	18.2%	🔍
192.168.1.33	🟦	1490	18.1%	🔍
192.168.1.38	🟪	754	9.1%	🔍
192.168.1.36	🟧	753	9.1%	🔍
192.168.1.34	🟪	752	9.1%	🔍
192.168.1.37	🟨	750	9.1%	🔍
192.168.1.32	🟦	749	9.1%	🔍
192.168.1.35	🟩	749	9.1%	🔍
192.168.1.39	🟨	746	9.1%	🔍
Total		8243	100%	

Each field is described in the following table.

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

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

Table 116 Report > Network Security > 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.

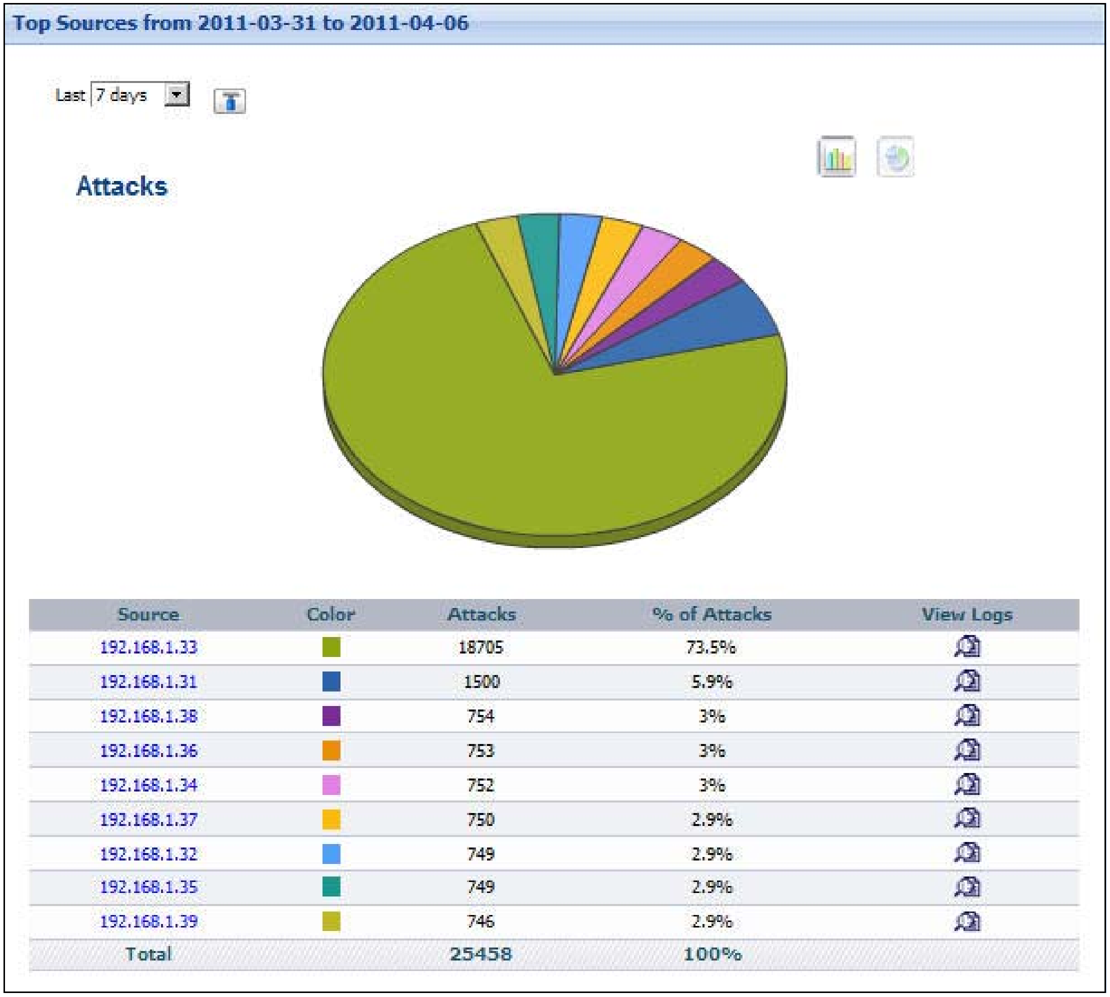
7.2.5 Top Attack Sources

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

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

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

Figure 129 Report > Network Security > Attack > Top Sources

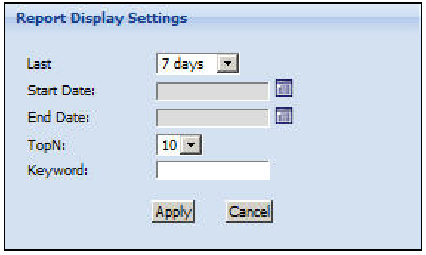


Top Sources from 2011-03-31 to 2011-04-06

Source	Color	Attacks	% of Attacks	View Logs
192.168.1.33	🟩	18705	73.5%	🔍
192.168.1.31	🟦	1500	5.9%	🔍
192.168.1.38	🟪	754	3%	🔍
192.168.1.36	🟧	753	3%	🔍
192.168.1.34	🟪	752	3%	🔍
192.168.1.37	🟨	750	2.9%	🔍
192.168.1.32	🟦	749	2.9%	🔍
192.168.1.35	🟩	749	2.9%	🔍
192.168.1.39	🟨	746	2.9%	🔍
Total		25458	100%	

Each field is described in the following table.

Table 117 Report > Network Security > Attack > Top Sources

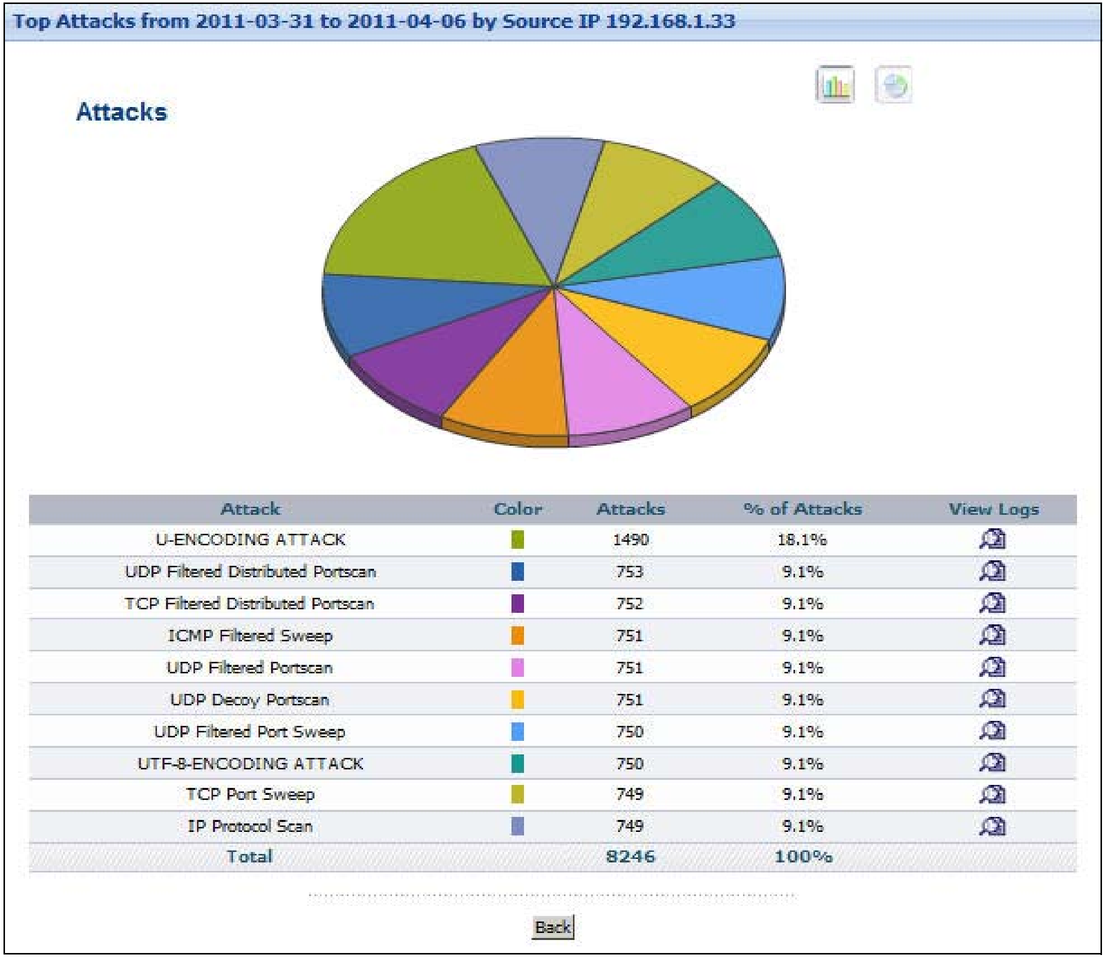
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of DoS attacks in the selected device, sorted by the number of attacks by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a source to look at the top categories of DoS attacks by the selected source.
Color	This field displays what color represents each source in the graph.
Attacks	This field displays the number of DoS attacks by each source.
% of Attacks	This field displays what percentage of all DoS attacks was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.2.6 Top Attack Sources Drill-Down

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

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

Figure 130 Report > Network Security > Attack > Top Sources > Drill-Down



Top Attacks from 2011-03-31 to 2011-04-06 by Source IP 192.168.1.33

Attacks

Attack	Color	Attacks	% of Attacks	View Logs
U-ENCODING ATTACK	🟩	1490	18.1%	🔍
UDP Filtered Distributed Portscan	🟦	753	9.1%	🔍
TCP Filtered Distributed Portscan	🟪	752	9.1%	🔍
ICMP Filtered Sweep	🟧	751	9.1%	🔍
UDP Filtered Portscan	🟪	751	9.1%	🔍
UDP Decoy Portscan	🟨	751	9.1%	🔍
UDP Filtered Port Sweep	🟦	750	9.1%	🔍
UTF-8-ENCODING ATTACK	🟩	750	9.1%	🔍
TCP Port Sweep	🟨	749	9.1%	🔍
IP Protocol Scan	🟦	749	9.1%	🔍
Total		8246	100%	

Each field is described in the following table.

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

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

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

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

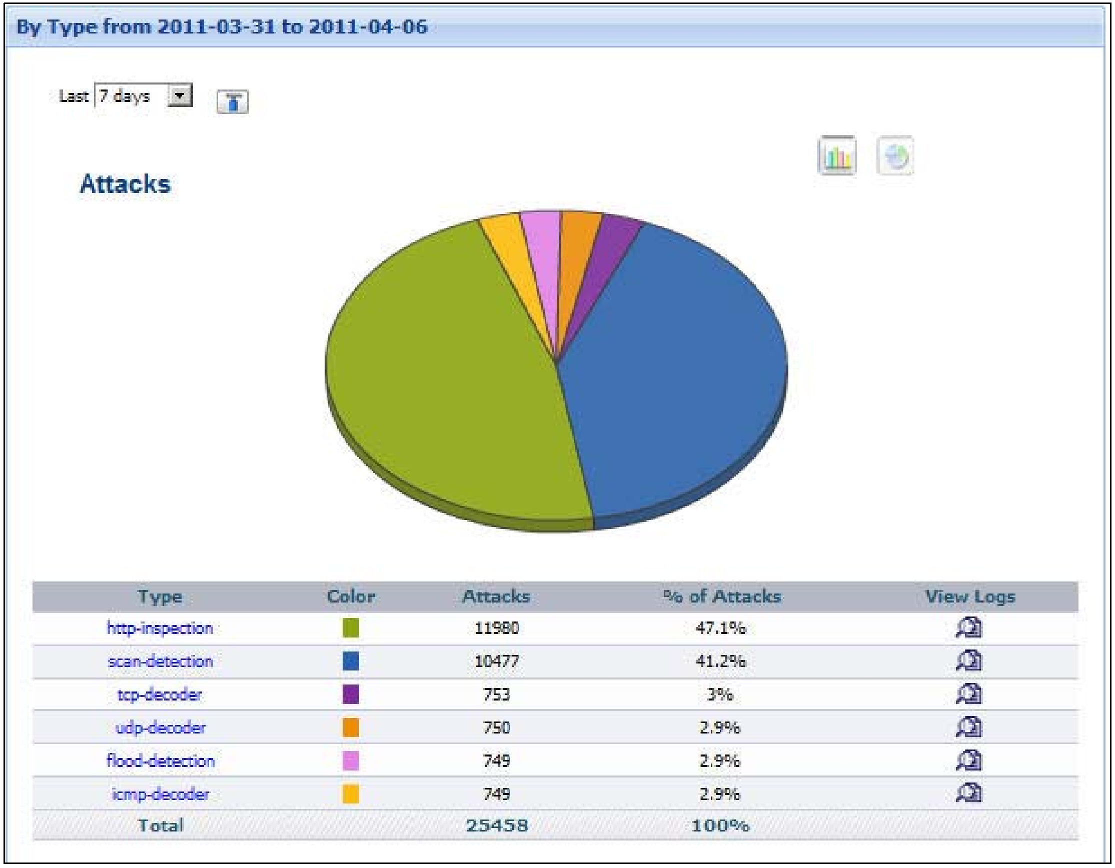
7.2.7 Attack Types

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

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

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

Figure 131 Report > Network Security > Attack > By Type



By Type from 2011-03-31 to 2011-04-06

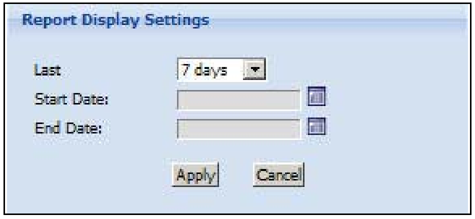
Last 7 days

Attacks

Type	Color	Attacks	% of Attacks	View Logs
http-inspection	🟩	11980	47.1%	🔍
scan-detection	🟦	10477	41.2%	🔍
tcp-decoder	🟪	753	3%	🔍
udp-decoder	🟧	750	2.9%	🔍
flood-detection	■	749	2.9%	🔍
icmp-decoder	🟨	749	2.9%	🔍
Total		25458	100%	

Each field is described in the following table.

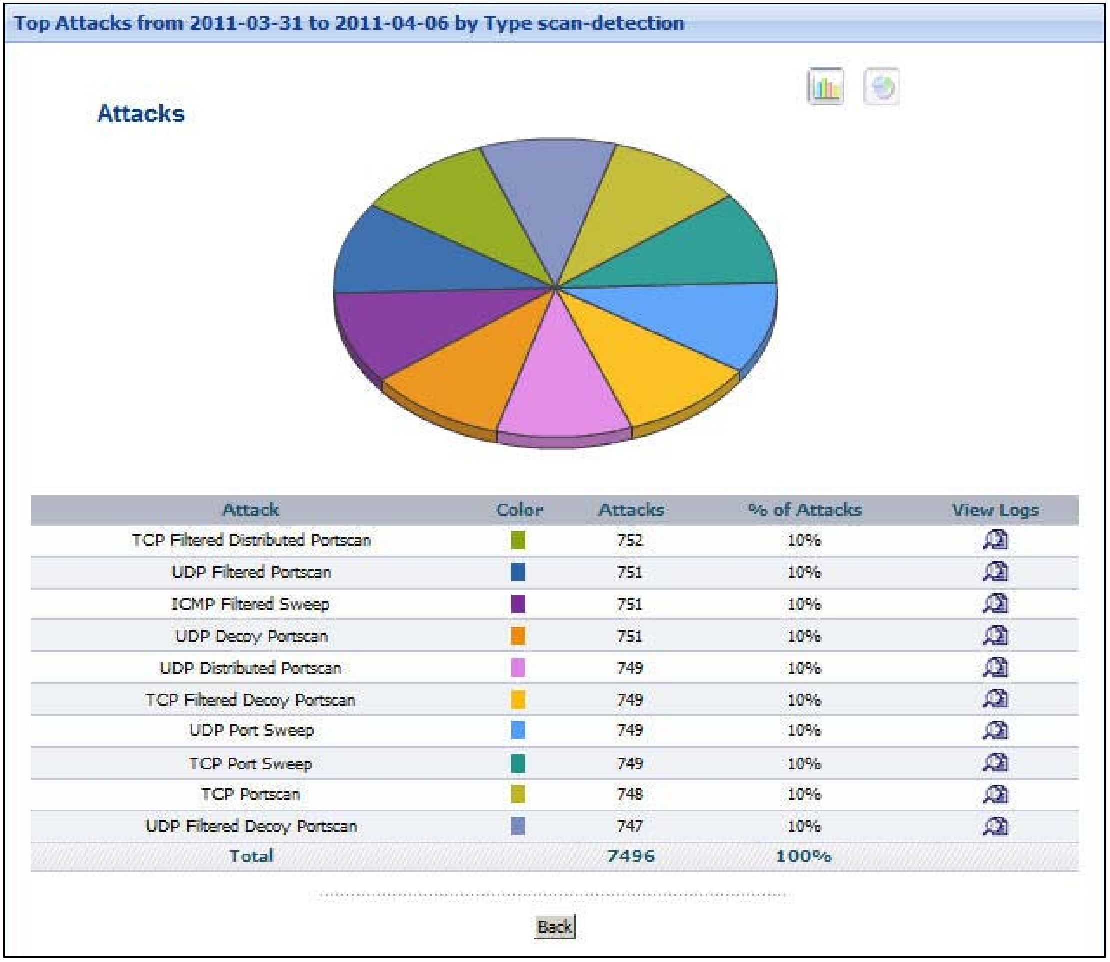
Table 119 Report > Network Security > Attack > By Type

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Type	This field displays the categories of DoS attacks in the selected device, sorted by the number of attacks by each one. Click on a category to look at the DoS attacks in the selected category.
Color	This field displays what color represents each category in the graph.
Attacks	This field displays how many DoS attacks from each category the device stopped.
% of Attacks	This field displays what percentage of all DoS attacks come from each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

7.2.8 Attack Types Drill-Down

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

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



Top Attacks from 2011-03-31 to 2011-04-06 by Type scan-detection

Attacks

Attack	Color	Attacks	% of Attacks	View Logs
TCP Filtered Distributed Portscan	🟩	752	10%	🔍
UDP Filtered Portscan	🟦	751	10%	🔍
ICMP Filtered Sweep	🟪	751	10%	🔍
UDP Decoy Portscan	🟧	751	10%	🔍
UDP Distributed Portscan	🟪	749	10%	🔍
TCP Filtered Decoy Portscan	🟨	749	10%	🔍
UDP Port Sweep	🟦	749	10%	🔍
TCP Port Sweep	🟩	749	10%	🔍
TCP Portscan	🟨	748	10%	🔍
UDP Filtered Decoy Portscan	🟪	747	10%	🔍
Total		7496	100%	

Figure 132 Report > Network Security > Attack > By Type > Drill-Down

Each field is described in the following table.

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

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

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

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

7.3 Intrusion Hits

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

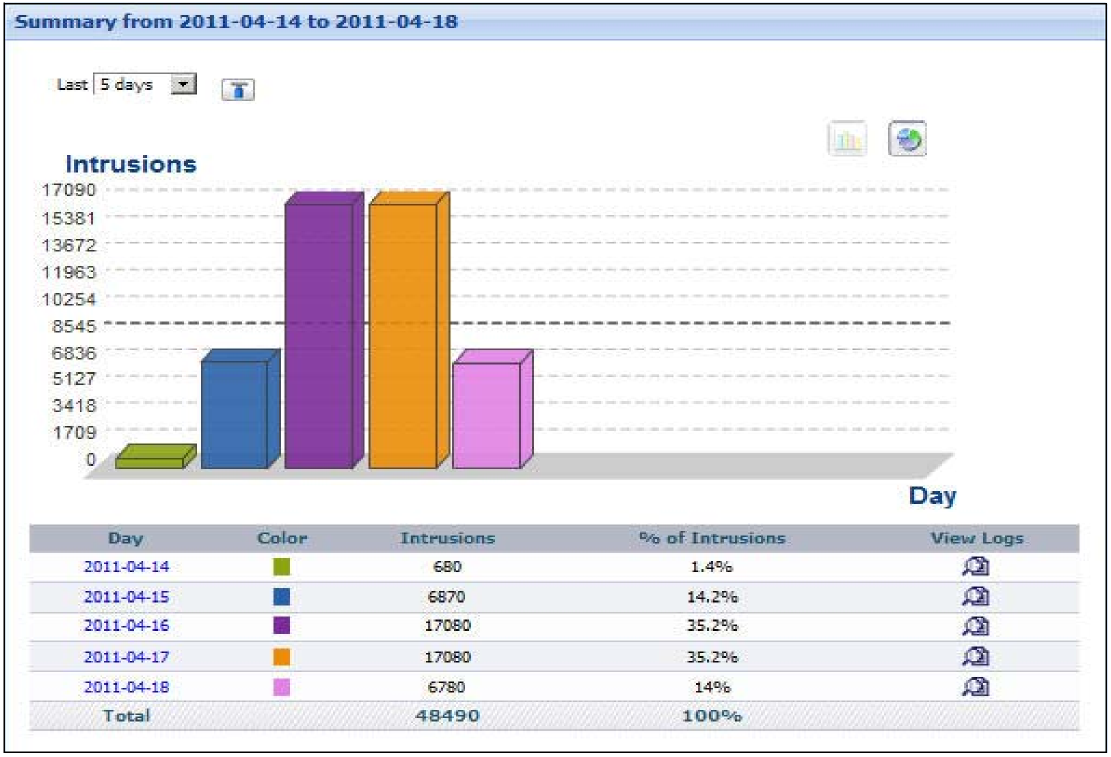
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP** > **Signature**, and make sure the ZyXEL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

7.3.1 Intrusion Hits Summary

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

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

Figure 133 Report > Network Security > Intrusion Hits > Summary



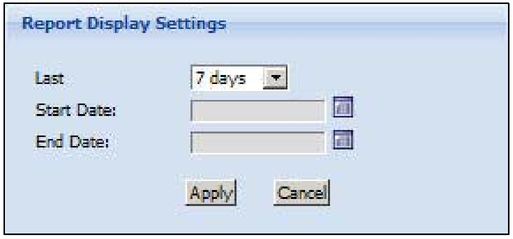
Summary from 2011-04-14 to 2011-04-18

Last 5 days

Day	Color	Intrusions	% of Intrusions	View Logs
2011-04-14	🟩	680	1.4%	🔍
2011-04-15	🟦	6870	14.2%	🔍
2011-04-16	🟪	17080	35.2%	🔍
2011-04-17	🟧	17080	35.2%	🔍
2011-04-18	■	6780	14%	🔍
Total		48490	100%	

Each field is described in the following table.

Table 121 Report > Network Security > Intrusion Hits > Summary

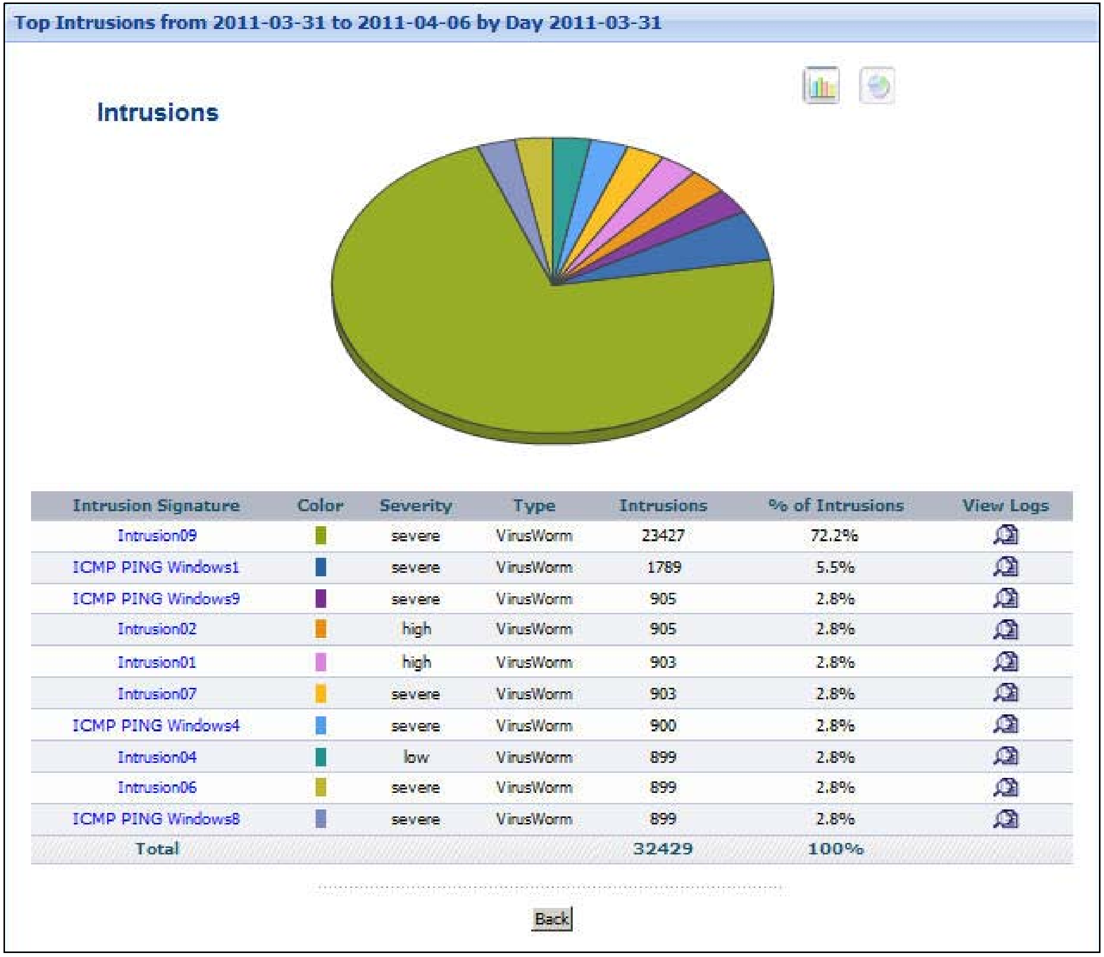
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the intrusion signatures in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Intrusions	This field displays the number of intrusions in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.3.2 Intrusion Hits Summary Drill-Down

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

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

Figure 134 Report > Network Security > Intrusion Hits > Summary > Drill-Down



Top Intrusions from 2011-03-31 to 2011-04-06 by Day 2011-03-31

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	VirusWorm	23427	72.2%	🔍
ICMP PING Windows1	🟦	severe	VirusWorm	1789	5.5%	🔍
ICMP PING Windows9	🟪	severe	VirusWorm	905	2.8%	🔍
Intrusion02	🟧	high	VirusWorm	905	2.8%	🔍
Intrusion01	🟪	high	VirusWorm	903	2.8%	🔍
Intrusion07	🟨	severe	VirusWorm	903	2.8%	🔍
ICMP PING Windows4	🟦	severe	VirusWorm	900	2.8%	🔍
Intrusion04	🟩	low	VirusWorm	899	2.8%	🔍
Intrusion06	🟨	severe	VirusWorm	899	2.8%	🔍
ICMP PING Windows8	🟦	severe	VirusWorm	899	2.8%	🔍
Total				32429	100%	

Each field is described in the following table.

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

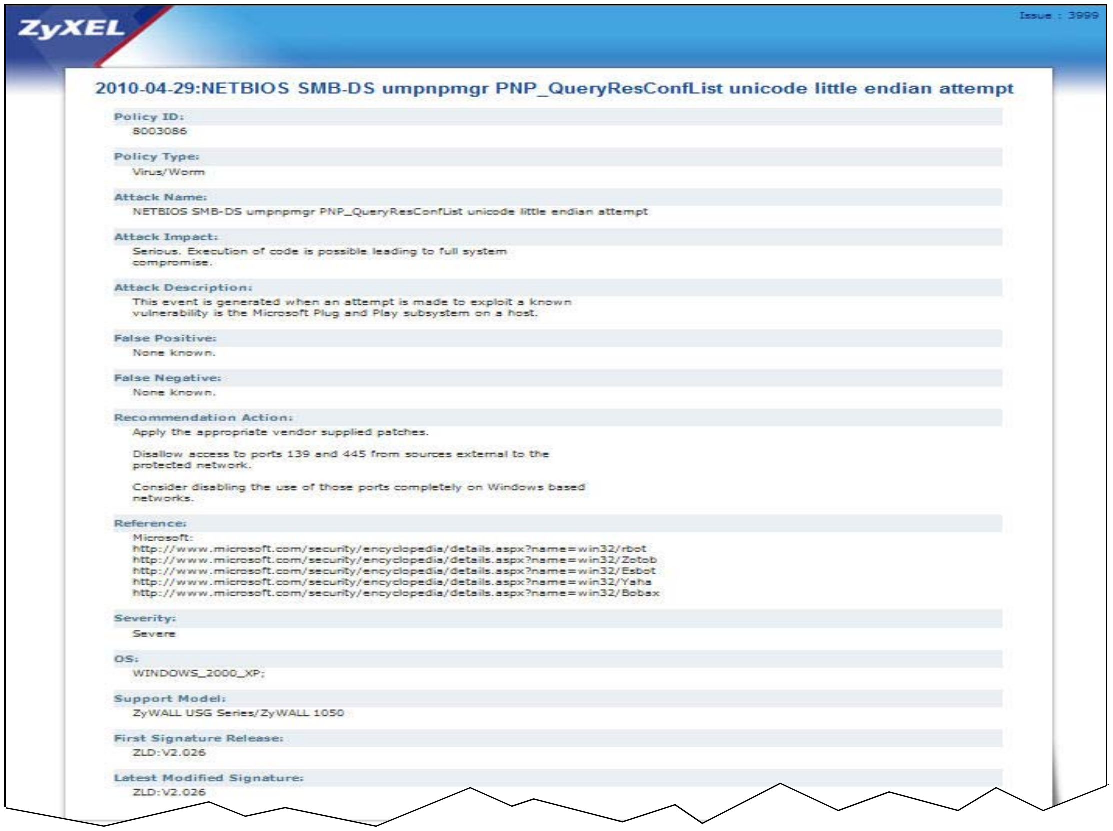
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 135 on page 243).
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 122 Report > Network Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

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

Figure 135 Security Issue Details



2010-04-29:NETBIOS SMB-DS umpnpmgr PNP_QueryResConfList unicode little endian attempt

Policy ID:
8003086

Policy Type:
Virus/Worm

Attack Name:
NETBIOS SMB-DS umpnpmgr PNP_QueryResConfList unicode little endian attempt

Attack Impact:
Serious. Execution of code is possible leading to full system compromise.

Attack Description:
This event is generated when an attempt is made to exploit a known vulnerability is the Microsoft Plug and Play subsystem on a host.

False Positive:
None known.

False Negative:
None known.

Recommendation Action:
Apply the appropriate vendor supplied patches.

Disallow access to ports 139 and 445 from sources external to the protected network.

Consider disabling the use of those ports completely on Windows based networks.

Reference:
Microsoft:
http://www.microsoft.com/security/encyclopedia/details.aspx?name=win32/rbot
http://www.microsoft.com/security/encyclopedia/details.aspx?name=win32/Zotob
http://www.microsoft.com/security/encyclopedia/details.aspx?name=win32/Esbot
http://www.microsoft.com/security/encyclopedia/details.aspx?name=win32/Yaha
http://www.microsoft.com/security/encyclopedia/details.aspx?name=win32/Bobax

Severity:
Severe

OS:
WINDOWS_2000_XP;

Support Model:
ZyWALL USG Series/ZyWALL 1050

First Signature Release:
ZLD:V2.026

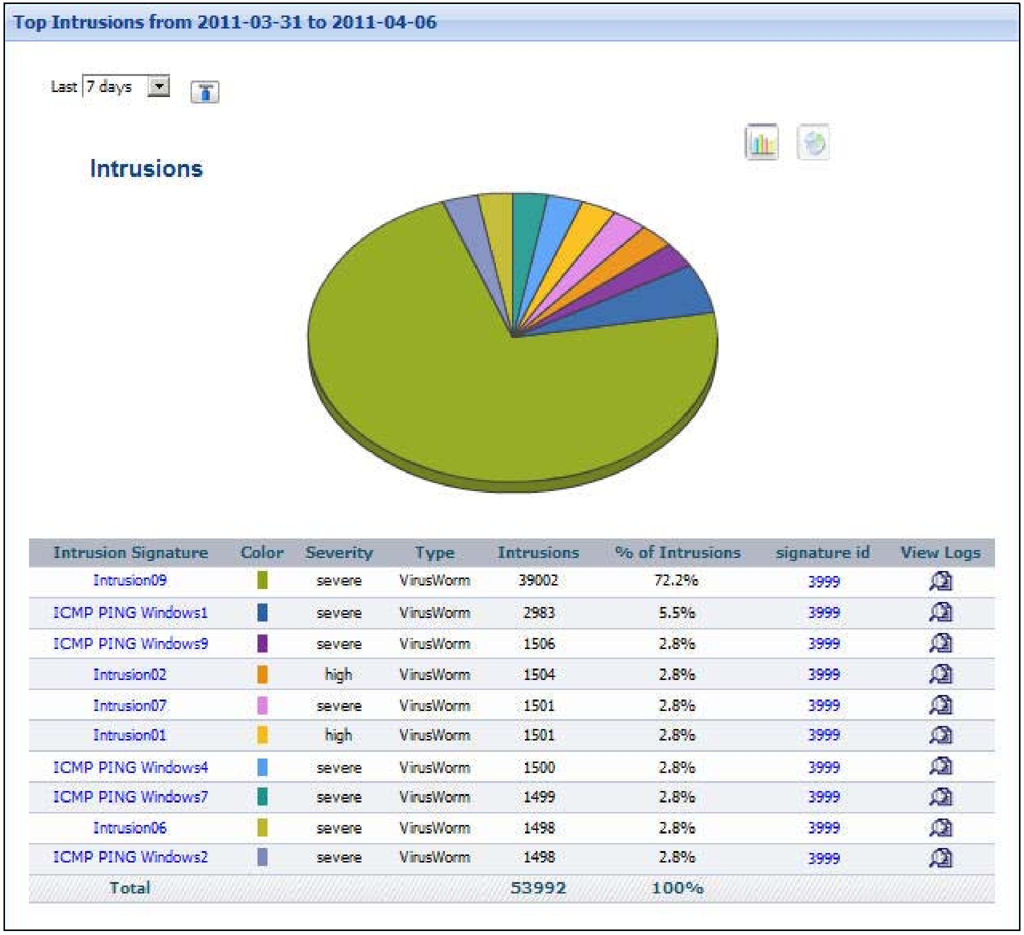
Latest Modified Signature:
ZLD:V2.026

7.3.3 Top Intrusion Hits Signatures

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

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

Figure 136 Report > Network Security > Intrusion Hits > Top Intrusions



Top Intrusions from 2011-03-31 to 2011-04-06

Last 7 days

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	signature id	View Logs
Intrusion09	🟩	severe	VirusWorm	39002	72.2%	3999	🔍
ICMP PING Windows1	🟦	severe	VirusWorm	2983	5.5%	3999	🔍
ICMP PING Windows9	🟪	severe	VirusWorm	1506	2.8%	3999	🔍
Intrusion02	🟧	high	VirusWorm	1504	2.8%	3999	🔍
Intrusion07	🟪	severe	VirusWorm	1501	2.8%	3999	🔍
Intrusion01	🟨	high	VirusWorm	1501	2.8%	3999	🔍
ICMP PING Windows4	🟦	severe	VirusWorm	1500	2.8%	3999	🔍
ICMP PING Windows7	🟩	severe	VirusWorm	1499	2.8%	3999	🔍
Intrusion06	🟨	severe	VirusWorm	1498	2.8%	3999	🔍
ICMP PING Windows2	🟪	severe	VirusWorm	1498	2.8%	3999	🔍
Total				53992	100%		

Each field is described in the following table.

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

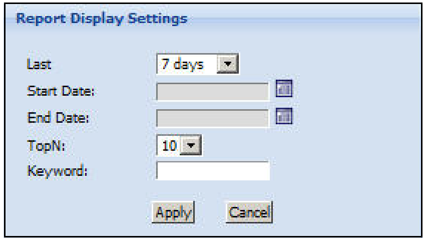
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Intrusion Signature** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP** > **Signature** > **Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
signature id	This is the security issue identification number. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 135 on page 243).

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

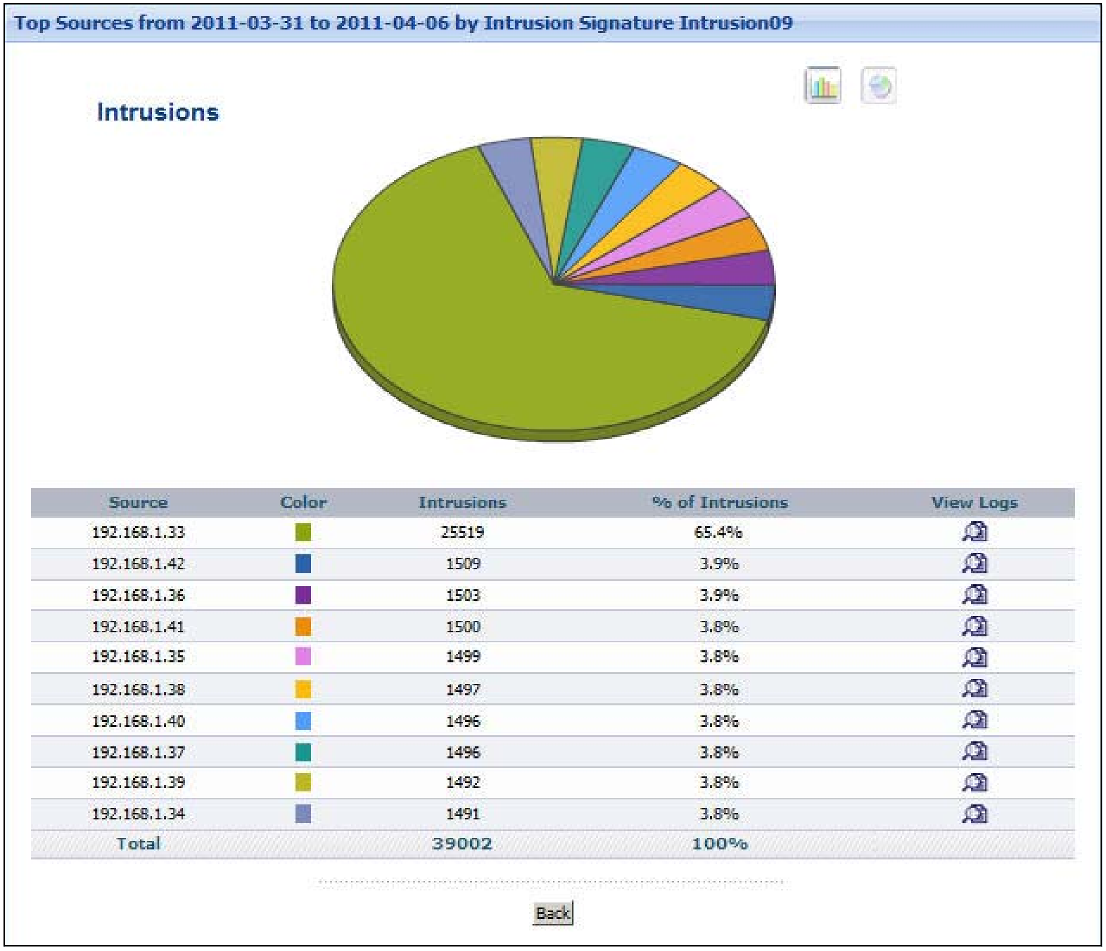
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

7.3.4 Top Intrusion Hits Signatures Drill-Down

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

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

Figure 137 Report > Network Security > Intrusion Hits > Top Intrusions > Drill-Down



Top Sources from 2011-03-31 to 2011-04-06 by Intrusion Signature Intrusion09

Source	Color	Intrusions	% of Intrusions	View Logs
192.168.1.33	■	25519	65.4%	🔍
192.168.1.42	■	1509	3.9%	🔍
192.168.1.36	■	1503	3.9%	🔍
192.168.1.41	■	1500	3.8%	🔍
192.168.1.35	■	1499	3.8%	🔍
192.168.1.38	■	1497	3.8%	🔍
192.168.1.40	■	1496	3.8%	🔍
192.168.1.37	■	1496	3.8%	🔍
192.168.1.39	■	1492	3.8%	🔍
192.168.1.34	■	1491	3.8%	🔍
Total		39002	100%	

Each field is described in the following table.

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

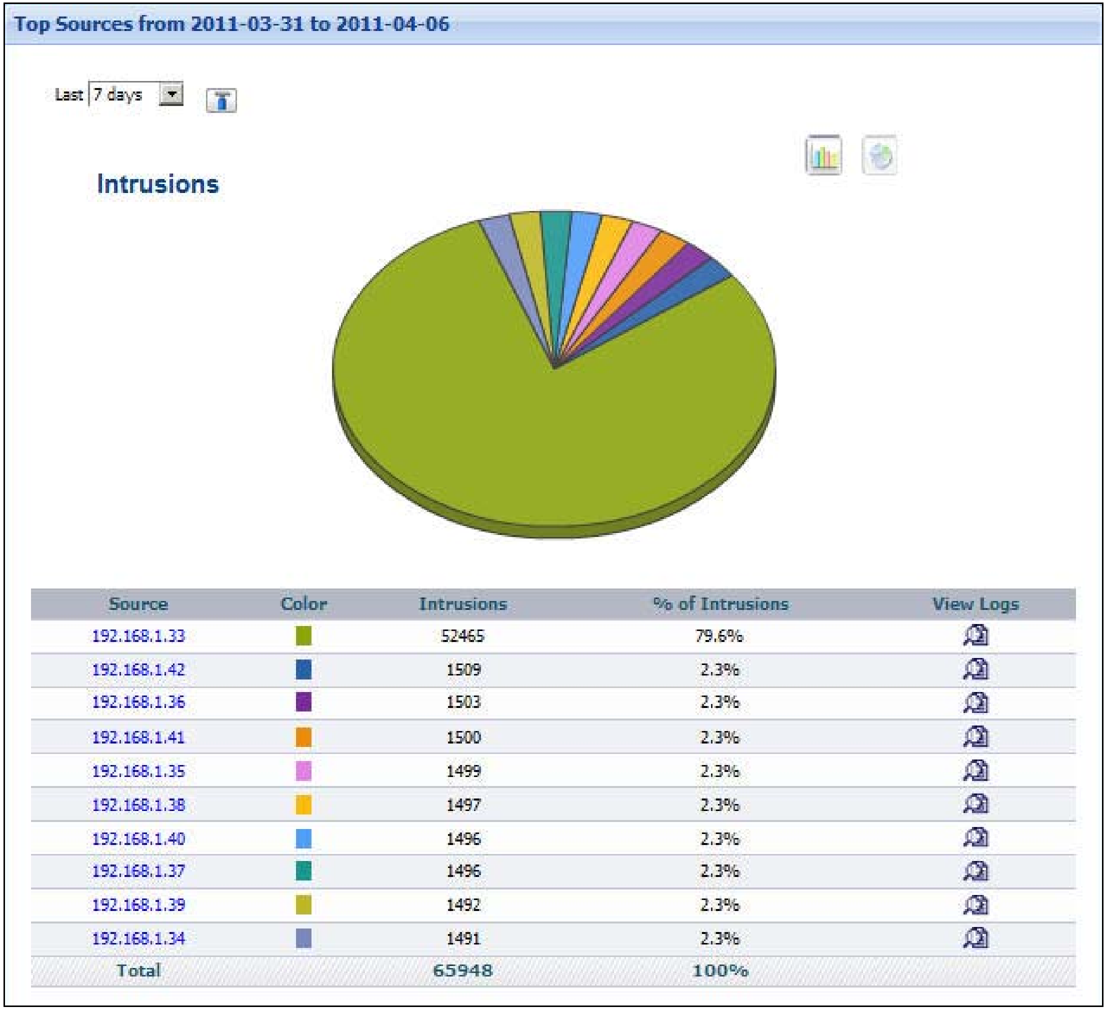
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

7.3.5 Top Intrusion Hits Sources

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

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

Figure 138 Report > Network Security > Intrusion Hits > Top Sources



Top Sources from 2011-03-31 to 2011-04-06

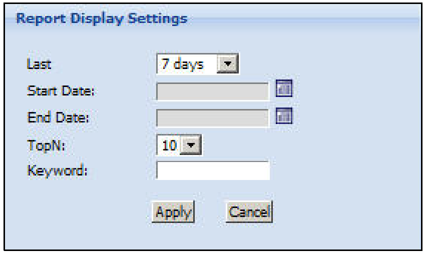
Last 7 days

Intrusions

Source	Color	Intrusions	% of Intrusions	View Logs
192.168.1.33	🟩	52465	79.6%	🔍
192.168.1.42	🟦	1509	2.3%	🔍
192.168.1.36	🟪	1503	2.3%	🔍
192.168.1.41	🟧	1500	2.3%	🔍
192.168.1.35	🟪	1499	2.3%	🔍
192.168.1.38	🟨	1497	2.3%	🔍
192.168.1.40	🟦	1496	2.3%	🔍
192.168.1.37	🟩	1496	2.3%	🔍
192.168.1.39	🟨	1492	2.3%	🔍
192.168.1.34	🟦	1491	2.3%	🔍
Total		65948	100%	

Each field is described in the following table.

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

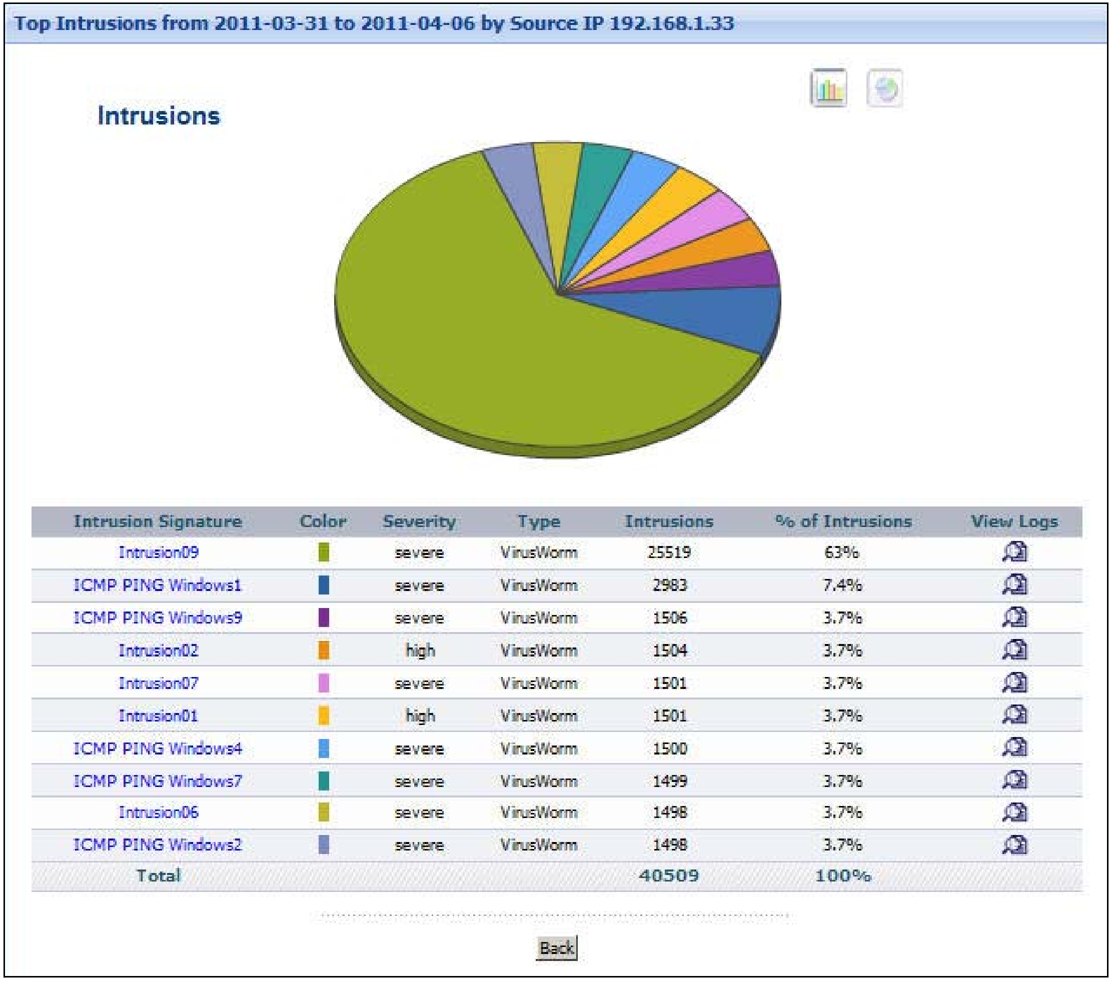
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a source to look at the top intrusion signatures for the selected source.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.3.6 Top Intrusion Hits Sources Drill-Down

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

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

Figure 139 Report > Network Security > Intrusion Hits > Top Sources > Drill-Down



Top Intrusions from 2011-03-31 to 2011-04-06 by Source IP 192.168.1.33

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	VirusWorm	25519	63%	🔍
ICMP PING Windows1	🟦	severe	VirusWorm	2983	7.4%	🔍
ICMP PING Windows9	🟪	severe	VirusWorm	1506	3.7%	🔍
Intrusion02	🟧	high	VirusWorm	1504	3.7%	🔍
Intrusion07	🟪	severe	VirusWorm	1501	3.7%	🔍
Intrusion01	🟨	high	VirusWorm	1501	3.7%	🔍
ICMP PING Windows4	🟦	severe	VirusWorm	1500	3.7%	🔍
ICMP PING Windows7	🟩	severe	VirusWorm	1499	3.7%	🔍
Intrusion06	🟨	severe	VirusWorm	1498	3.7%	🔍
ICMP PING Windows2	🟦	severe	VirusWorm	1498	3.7%	🔍
Total				40509	100%	

Each field is described in the following table.

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

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

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

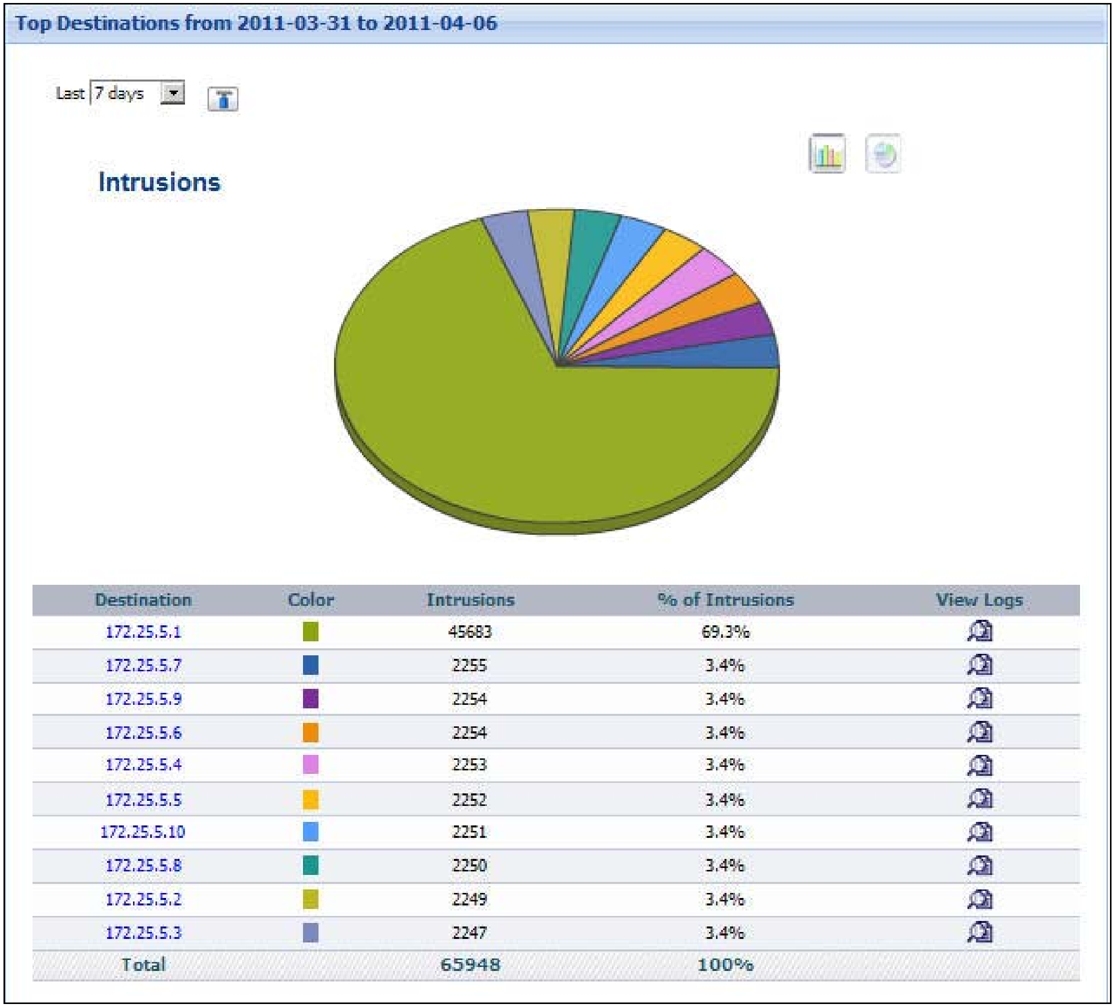
LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by the selected source using each intrusion signature.
% of Intrusions	This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

7.3.7 Top Intrusion Hits Destinations

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

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

Figure 140 Report > Network Security > Intrusion Hits > Top Destinations

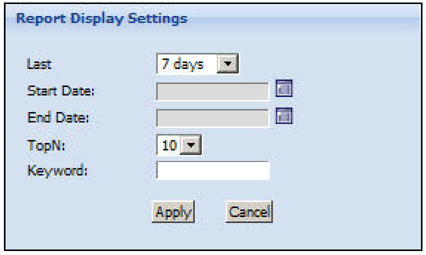


Top Destinations from 2011-03-31 to 2011-04-06

Destination	Color	Intrusions	% of Intrusions	View Logs
172.25.5.1	🟩	45683	69.3%	🔍
172.25.5.7	🟦	2255	3.4%	🔍
172.25.5.9	🟪	2254	3.4%	🔍
172.25.5.6	🟧	2254	3.4%	🔍
172.25.5.4	🟪	2253	3.4%	🔍
172.25.5.5	🟨	2252	3.4%	🔍
172.25.5.10	🟦	2251	3.4%	🔍
172.25.5.8	🟩	2250	3.4%	🔍
172.25.5.2	🟨	2249	3.4%	🔍
172.25.5.3	🟦	2247	3.4%	🔍
Total		65948	100%	

Each field is described in the following table.

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

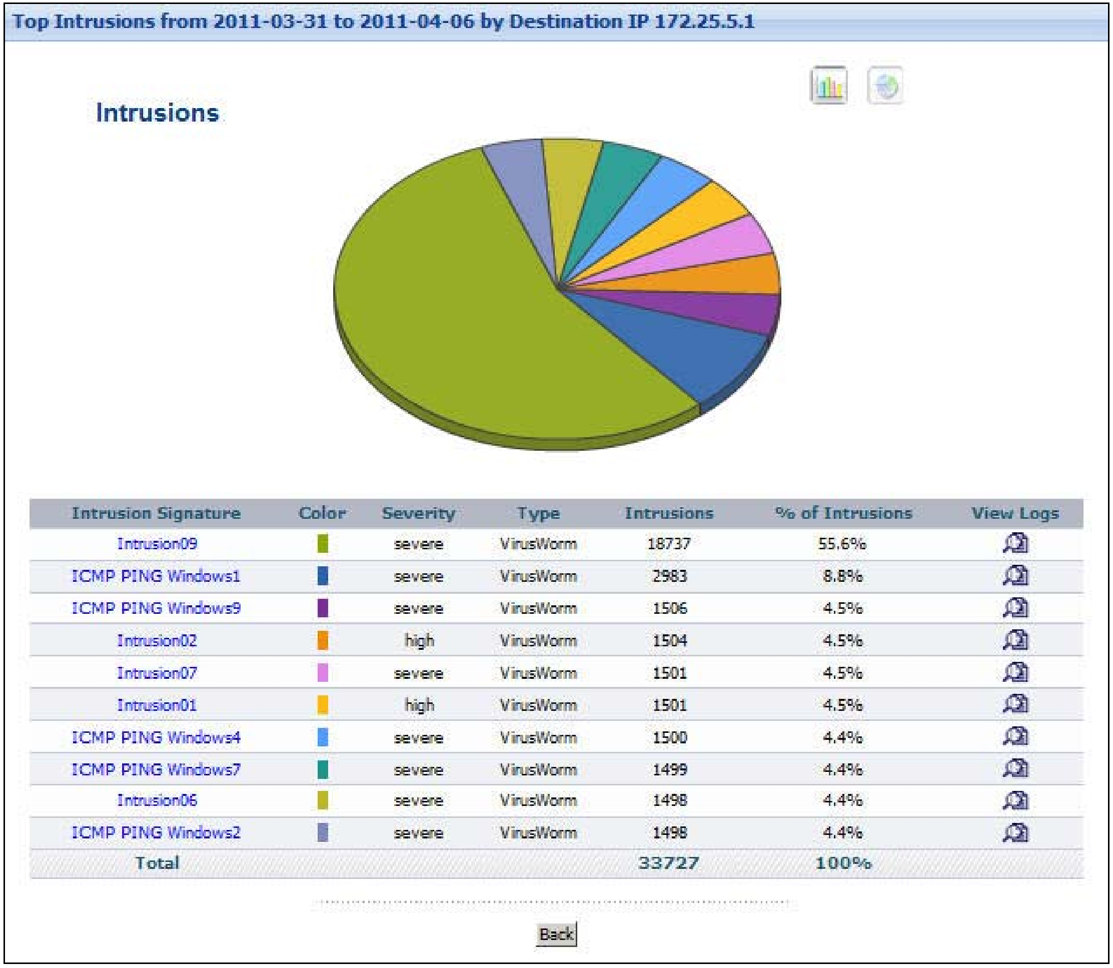
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System > General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a destination to look at the top intrusion signatures for the selected destination.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

7.3.8 Top Intrusion Hits Destinations Drill-Down

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

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

Figure 141 Report > Network Security > Intrusion Hits > Top Destinations > Drill-Down



Top Intrusions from 2011-03-31 to 2011-04-06 by Destination IP 172.25.5.1

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	VirusWorm	18737	55.6%	🔍
ICMP PING Windows1	🟦	severe	VirusWorm	2983	8.8%	🔍
ICMP PING Windows9	🟪	severe	VirusWorm	1506	4.5%	🔍
Intrusion02	🟧	high	VirusWorm	1504	4.5%	🔍
Intrusion07	🟪	severe	VirusWorm	1501	4.5%	🔍
Intrusion01	🟨	high	VirusWorm	1501	4.5%	🔍
ICMP PING Windows4	🟦	severe	VirusWorm	1500	4.4%	🔍
ICMP PING Windows7	🟩	severe	VirusWorm	1499	4.4%	🔍
Intrusion06	🟨	severe	VirusWorm	1498	4.4%	🔍
ICMP PING Windows2	🟦	severe	VirusWorm	1498	4.4%	🔍
Total				33727	100%	

Each field is described in the following table.

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

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

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

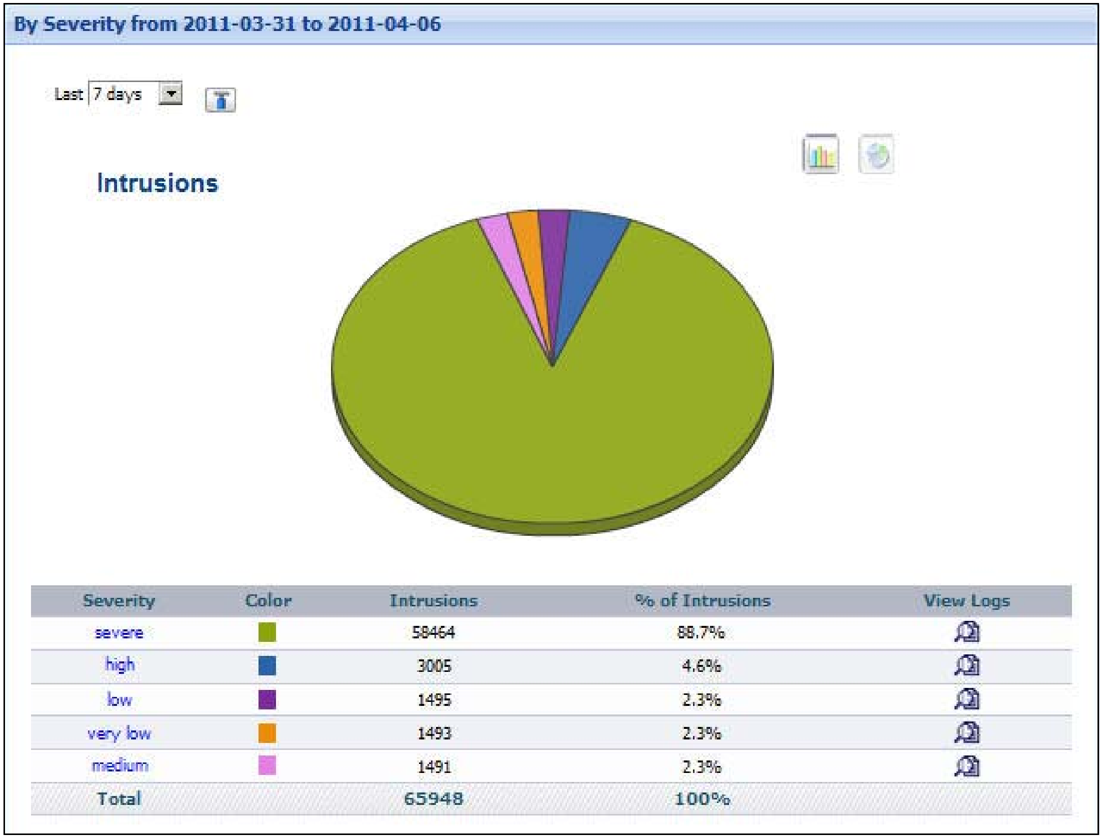
LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP** > **Signature** > **Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of each intrusion signature sent to the selected destination.
% of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

7.3.9 Intrusion Hits Severities

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

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

Figure 142 Report > Network Security > Intrusion Hits > By Severity



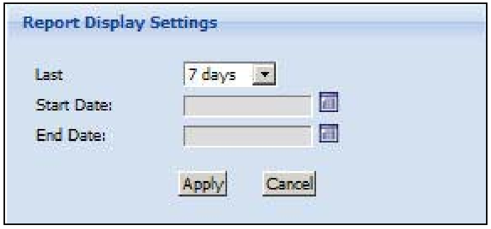
By Severity from 2011-03-31 to 2011-04-06

Last 7 days

Severity	Color	Intrusions	% of Intrusions	View Logs
severe	🟩	58464	88.7%	🔍
high	🟦	3005	4.6%	🔍
low	🟪	1495	2.3%	🔍
very low	🟧	1493	2.3%	🔍
medium	■	1491	2.3%	🔍
Total		65948	100%	

Each field is described in the following table.

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

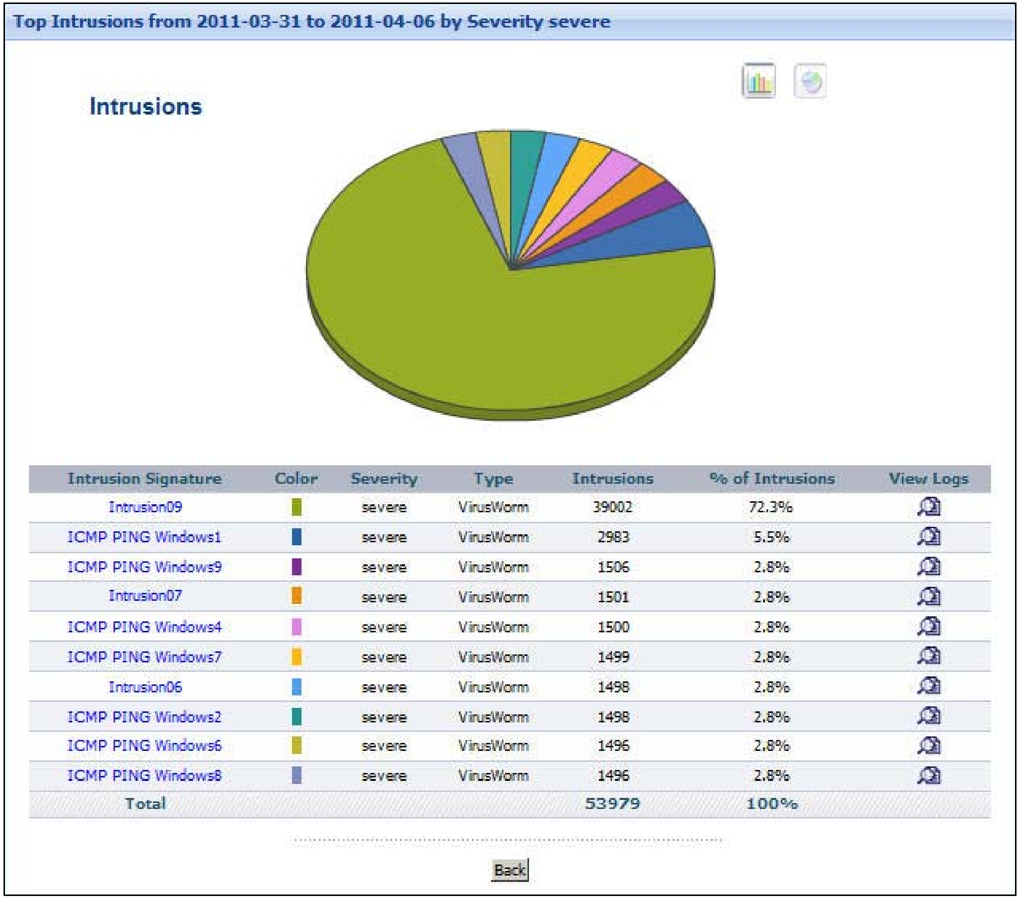
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

7.3.10 Intrusion Hits Severities Drill-Down

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

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

Figure 143 Report > Network Security > Intrusion Hits > By Severity > Drill-Down



Top Intrusions from 2011-03-31 to 2011-04-06 by Severity severe

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	VirusWorm	39002	72.3%	🔍
ICMP PING Windows1	🟦	severe	VirusWorm	2983	5.5%	🔍
ICMP PING Windows9	🟪	severe	VirusWorm	1506	2.8%	🔍
Intrusion07	🟧	severe	VirusWorm	1501	2.8%	🔍
ICMP PING Windows4	🟪	severe	VirusWorm	1500	2.8%	🔍
ICMP PING Windows7	🟨	severe	VirusWorm	1499	2.8%	🔍
Intrusion06	🟦	severe	VirusWorm	1498	2.8%	🔍
ICMP PING Windows2	🟩	severe	VirusWorm	1498	2.8%	🔍
ICMP PING Windows6	🟨	severe	VirusWorm	1496	2.8%	🔍
ICMP PING Windows8	🟪	severe	VirusWorm	1496	2.8%	🔍
Total				53979	100%	

Each field is described in the following table.

Table 130 Report > Network Security > Intrusion Hits > By Severity > Drill-Down

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

Table 130 Report > Network Security > Intrusion Hits > By Severity > 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 intrusion signatures above.
Back	Click this to return to the main report.

7.4 Antivirus

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

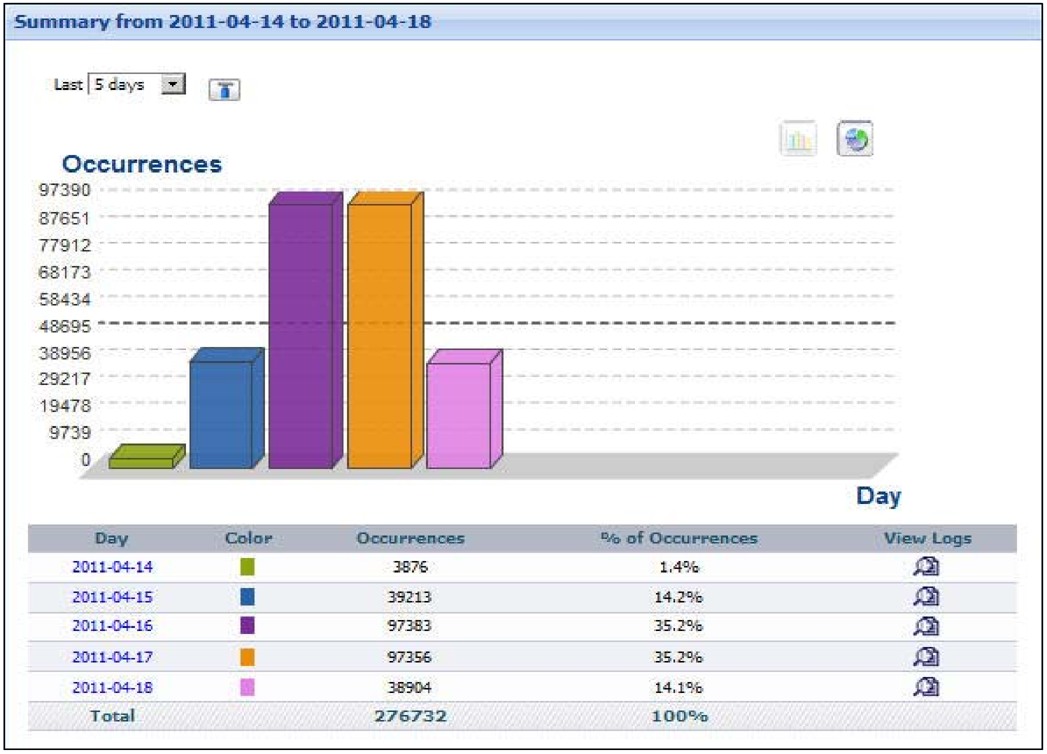
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus** > **General**. ZyXEL devices can log viruses based on the **Service** the virus was using. Make sure the ZyXEL device logs viruses you want to include in Vantage Report.

7.4.1 Antivirus Summary

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

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

Figure 144 Report > Network Security > AntiVirus > Summary

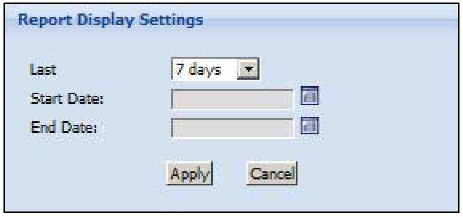


Summary from 2011-04-14 to 2011-04-18

Day	Color	Occurrences	% of Occurrences	View Logs
2011-04-14	🟩	3876	1.4%	🔍
2011-04-15	🟦	39213	14.2%	🔍
2011-04-16	🟪	97383	35.2%	🔍
2011-04-17	🟧	97356	35.2%	🔍
2011-04-18	■	38904	14.1%	🔍
Total		276732	100%	

Each field is described in the following table.

Table 131 Report > Network Security > AntiVirus > Summary

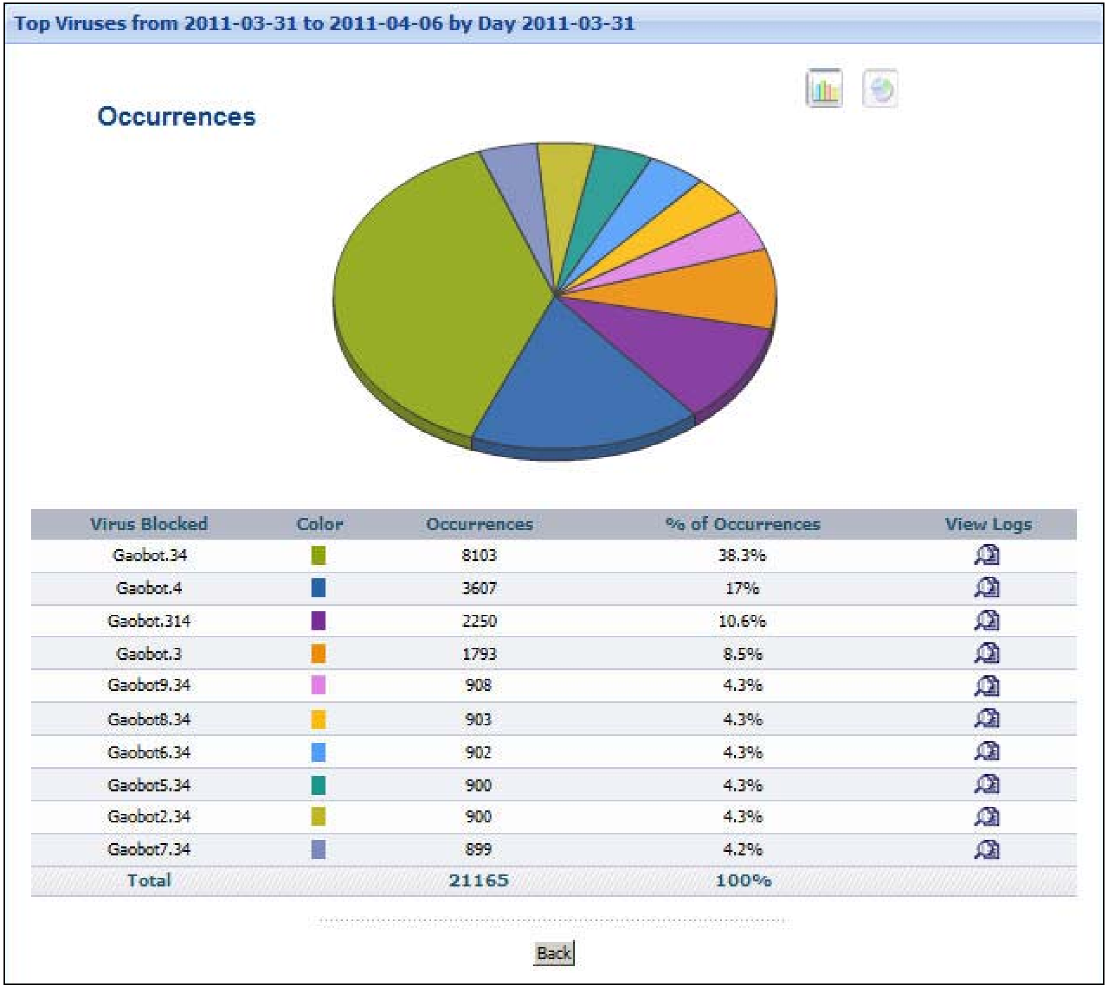
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Apply Cancel 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

7.4.2 Virus Summary Drill-Down

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

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

Figure 145 Report > Network Security > AntiVirus > Summary > Drill-Down



Top Viruses from 2011-03-31 to 2011-04-06 by Day 2011-03-31

Occurrences

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	■	8103	38.3%	🔍
Gaobot.4	■	3607	17%	🔍
Gaobot.314	■	2250	10.6%	🔍
Gaobot.3	■	1793	8.5%	🔍
Gaobot9.34	■	908	4.3%	🔍
Gaobot8.34	■	903	4.3%	🔍
Gaobot6.34	■	902	4.3%	🔍
Gaobot5.34	■	900	4.3%	🔍
Gaobot2.34	■	900	4.3%	🔍
Gaobot7.34	■	899	4.2%	🔍
Total		21165	100%	

Each field is described in the following table.

Table 132 Report > Network Security > AntiVirus > Summary > Drill-Down

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

Table 132 Report > Network Security > AntiVirus > Summary > Drill-Down

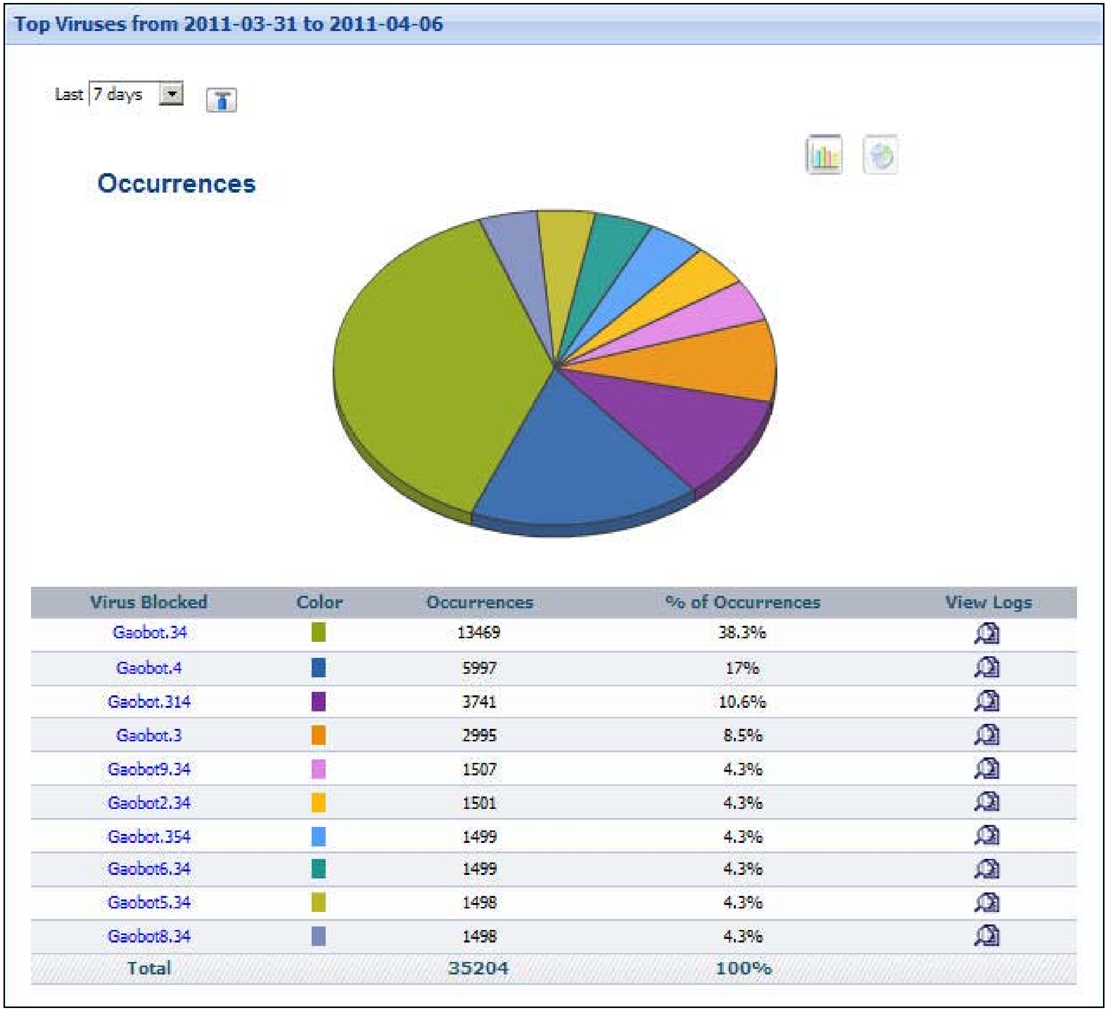
LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to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

7.4.3 Top Viruses

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

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

Figure 146 Report > Network Security > AntiVirus > Top Viruses



Top Viruses from 2011-03-31 to 2011-04-06

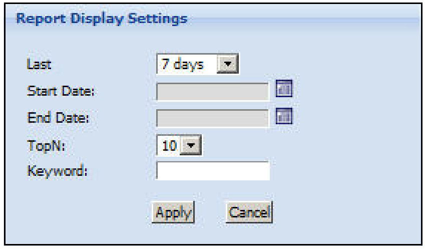
Last 7 days

Occurrences

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	13469	38.3%	🔍
Gaobot.4	🟦	5997	17%	🔍
Gaobot.314	🟪	3741	10.6%	🔍
Gaobot.3	🟧	2995	8.5%	🔍
Gaobot9.34	🟪	1507	4.3%	🔍
Gaobot2.34	🟨	1501	4.3%	🔍
Gaobot.354	🟦	1499	4.3%	🔍
Gaobot6.34	🟩	1499	4.3%	🔍
Gaobot5.34	🟨	1498	4.3%	🔍
Gaobot8.34	🟪	1498	4.3%	🔍
Total		35204	100%	

Each field is described in the following table.

Table 133 Report > Network Security > AntiVirus > Top Viruses

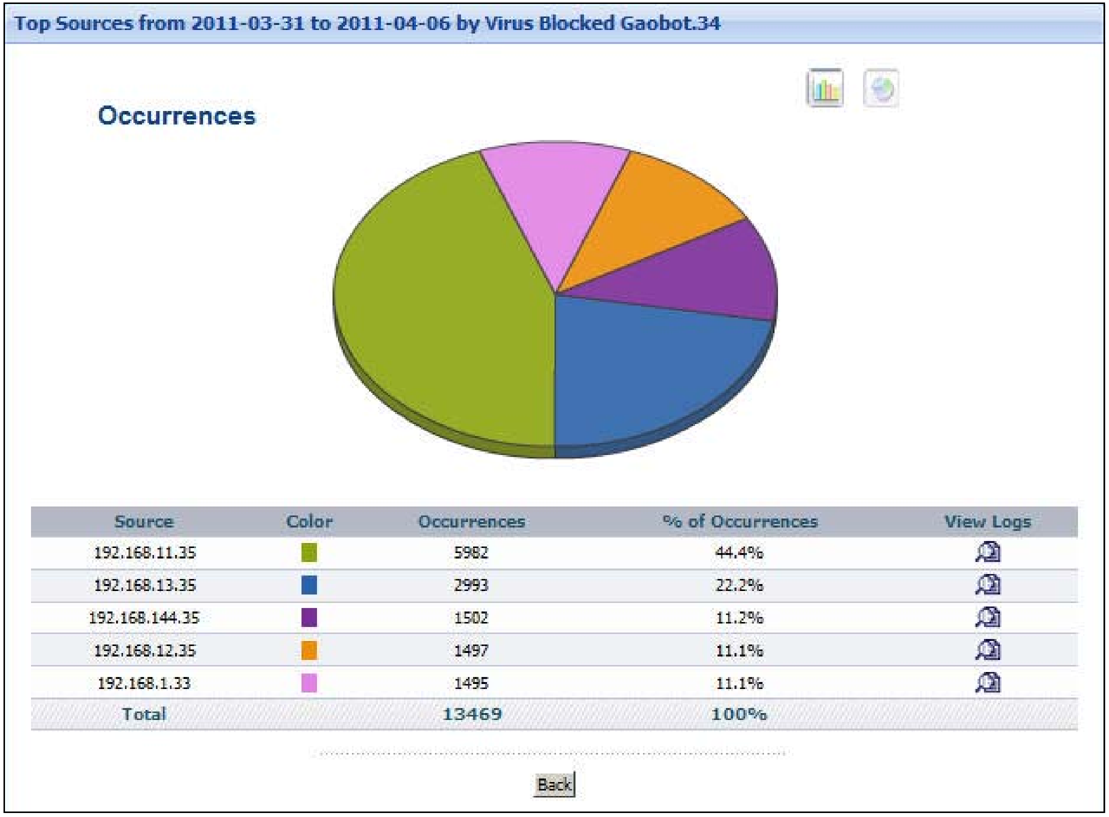
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Virus Blocked** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.
% of Occurrences	This field displays what percentage each virus's occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

7.4.4 Top Viruses Drill-Down

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

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

Figure 147 Report > Network Security > AntiVirus > Top Viruses > Drill-Down



Top Sources from 2011-03-31 to 2011-04-06 by Virus Blocked Gaobot.34

Source	Color	Occurrences	% of Occurrences	View Logs
192.168.11.35	🟩	5982	44.4%	🔍
192.168.13.35	🟦	2993	22.2%	🔍
192.168.144.35	🟪	1502	11.2%	🔍
192.168.12.35	🟧	1497	11.1%	🔍
192.168.1.33	■	1495	11.1%	🔍
Total		13469	100%	

Each field is described in the following table.

Table 134 Report > Network Security > AntiVirus > Top Viruses > Drill-Down

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

Table 134 Report > Network Security > AntiVirus > Top Viruses > Drill-Down

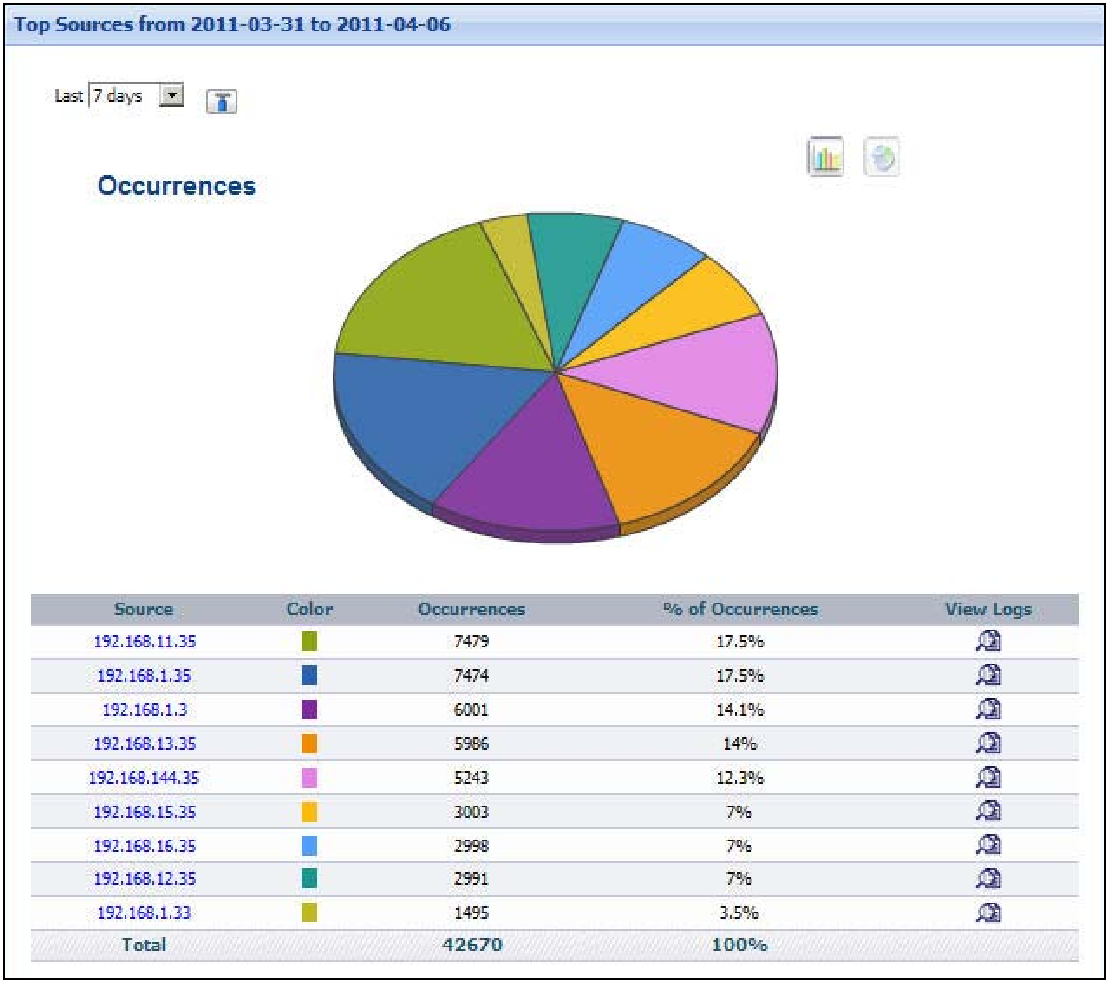
LABEL	DESCRIPTION
Total	This entry displays the totals for the sources above. If the number of sources of the selected virus of the selected virus is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this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

7.4.5 Top Virus Sources

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

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

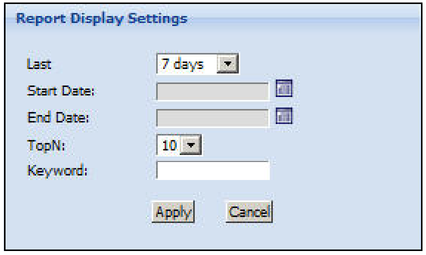
Figure 148 Report > Network Security > AntiVirus > Top Sources



Source	Color	Occurrences	% of Occurrences	View Logs
192.168.11.35	🟩	7479	17.5%	🔍
192.168.1.35	🟦	7474	17.5%	🔍
192.168.1.3	🟪	6001	14.1%	🔍
192.168.13.35	🟧	5986	14%	🔍
192.168.144.35	🟪	5243	12.3%	🔍
192.168.15.35	🟨	3003	7%	🔍
192.168.16.35	🟦	2998	7%	🔍
192.168.12.35	🟩	2991	7%	🔍
192.168.1.33	🟨	1495	3.5%	🔍
Total		42670	100%	

Each field is described in the following table.

Table 135 Report > Network Security > AntiVirus > Top Sources

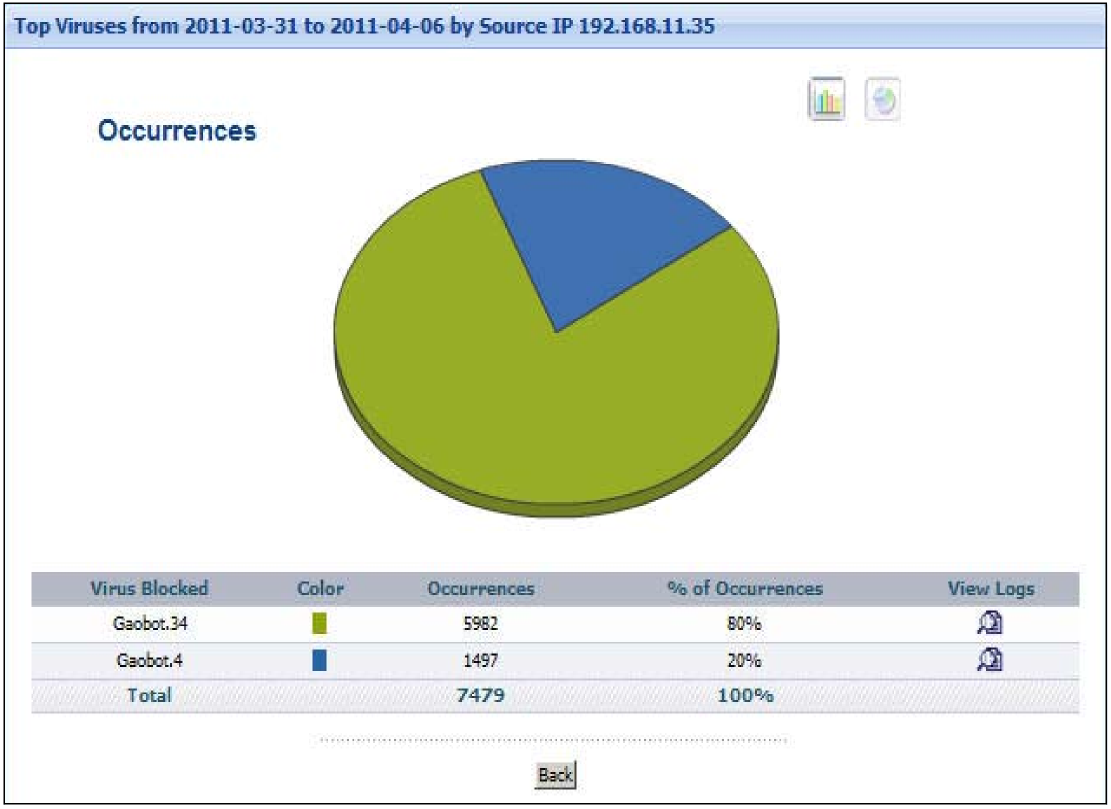
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top viruses for the selected source.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

7.4.6 Top Virus Sources Drill-Down

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

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

Figure 149 Report > Network Security > AntiVirus > Top Sources > Drill-Down



Top Viruses from 2011-03-31 to 2011-04-06 by Source IP 192.168.11.35

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	5982	80%	🔍
Gaobot.4	🟦	1497	20%	🔍
Total		7479	100%	

Each field is described in the following table.

Table 136 Report > Network Security > AntiVirus > Top Sources > Drill-Down

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

Table 136 Report > Network Security > AntiVirus > Top Sources > Drill-Down

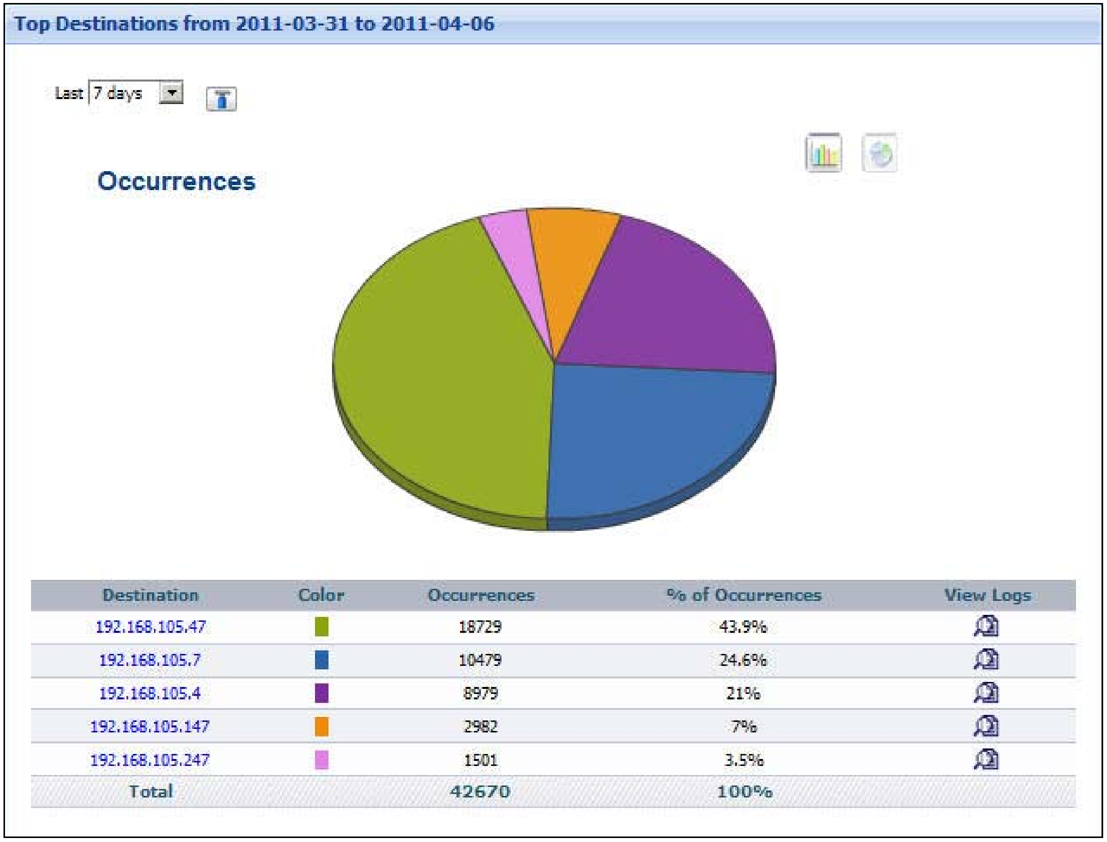
LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the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

7.4.7 Top Virus Destinations

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

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

Figure 150 Report > Network Security > AntiVirus > Top Destinations

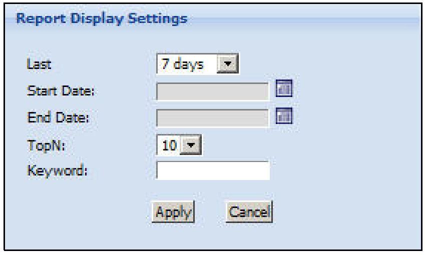


Top Destinations from 2011-03-31 to 2011-04-06

Destination	Color	Occurrences	% of Occurrences	View Logs
192.168.105.47	🟩	18729	43.9%	🔍
192.168.105.7	🟦	10479	24.6%	🔍
192.168.105.4	🟪	8979	21%	🔍
192.168.105.147	🟧	2982	7%	🔍
192.168.105.247	■	1501	3.5%	🔍
Total		42670	100%	

Each field is described in the following table.

Table 137 Report > Network Security > AntiVirus > Top Destinations

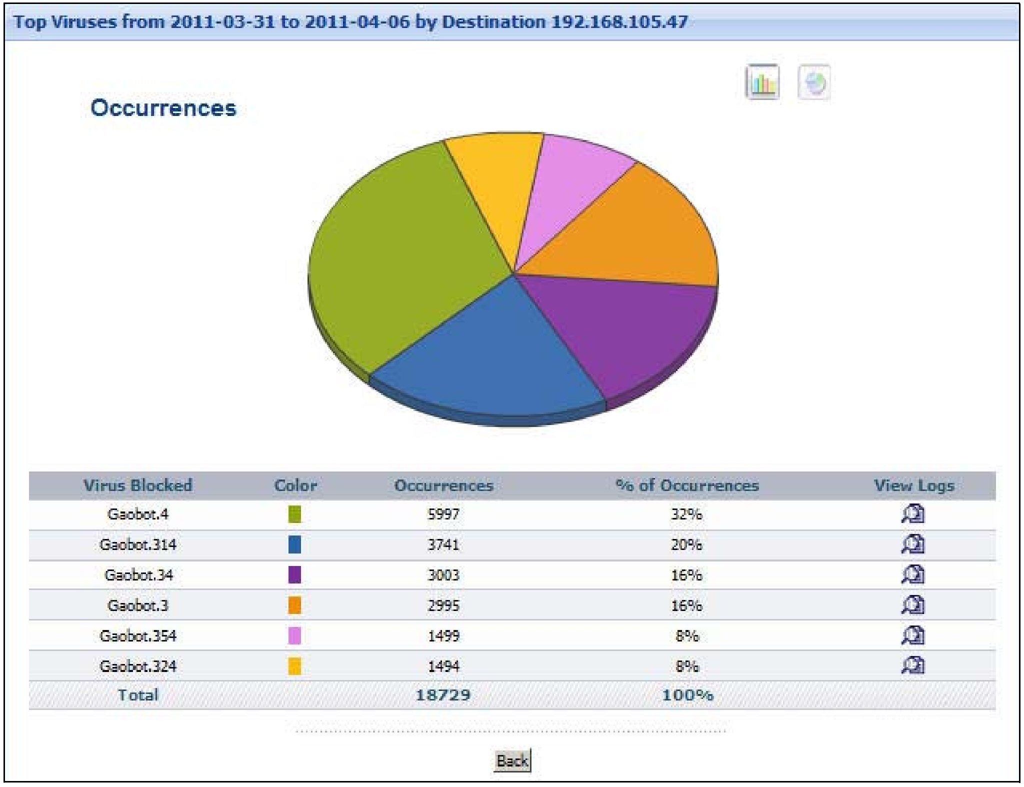
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

7.4.8 Top Virus Destinations Drill-Down

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

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

Figure 151 Report > Network Security > AntiVirus > Top Destinations > Drill-Down



Top Viruses from 2011-03-31 to 2011-04-06 by Destination 192.168.105.47

Occurrences

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.4	🟩	5997	32%	🔍
Gaobot.314	🟦	3741	20%	🔍
Gaobot.34	🟪	3003	16%	🔍
Gaobot.3	🟧	2995	16%	🔍
Gaobot.354	■	1499	8%	🔍
Gaobot.324	🟨	1494	8%	🔍
Total		18729	100%	

Each field is described in the following table.

Table 138 Report > Network Security > AntiVirus > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from going to the selected destination, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of times each virus was sent to the selected destination.
% of Occurrences	This field displays what percentage each virus made of the viruses sent to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

E-Mail Security

This chapter discusses how to use reports to look at E-Mail related security threats that were detected by the ZyXEL device's firewall.

8.1 Virus Found

These reports look at viruses that were detected by the ZyXEL device's anti-virus feature. The reports include viruses received through the following E-Mail related protocols: Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4 (IMAP4).

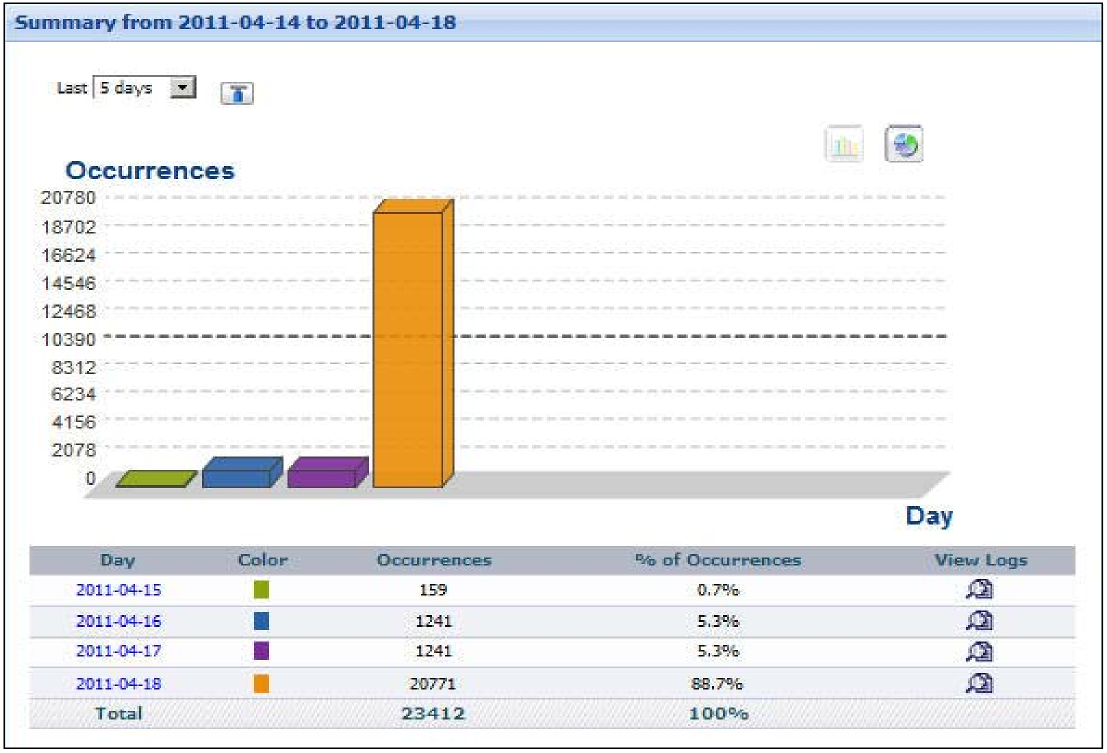
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus** > **General**. ZyXEL devices can log viruses based on the **Service** the virus was using. Make sure the ZyXEL device logs viruses you want to include in Vantage Report.

8.1.1 Virus Found Summary

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

Click **Report > E-Mail Security > Virus Found > Summary** to open this screen.

Figure 152 Report > E-Mail Security > Virus Found > Summary



Summary from 2011-04-14 to 2011-04-18

Last 5 days

Day	Color	Occurrences	% of Occurrences	View Logs
2011-04-15	🟩	159	0.7%	🔍
2011-04-16	🟦	1241	5.3%	🔍
2011-04-17	🟪	1241	5.3%	🔍
2011-04-18	🟧	20771	88.7%	🔍
Total		23412	100%	

Each field is described in the following table.

Table 139 Report > E-Mail Security > Virus Found > Summary

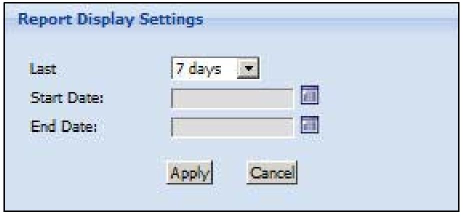
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Apply Cancel 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 139 Report > E-Mail Security > Virus Found > Summary

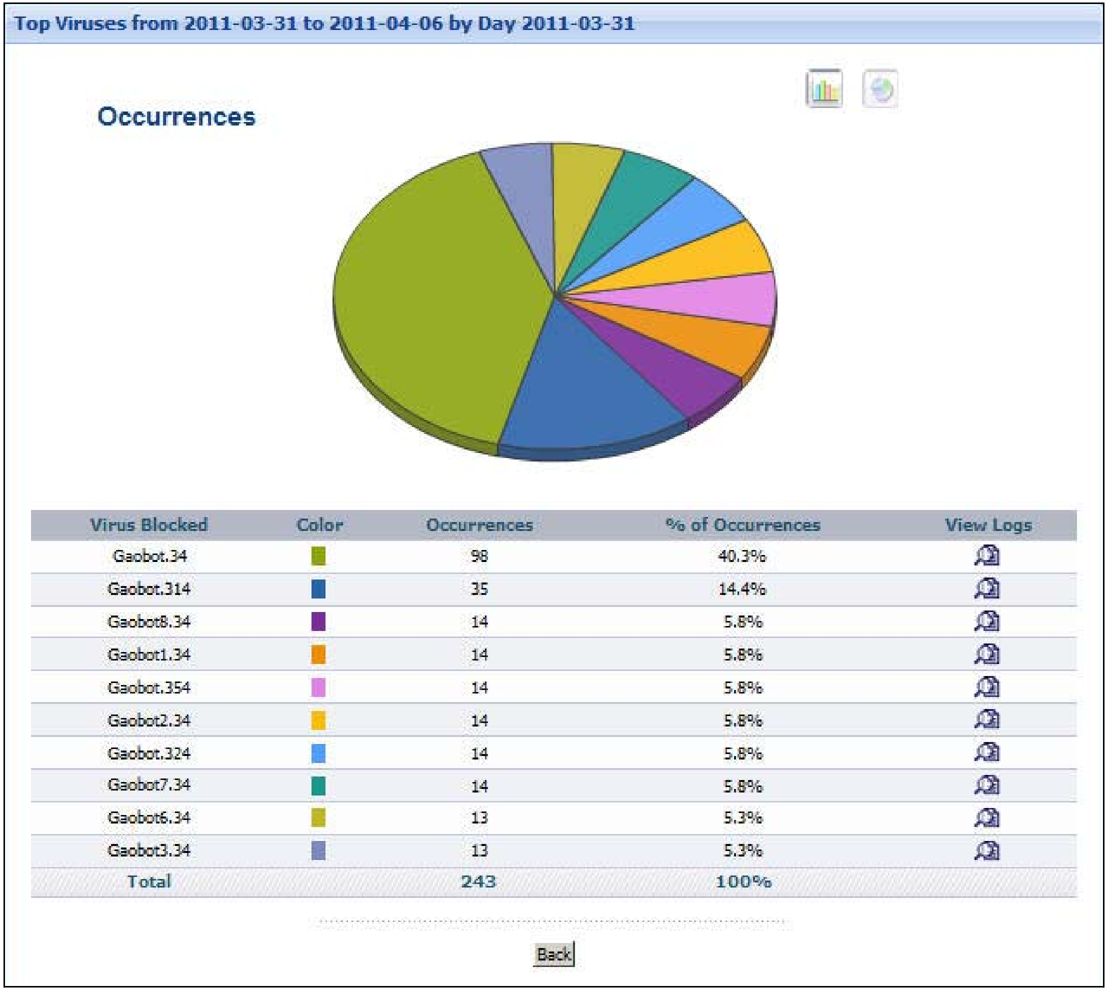
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.1.2 Virus Found Summary Drill-Down

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

Click on a specific time interval in **Report > E-Mail Security > Virus Found > Summary** to open this screen.

Figure 153 Report > E-Mail Security > Virus Found > Summary > Drill-Down



Top Viruses from 2011-03-31 to 2011-04-06 by Day 2011-03-31

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	98	40.3%	🔍
Gaobot.314	🟦	35	14.4%	🔍
Gaobot8.34	🟪	14	5.8%	🔍
Gaobot1.34	🟧	14	5.8%	🔍
Gaobot.354	🟪	14	5.8%	🔍
Gaobot2.34	🟨	14	5.8%	🔍
Gaobot.324	🟦	14	5.8%	🔍
Gaobot7.34	🟩	14	5.8%	🔍
Gaobot6.34	🟨	13	5.3%	🔍
Gaobot3.34	🟦	13	5.3%	🔍
Total		243	100%	

Each field is described in the following table.

Table 140 Report > E-Mail Security > Virus Found > Summary > Drill-Down

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

Table 140 Report > E-Mail Security > Virus Found > Summary > Drill-Down

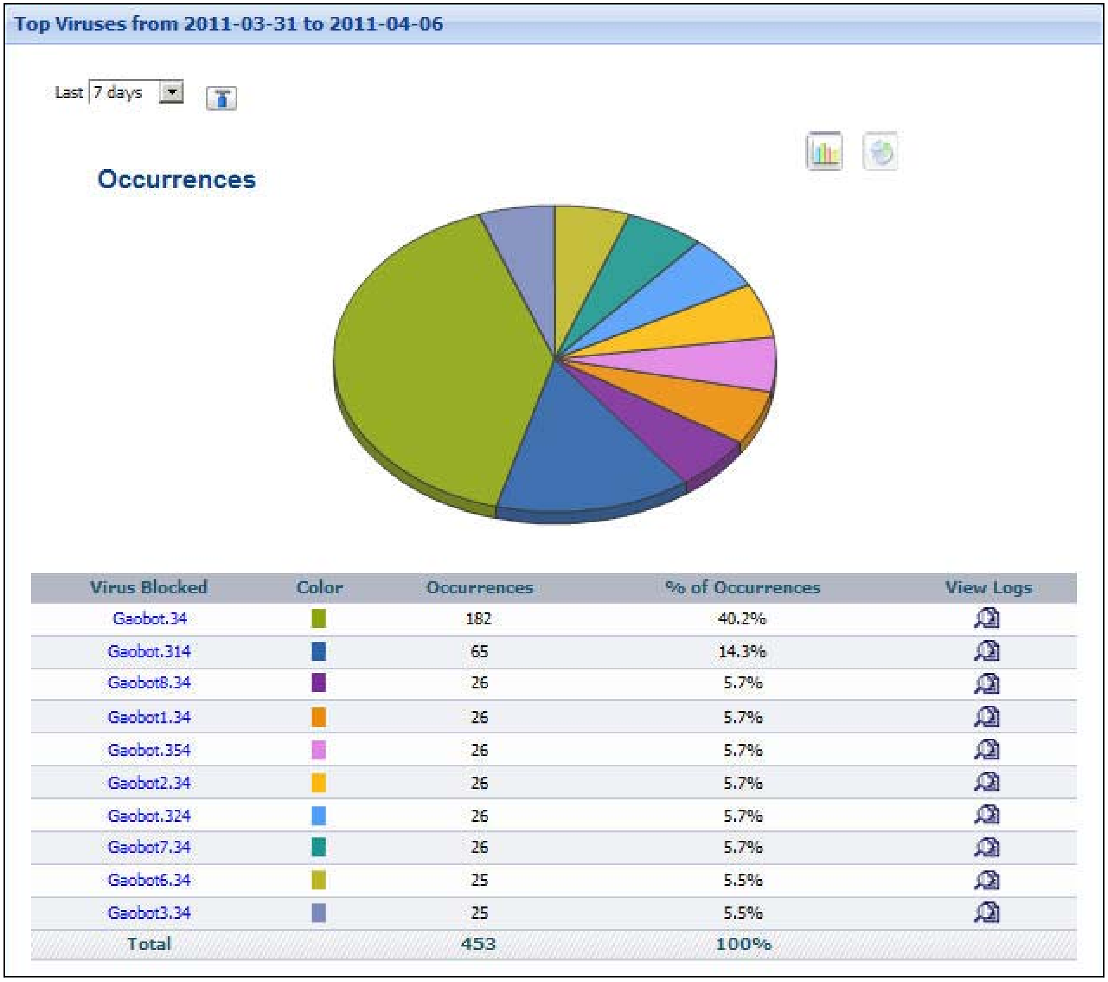
LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to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

8.1.3 Top Viruses

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

Click **Report > E-Mail Security > Virus Found > Top Viruses** to open this screen.

Figure 154 Report > E-Mail Security > Virus Found > Top Viruses

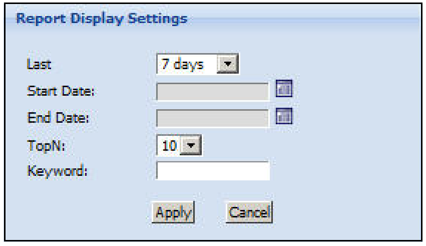


Top Viruses from 2011-03-31 to 2011-04-06

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	182	40.2%	
Gaobot.314	🟦	65	14.3%	
Gaobot8.34	🟪	26	5.7%	
Gaobot1.34	🟧	26	5.7%	
Gaobot.354	🟪	26	5.7%	
Gaobot2.34	🟨	26	5.7%	
Gaobot.324	🟦	26	5.7%	
Gaobot7.34	🟩	26	5.7%	
Gaobot6.34	🟨	25	5.5%	
Gaobot3.34	🟪	25	5.5%	
Total		453	100%	

Each field is described in the following table.

Table 141 Report > E-Mail Security > Virus Found > Top Viruses

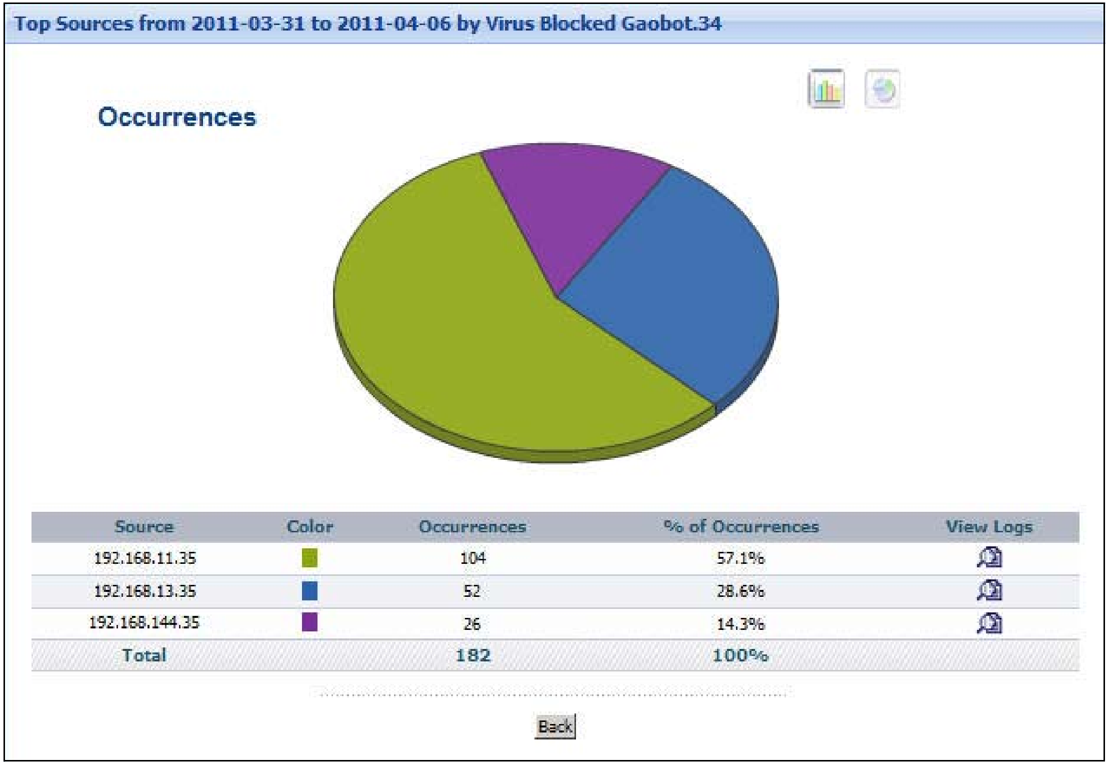
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Virus Blocked** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.
% of Occurrences	This field displays what percentage each virus’s occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

8.1.4 Top Viruses Drill-Down

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

Click on a specific virus in **Report > E-Mail Security > Virus Found > Top Viruses** to open this screen.

Figure 155 Report > E-Mail Security > Virus Found > Top Viruses > Drill-Down



Top Sources from 2011-03-31 to 2011-04-06 by Virus Blocked Gaobot.34

Source	Color	Occurrences	% of Occurrences	View Logs
192.168.11.35	🟩	104	57.1%	🔍
192.168.13.35	🟦	52	28.6%	🔍
192.168.144.35	🟪	26	14.3%	🔍
Total		182	100%	

Each field is described in the following table.

Table 142 Report > E-Mail Security > Virus Found > Top Viruses > Drill-Down

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

Table 142 Report > E-Mail Security > Virus Found > Top Viruses > Drill-Down

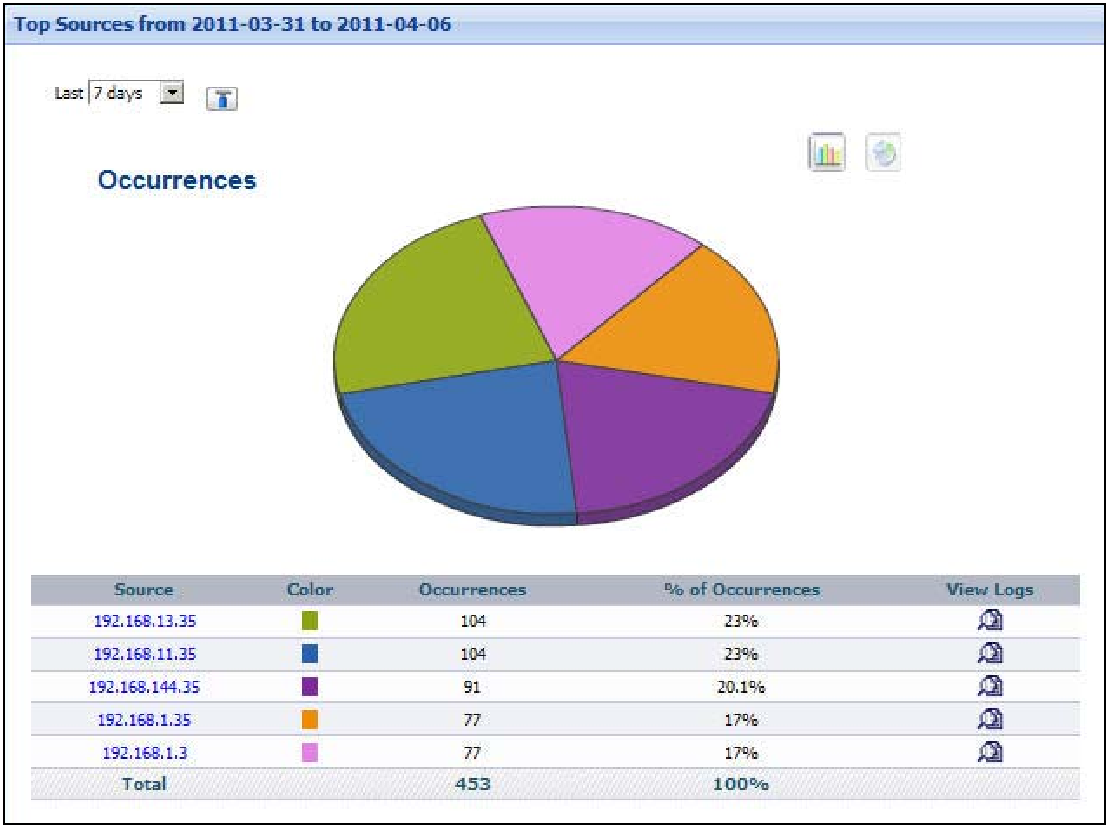
LABEL	DESCRIPTION
Total	This entry displays the totals for the sources above. If the number of sources of the selected virus of the selected virus is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this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

8.1.5 Top Virus Sources

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

Click **Report > E-Mail Security > Virus Found > Top Sources** to open this screen.

Figure 156 Report > E-Mail Security > Virus Found > Top Sources



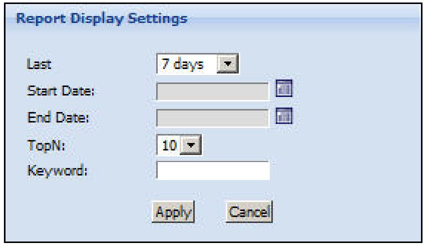
Top Sources from 2011-03-31 to 2011-04-06

Last 7 days

Source	Color	Occurrences	% of Occurrences	View Logs
192.168.13.35	🟩	104	23%	
192.168.11.35	🟦	104	23%	
192.168.144.35	🟪	91	20.1%	
192.168.1.35	🟧	77	17%	
192.168.1.3	🟪	77	17%	
Total		453	100%	

Each field is described in the following table.

Table 143 Report > E-Mail Security > Virus Found > Top Sources

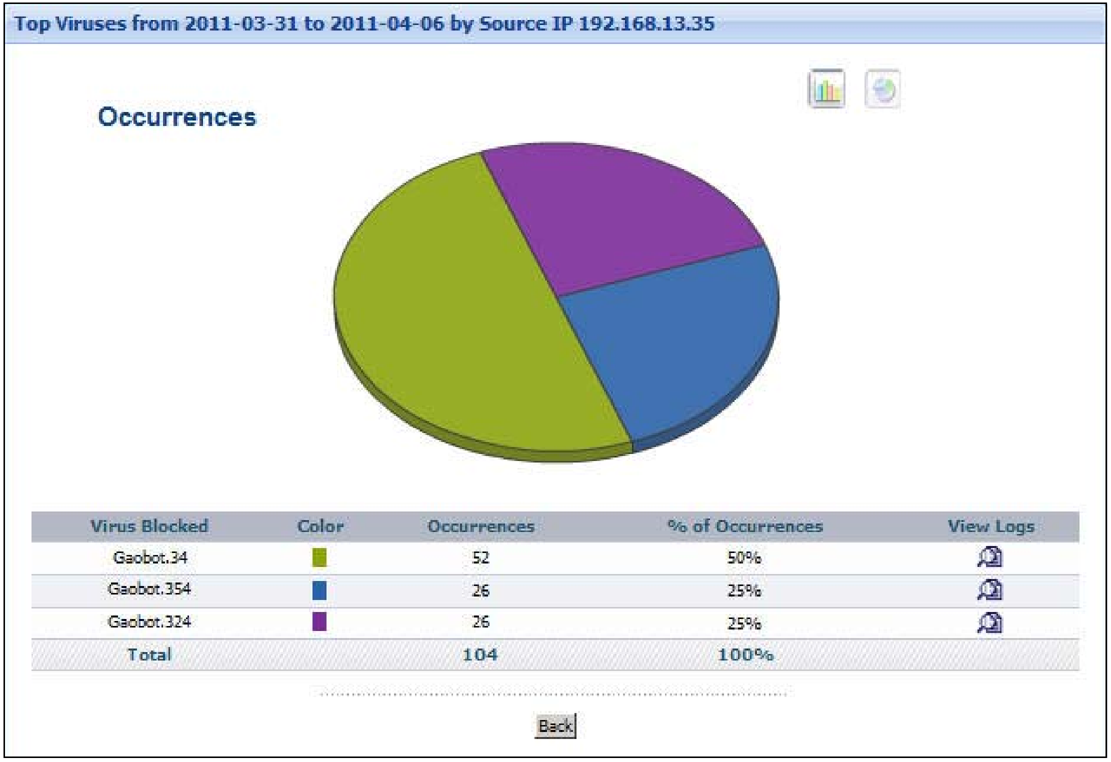
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a source to look at the top viruses for the selected source.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.1.6 Top Virus Sources Drill-Down

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

Click on a specific source in **Report > E-Mail Security > Virus Found > Top Sources** to open this screen.

Figure 157 Report > E-Mail Security > Virus Found > Top Sources > Drill-Down



Top Viruses from 2011-03-31 to 2011-04-06 by Source IP 192.168.13.35

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	52	50%	🔍
Gaobot.354	🟦	26	25%	🔍
Gaobot.324	🟪	26	25%	🔍
Total		104	100%	

Each field is described in the following table.

Table 144 Report > E-Mail Security > Virus Found > Top Sources > Drill-Down

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

Table 144 Report > E-Mail Security > Virus Found > Top Sources > Drill-Down

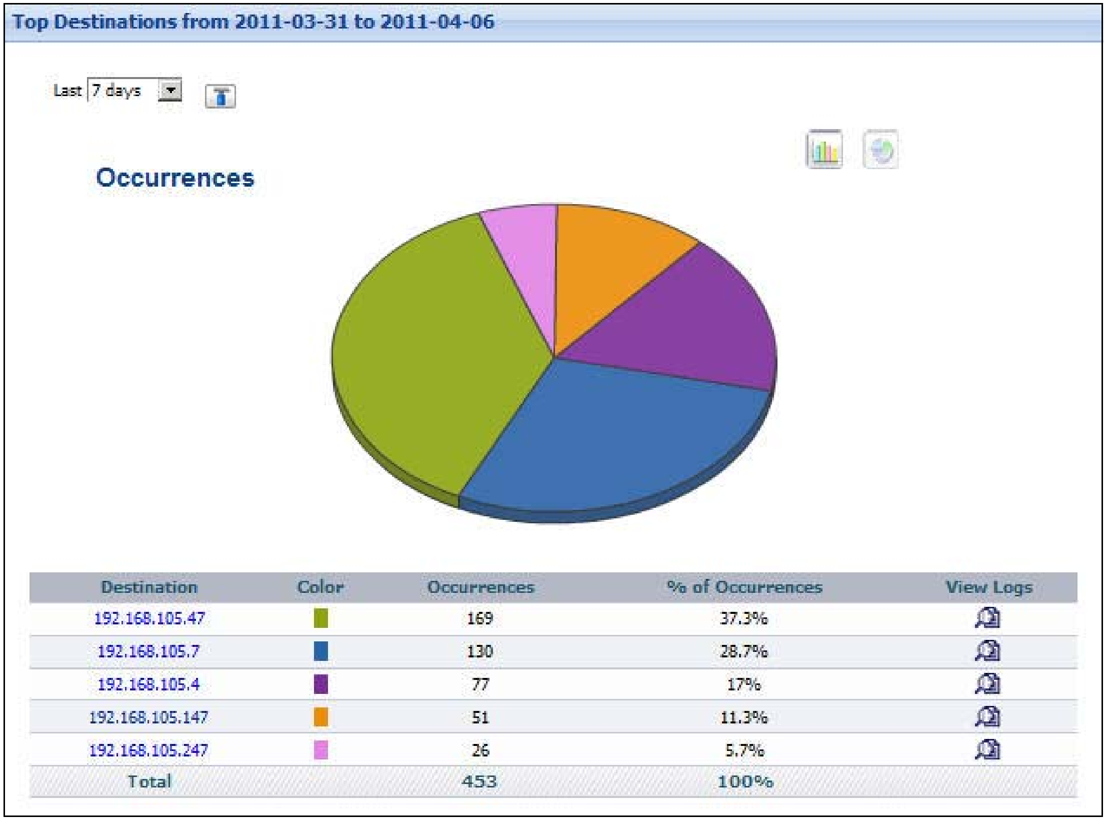
LABEL	DESCRIPTION
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the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

8.1.7 Top Virus Destinations

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

Click **Report > E-Mail Security > Virus Found > Top Destinations** to open this screen.

Figure 158 Report > E-Mail Security > Virus Found > Top Destinations



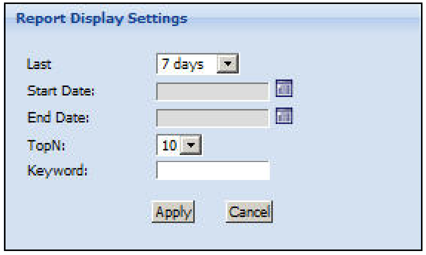
Top Destinations from 2011-03-31 to 2011-04-06

Last 7 days

Destination	Color	Occurrences	% of Occurrences	View Logs
192.168.105.47	🟩	169	37.3%	🔍
192.168.105.7	🟦	130	28.7%	🔍
192.168.105.4	🟪	77	17%	🔍
192.168.105.147	🟧	51	11.3%	🔍
192.168.105.247	▨	26	5.7%	🔍
Total		453	100%	

Each field is described in the following table.

Table 145 Report > E-Mail Security > Virus Found > Top Destinations

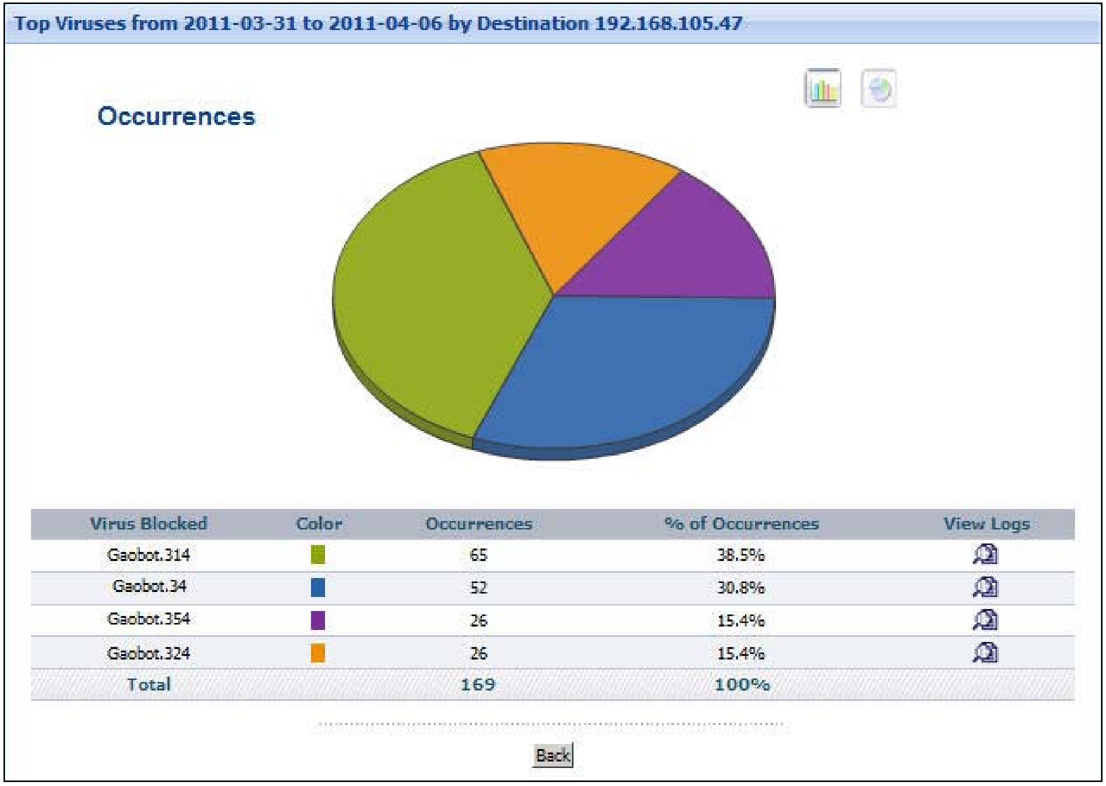
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

8.1.8 Top Virus Destinations Drill-Down

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

Click on a specific destination in **Report > E-Mail Security > Virus Found > Top Destinations** to open this screen.

Figure 159 Report > E-Mail Security > Virus Found > Top Destinations > Drill-Down



Top Viruses from 2011-03-31 to 2011-04-06 by Destination 192.168.105.47

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.314	🟩	65	38.5%	🔍
Gaobot.34	🟦	52	30.8%	🔍
Gaobot.354	🟪	26	15.4%	🔍
Gaobot.324	🟧	26	15.4%	🔍
Total		169	100%	

Each field is described in the following table.

Table 146 Report > E-Mail Security > Virus Found > Top Destinations > Drill-Down

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

Table 146 Report > E-Mail Security > Virus Found > 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.

8.2 Spam

These reports look at spam messages that were detected by the ZyXEL device's anti-spam feature. You can also look at the top senders and sources of spam messages.

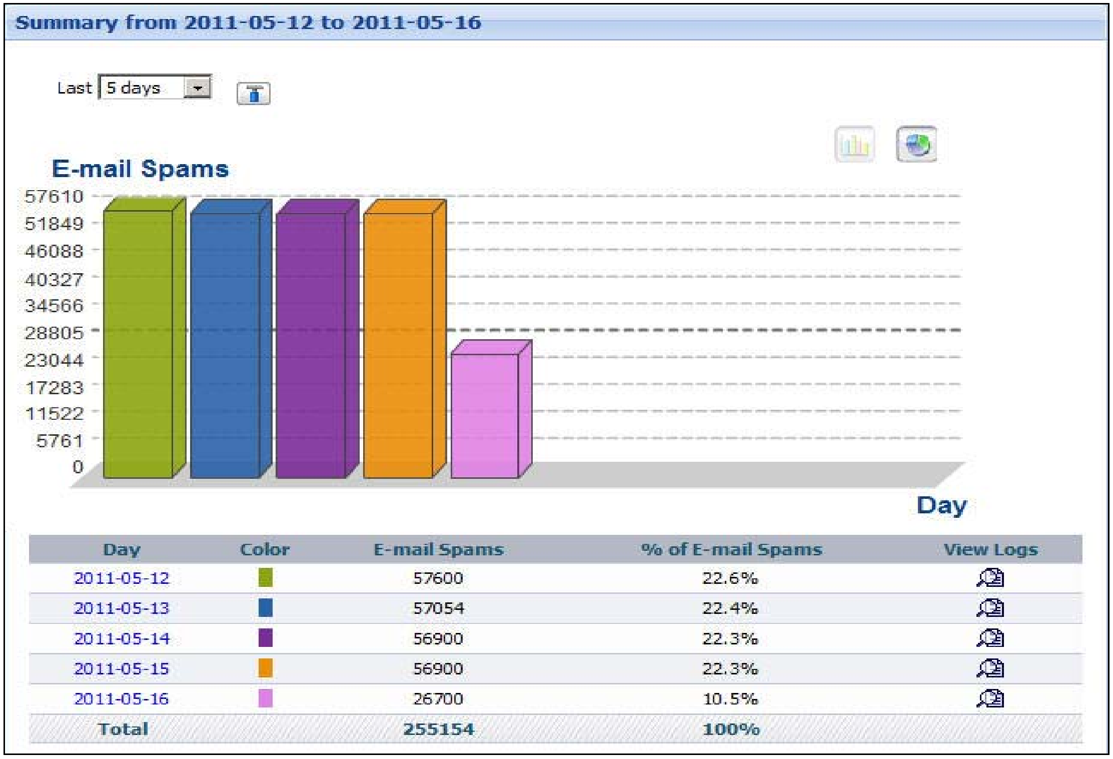
Note: To look at anti-spam reports, each ZyXEL device must record anti-spam messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Spam** is enabled.

8.2.1 Spam Summary

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

Click **Report > E-Mail Security > Spam > Summary** to open this screen.

Figure 160 Report > E-Mail Security > Spam > Summary



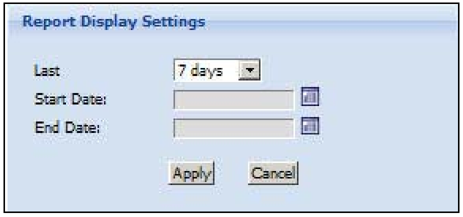
Summary from 2011-05-12 to 2011-05-16

Last: 5 days

Day	Color	E-mail Spams	% of E-mail Spams	View Logs
2011-05-12	🟩	57600	22.6%	🔍
2011-05-13	🟦	57054	22.4%	🔍
2011-05-14	🟪	56900	22.3%	🔍
2011-05-15	🟧	56900	22.3%	🔍
2011-05-16	■	26700	10.5%	🔍
Total		255154	100%	

Each field is described in the following table.

Table 147 Report > E-Mail Security > Spam > Summary

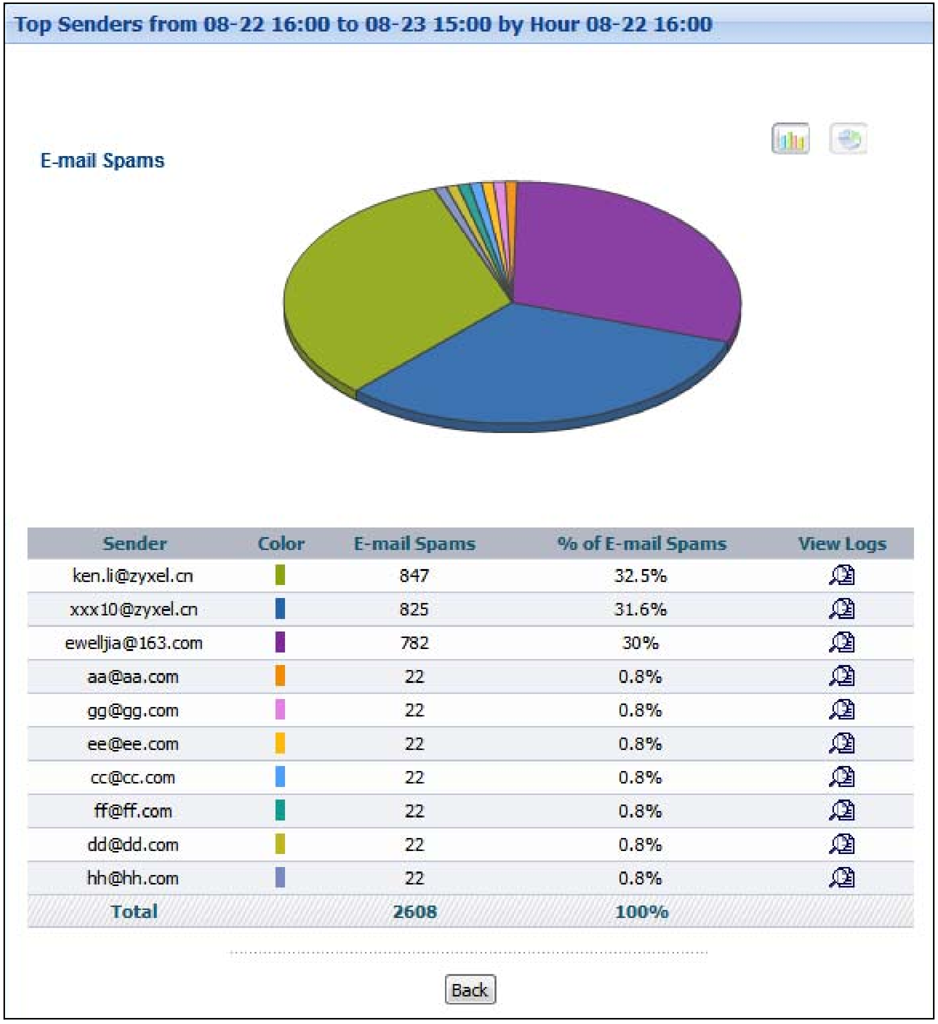
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top spam messages in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
E-mail Spams	This field displays the number of spam messages in the selected time interval.
% of E-mail Spams	This field displays what percentage of all spam messages was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.2.2 Spam Summary Drill-Down

Use this report to look at the top senders of spam messages in a specific time interval.

Click on a specific time interval in **Report > E-Mail Security > Spam > Summary** to open this screen.

Figure 161 Report > E-Mail Security > Spam > Summary > Drill-Down



Top Senders from 08-22 16:00 to 08-23 15:00 by Hour 08-22 16:00

Sender	Color	E-mail Spams	% of E-mail Spams	View Logs
ken.li@zyxel.cn	🟩	847	32.5%	🔍
xxx10@zyxel.cn	🟦	825	31.6%	🔍
ewelljia@163.com	🟪	782	30%	🔍
aa@aa.com	🟧	22	0.8%	🔍
gg@gg.com	🟪	22	0.8%	🔍
ee@ee.com	🟨	22	0.8%	🔍
cc@cc.com	🟦	22	0.8%	🔍
ff@ff.com	🟩	22	0.8%	🔍
dd@dd.com	🟨	22	0.8%	🔍
hh@hh.com	🟦	22	0.8%	🔍
Total		2608	100%	

Each field is described in the following table.

Table 148 Report > E-Mail Security > Spam > Summary > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Sender	This field displays the top senders of spam during the selected time interval, sorted by the number of spam messages sent by each. Each sender is identified by its e-mail address.
Color	This field displays what color represents each sender in the graph.
E-mail Spams	This field displays how many spam messages each sender sent.
% of E-mail Spams	This field displays what percentage of all spam messages in the selected time interval was sent by each sender.

Table 148 Report > E-Mail Security > Spam > Summary > Drill-Down

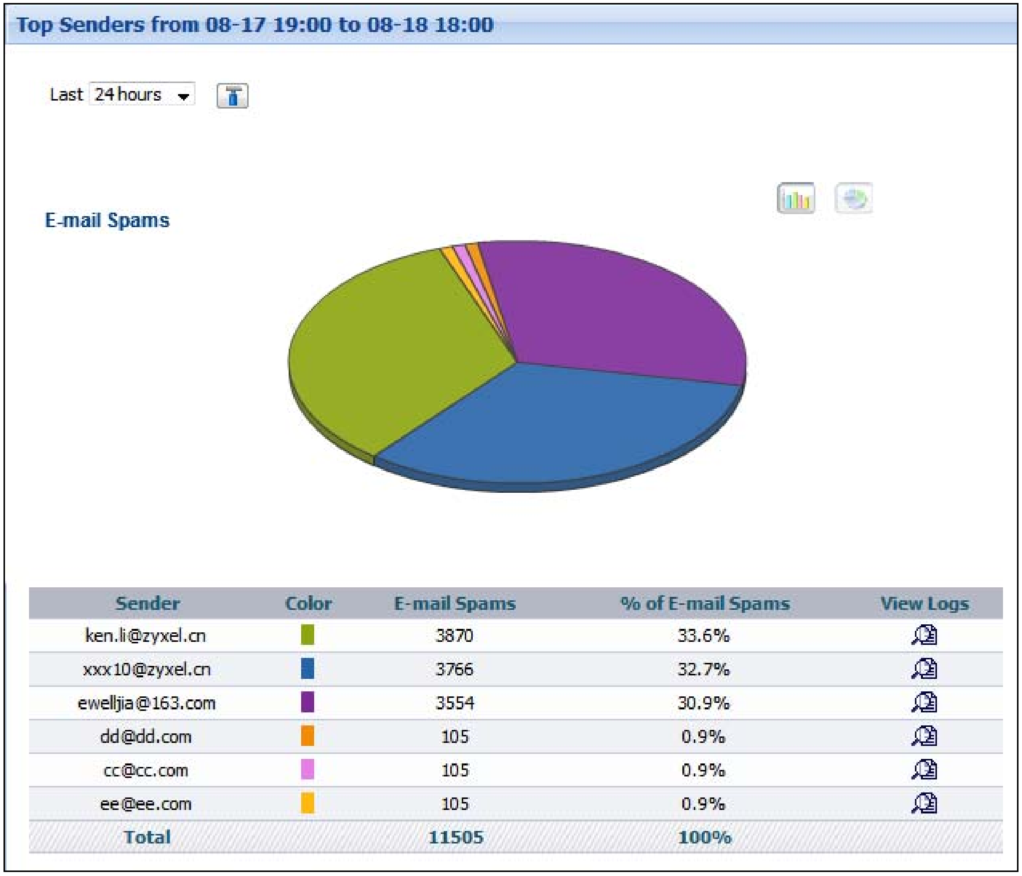
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the senders above. If the number of senders in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower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

8.2.3 Top Spam Senders

Use this report to look at the e-mail addresses of the top senders of spam messages and how many spam e-mails they sent.

Click **Report > E-Mail Security > Spam > Top Senders** to open this screen.

Figure 162 Report > E-Mail Security > Spam > Top Senders



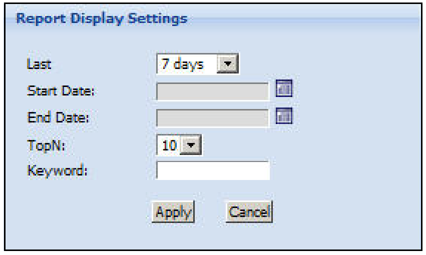
Top Senders from 08-17 19:00 to 08-18 18:00

Last 24 hours

Sender	Color	E-mail Spams	% of E-mail Spams	View Logs
ken.li@zyxel.cn	🟩	3870	33.6%	🔍
xxx10@zyxel.cn	🟦	3766	32.7%	🔍
ewelljia@163.com	🟪	3554	30.9%	🔍
dd@dd.com	🟧	105	0.9%	🔍
cc@cc.com	■	105	0.9%	🔍
ee@ee.com	🟨	105	0.9%	🔍
Total		11505	100%	

Each field is described in the following table.

Table 149 Report > E-Mail Security > Spam > Top Senders

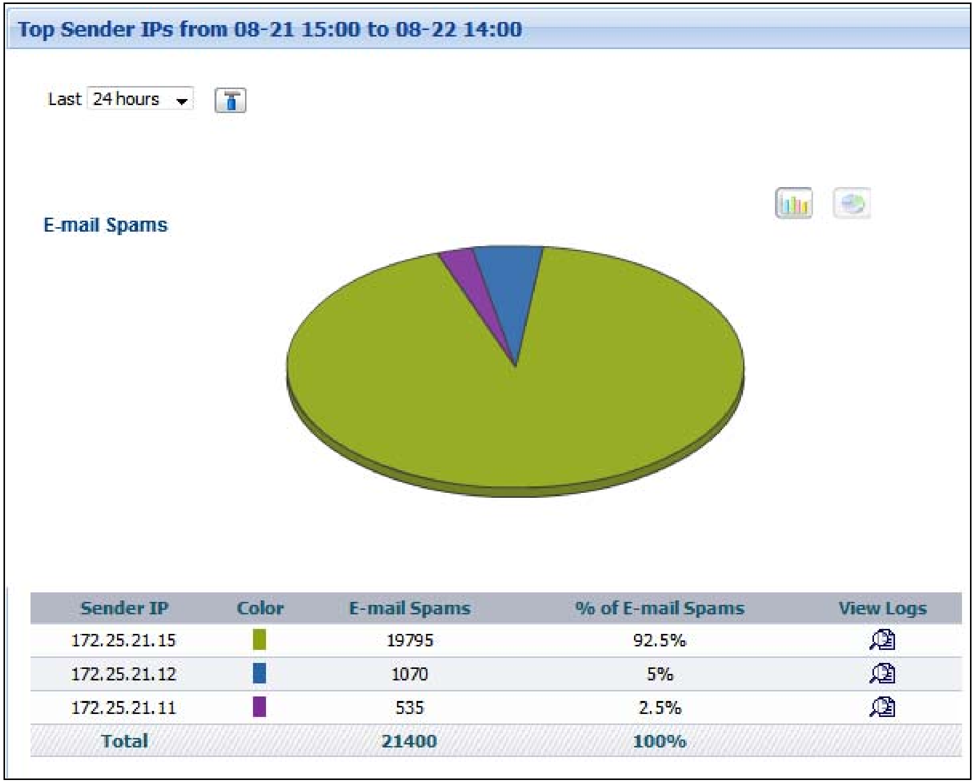
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Sender** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Sender	This field displays the top senders of spam. Each sender is identified by its e-mail address.
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 row displays the totals for the entries above.

8.2.4 Top Spam Sender IP Addresses

Use this report to look at the IP addresses of the top senders of spam messages and how many spam e-mails they sent.

Click **Report > E-Mail Security > Spam > Top Sender IPs** to open this screen.

Figure 163 Report > E-Mail Security > Spam > Top Sender IPs



Top Sender IPs from 08-21 15:00 to 08-22 14:00

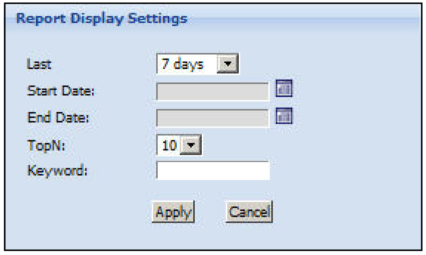
Last 24 hours

E-mail Spams

Sender IP	Color	E-mail Spams	% of E-mail Spams	View Logs
172.25.21.15	🟩	19795	92.5%	🔍
172.25.21.12	🟦	1070	5%	🔍
172.25.21.11	🟪	535	2.5%	🔍
Total		21400	100%	

Each field is described in the following table.

Table 150 Report > E-Mail Security > Spam > Top Sender IPs

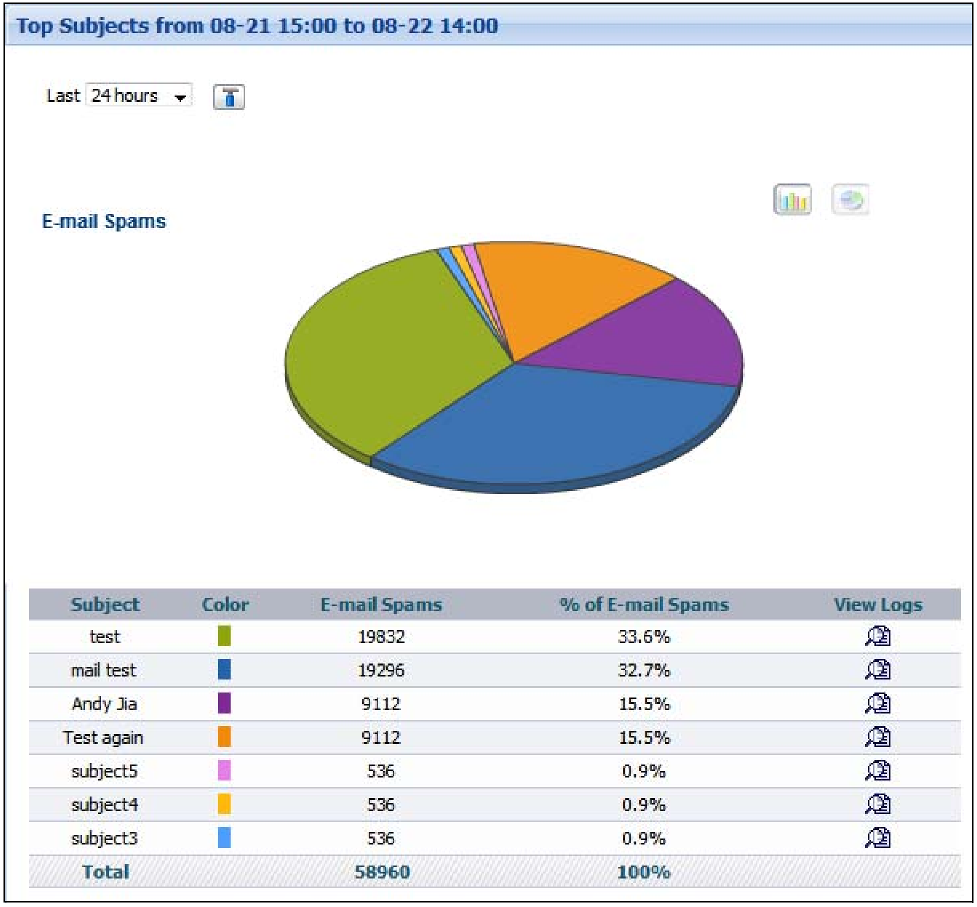
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Sender** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Sender IP	This field displays the IP addresses of the top senders of spam.
Color	This field displays what color represents each sender IP address in the graph.
E-mail Spams	This field displays how many spam messages each sender IP address sent.
% of E-mail Spams	This field displays what percentage of all spam messages was sent by each sender IP address.
View Logs	Click this icon to see the logs that go with the record.
Total	This row displays the totals for the entries above.

8.2.5 Top Spam Subjects

Use this report to look at the subject lines of the most common spam e-mails.

Click **Report > E-Mail Security > Spam > Top Subjects** to open this screen.

Figure 164 Report > E-Mail Security > Spam > Top Subjects



Top Subjects from 08-21 15:00 to 08-22 14:00

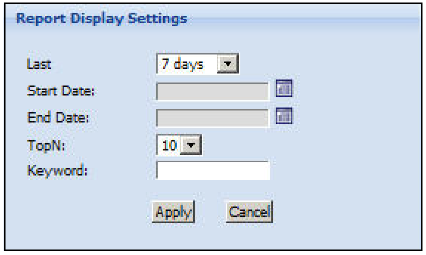
Last 24 hours

E-mail Spams

Subject	Color	E-mail Spams	% of E-mail Spams	View Logs
test	🟩	19832	33.6%	🔍
mail test	🟦	19296	32.7%	🔍
Andy Jia	🟪	9112	15.5%	🔍
Test again	🟧	9112	15.5%	🔍
subject5	🟪	536	0.9%	🔍
subject4	🟨	536	0.9%	🔍
subject3	🟦	536	0.9%	🔍
Total		**58960**	**100%**	

Each field is described in the following table.

Table 151 Report > E-Mail Security > Spam > Top Subjects

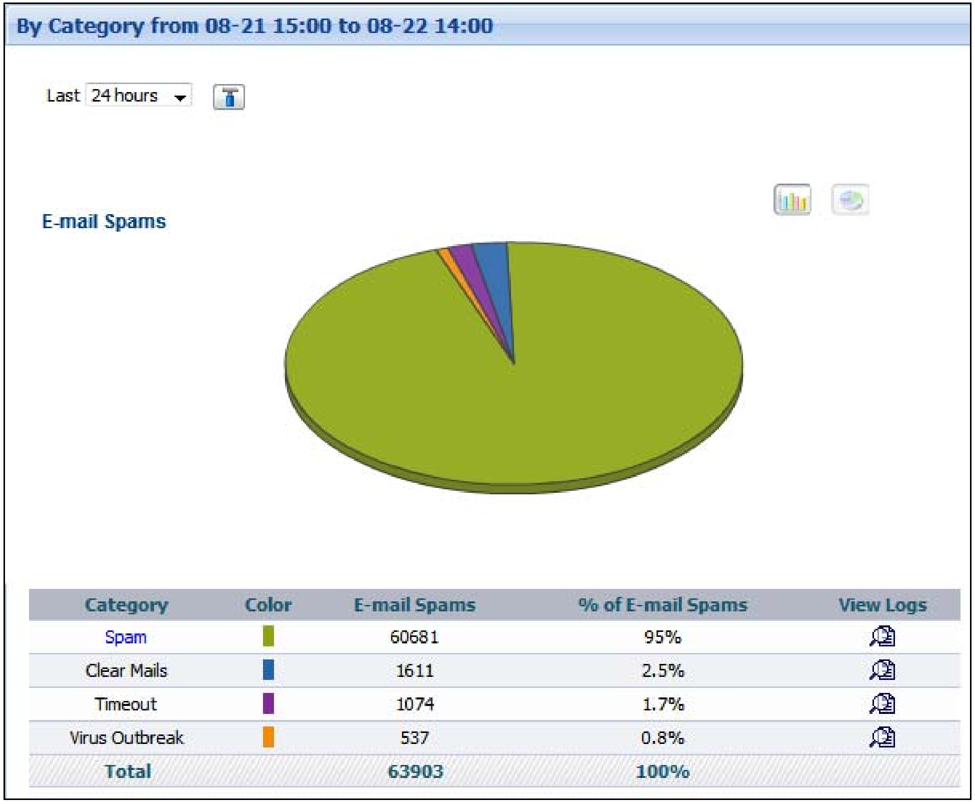
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Sender** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Subject	This field displays the subject lines of the most common spam e-mails.
Color	This field displays what color represents each subject in the graph.
E-mail Spams	This field displays how many spam messages with each subject were processed.
% of E-mail Spams	This field displays what percentage of all spam messages used the listed subject.
View Logs	Click this icon to see the logs that go with the record.
Total	This row displays the totals for the entries above.

8.2.6 Spam By Category

Use this report to look at which spam categories had the most spam e-mails.

Click **Report > E-Mail Security > Spam > By Category** to open this screen.

Figure 165 Report > E-Mail Security > Spam > By Category



By Category from 08-21 15:00 to 08-22 14:00

Last: 24 hours

E-mail Spams

Category	Color	E-mail Spams	% of E-mail Spams	View Logs
Spam	🟩	60681	95%	🔍
Clear Mails	🟦	1611	2.5%	🔍
Timeout	🟪	1074	1.7%	🔍
Virus Outbreak	🟧	537	0.8%	🔍
Total		63903	100%	

Each field is described in the following table.

Table 152 Report > E-Mail Security > Spam > By Category

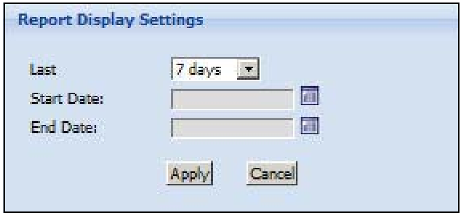
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: 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 152 Report > E-Mail Security > Spam > By Category

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.
Category	This field displays the category of spam e-mails.
Color	This field displays what color represents each category in the graph.
E-mail Spams	This field displays how many spam messages belonging to each category were processed.
% of E-mail Spams	This field displays what percentage of all spam messages belonged to the listed category.
View Logs	Click this icon to see the logs that go with the record.
Total	This row displays the totals for the entries above.

8.3 Intrusion Hits

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

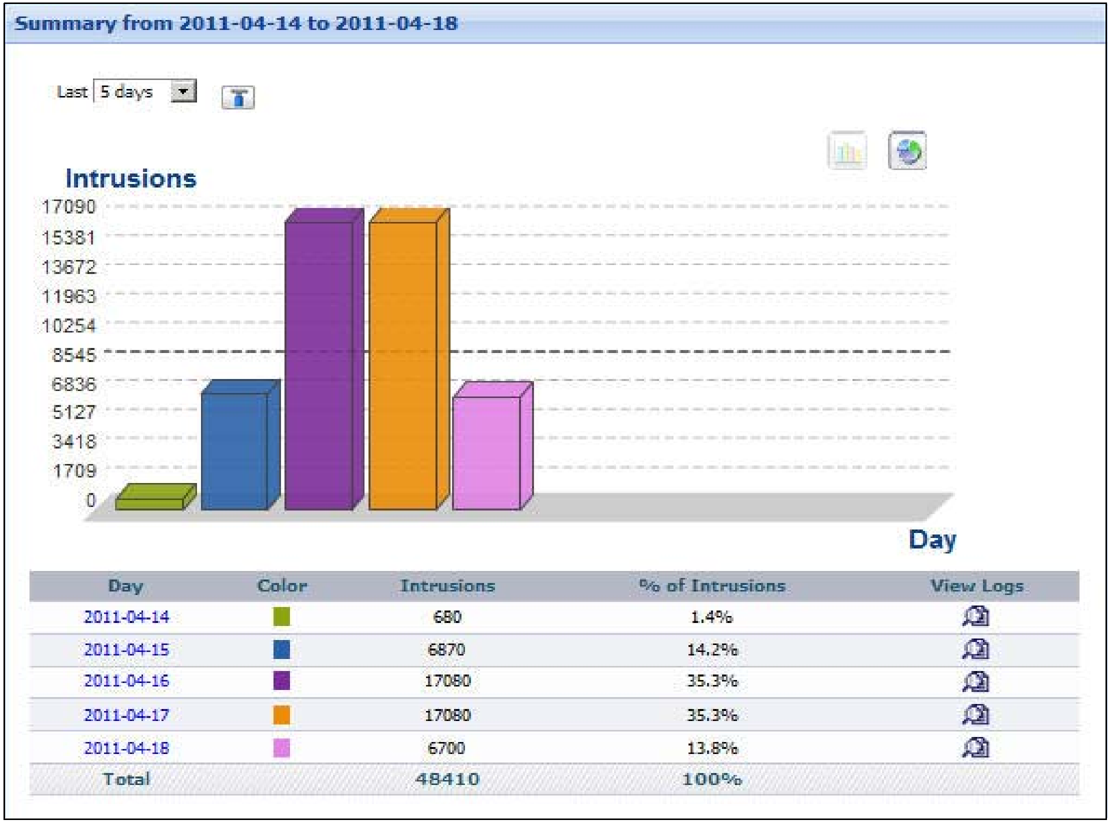
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP** > **Signature**, and make sure the ZyXEL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

8.3.1 Intrusion Hits Summary

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

Click **Report > E-Mail Security > Intrusion Hits > Summary** to open this screen.

Figure 166 Report > E-Mail Security > Intrusion Hits > Summary



Summary from 2011-04-14 to 2011-04-18

Last 5 days

Day	Color	Intrusions	% of Intrusions	View Logs
2011-04-14	🟩	680	1.4%	🔍
2011-04-15	🟦	6870	14.2%	🔍
2011-04-16	🟪	17080	35.3%	🔍
2011-04-17	🟧	17080	35.3%	🔍
2011-04-18	■	6700	13.8%	🔍
Total		48410	100%	

Each field is described in the following table.

Table 153 Report > E-Mail Security > Intrusion Hits > Summary

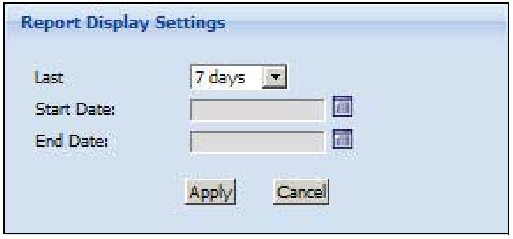
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Apply Cancel 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.

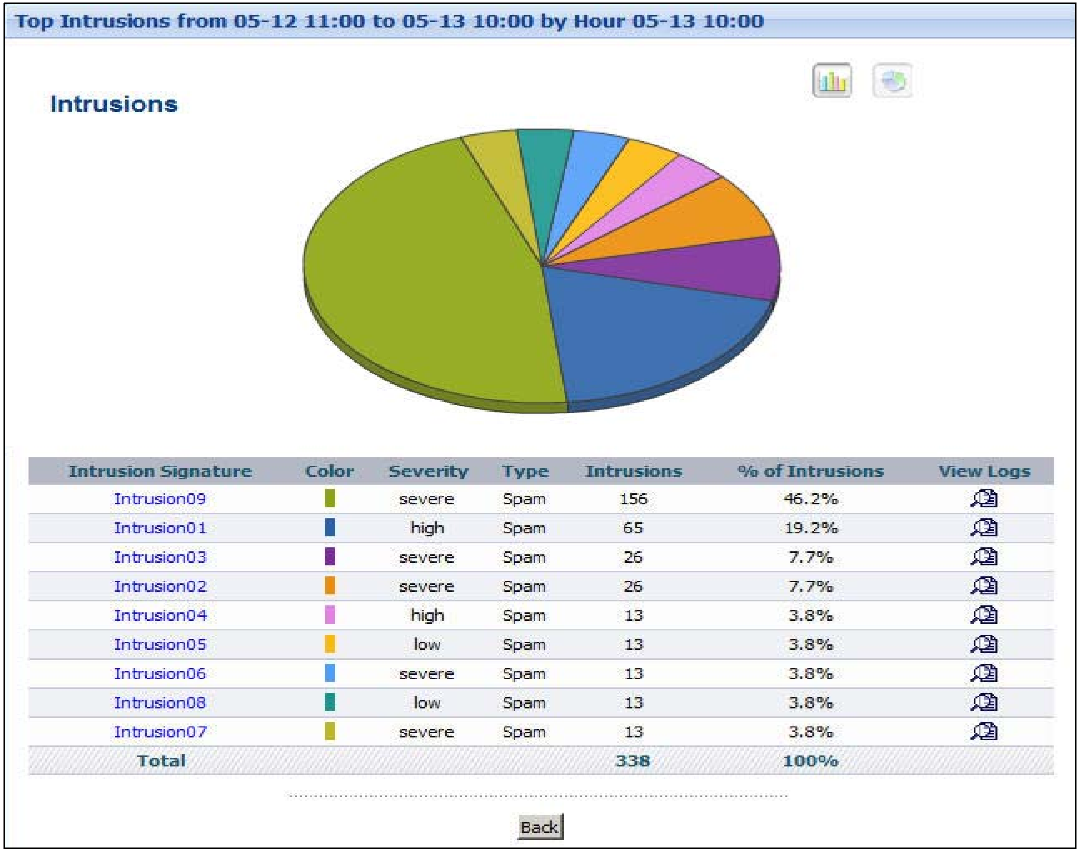
Table 153 Report > E-Mail Security > Intrusion Hits > Summary

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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the intrusion signatures in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Intrusions	This field displays the number of intrusions in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

8.3.2 Intrusion Hits Summary Drill-Down

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

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



Top Intrusions from 05-12 11:00 to 05-13 10:00 by Hour 05-13 10:00

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	Spam	156	46.2%	🔍
Intrusion01	🟦	high	Spam	65	19.2%	🔍
Intrusion03	🟪	severe	Spam	26	7.7%	🔍
Intrusion02	🟧	severe	Spam	26	7.7%	🔍
Intrusion04	🟪	high	Spam	13	3.8%	🔍
Intrusion05	🟨	low	Spam	13	3.8%	🔍
Intrusion06	🟦	severe	Spam	13	3.8%	🔍
Intrusion08	🟩	low	Spam	13	3.8%	🔍
Intrusion07	🟨	severe	Spam	13	3.8%	🔍
Total				338	100%	

Figure 167 Report > E-Mail Security > Intrusion Hits > Summary > Drill-Down

Each field is described in the following table.

Table 154 Report > E-Mail Security > Intrusion Hits > Summary > Drill-Down

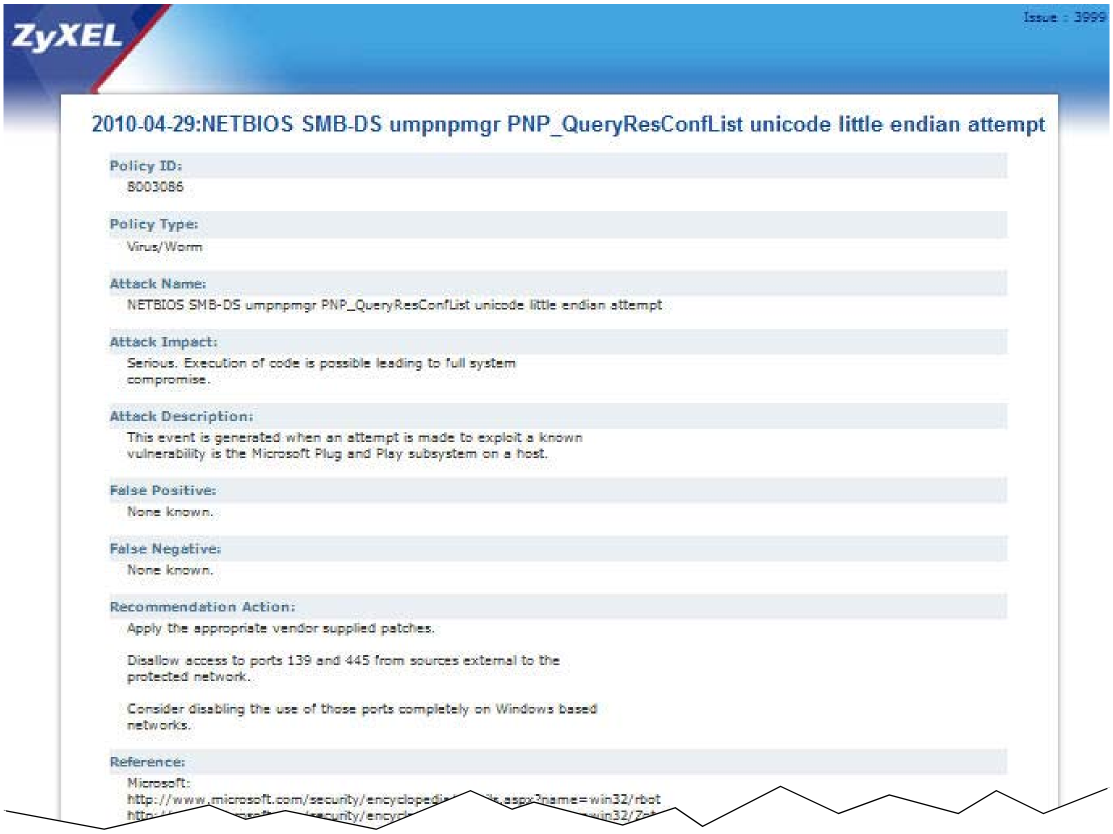
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 168 on page 296).
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP** > **Signature** > **Attack Type** in most ZyXEL devices.
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.

Table 154 Report > E-Mail Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

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

Figure 168 Security Issue Details



2010-04-29:NETBIOS SMB-DS umpnpmgr PNP_QueryResConfList unicode little endian attempt

Policy ID:
8003086

Policy Type:
Virus/Worm

Attack Name:
NETBIOS SMB-DS umpnpmgr PNP_QueryResConfList unicode little endian attempt

Attack Impact:
Serious. Execution of code is possible leading to full system compromise.

Attack Description:
This event is generated when an attempt is made to exploit a known vulnerability is the Microsoft Plug and Play subsystem on a host.

False Positive:
None known.

False Negative:
None known.

Recommendation Action:
Apply the appropriate vendor supplied patches.

Disallow access to ports 139 and 445 from sources external to the protected network.

Consider disabling the use of those ports completely on Windows based networks.

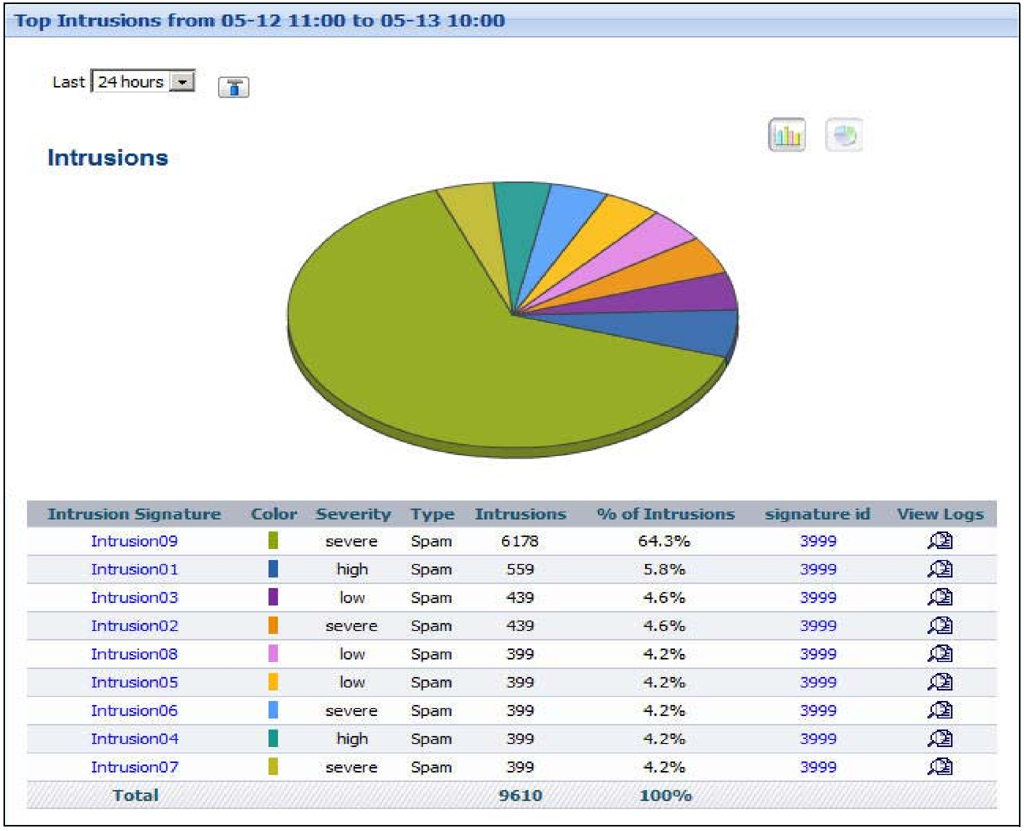
Reference:
Microsoft:
http://www.microsoft.com/security/encyclopedia/details.aspx?name=win32/rbot
http:[illegible]security/encyc[illegible]win32/Zot

8.3.3 Top Intrusion Hits Signatures

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

Click **Report > E-Mail Security > Intrusion Hits > Top Intrusions** to open this screen.

Figure 169 Report > E-Mail Security > Intrusion Hits > Top Intrusions



Top Intrusions from 05-12 11:00 to 05-13 10:00

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	signature id	View Logs
Intrusion09	🟩	severe	Spam	6178	64.3%	3999	🔍
Intrusion01	🟦	high	Spam	559	5.8%	3999	🔍
Intrusion03	🟪	low	Spam	439	4.6%	3999	🔍
Intrusion02	🟧	severe	Spam	439	4.6%	3999	🔍
Intrusion08	■	low	Spam	399	4.2%	3999	🔍
Intrusion05	🟨	low	Spam	399	4.2%	3999	🔍
Intrusion06	🟦	severe	Spam	399	4.2%	3999	🔍
Intrusion04	🟩	high	Spam	399	4.2%	3999	🔍
Intrusion07	🟨	severe	Spam	399	4.2%	3999	🔍
Total				9610	100%		

Each field is described in the following table.

Table 155 Report > E-Mail Security > Intrusion Hits > Top Intrusions

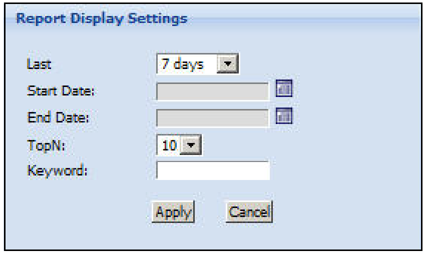
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Intrusion Signature** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP** > **Signature** > **Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
signature id	This is the security issue identification number. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 168 on page 296).

Table 155 Report > E-Mail Security > Intrusion Hits > Top Intrusions

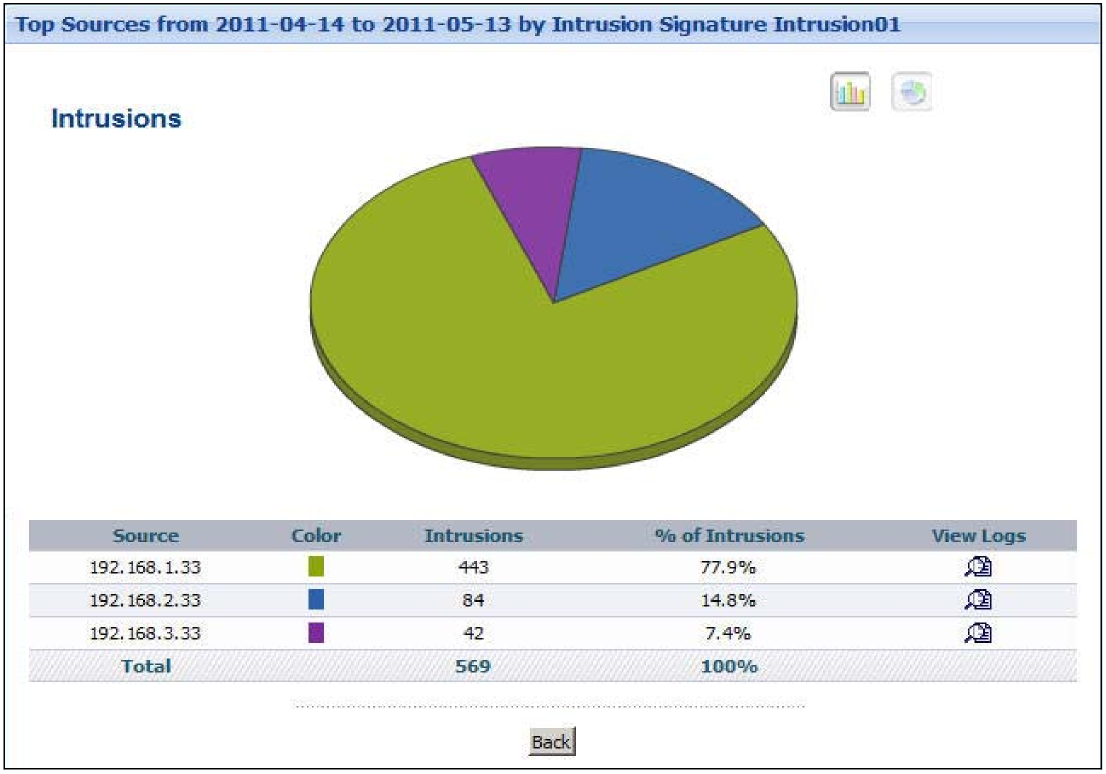
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

8.3.4 Top Intrusion Hits Signatures Drill-Down

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

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

Figure 170 Report > E-Mail Security > Intrusion Hits > Top Intrusions > Drill-Down



Top Sources from 2011-04-14 to 2011-05-13 by Intrusion Signature Intrusion01

Source	Color	Intrusions	% of Intrusions	View Logs
192.168.1.33	🟩	443	77.9%	🔍
192.168.2.33	🟦	84	14.8%	🔍
192.168.3.33	🟪	42	7.4%	🔍
Total		569	100%	

Each field is described in the following table.

Table 156 Report > E-Mail Security > Intrusion Hits > Top Intrusions > Drill-Down

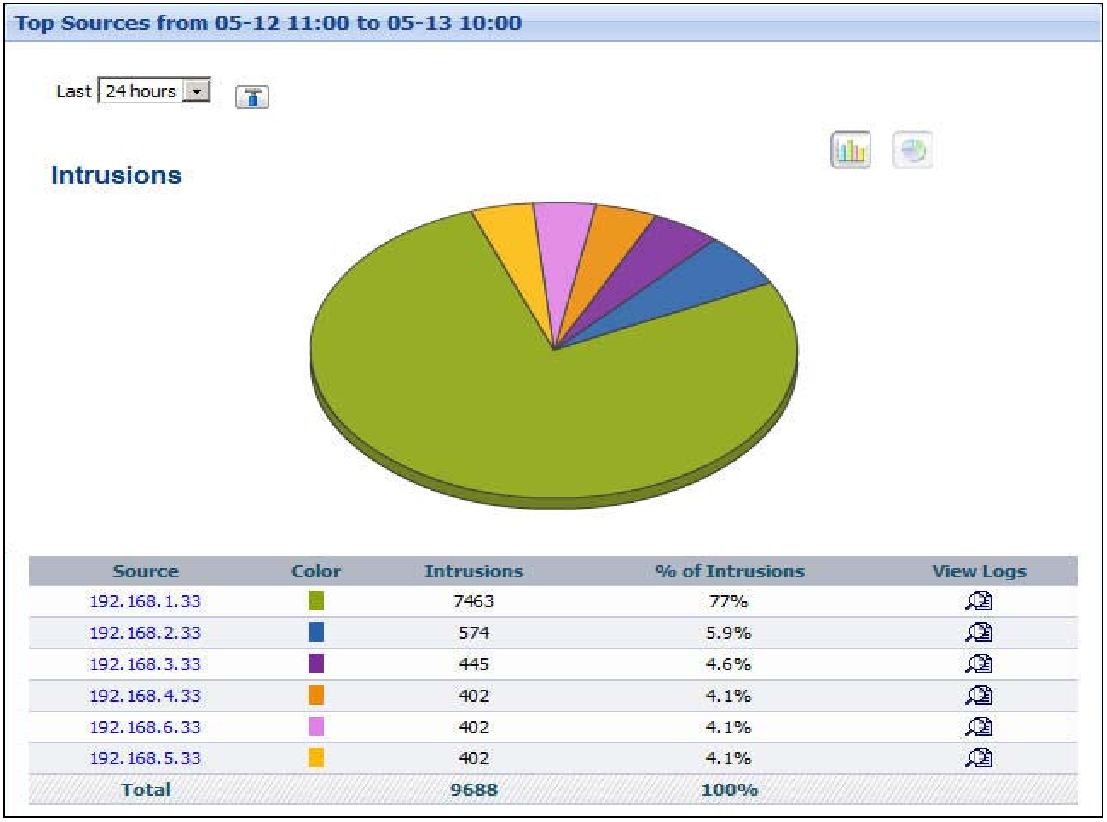
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

8.3.5 Top Intrusion Hits Sources

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

Click **Report > E-Mail Security > Intrusion Hits > Top Sources** to open this screen.

Figure 171 Report > E-Mail Security > Intrusion Hits > Top Sources



Top Sources from 05-12 11:00 to 05-13 10:00

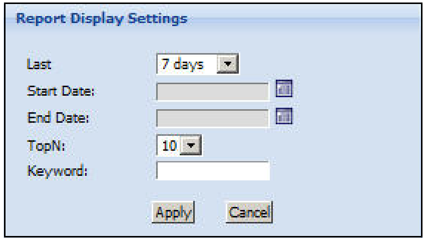
Last 24 hours

Intrusions

Source	Color	Intrusions	% of Intrusions	View Logs
192.168.1.33	🟩	7463	77%	🔍
192.168.2.33	🟦	574	5.9%	🔍
192.168.3.33	🟪	445	4.6%	🔍
192.168.4.33	🟧	402	4.1%	🔍
192.168.6.33	■	402	4.1%	🔍
192.168.5.33	🟨	402	4.1%	🔍
Total		9688	100%	

Each field is described in the following table.

Table 157 Report > E-Mail Security > Intrusion Hits > Top Sources

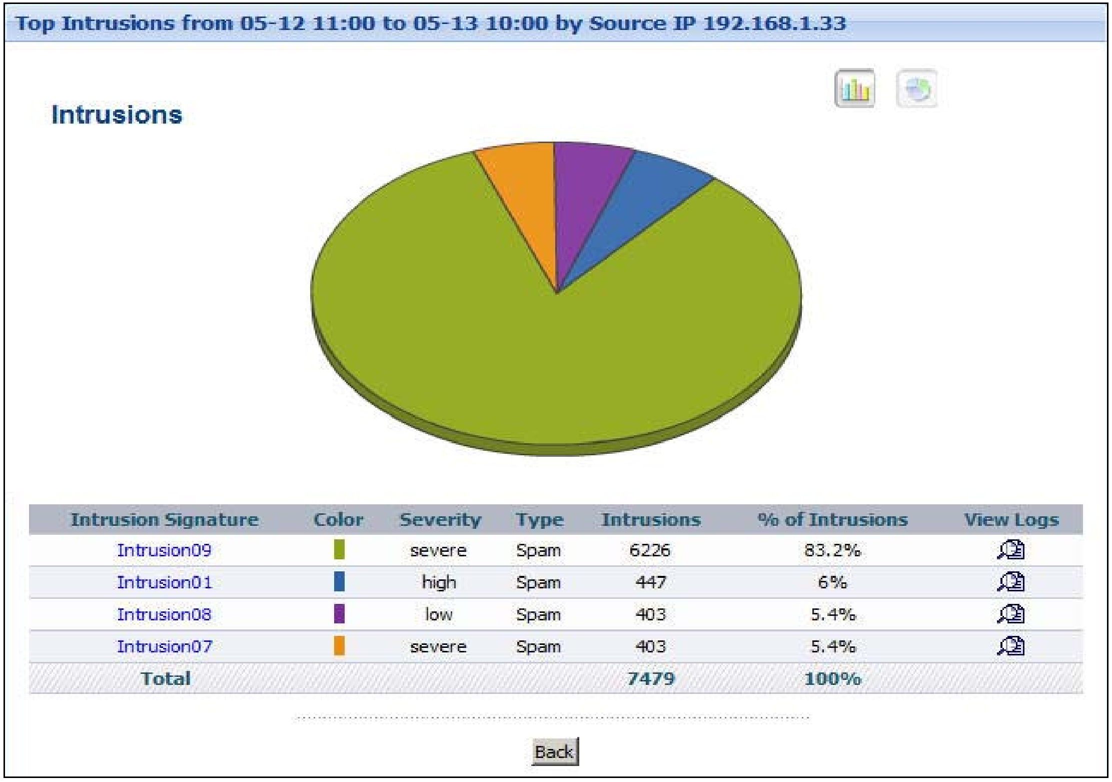
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top intrusion signatures for the selected source.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

8.3.6 Top Intrusion Hits Sources Drill-Down

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

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

Figure 172 Report > E-Mail Security > Intrusion Hits > Top Sources > Drill-Down



Top Intrusions from 05-12 11:00 to 05-13 10:00 by Source IP 192.168.1.33

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	Spam	6226	83.2%	🔍
Intrusion01	🟦	high	Spam	447	6%	🔍
Intrusion08	🟪	low	Spam	403	5.4%	🔍
Intrusion07	🟧	severe	Spam	403	5.4%	🔍
Total				7479	100%	

Each field is described in the following table.

Table 158 Report > E-Mail Security > Intrusion Hits > Top Sources > Drill-Down

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

Table 158 Report > E-Mail Security > Intrusion Hits > Top Sources > Drill-Down

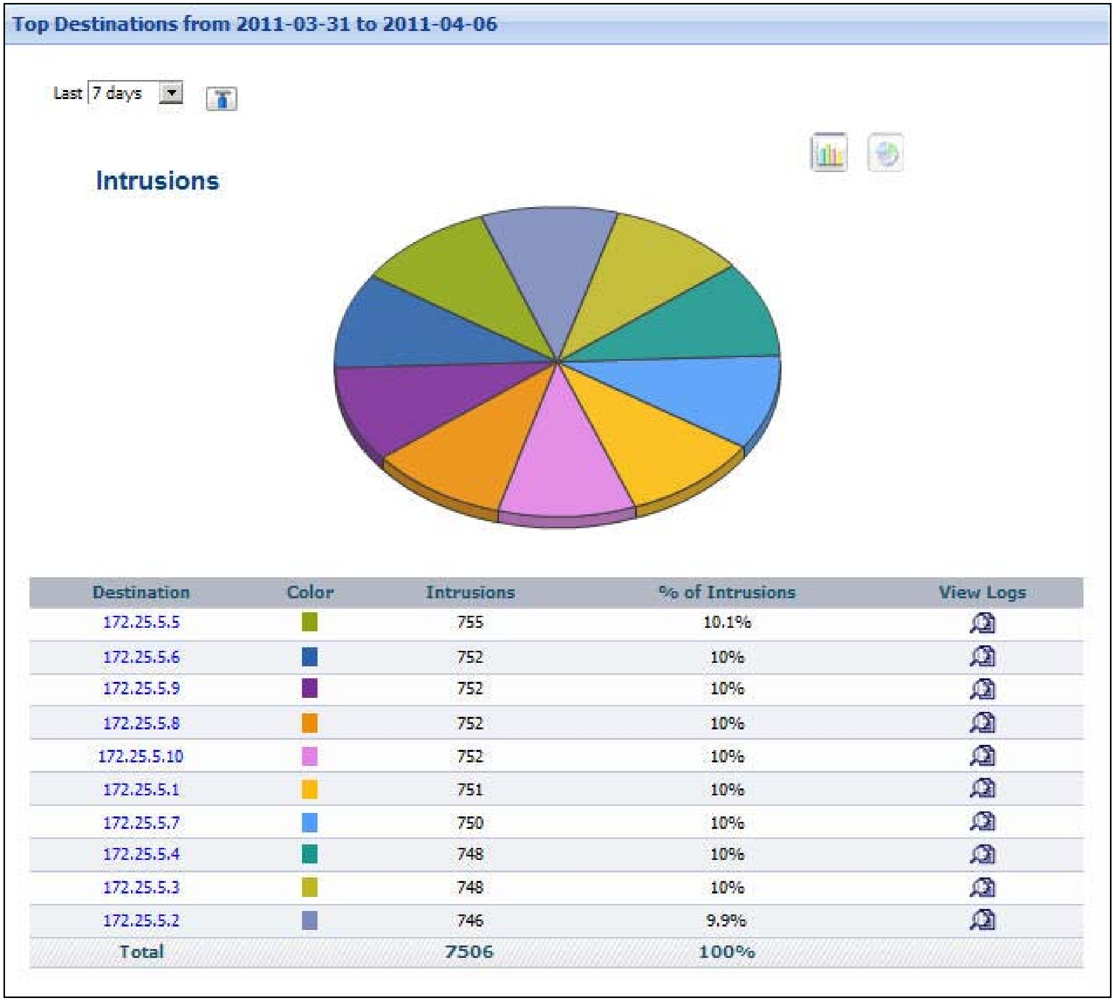
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures from the selected source is greater than the maximum number of records displayed in this table, this total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

8.3.7 Top Intrusion Hits Destinations

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

Click **Report > E-Mail Security > Intrusion Hits > Top Destinations** to open this screen.

Figure 173 Report > E-Mail Security > Intrusion Hits > Top Destinations

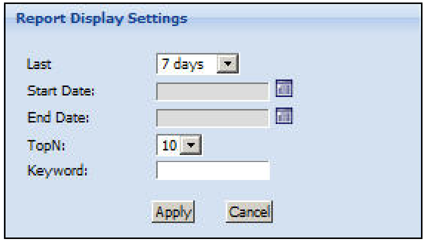


Top Destinations from 2011-03-31 to 2011-04-06

Destination	Color	Intrusions	% of Intrusions	View Logs
172.25.5.5	🟩	755	10.1%	🔍
172.25.5.6	🟦	752	10%	🔍
172.25.5.9	🟪	752	10%	🔍
172.25.5.8	🟧	752	10%	🔍
172.25.5.10	🟪	752	10%	🔍
172.25.5.1	🟨	751	10%	🔍
172.25.5.7	🟦	750	10%	🔍
172.25.5.4	🟩	748	10%	🔍
172.25.5.3	🟨	748	10%	🔍
172.25.5.2	🟦	746	9.9%	🔍
Total		7506	100%	

Each field is described in the following table.

Table 159 Report > E-Mail Security > Intrusion Hits > Top Destinations

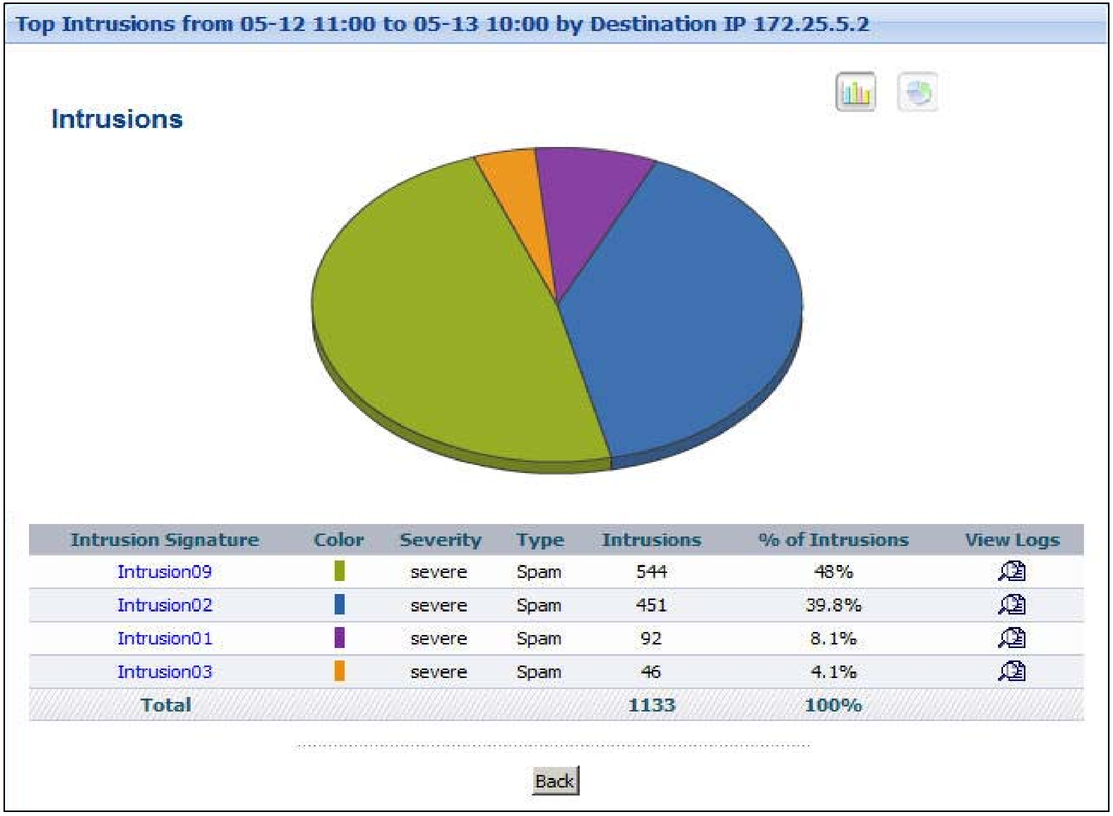
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a destination to look at the top intrusion signatures for the selected destination.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

8.3.8 Top Intrusion Hits Destinations Drill-Down

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

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

Figure 174 Report > E-Mail Security > Intrusion Hits > Top Destinations > Drill-Down



Top Intrusions from 05-12 11:00 to 05-13 10:00 by Destination IP 172.25.5.2

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	Spam	544	48%	🔍
Intrusion02	🟦	severe	Spam	451	39.8%	🔍
Intrusion01	🟪	severe	Spam	92	8.1%	🔍
Intrusion03	🟧	severe	Spam	46	4.1%	🔍
Total				1133	100%	

Each field is described in the following table.

Table 160 Report > E-Mail Security > Intrusion Hits > Top Destinations > Drill-Down

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

Table 160 Report > E-Mail Security > Intrusion Hits > Top Destinations > Drill-Down

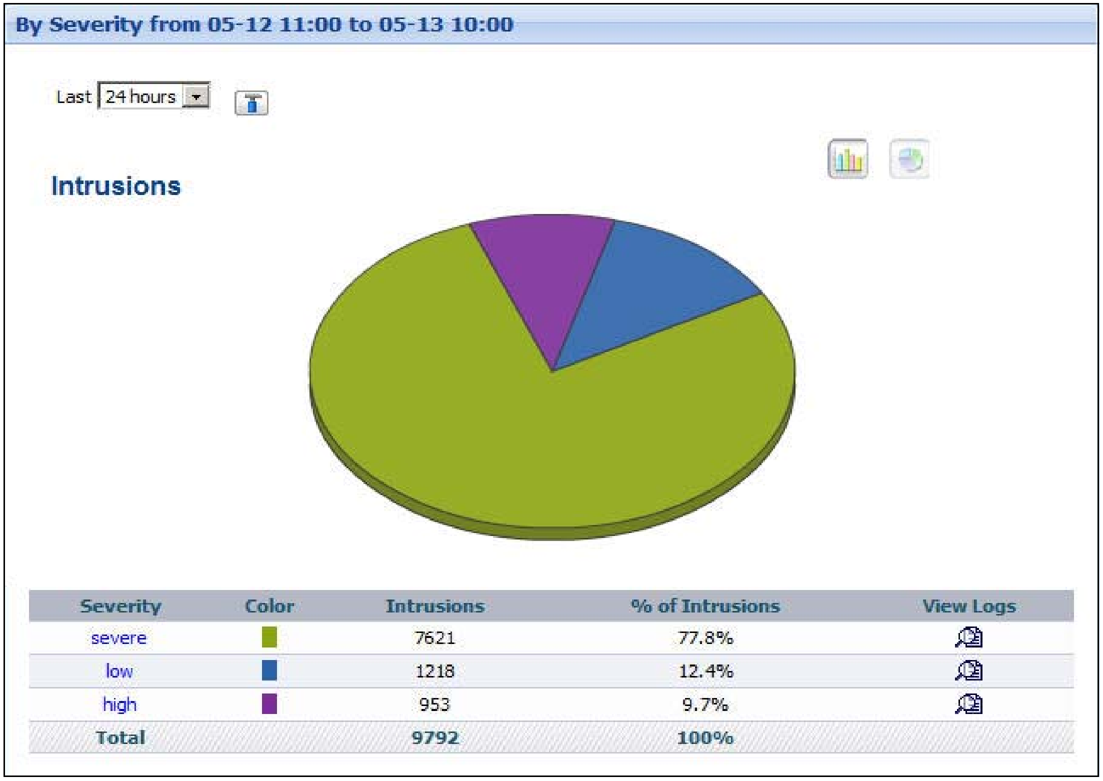
LABEL	DESCRIPTION
% of Intrusions	This field displays what percentage of all intrusions sent to the selected destination belong to each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above. If the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

8.3.9 Intrusion Hits Severities

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

Click **Report > E-Mail Security > Intrusion Hits > By Severity** to open this screen.

Figure 175 Report > E-Mail Security > Intrusion Hits > By Severity



By Severity from 05-12 11:00 to 05-13 10:00

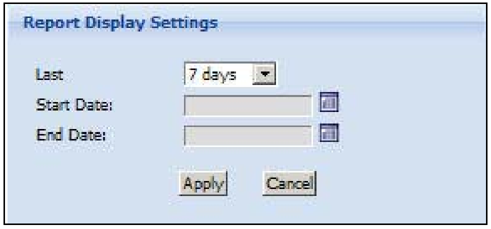
Last 24 hours

Intrusions

Severity	Color	Intrusions	% of Intrusions	View Logs
severe	🟩	7621	77.8%	🔍
low	🟦	1218	12.4%	🔍
high	🟪	953	9.7%	🔍
Total		9792	100%	

Each field is described in the following table.

Table 161 Report > E-Mail Security > Intrusion Hits > By Severity

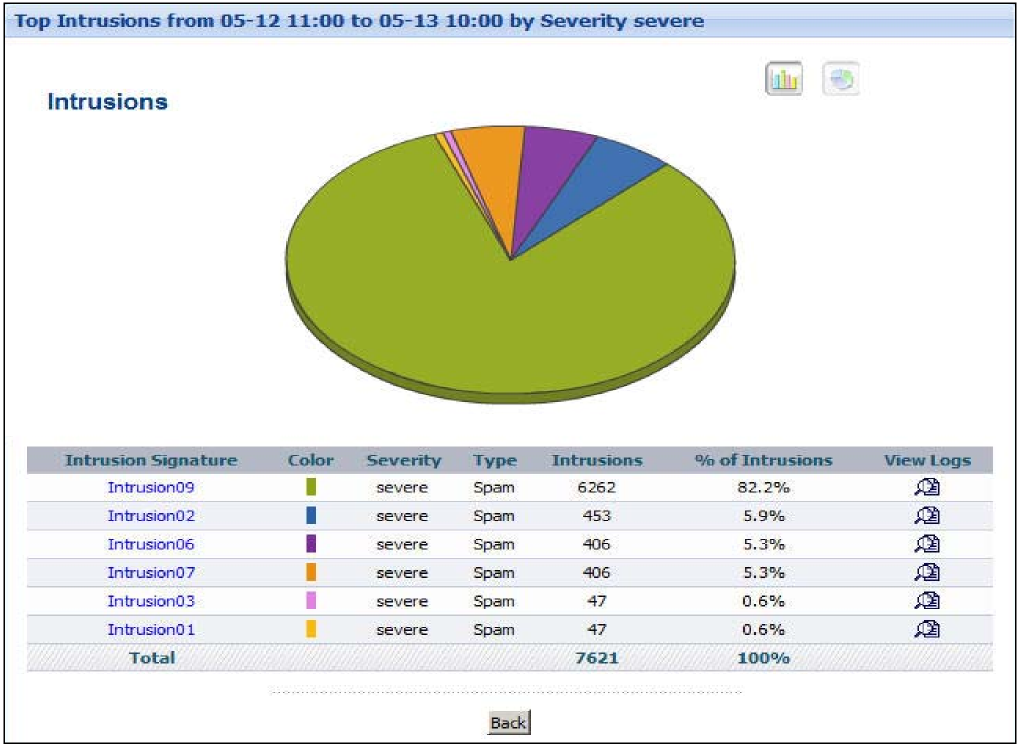
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

8.3.10 Intrusion Hits Severities Drill-Down

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

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

Figure 176 Report > E-Mail Security > Intrusion Hits > By Severity > Drill-Down


Top Intrusions from 05-12 11:00 to 05-13 10:00 by Severity severe
Intrusions
Back

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Intrusion09	🟩	severe	Spam	6262	82.2%	🔍
Intrusion02	🟦	severe	Spam	453	5.9%	🔍
Intrusion06	🟪	severe	Spam	406	5.3%	🔍
Intrusion07	🟧	severe	Spam	406	5.3%	🔍
Intrusion03	■	severe	Spam	47	0.6%	🔍
Intrusion01	🟨	severe	Spam	47	0.6%	🔍
Total				7621	100%	

Each field is described in the following table.

Table 162 Report > E-Mail Security > Intrusion Hits > By Severity > Drill-Down

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

9

Web Security

This chapter discusses how to use reports to look at Web related security threats that were detected by the ZyXEL device's firewall.

9.1 Security Threat

These reports look at the number of attempts to access Web security related blocked web sites by time interval as well as top blocked sites and hosts. Specifically, these reports include web sites detected by the ZYXEL device's content filter in the following categories: Phishing, Spyware/ Malware Sources, Spyware Effects/Privacy Concerns and Proxy Avoidance.

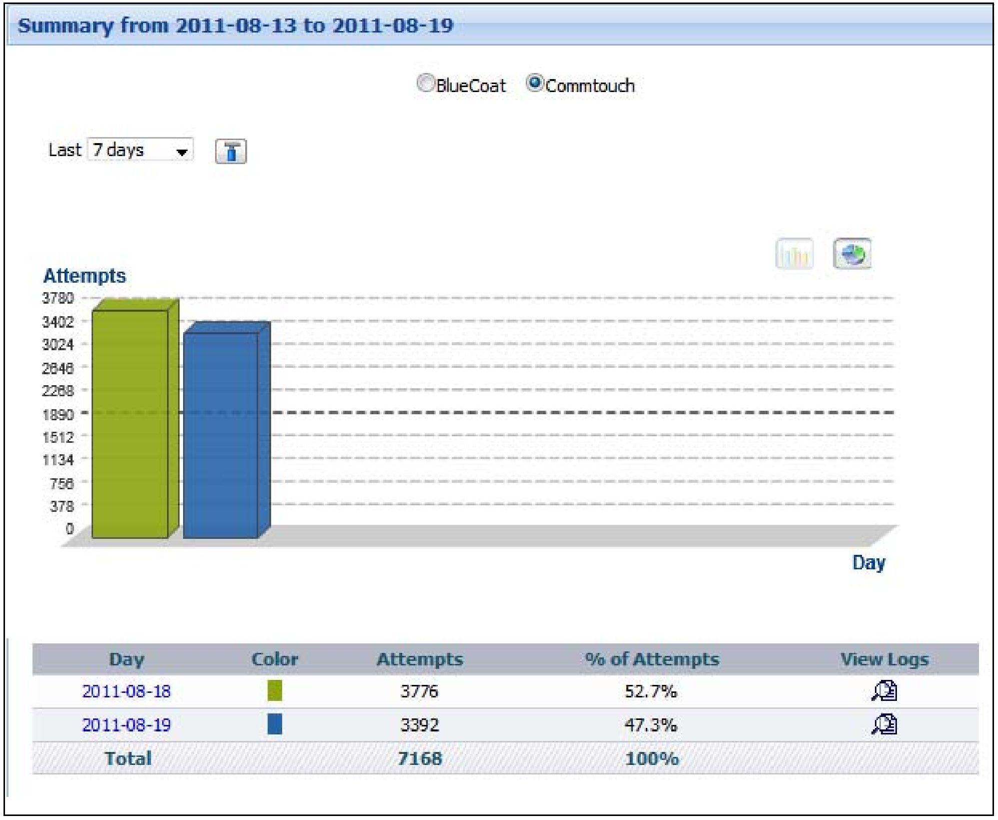
Note: To look at security policy reports, each ZyXEL device must record blocked web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Blocked Web Sites** is enabled.

9.1.1 Security Threat Summary

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

Click **Report > Web Security > Security Threat > Summary** to open this screen.

Figure 177 Report > Web Security > Security Threat > Summary



Summary from 2011-08-13 to 2011-08-19

○ BlueCoat ● Commtouch

Last 7 days

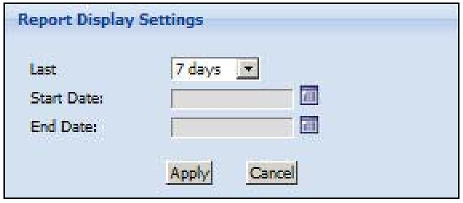
Day	Color	Attempts	% of Attempts	View Logs
2011-08-18	🟩	3776	52.7%	
2011-08-19	🟦	3392	47.3%	
Total		7168	100%	

Each field is described in the following table.

Table 163 Report > Web Security > Security Threat > Summary

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 163 Report > Web Security > Security Threat > Summary

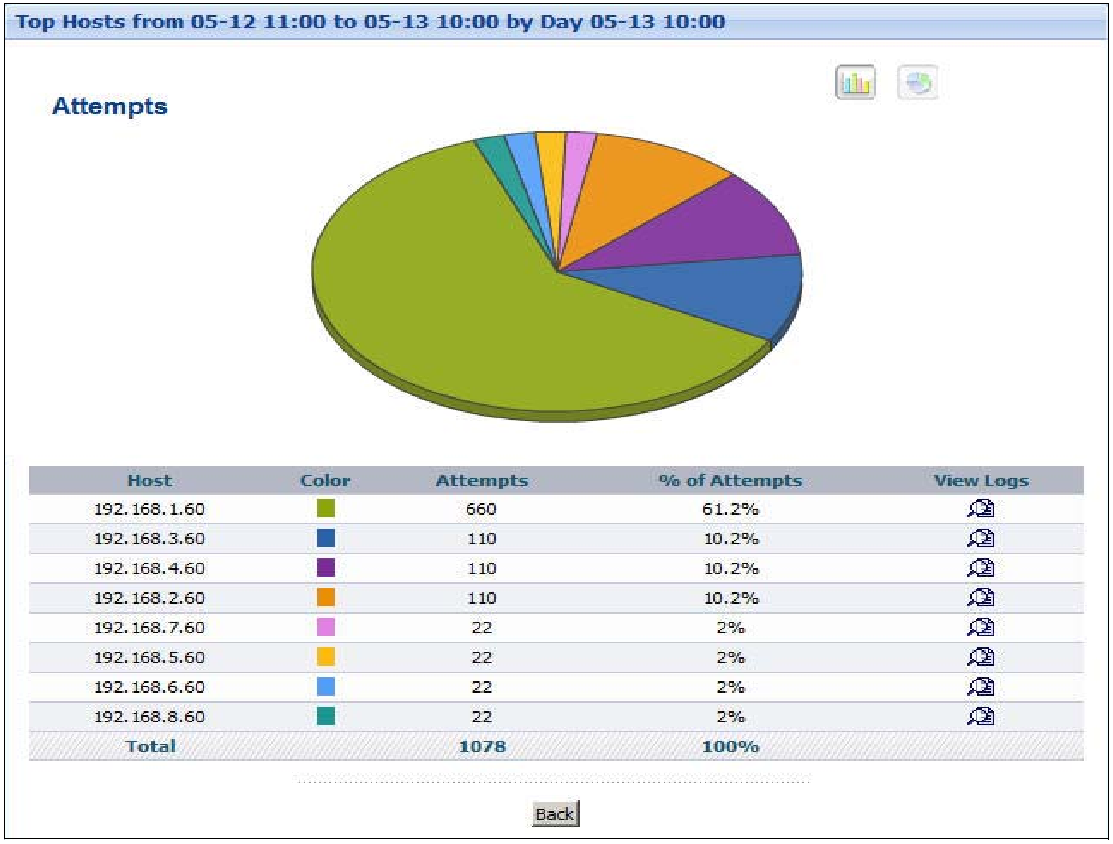
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Apply Cancel Select a specific **Start Date** and **End Date**. 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts by each source to access blocked web sites in the selected time interval.
% of Attempts	This field displays what percentage of all blocked web access attempts was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

9.1.2 Security Threat Summary Drill-Down

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

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

Figure 178 Report > Web Security > Security Threat > Summary > Drill-Down



Top Hosts from 05-12 11:00 to 05-13 10:00 by Day 05-13 10:00

Attempts

Host	Color	Attempts	% of Attempts	View Logs
192.168.1.60	🟩	660	61.2%	🔍
192.168.3.60	🟦	110	10.2%	🔍
192.168.4.60	🟪	110	10.2%	🔍
192.168.2.60	🟧	110	10.2%	🔍
192.168.7.60	🟪	22	2%	🔍
192.168.5.60	🟨	22	2%	🔍
192.168.6.60	🟦	22	2%	🔍
192.168.8.60	🟩	22	2%	🔍
Total		1078	100%	

Each field is described in the following table.

Table 164 Report > Web Security > Security Threat > Summary > Drill-Down

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

Table 164 Report > Web Security > Security Threat > 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.

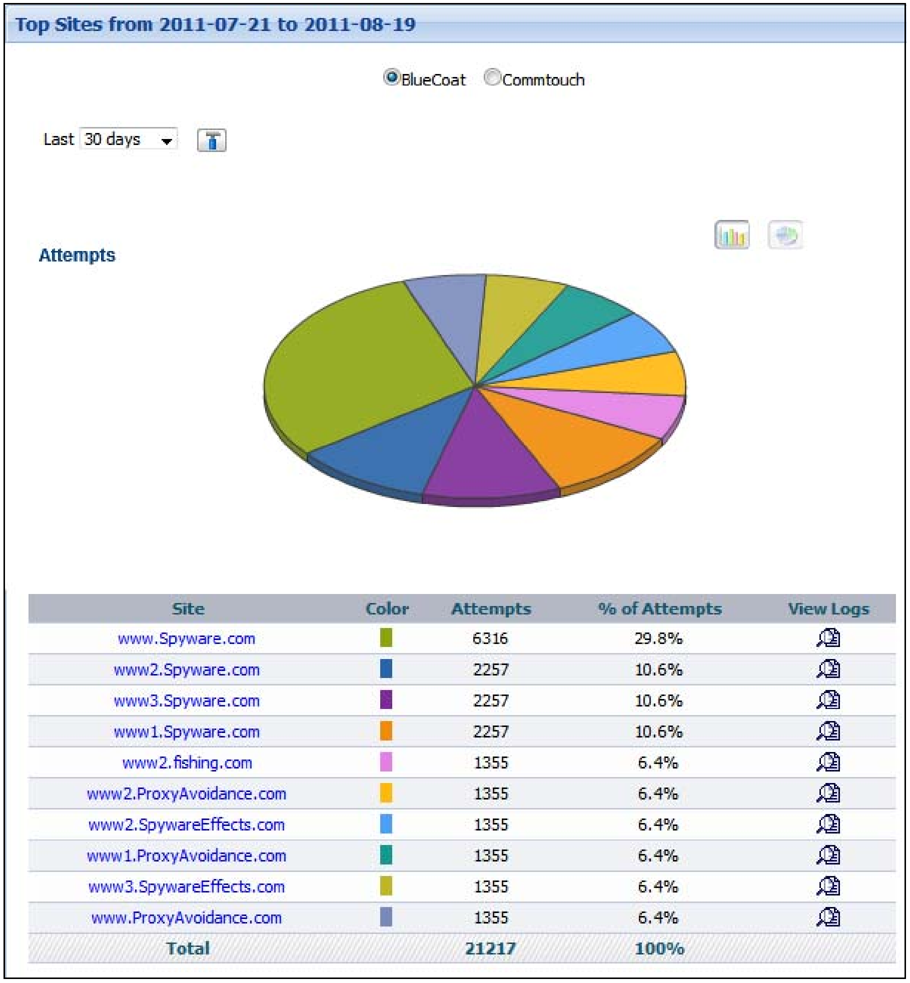
9.1.3 Security Threat Top Web Sites

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

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

Click **Report > Web Security > Security Threat > Top Sites** to open this screen.

Figure 179 Report > Web Security > Security Threat > Top Sites



Top Sites from 2011-07-21 to 2011-08-19

● BlueCoat ○ Commtouch

Last 30 days ▾

Attempts

Site	Color	Attempts	% of Attempts	View Logs
www.Spyware.com	■	6316	29.8%	🔍
www2.Spyware.com	■	2257	10.6%	🔍
www3.Spyware.com	■	2257	10.6%	🔍
www1.Spyware.com	■	2257	10.6%	🔍
www2.fishing.com	■	1355	6.4%	🔍
www2.ProxyAvoidance.com	■	1355	6.4%	🔍
www2.SpywareEffects.com	■	1355	6.4%	🔍
www1.ProxyAvoidance.com	■	1355	6.4%	🔍
www3.SpywareEffects.com	■	1355	6.4%	🔍
www.ProxyAvoidance.com	■	1355	6.4%	🔍
Total		21217	100%	

Each field is described in the following table.

Table 165 Report > Web Security > Security Threat > Top Sites

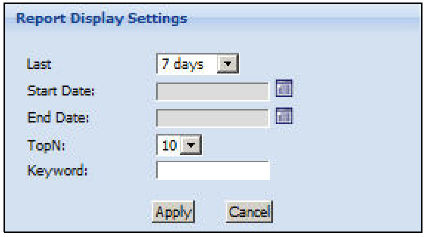
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of blocked web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays how much traffic (in megabytes) the device handled for each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made to each destination.

Table 165 Report > Web Security > Security Threat > Top Sites

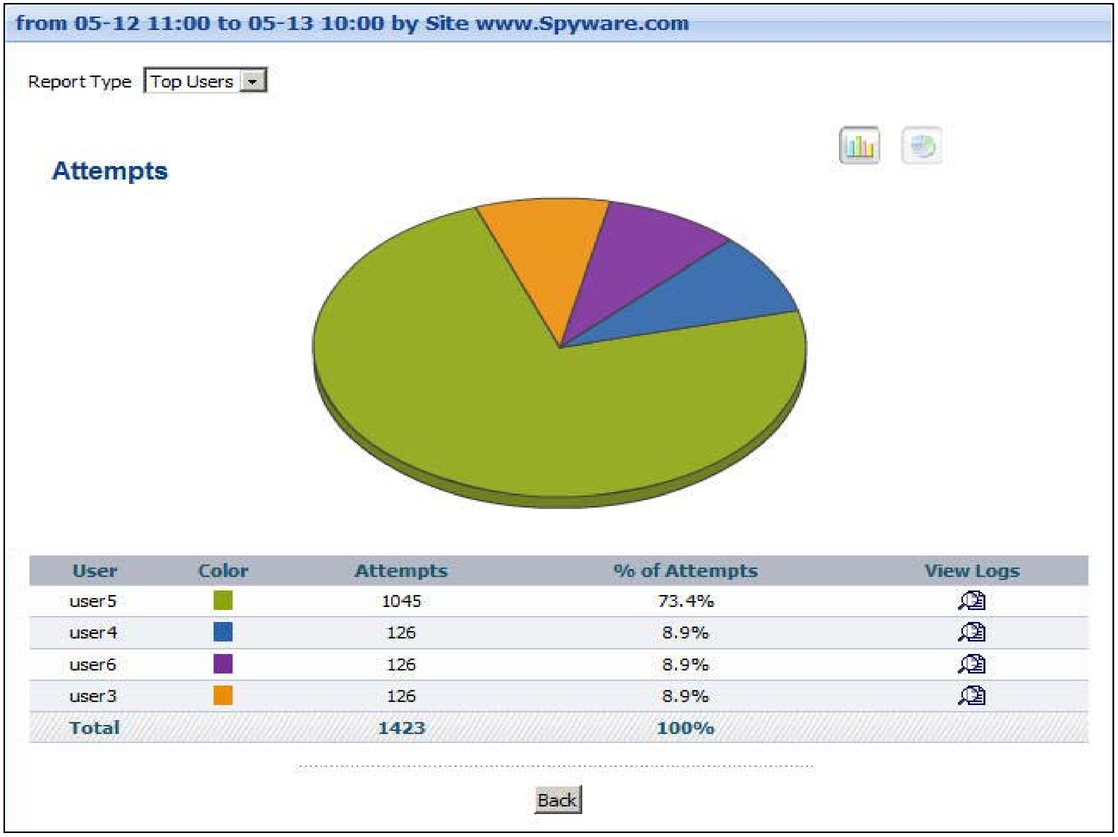
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

9.1.4 Security Threat Top Sites Drill-Down

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

Click on a specific destination in **Report > Web Security > Security Threat > Top Sites** to open this screen.

Figure 180 Report > Web Security > Security Threat > Top Sites > Drill-Down



from 05-12 11:00 to 05-13 10:00 by Site www.Spyware.com

Report Type: Top Users

User	Color	Attempts	% of Attempts	View Logs
user5	🟩	1045	73.4%	🔍
user4	🟦	126	8.9%	🔍
user6	🟪	126	8.9%	🔍
user3	🟧	126	8.9%	🔍
Total		1423	100%	

Each field is described in the following table.

Table 166 Report > Web Security > Security Threat > Top Sites > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Users**, **Top Hosts** or **By Hour** as the content to be displayed.

Table 166 Report > Web Security > Security Threat > Top Sites > Drill-Down

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

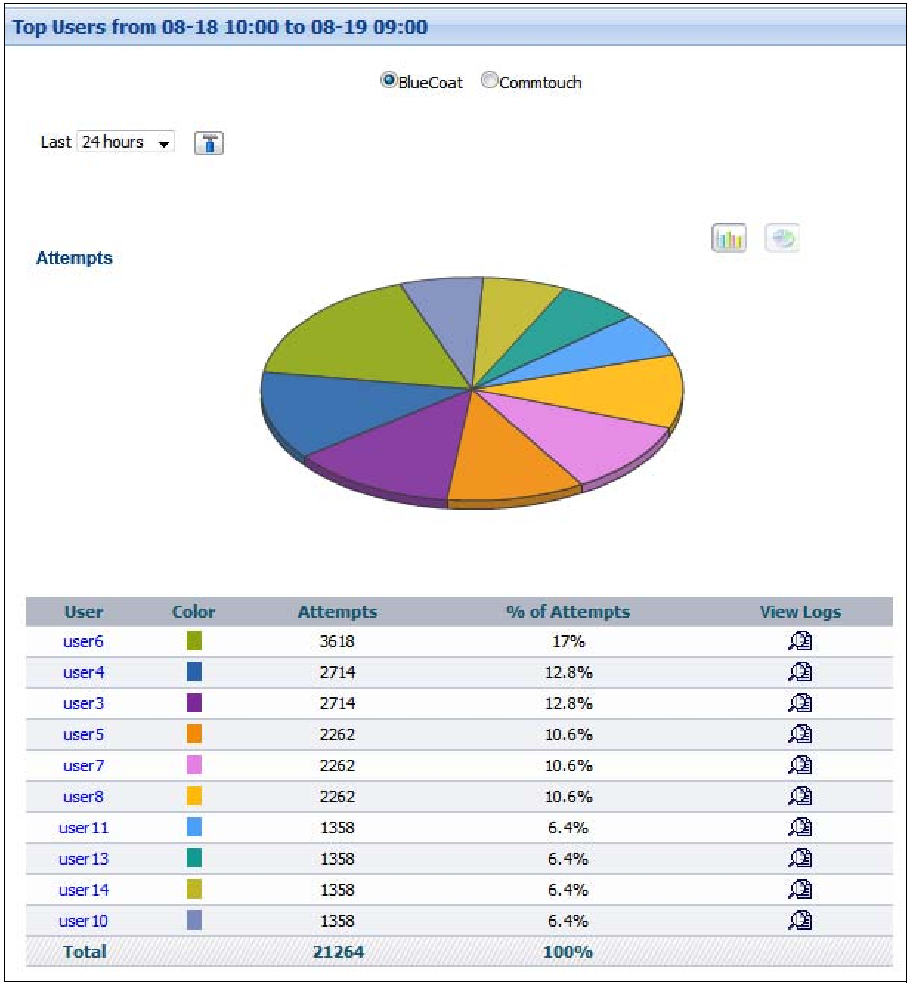
9.1.5 Security Threat Top Users

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

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

Click **Report > Web Security > Security Threat > Top Users** to open this screen.

Figure 181 Report > Web Security > Security Threat > Top Users



Top Users from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

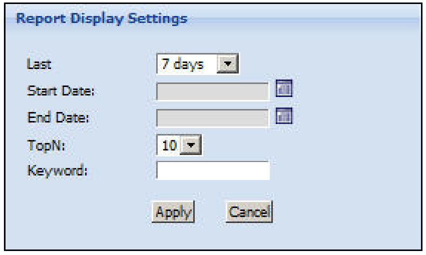
User	Color	Attempts	% of Attempts	View Logs
user6	■	3618	17%	🔍
user4	■	2714	12.8%	🔍
user3	■	2714	12.8%	🔍
user5	■	2262	10.6%	🔍
user7	■	2262	10.6%	🔍
user8	■	2262	10.6%	🔍
user11	■	1358	6.4%	🔍
user13	■	1358	6.4%	🔍
user14	■	1358	6.4%	🔍
user10	■	1358	6.4%	🔍
Total		21264	100%	

Each field is described in the following table.

Table 167 Report > Web Security > Security Threat > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 167 Report > Web Security > Security Threat > Top Users

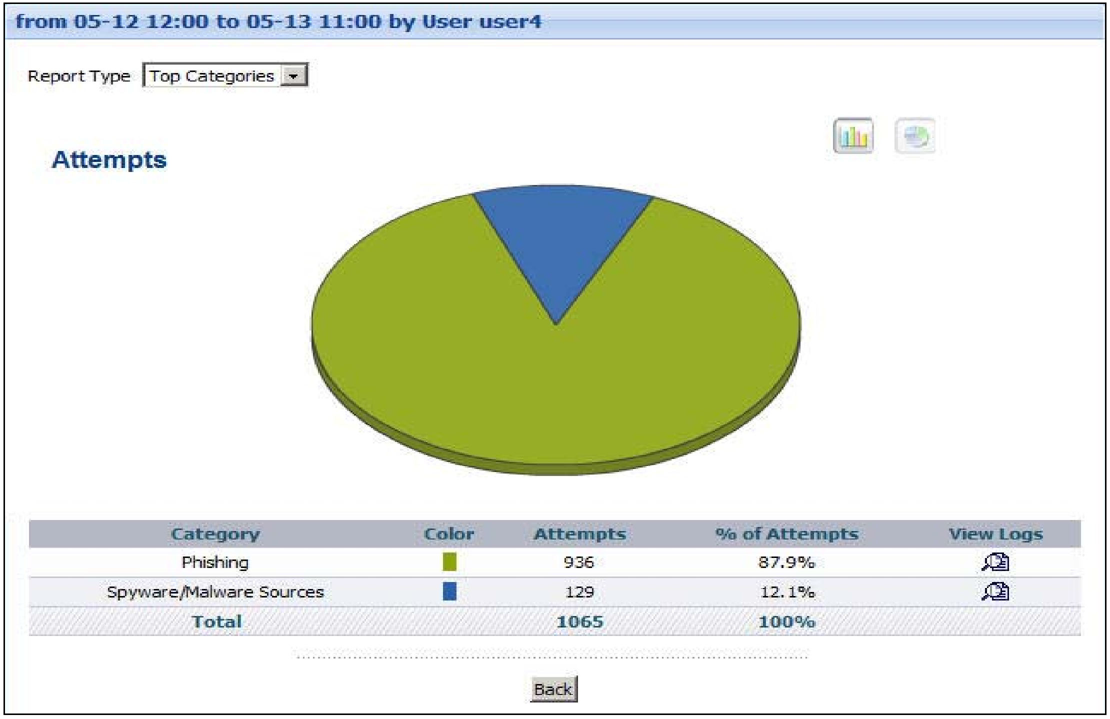
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users for which the device blocked the most web site access attempts, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each user.
% of Attempts	This field displays what percentage the user had of all blocked attempts to access web sites.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.1.6 Security Threat Top Users Drill-Down

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

Click on a specific source in **Report > Web Security > Security Threat > Top Users** to open this screen.

Figure 182 Report > Web Security > Security Threat > Top Users > Drill-Down



from 05-12 12:00 to 05-13 11:00 by User user4

Report Type: Top Categories

Attempts

Category	Color	Attempts	% of Attempts	View Logs
Phishing	🟩	936	87.9%	🔍
Spyware/Malware Sources	🟦	129	12.1%	🔍
Total		1065	100%	

Each field is described in the following table.

Table 168 Report > Web Security > Security Threat > Top Users > Drill-Down

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

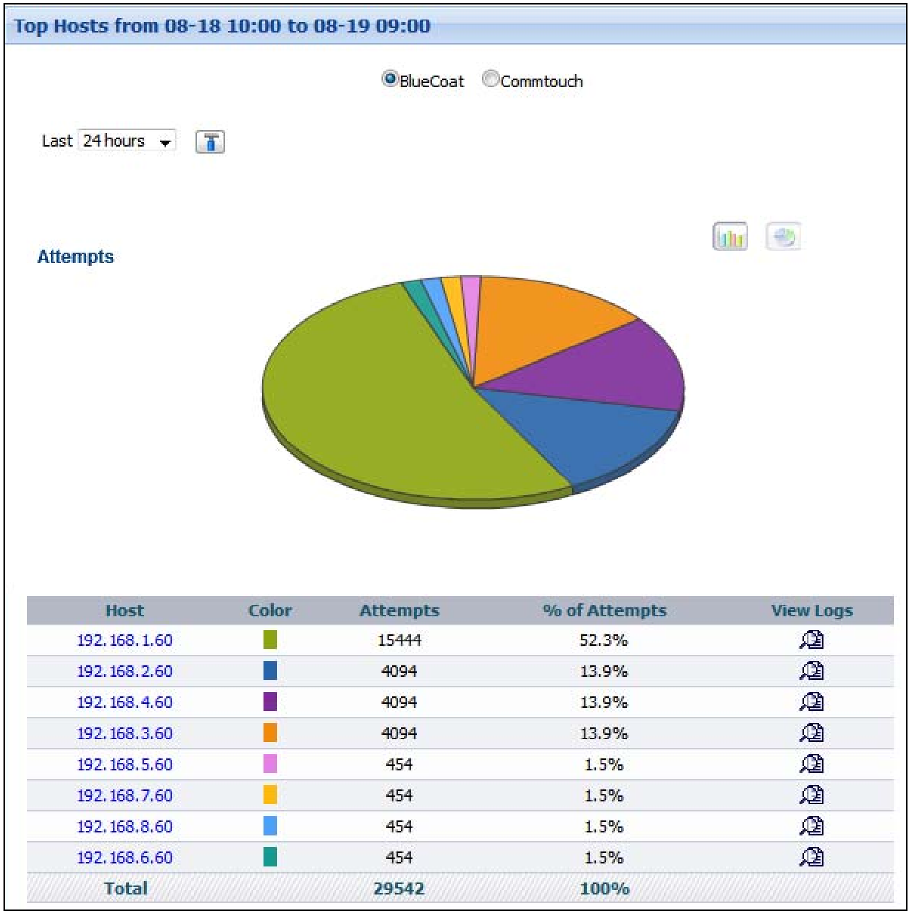
9.1.7 Security Threat Top Hosts

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

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

Click **Report > Web Security > Security Threat > Top Hosts** to open this screen.

Figure 183 Report > Web Security > Security Threat > Top Hosts



Top Hosts from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

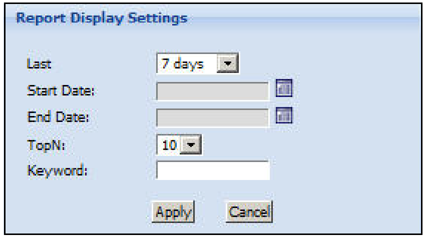
Host	Color	Attempts	% of Attempts	View Logs
192.168.1.60	🟩	15444	52.3%	🔍
192.168.2.60	🟦	4094	13.9%	🔍
192.168.4.60	🟪	4094	13.9%	🔍
192.168.3.60	🟧	4094	13.9%	🔍
192.168.5.60	■	454	1.5%	🔍
192.168.7.60	🟨	454	1.5%	🔍
192.168.8.60	🟦	454	1.5%	🔍
192.168.6.60	🟩	454	1.5%	🔍
Total		29542	100%	

Each field is described in the following table.

Table 169 Report > Web Security > Security Threat > Top Hosts

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.

Table 169 Report > Web Security > Security Threat > Top Hosts

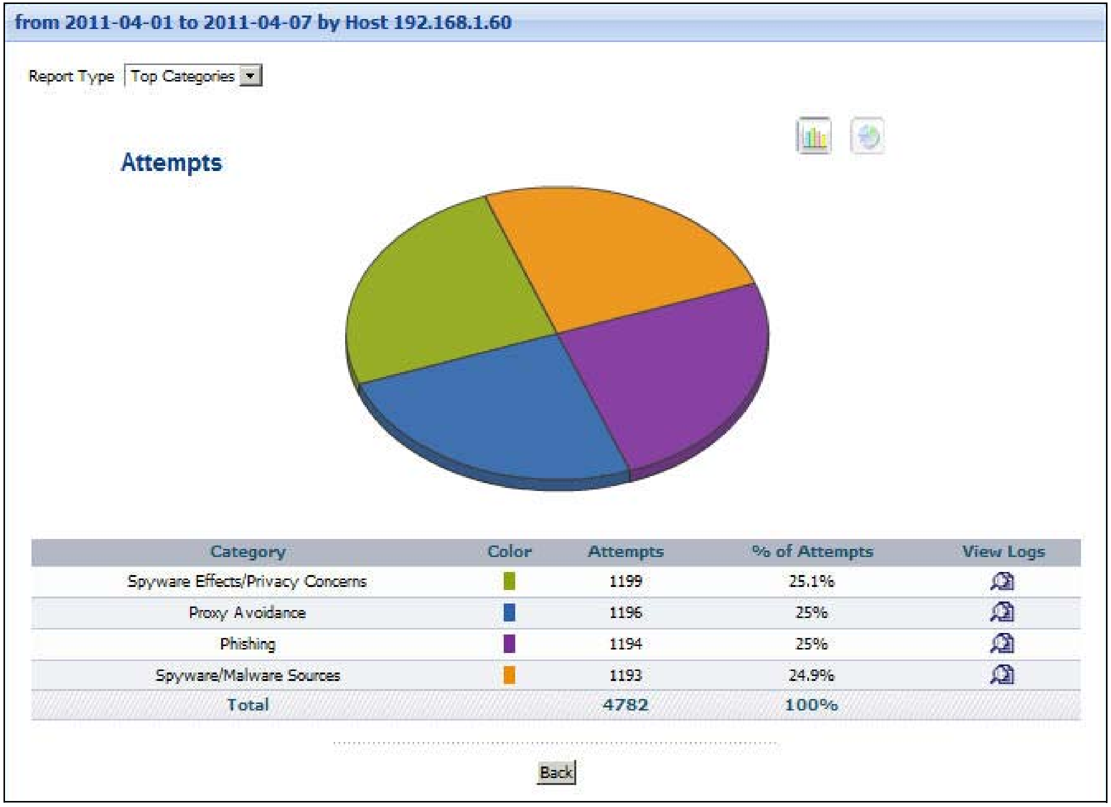
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of web site access attempts the device blocked from each source.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.1.8 Security Threat Top Hosts Drill-Down

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

Click on a specific source in **Report > Web Security > Security Threat > Top Hosts** to open this screen.

Figure 184 Report > Web Security > Security Threat > Top Hosts > Drill-Down



from 2011-04-01 to 2011-04-07 by Host 192.168.1.60

Report Type: Top Categories

Attempts

Category	Color	Attempts	% of Attempts	View Logs
Spyware Effects/Privacy Concerns	🟩	1199	25.1%	🔍
Proxy Avoidance	🟦	1196	25%	🔍
Phishing	🟪	1194	25%	🔍
Spyware/Malware Sources	🟧	1193	24.9%	🔍
Total		4782	100%	

Each field is described in the following table.

Table 170 Report > Web Security > Security Threat > Top Hosts > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Categories**, **Top Sites** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic from the selected source, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.

Table 170 Report > Web Security > Security Threat > Top Hosts > Drill-Down

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

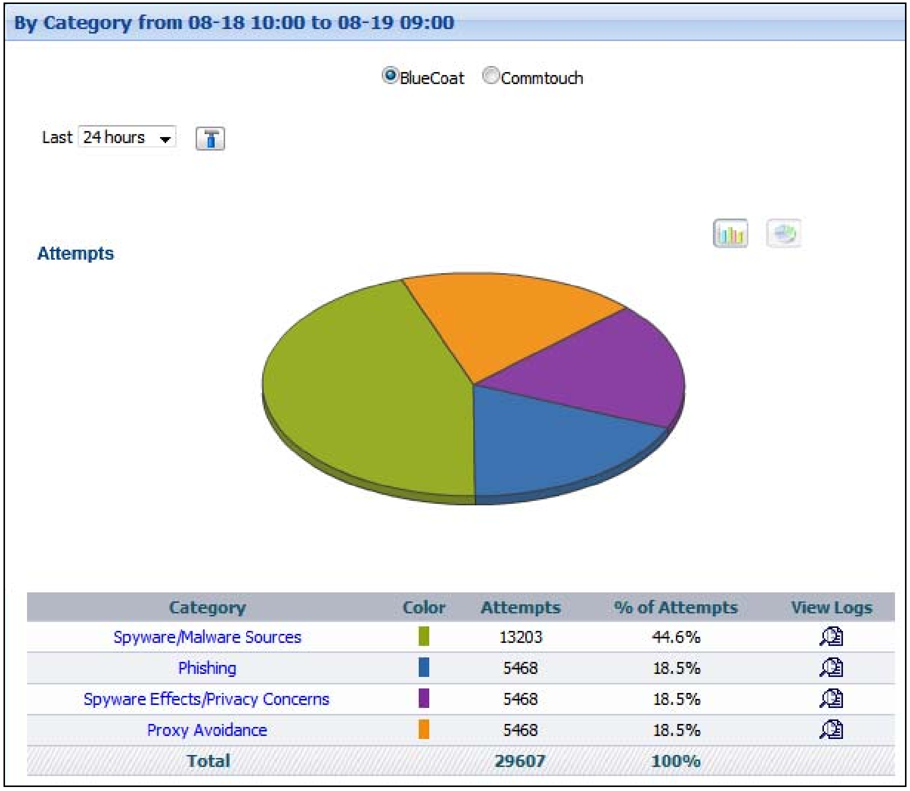
9.1.9 Security Threat Categories

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

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

Click **Report > Web Security > Security Threat > By Category** to open this screen.

Figure 185 Report > Web Security > Security Threat > By Category



By Category from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

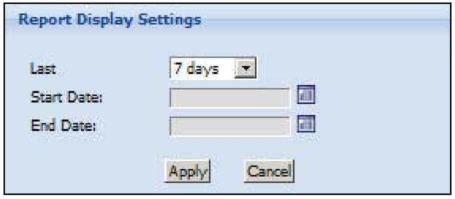
Last 24 hours

Attempts

Category	Color	Attempts	% of Attempts	View Logs
Spyware/Malware Sources	🟩	13203	44.6%	🔍
Phishing	🟦	5468	18.5%	🔍
Spyware Effects/Privacy Concerns	🟪	5468	18.5%	🔍
Proxy Avoidance	🟧	5468	18.5%	🔍
Total		29607	100%	

Each field is described in the following table.

Table 171 Report > Web Security > Security Threat > By Category

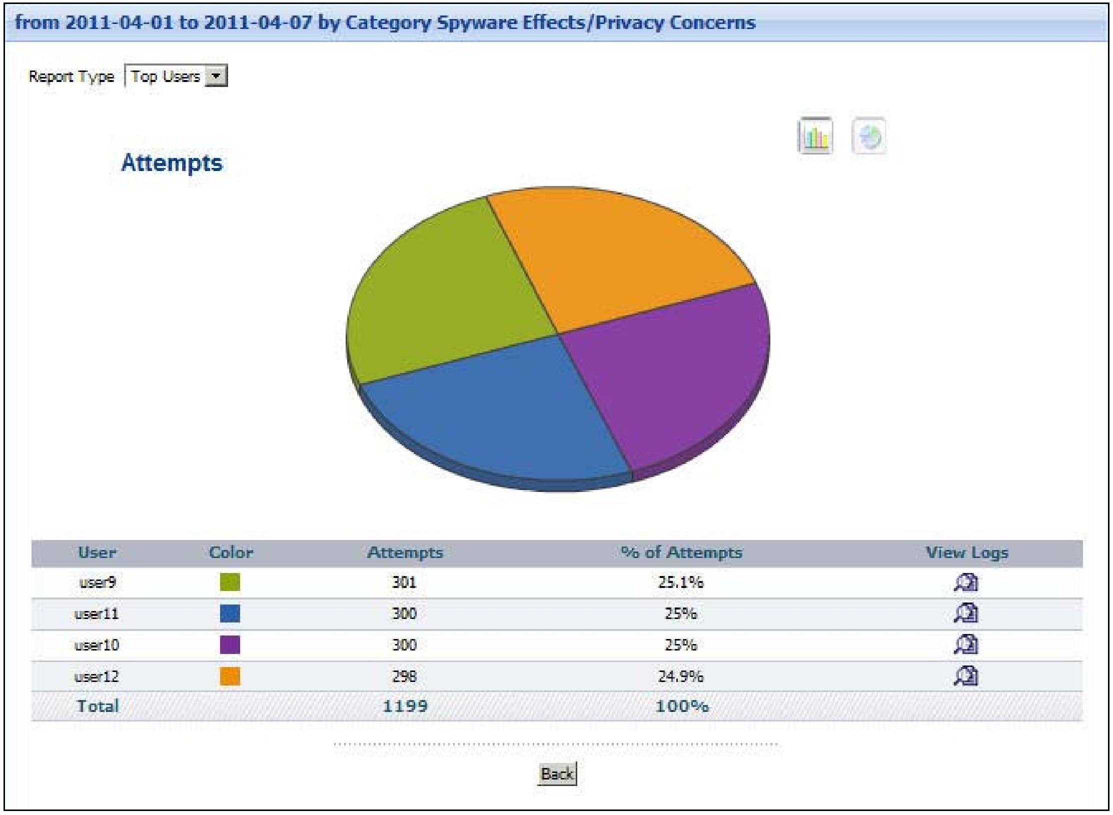
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access allowed web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

9.1.10 Security Threat Categories Drill-Down

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

Click on a specific category in **Report > Web Security > Security Threat > By Category** to open this screen.

Figure 186 Report > Web Security > Security Threat > By Category > Drill-Down



from 2011-04-01 to 2011-04-07 by Category Spyware Effects/Privacy Concerns

Report Type: Top Users

Attempts

User	Color	Attempts	% of Attempts	View Logs
user9	🟩	301	25.1%	🔍
user11	🟦	300	25%	🔍
user10	🟪	300	25%	🔍
user12	🟧	298	24.9%	🔍
Total		1199	100%	

Each field is described in the following table.

Table 172 Report > Web Security > Security Threat > By Category > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Users**, **Top Sites**, **Top Hosts** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the destinations of blocked web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
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.

Table 172 Report > Web Security > Security Threat > By Category > Drill-Down

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

9.2 Virus Found

These reports look at Web security related viruses that were detected by the ZyXEL device's anti-virus feature. Specifically, these reports will include viruses received through the HTTP protocol.

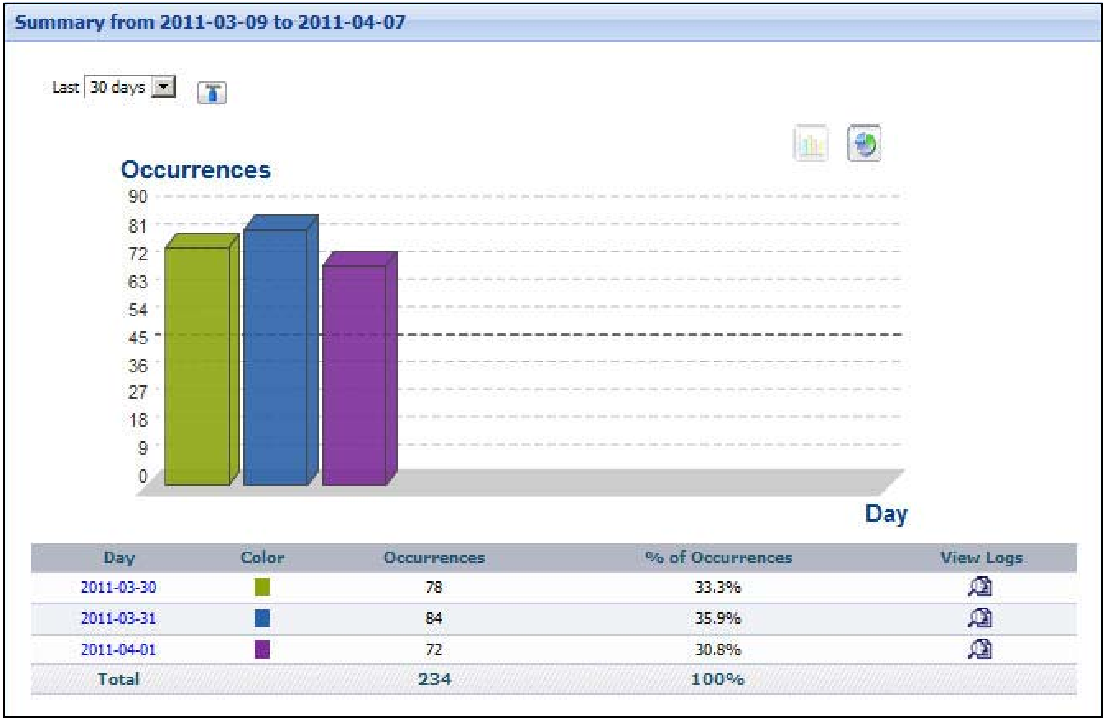
Note: To look at anti-virus reports, each ZyXEL device must record anti-virus messages in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Virus** is enabled. Then, go to **Anti-Virus** > **General**. ZyXEL devices can log viruses based on the **Service** the virus was using. Make sure the ZyXEL device logs viruses you want to include in Vantage Report.

9.2.1 Virus Found Summary

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

Click **Report > Web Security > Virus Found > Summary** to open this screen.

Figure 187 Report > Web Security > Virus Found > Summary



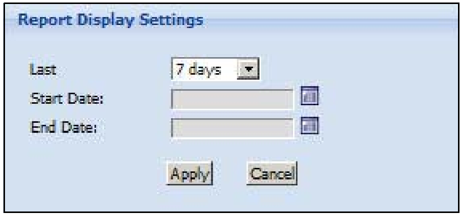
Summary from 2011-03-09 to 2011-04-07

Last 30 days

Day	Color	Occurrences	% of Occurrences	View Logs
2011-03-30	🟩	78	33.3%	🔍
2011-03-31	🟦	84	35.9%	🔍
2011-04-01	🟪	72	30.8%	🔍
Total		234	100%	

Each field is described in the following table.

Table 173 Report > Web Security > Virus Found > Summary

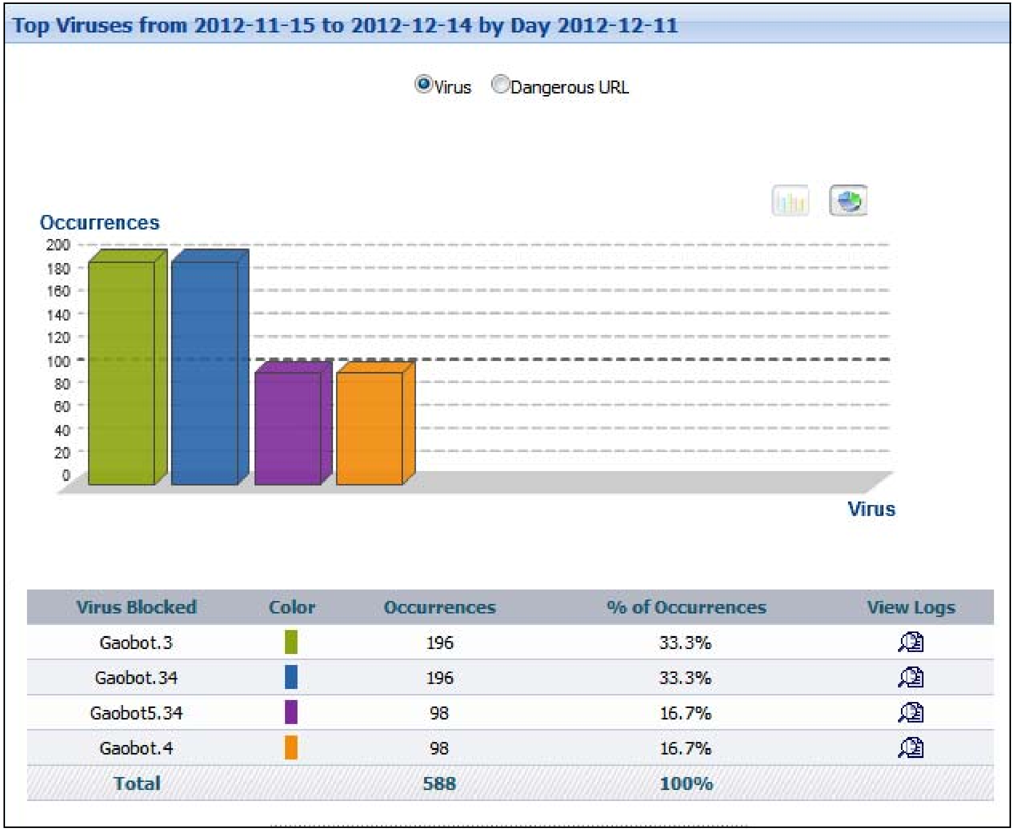
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last 7 days Start Date: End Date: Apply Cancel 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the viruses in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Occurrences	This field displays the number of occurrences in the selected time interval.
% of Occurrences	This field displays what percentage of all occurrences was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

9.2.2 Virus Found Summary Drill-Down

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

Click on a specific time interval in **Report > Web Security > Virus Found > Summary** to open this screen.

Figure 188 Report > Web Security > Virus Found > Summary > Drill-Down



Top Viruses from 2012-11-15 to 2012-12-14 by Day 2012-12-11

● Virus ○ Dangerous URL

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.3	🟩	196	33.3%	🔍
Gaobot.34	🟦	196	33.3%	🔍
Gaobot5.34	🟪	98	16.7%	🔍
Gaobot.4	🟧	98	16.7%	🔍
Total		588	100%	

Each field is described in the following table.

Table 174 Report > Web Security > Virus Found > Summary > Drill-Down

LABEL	DESCRIPTION
Virus	Select this to view the number of virus occurrences the selected device prevented.
Dangerous URL	Select this to view the number of URLs the selected device prevented users from accessing because the device detected a virus in the web page.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System > General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the 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 when you select **Virus**. It shows the viruses stopped in the selected time interval, sorted by the number of occurrences of each one.
URL	This field displays when you select **Dangerous URL**. It shows the virus-infected URLs the selected device prevented users from accessing.
Color	This field displays what color represents each virus or virus-infected URL in the graph.
Occurrences	This field displays the number of occurrences of each virus or attempts to access each dangerous URL in the selected time interval.
% of Occurrences	This field displays what percentage each virus or virus-infected URL made out of all occurrences in the selected time interval.

Table 174 Report > Web Security > Virus Found > Summary > Drill-Down

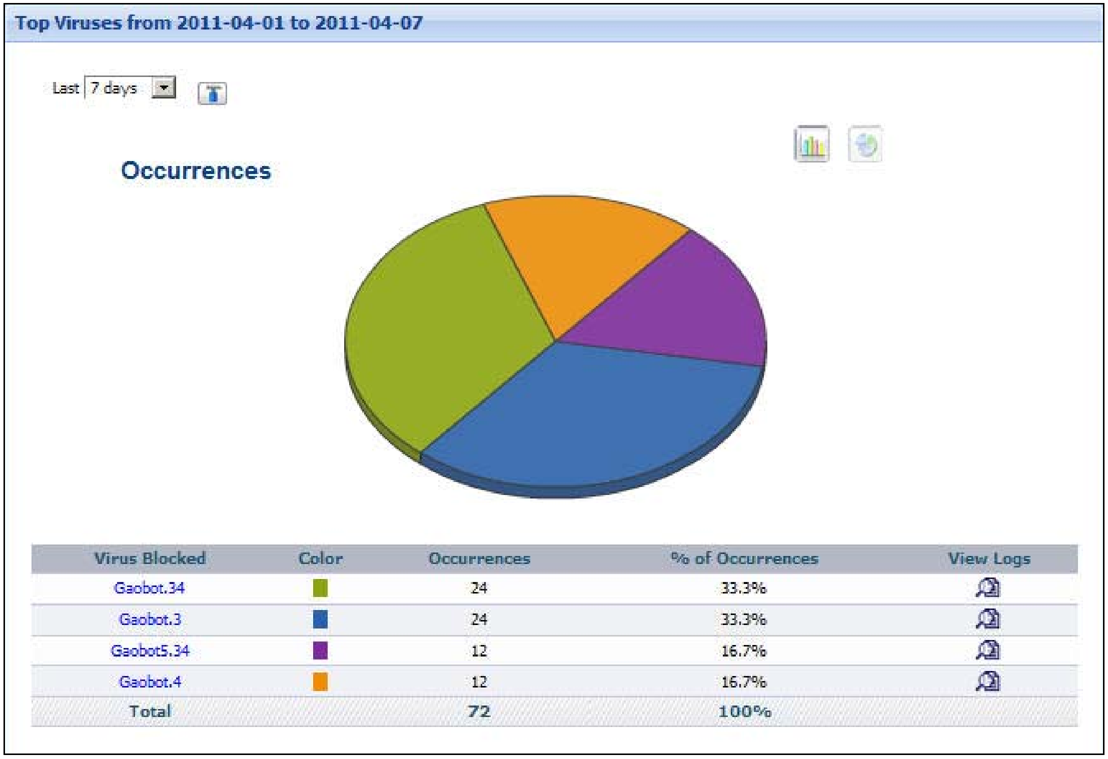
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses or virus-infected URLs above. If the number of viruses or dangerous URLs in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.2.3 Top Viruses

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

Click **Report > Web Security > Virus Found > Top Viruses** to open this screen.

Figure 189 Report > Web Security > Virus Found > Top Viruses

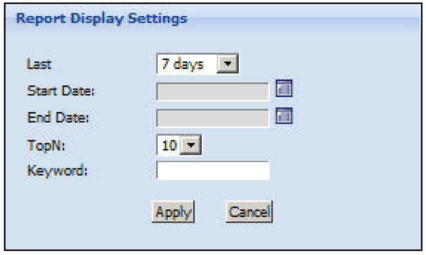


Top Viruses from 2011-04-01 to 2011-04-07

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	24	33.3%	🔍
Gaobot.3	🟦	24	33.3%	🔍
Gaobot5.34	🟪	12	16.7%	🔍
Gaobot.4	🟧	12	16.7%	🔍
Total		72	100%	

Each field is described in the following table.

Table 175 Report > Web Security > Virus Found > Top Viruses

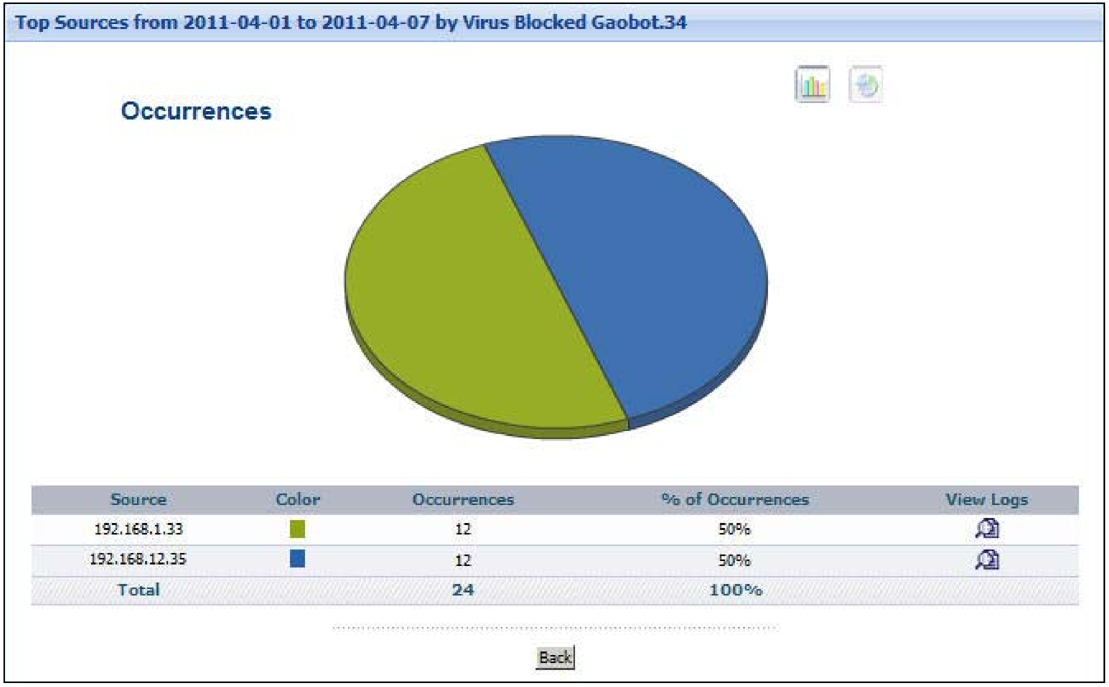
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Virus Blocked** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped in the selected device, sorted by the number of occurrences by each one. Click on a virus to look at the top sources for the selected virus.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences of each virus.
% of Occurrences	This field displays what percentage each virus's occurrences made out of all the detected virus occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above.

9.2.4 Top Viruses Drill-Down

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

Click on a specific virus in **Report > Web Security > Virus Found > Top Viruses** to open this screen.

Figure 190 Report > Web Security > Virus Found > Top Viruses > Drill-Down



Top Sources from 2011-04-01 to 2011-04-07 by Virus Blocked Gaobot.34

Source	Color	Occurrences	% of Occurrences	View Logs
192.168.1.33	🟩	12	50%	🔍
192.168.12.35	🟦	12	50%	🔍
Total		24	100%	

Each field is described in the following table.

Table 176 Report > Web Security > Virus Found > Top Viruses > Drill-Down

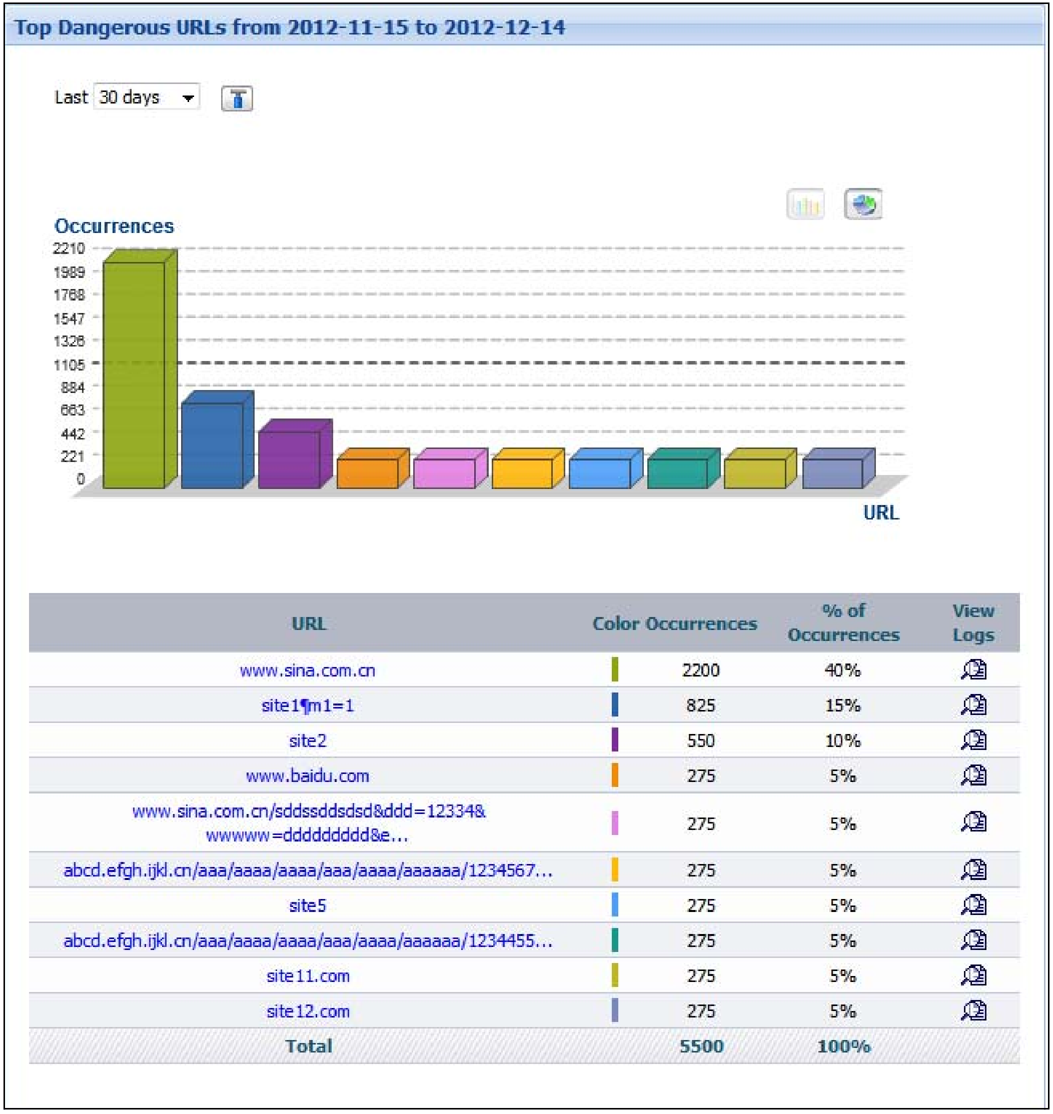
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

9.2.5 Top Dangerous URLs

Use this report to look at the top virus-infected URLs to which the device blocked access by number of occurrences.

Click **Report > Web Security > Virus Found > Top Dangerous URLs** to open this screen.

Figure 191 Report > Web Security > Virus Found > Top Dangerous URLs



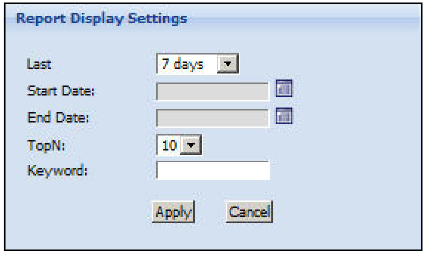
Top Dangerous URLs from 2012-11-15 to 2012-12-14

Last 30 days

URL	Color	Occurrences	% of Occurrences	View Logs
www.sina.com.cn	▮	2200	40%	🔍
site1¶m1=1	▮	825	15%	🔍
site2	▮	550	10%	🔍
www.baidu.com	▮	275	5%	🔍
www.sina.com.cn/sddssddsdsd&ddd=12334& wwwwww=dddddddd&e...	▮	275	5%	🔍
abcd.efgh.ijkl.cn/aaa/aaaa/aaaa/aaa/aaaa/aaaaaa/1234567...	▮	275	5%	🔍
site5	▮	275	5%	🔍
abcd.efgh.ijkl.cn/aaa/aaaa/aaaa/aaa/aaaa/aaaaaa/1234455...	▮	275	5%	🔍
site11.com	▮	275	5%	🔍
site12.com	▮	275	5%	🔍
Total		5500	100%	

Each field is described in the following table.

Table 177 Report > Web Security > Virus Found > Top Dangerous URLs

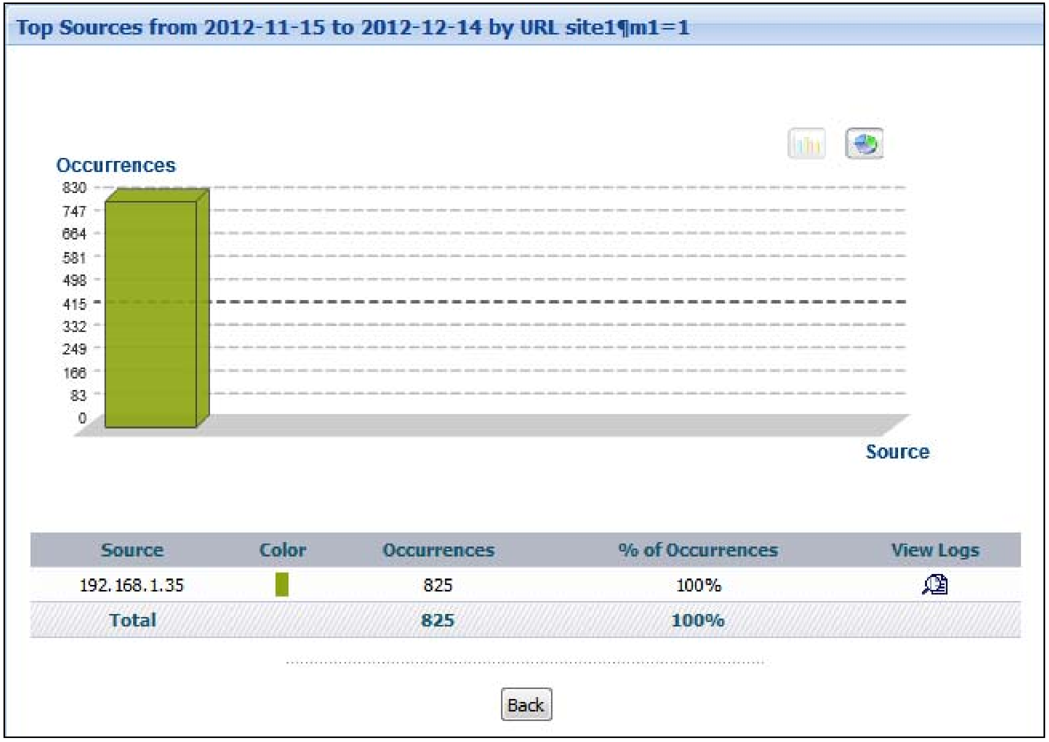
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending with (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Click the settings icon to display the **Report Display Settings** screen. Use these fields to specify the historical information to include in the report.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select how many days or 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**. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the URLs. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
URL	This field displays the top dangerous URLs the selected device stopped users from accessing, sorted by the number of occurrences by each one. Click on a URL to look at the top sources for attempts to access the URL.
Color	This field displays what color represents each URL in the graph.
Occurrences	This field displays the number of occurrences of each URL.
% of Occurrences	This field displays what percentage each URL’s occurrences made out of all the detected dangerous URL occurrences.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the URLs above.

9.2.6 Top Dangerous URLs Drill-Down

Use this report to look at the top sources of attempts to access virus-infected URLs.

Click on a specific URL in **Report > Web Security > Virus Found > Top Dangerous URLs** to open this screen.

Figure 192 Report > Web Security > Virus Found > Top Dangerous URLs > Drill-Down



Top Sources from 2012-11-15 to 2012-12-14 by URL site1¶m1=1

Source	Color	Occurrences	% of Occurrences	View Logs
192.168.1.35	🟩	825	100%	🔍
Total		825	100%	

Each field is described in the following table.

Table 178 Report > Web Security > Virus Found > Top Dangerous URLs > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of attempts to access the selected dangerous URL, sorted by the number of occurrences for each URL. 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.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences of the selected dangerous URL from each source.
% of Occurrences	This field displays what percentage of all occurrences of the selected URL comes from each source.
View Logs	Click this icon to see the logs that go with the record.

Table 178 Report > Web Security > Virus Found > Top Dangerous URLs > Drill-Down

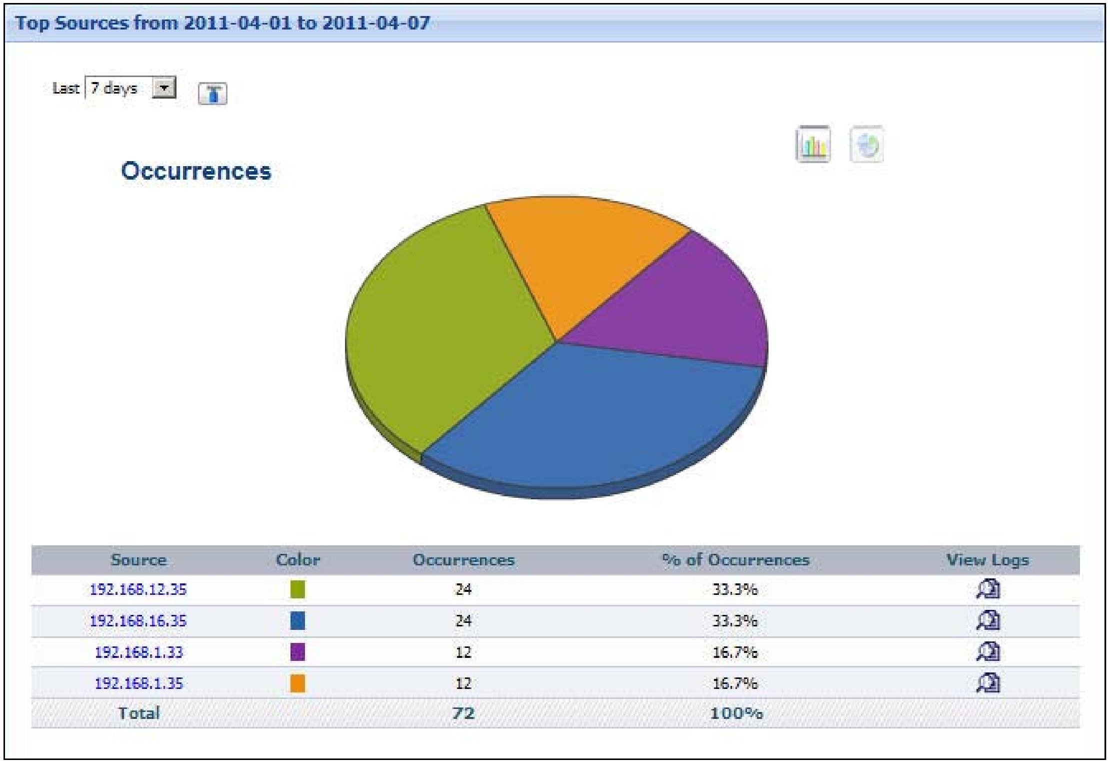
LABEL	DESCRIPTION
Total	This entry displays the totals for the sources above. If the number of sources of attempts to access the selected dangerous URL is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click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

9.2.7 Top Virus Sources

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

Click **Report > Web Security > Virus Found > Top Sources** to open this screen.

Figure 193 Report > Web Security > Virus Found > Top Sources



Top Sources from 2011-04-01 to 2011-04-07

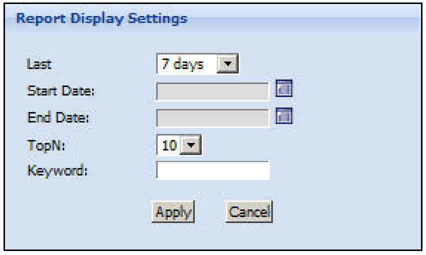
Last 7 days

Occurrences

Source	Color	Occurrences	% of Occurrences	View Logs
192.168.12.35	🟩	24	33.3%	🔍
192.168.16.35	🟦	24	33.3%	🔍
192.168.1.33	🟪	12	16.7%	🔍
192.168.1.35	🟧	12	16.7%	🔍
Total		72	100%	

Each field is described in the following table.

Table 179 Report > Web Security > Virus Found > Top Sources

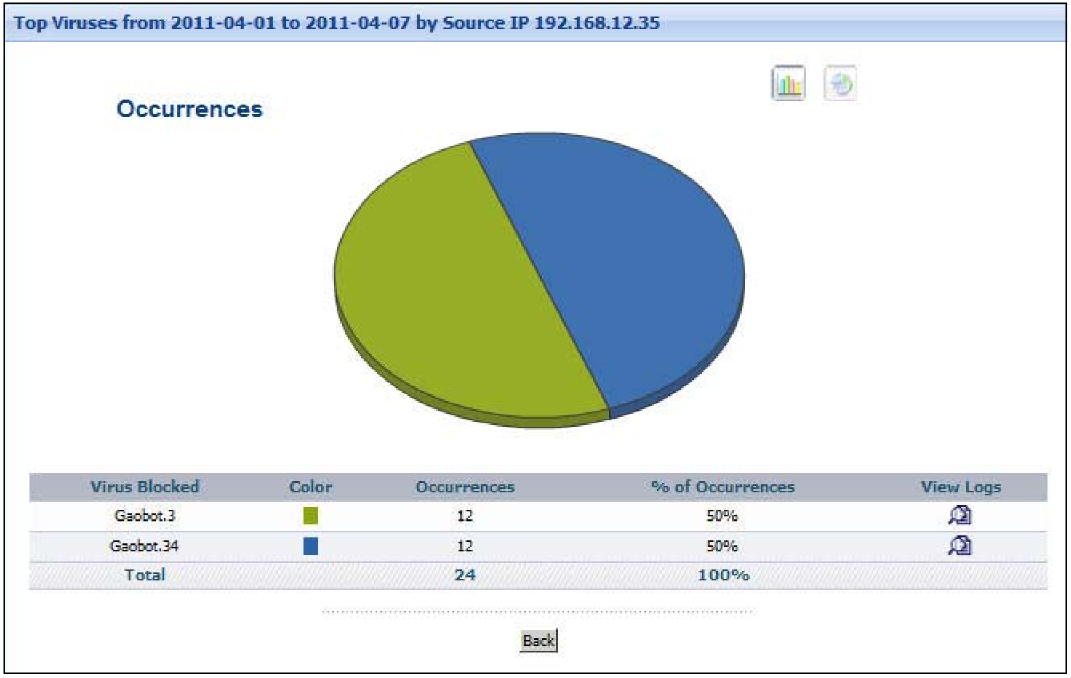
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of viruses stopped in the selected device, sorted by the number of occurrences from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a source to look at the top viruses for the selected source.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of occurrences from each source.
% of Occurrences	This field displays what percentage of all occurrences comes from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.2.8 Top Virus Sources Drill-Down

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

Click on a specific source in **Report > Web Security > Virus Found > Top Sources** to open this screen.

Figure 194 Report > Web Security > Virus Found > Top Sources > Drill-Down



Top Viruses from 2011-04-01 to 2011-04-07 by Source IP 192.168.12.35

Occurrences

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.3	🟩	12	50%	🔍
Gaobot.34	🟦	12	50%	🔍
Total		24	100%	

Each field is described in the following table.

Table 180 Report > Web Security > Virus Found > Top Sources > Drill-Down

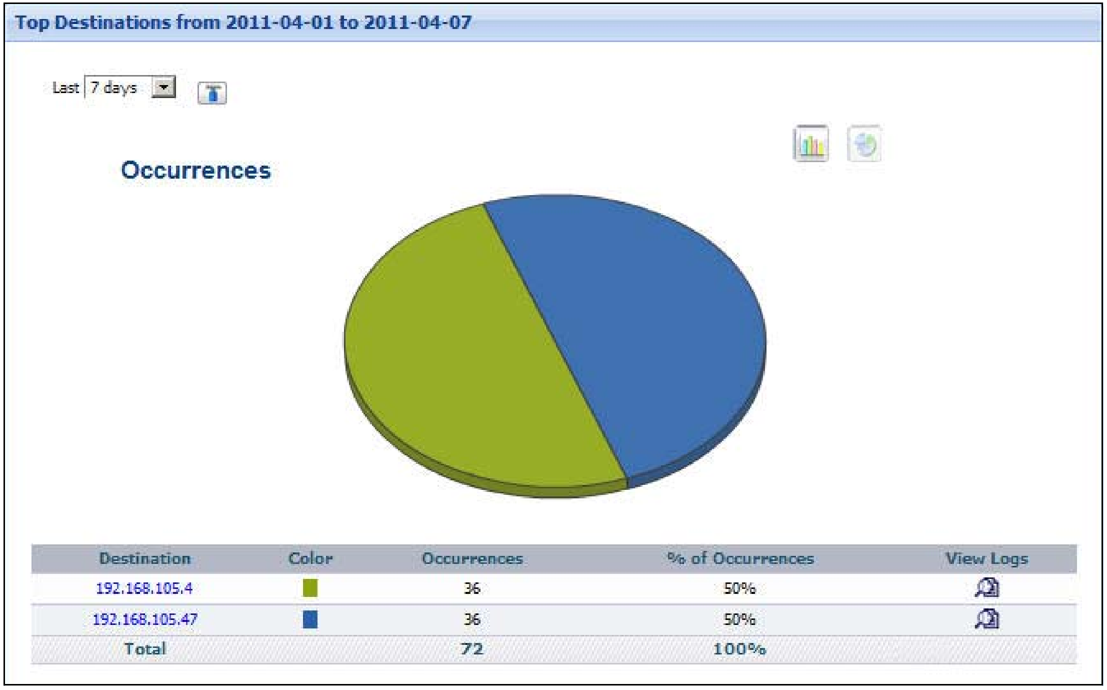
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from the selected source, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of occurrences from the selected source by each virus.
% of Occurrences	This field displays what percentage of all occurrences from the selected source was made by each virus.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.2.9 Top Virus Destinations

Use this report to look at the top destinations (targets or intended victims) of virus files. These are the IP addresses that the selected device stopped the most virus files from being sent to.

Click **Report > Web Security > Virus Found > Top Destinations** to open this screen.

Figure 195 Report > Web Security > Virus Found > Top Destinations



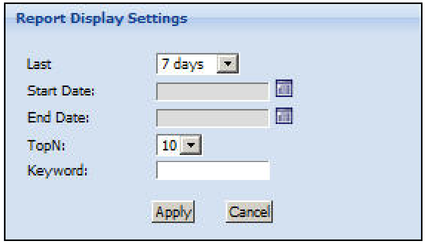
Top Destinations from 2011-04-01 to 2011-04-07

Last 7 days

Destination	Color	Occurrences	% of Occurrences	View Logs
192.168.105.4	🟩	36	50%	🔍
192.168.105.47	🟦	36	50%	🔍
Total		72	100%	

Each field is described in the following table.

Table 181 Report > Web Security > Virus Found > Top Destinations

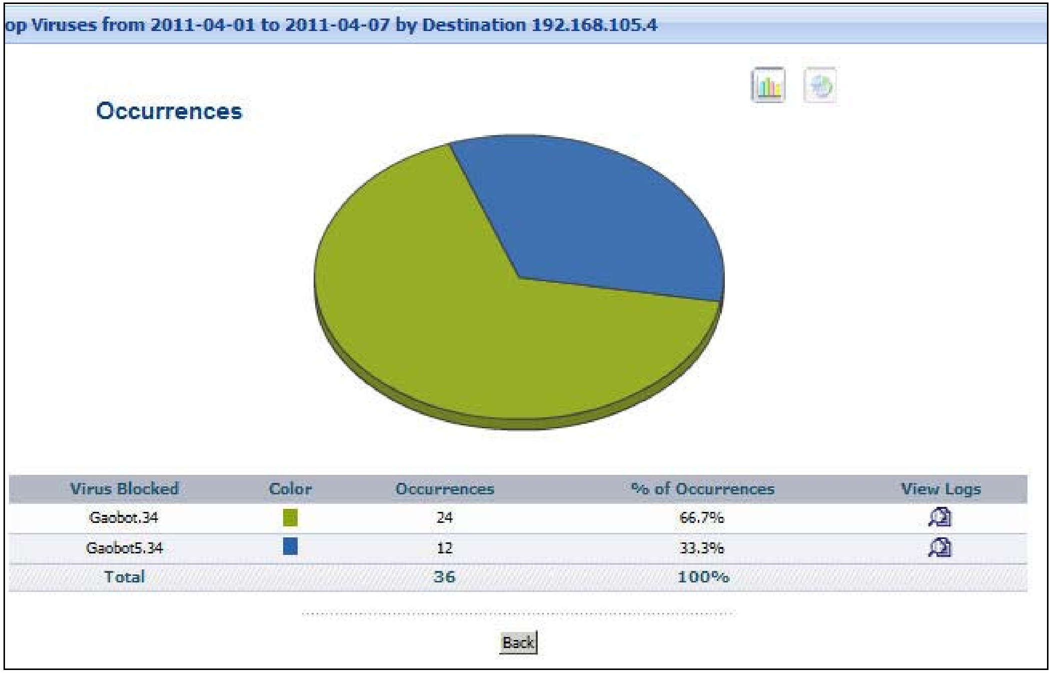
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report).
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of viruses blocked in the selected device, sorted by the number of occurrences at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address.
Color	This field displays what color represents each destination in the graph.
Occurrences	This field displays the number of occurrences at each destination if the selected device had not blocked the virus.
% of Occurrences	This field displays what percentage of all occurrences were going to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

9.2.10 Top Virus Destinations Drill-Down

Use this report to look at the top viruses sent towards any top virus destination.

Click on a specific destination in **Report > Web Security > Virus Found > Top Destinations** to open this screen.

Figure 196 Report > Web Security > Virus Found > Top Destinations > Drill-Down



op Viruses from 2011-04-01 to 2011-04-07 by Destination 192.168.105.4

Virus Blocked	Color	Occurrences	% of Occurrences	View Logs
Gaobot.34	🟩	24	66.7%	🔍
Gaobot5.34	🟦	12	33.3%	🔍
Total		36	100%	

Each field is described in the following table.

Table 182 Report > Web Security > Virus Found > Top Destinations > Drill-Down

LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Virus Blocked	This field displays the top viruses stopped from going to the selected destination, sorted by the number of occurrences by each one.
Color	This field displays what color represents each virus in the graph.
Occurrences	This field displays the number of times each virus was sent to the selected destination.
% of Occurrences	This field displays what percentage each virus made of the viruses sent to the selected destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the viruses above. If the number of viruses sent to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to return to the main report.

9.3 Intrusion Hits

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

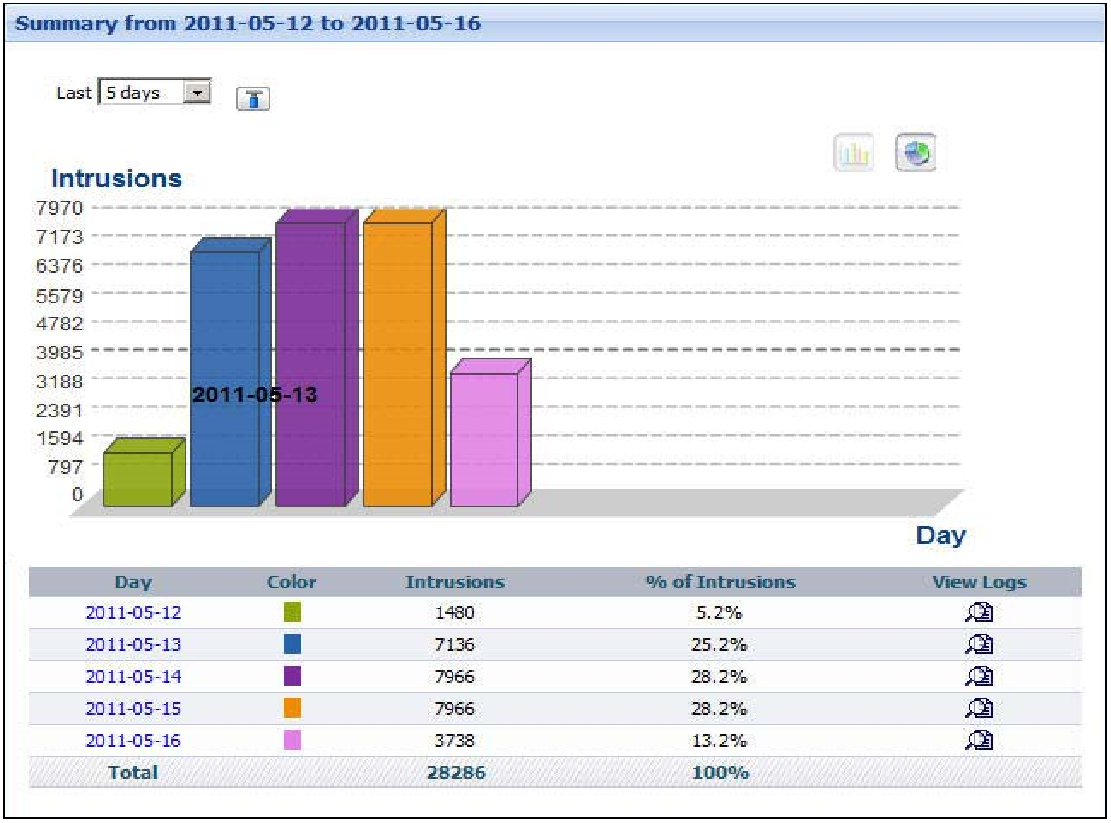
Note: To look at intrusion reports, each ZyXEL device must record intrusions in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **IDP** is enabled. Then, go to **IDP** > **Signature**, and make sure the ZyXEL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

9.3.1 Intrusion Hits Summary

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

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

Figure 197 Report > Web Security > Intrusion Hits > Summary



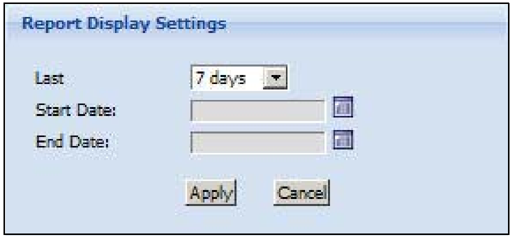
Summary from 2011-05-12 to 2011-05-16

Last 5 days

Day	Color	Intrusions	% of Intrusions	View Logs
2011-05-12	🟩	1480	5.2%	🔍
2011-05-13	🟦	7136	25.2%	🔍
2011-05-14	🟪	7966	28.2%	🔍
2011-05-15	🟧	7966	28.2%	🔍
2011-05-16	■	3738	13.2%	🔍
Total		28286	100%	

Each field is described in the following table.

Table 183 Report > Web Security > Intrusion Hits > Summary

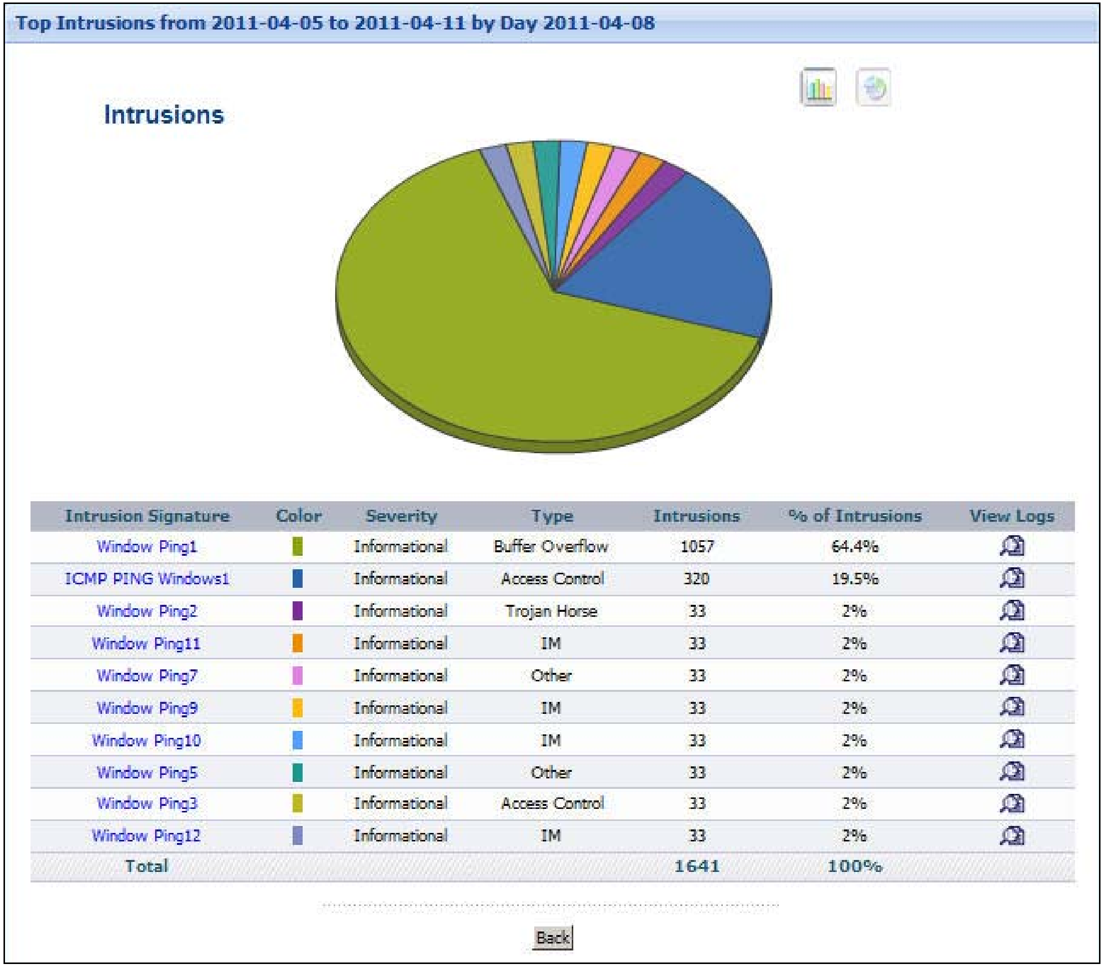
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the intrusion signatures in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Intrusions	This field displays the number of intrusions in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions was made in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

9.3.2 Intrusion Hits Summary Drill-Down

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

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

Figure 198 Report > Web Security > Intrusion Hits > Summary > Drill-Down



Top Intrusions from 2011-04-05 to 2011-04-11 by Day 2011-04-08

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Window Ping1	🟩	Informational	Buffer Overflow	1057	64.4%	🔍
ICMP PING Windows1	🟦	Informational	Access Control	320	19.5%	🔍
Window Ping2	🟪	Informational	Trojan Horse	33	2%	🔍
Window Ping11	🟧	Informational	IM	33	2%	🔍
Window Ping7	🟪	Informational	Other	33	2%	🔍
Window Ping9	🟨	Informational	IM	33	2%	🔍
Window Ping10	🟦	Informational	IM	33	2%	🔍
Window Ping5	🟩	Informational	Other	33	2%	🔍
Window Ping3	🟨	Informational	Access Control	33	2%	🔍
Window Ping12	🟪	Informational	IM	33	2%	🔍
Total				1641	100%	

Each field is described in the following table.

Table 184 Report > Web Security > Intrusion Hits > Summary > Drill-Down

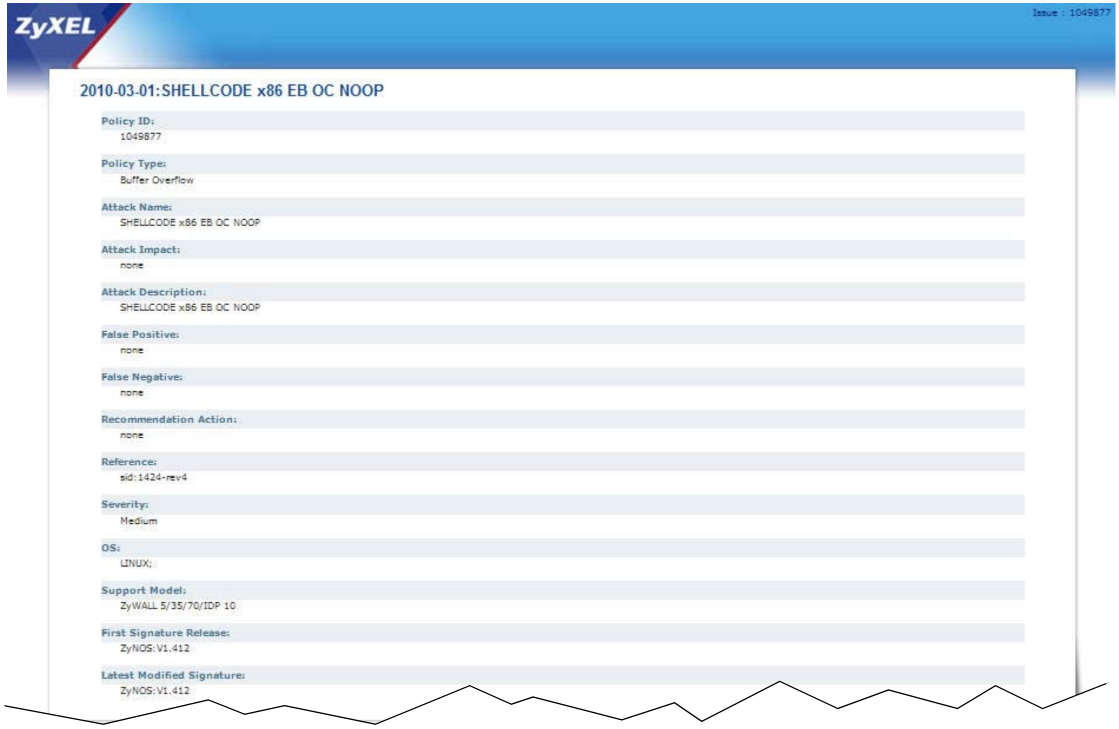
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the categories of intrusions in the selected time interval, sorted by the number of attempts by each one. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 199 on page 346).
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 184 Report > Web Security > Intrusion Hits > Summary > Drill-Down

LABEL	DESCRIPTION
Intrusions	This field displays how many intrusions occurred in the selected time interval.
% of Intrusions	This field displays what percentage of all intrusions in the selected time interval was made by each intrusion signature.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.
Back	Click this to return to the main report.

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

Figure 199 Security Issue Details



Issue : 1049877

2010-03-01:SHELLCODE x86 EB OC NOOP

Policy ID:
1049877

Policy Type:
Buffer Overflow

Attack Name:
SHELLCODE x86 EB OC NOOP

Attack Impact:
none

Attack Description:
SHELLCODE x86 EB OC NOOP

False Positive:
none

False Negative:
none

Recommendation Action:
none

Reference:
sid:1424-rev4

Severity:
Medium

OS:
LINUX;

Support Model:
ZyWALL 5/35/70/IDP 10

First Signature Release:
ZyNOS:V1.412

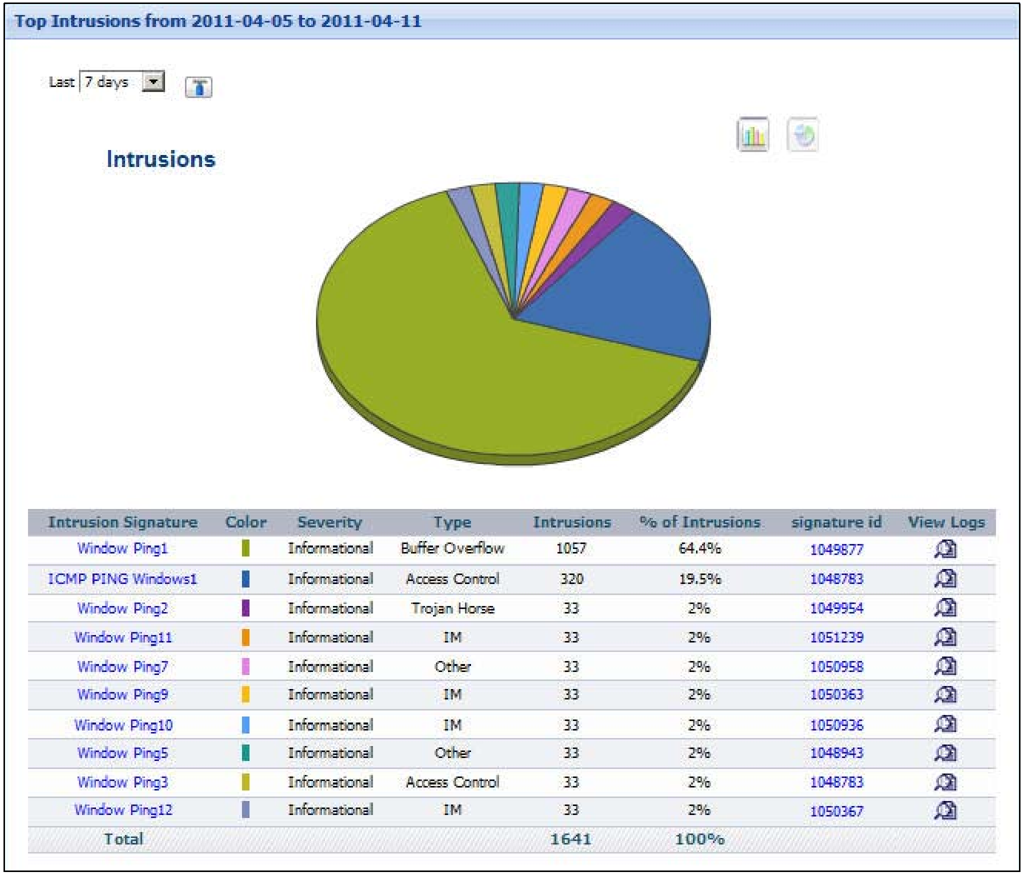
Latest Modified Signature:
ZyNOS:V1.412

9.3.3 Top Intrusion Hits Signatures

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

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

Figure 200 Report > Web Security > Intrusion Hits > Top Intrusions



Top Intrusions from 2011-04-05 to 2011-04-11

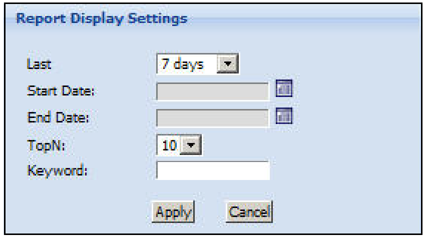
Last 7 days

Intrusions

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	signature id	View Logs
Window Ping1	🟩	Informational	Buffer Overflow	1057	64.4%	1049877	
ICMP PING Windows1	🟦	Informational	Access Control	320	19.5%	1048783	
Window Ping2	🟪	Informational	Trojan Horse	33	2%	1049954	
Window Ping11	🟧	Informational	IM	33	2%	1051239	
Window Ping7	🟪	Informational	Other	33	2%	1050958	
Window Ping9	🟨	Informational	IM	33	2%	1050363	
Window Ping10	🟦	Informational	IM	33	2%	1050936	
Window Ping5	🟩	Informational	Other	33	2%	1048943	
Window Ping3	🟨	Informational	Access Control	33	2%	1048783	
Window Ping12	⬛	Informational	IM	33	2%	1050367	
Total				1641	100%		

Each field is described in the following table.

Table 185 Report > Web Security > Intrusion Hits > Top Intrusions

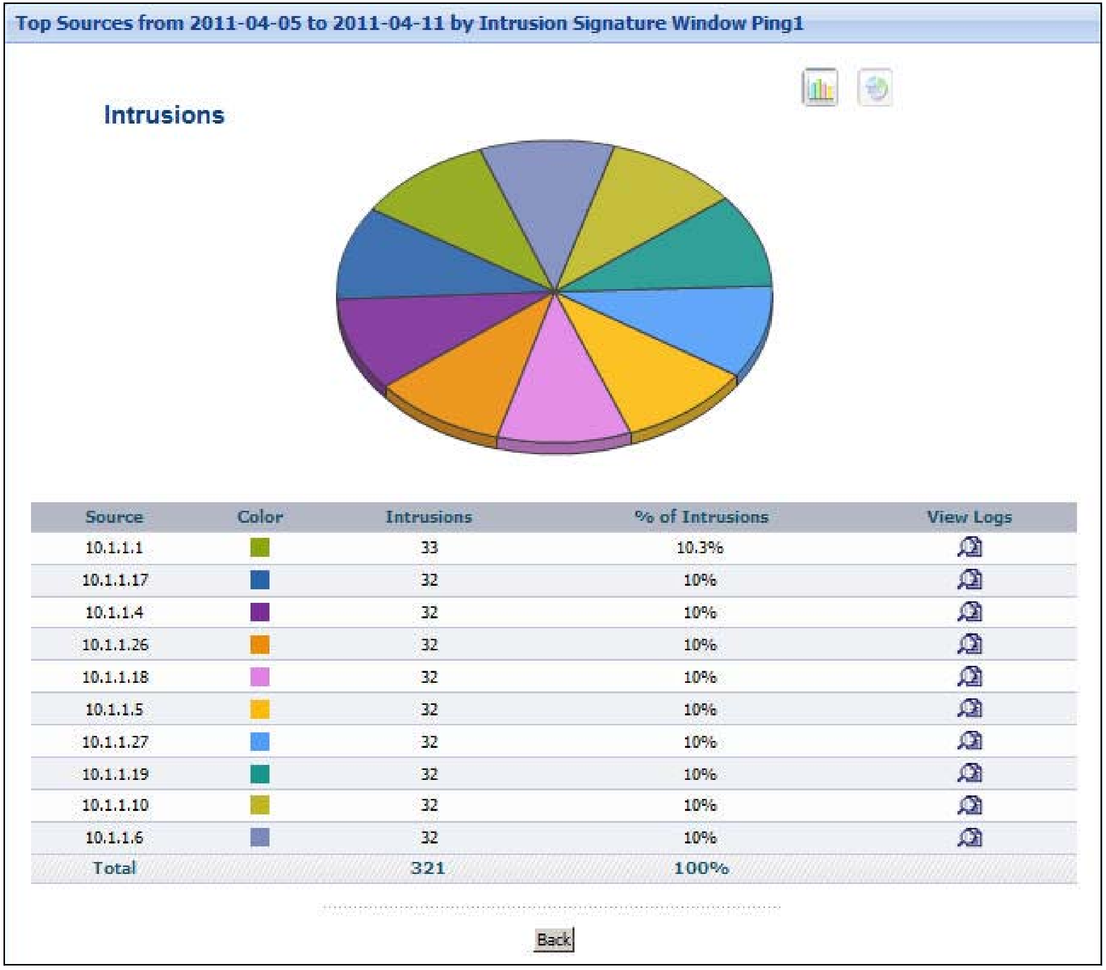
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Intrusion Signature** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Intrusion Signature	This field displays the top intrusion signatures in the selected device, sorted by the number of intrusions by each one. Click on an intrusion signature to look at the top sources for the selected signature.
Color	This field displays what color represents each intrusion signature in the graph.
Severity	This field displays the severity of each intrusion signature.
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP** > **Signature** > **Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by each intrusion signature.
% of Intrusions	This field displays what percentage of all intrusions was made by each intrusion signature.
signature id	This is the security issue identification number. Clicking on the entries in this column will open a new window with a description of this security issue (see Figure 199 on page 346).
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the intrusion signatures above.

9.3.4 Top Intrusion Hits Signatures Drill-Down

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

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

Figure 201 Report > Web Security > Intrusion Hits > Top Intrusions > Drill-Down



Top Sources from 2011-04-05 to 2011-04-11 by Intrusion Signature Window Ping1

Source	Color	Intrusions	% of Intrusions	View Logs
10.1.1.1	■	33	10.3%	🔍
10.1.1.17	■	32	10%	🔍
10.1.1.4	■	32	10%	🔍
10.1.1.26	■	32	10%	🔍
10.1.1.18	■	32	10%	🔍
10.1.1.5	■	32	10%	🔍
10.1.1.27	■	32	10%	🔍
10.1.1.19	■	32	10%	🔍
10.1.1.10	■	32	10%	🔍
10.1.1.6	■	32	10%	🔍
Total		321	100%	

Each field is described in the following table.

Table 186 Report > Web Security > Intrusion Hits > Top Intrusions > Drill-Down

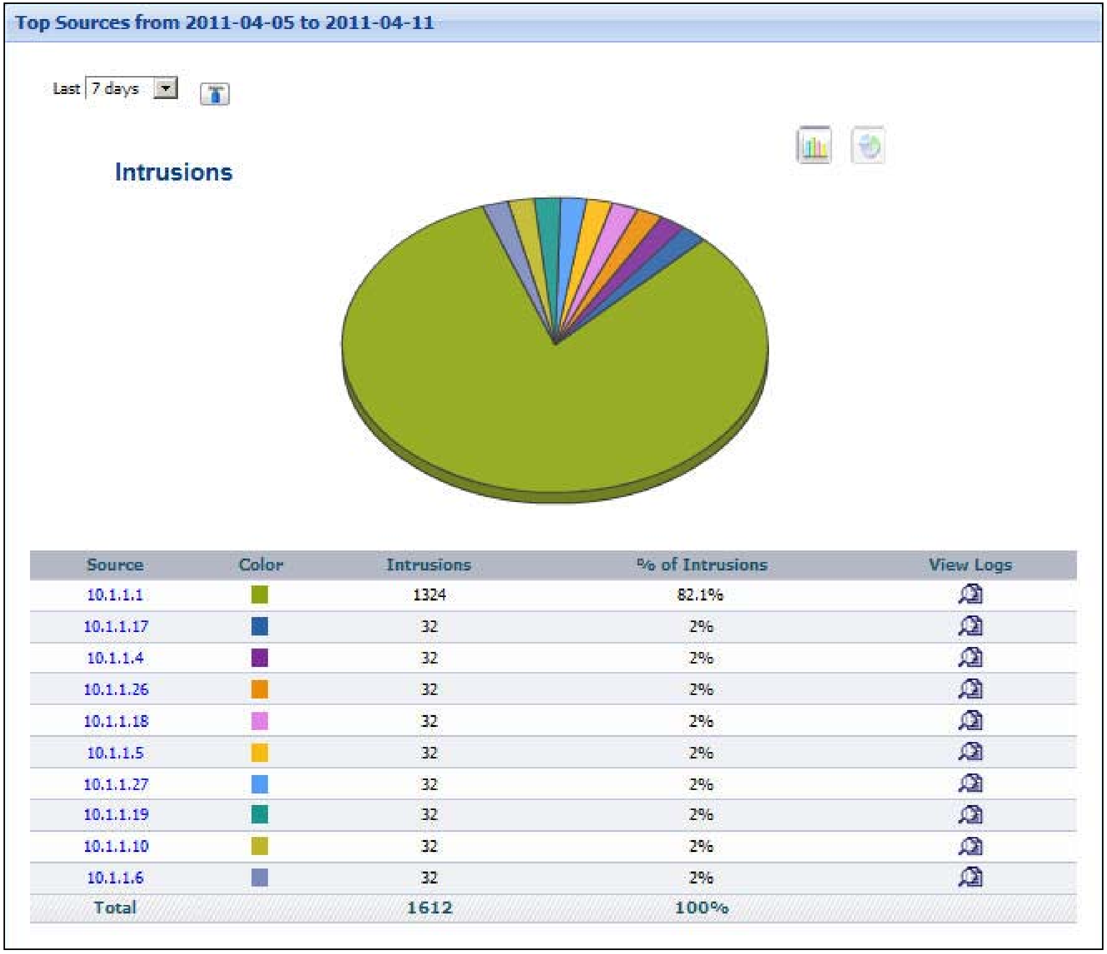
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display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

9.3.5 Top Intrusion Hits Sources

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

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

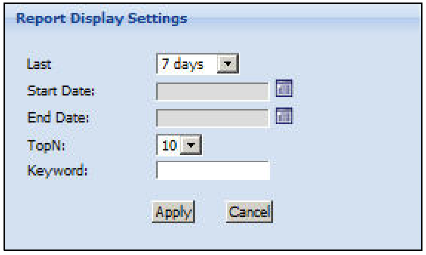
Figure 202 Report > Web Security > Intrusion Hits > Top Sources



Source	Color	Intrusions	% of Intrusions	View Logs
10.1.1.1	■	1324	82.1%	🔍
10.1.1.17	■	32	2%	🔍
10.1.1.4	■	32	2%	🔍
10.1.1.26	■	32	2%	🔍
10.1.1.18	■	32	2%	🔍
10.1.1.5	■	32	2%	🔍
10.1.1.27	■	32	2%	🔍
10.1.1.19	■	32	2%	🔍
10.1.1.10	■	32	2%	🔍
10.1.1.6	■	32	2%	🔍
Total		1612	100%	

Each field is described in the following table.

Table 187 Report > Web Security > Intrusion Hits > Top Sources

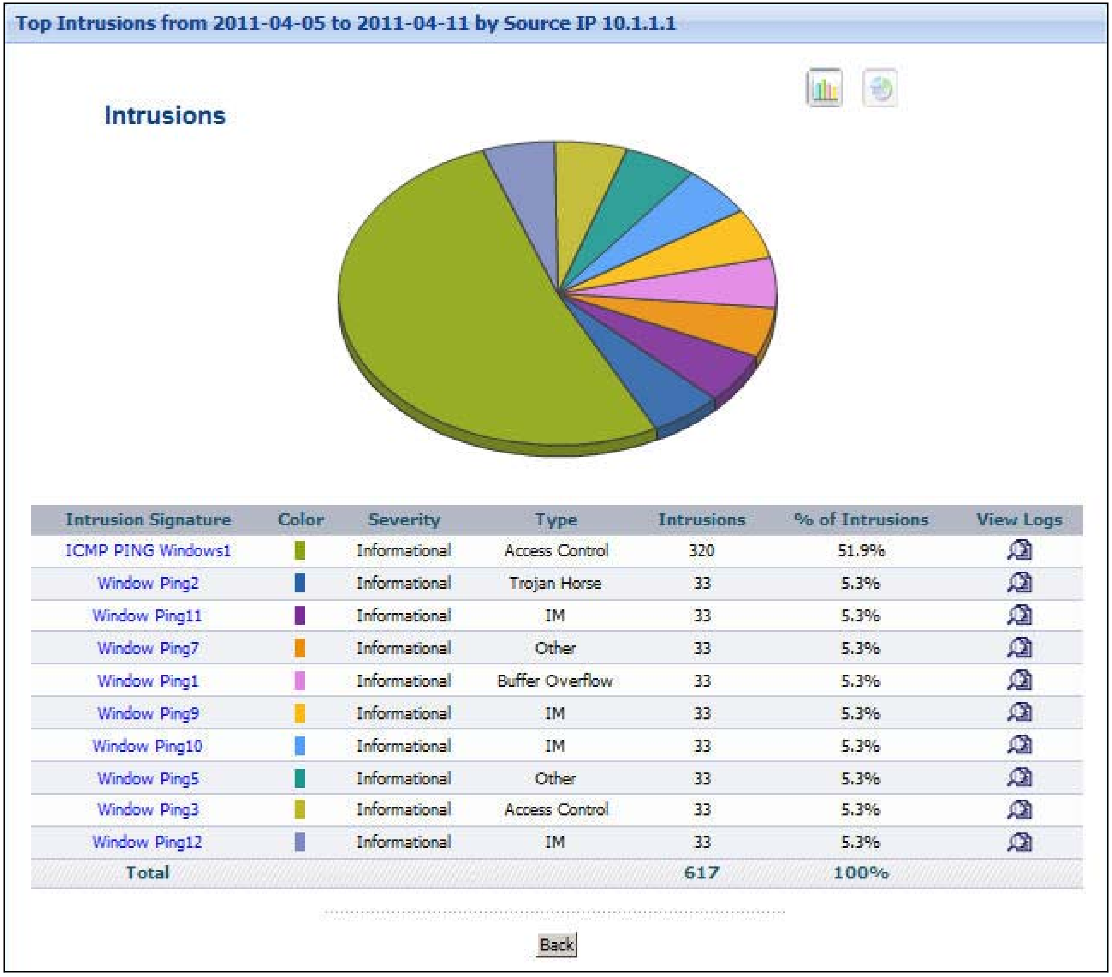
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Source** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Source	This field displays the top sources of intrusions in the selected device, sorted by the number of intrusions by each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). Click on a source to look at the top intrusion signatures for the selected source.
Color	This field displays what color represents each source in the graph.
Intrusions	This field displays the number of intrusions by each source.
% of Intrusions	This field displays what percentage of all intrusions was made by each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

9.3.6 Top Intrusion Hits Sources Drill-Down

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

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

Figure 203 Report > Web Security > Intrusion Hits > Top Sources > Drill-Down



Top Intrusions from 2011-04-05 to 2011-04-11 by Source IP 10.1.1.1

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
ICMP PING Windows1	■	Informational	Access Control	320	51.9%	🔍
Window Ping2	■	Informational	Trojan Horse	33	5.3%	🔍
Window Ping11	■	Informational	IM	33	5.3%	🔍
Window Ping7	■	Informational	Other	33	5.3%	🔍
Window Ping1	■	Informational	Buffer Overflow	33	5.3%	🔍
Window Ping9	■	Informational	IM	33	5.3%	🔍
Window Ping10	■	Informational	IM	33	5.3%	🔍
Window Ping5	■	Informational	Other	33	5.3%	🔍
Window Ping3	■	Informational	Access Control	33	5.3%	🔍
Window Ping12	■	Informational	IM	33	5.3%	🔍
Total				617	100%	

Each field is described in the following table.

Table 188 Report > Web Security > Intrusion Hits > Top Sources > Drill-Down

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

Table 188 Report > Web Security > Intrusion Hits > Top Sources > Drill-Down

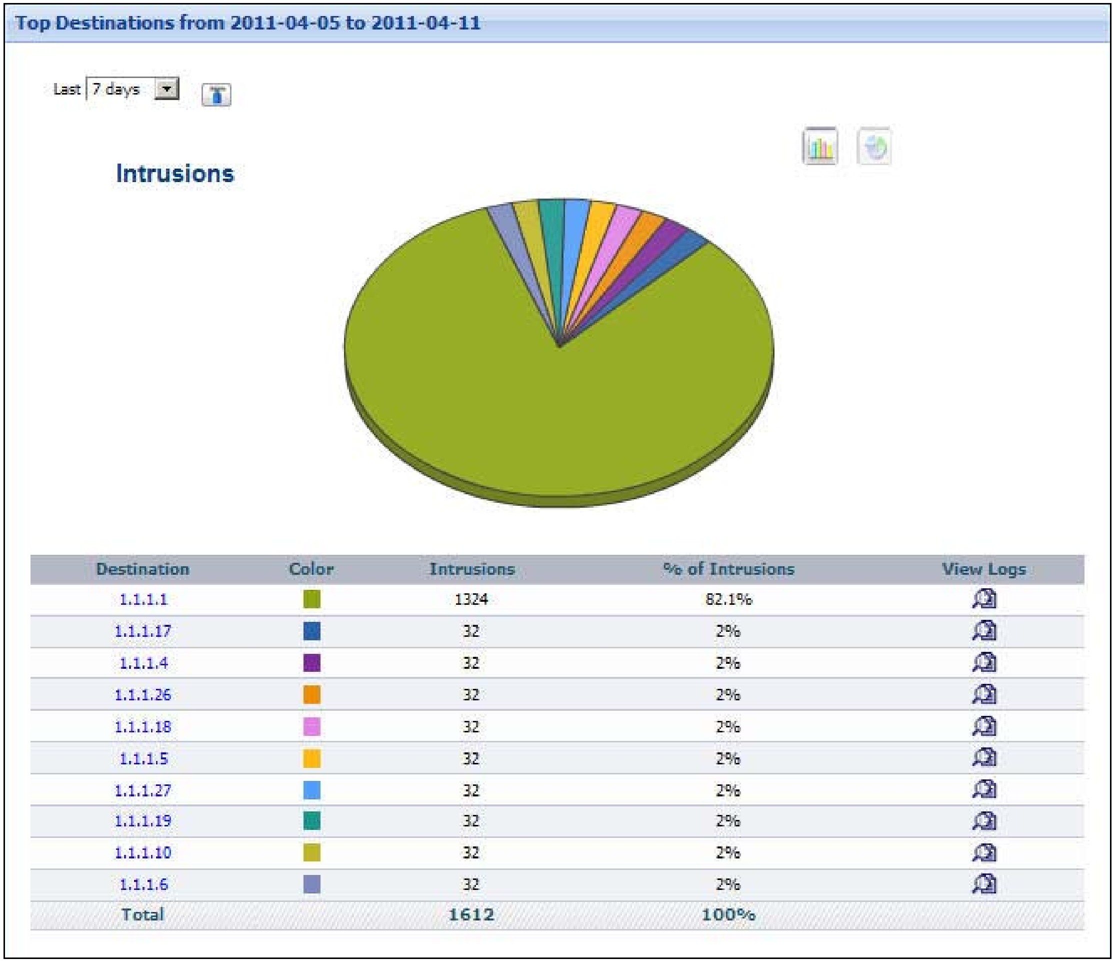
LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions by the selected source using each intrusion signature.
% of Intrusions	This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

9.3.7 Top Intrusion Hits Destinations

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

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

Figure 204 Report > Web Security > Intrusion Hits > Top Destinations



Top Destinations from 2011-04-05 to 2011-04-11

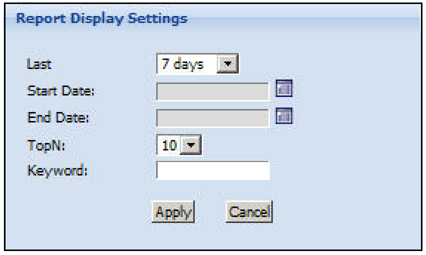
Last 7 days

Intrusions

Destination	Color	Intrusions	% of Intrusions	View Logs
1.1.1.1	🟩	1324	82.1%	🔍
1.1.1.17	🟦	32	2%	🔍
1.1.1.4	🟪	32	2%	🔍
1.1.1.26	🟧	32	2%	🔍
1.1.1.18	🟪	32	2%	🔍
1.1.1.5	🟨	32	2%	🔍
1.1.1.27	🟦	32	2%	🔍
1.1.1.19	🟩	32	2%	🔍
1.1.1.10	🟨	32	2%	🔍
1.1.1.6	🟦	32	2%	🔍
Total		1612	100%	

Each field is described in the following table.

Table 189 Report > Web Security > Intrusion Hits > Top Destinations

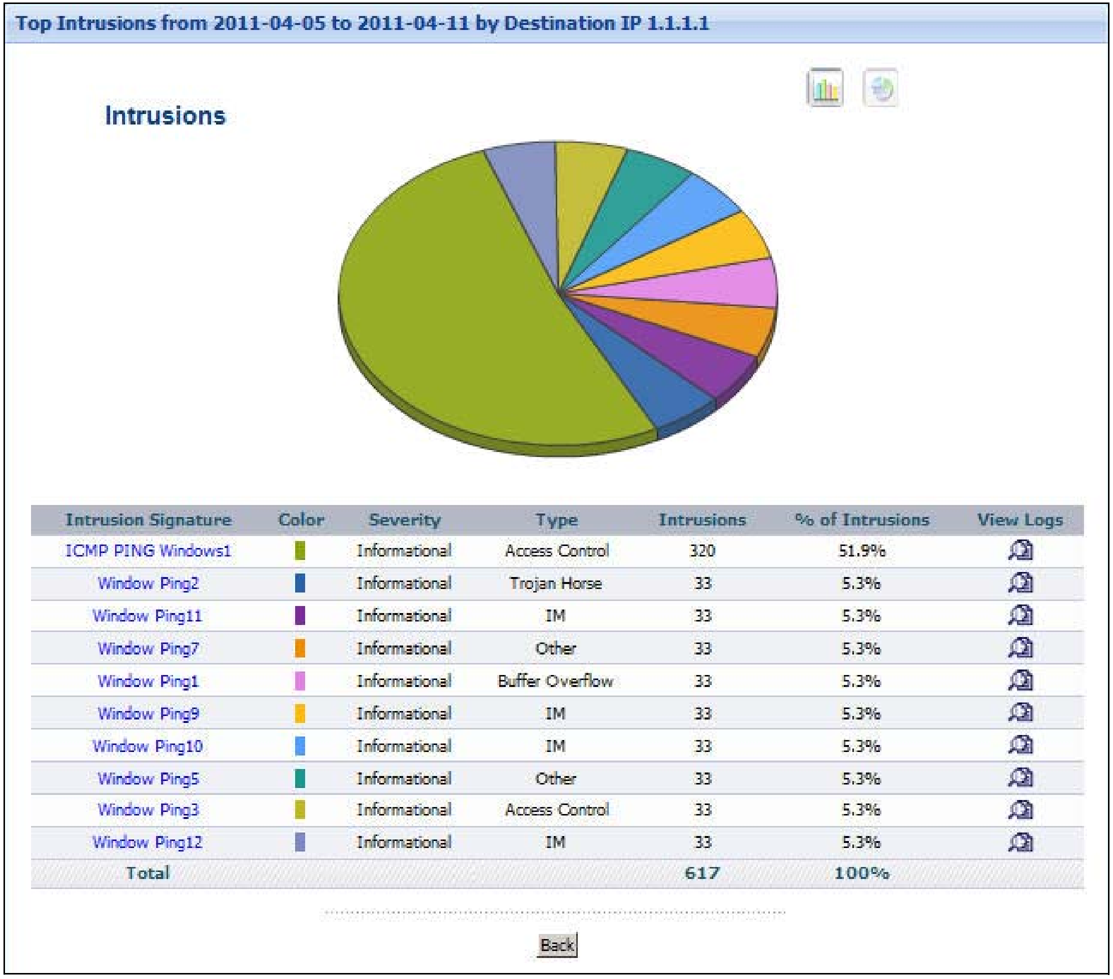
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Destination** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Destination	This field displays the top destinations of intrusions in the selected device, sorted by the number of intrusions destined for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System** > **General Configuration**, the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). Click on a destination to look at the top intrusion signatures for the selected destination.
Color	This field displays what color represents each destination in the graph.
Intrusions	This field displays the number of intrusions sent to each destination.
% of Intrusions	This field displays what percentage of all intrusions that were sent to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

9.3.8 Top Intrusion Hits Destinations Drill-Down

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

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

Figure 205 Report > Web Security > Intrusion Hits > Top Destinations > Drill-Down



Top Intrusions from 2011-04-05 to 2011-04-11 by Destination IP 1.1.1.1

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
ICMP PING Windows1	🟩	Informational	Access Control	320	51.9%	🔍
Window Ping2	🟦	Informational	Trojan Horse	33	5.3%	🔍
Window Ping11	🟪	Informational	IM	33	5.3%	🔍
Window Ping7	🟧	Informational	Other	33	5.3%	🔍
Window Ping1	🟪	Informational	Buffer Overflow	33	5.3%	🔍
Window Ping9	🟨	Informational	IM	33	5.3%	🔍
Window Ping10	🟦	Informational	IM	33	5.3%	🔍
Window Ping5	🟩	Informational	Other	33	5.3%	🔍
Window Ping3	🟨	Informational	Access Control	33	5.3%	🔍
Window Ping12	🟦	Informational	IM	33	5.3%	🔍
Total				617	100%	

Each field is described in the following table.

Table 190 Report > Web Security > Intrusion Hits > Top Destinations > Drill-Down

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

Table 190 Report > Web Security > Intrusion Hits > Top Destinations > Drill-Down

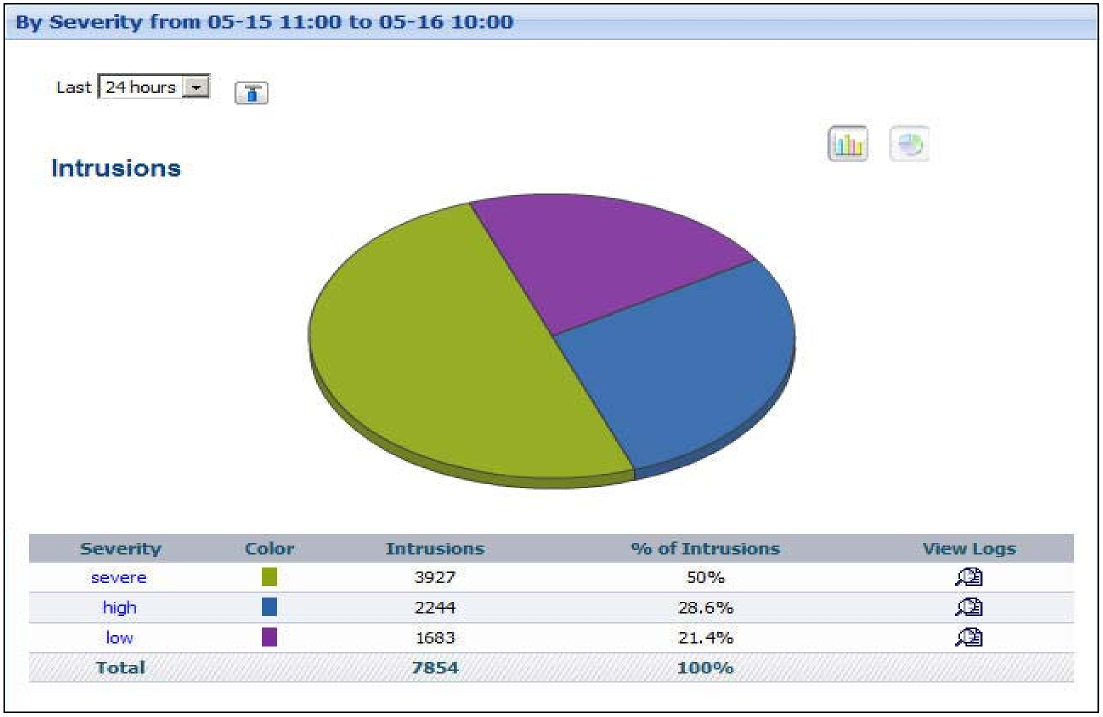
LABEL	DESCRIPTION
Type	This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP** > **Signature** > **Attack Type** in most ZyXEL devices.
Intrusions	This field displays the number of intrusions of each intrusion signature sent to the selected destination.
% of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

9.3.9 Intrusion Hits Severities

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

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

Figure 206 Report > Web Security > Intrusion Hits > By Severity



By Severity from 05-15 11:00 to 05-16 10:00

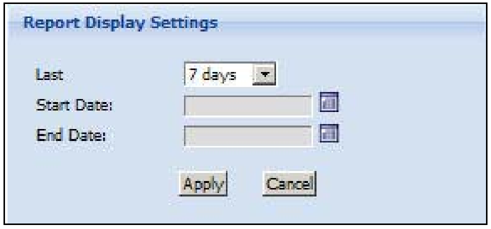
Last 24 hours

Intrusions

Severity	Color	Intrusions	% of Intrusions	View Logs
severe	🟩	3927	50%	🔍
high	🟦	2244	28.6%	🔍
low	🟪	1683	21.4%	🔍
Total		7854	100%	

Each field is described in the following table.

Table 191 Report > Web Security > Intrusion Hits > By Severity

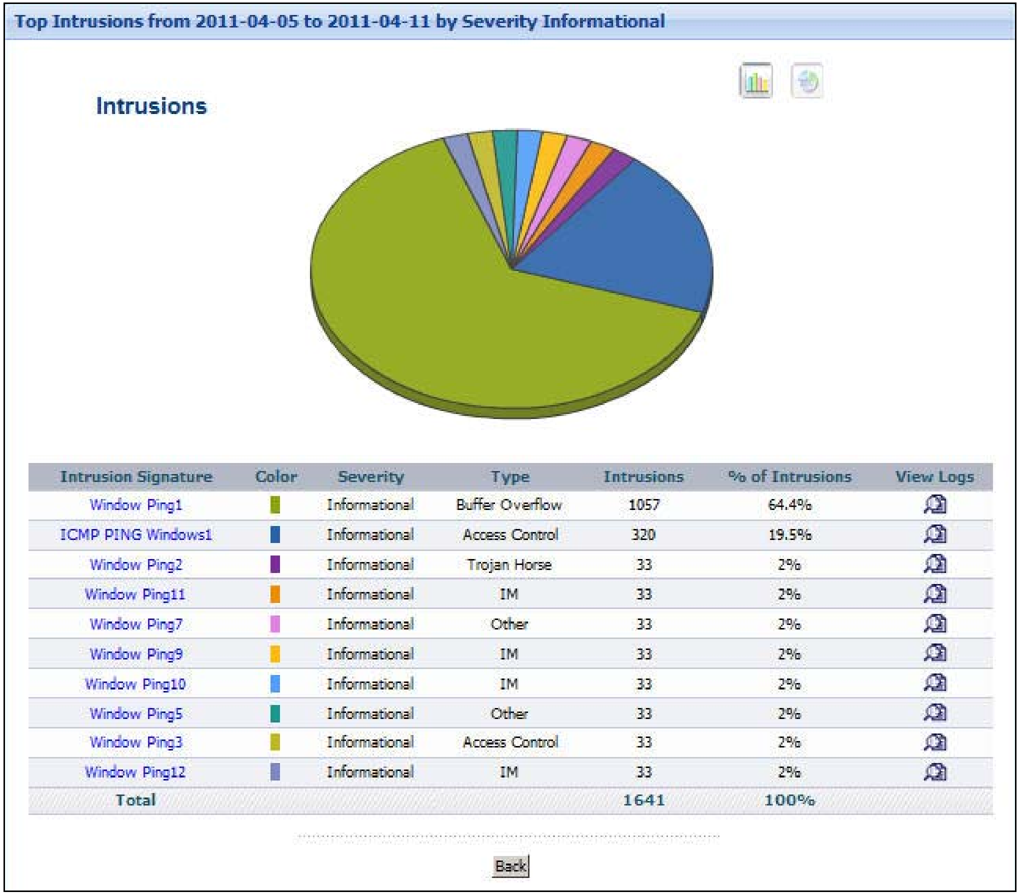
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Severity	This field displays the severity of intrusions in the selected device, sorted by the number of intrusions of each level. Click on a severity to look at the intrusion signatures for the selected severity.
Color	This field displays what color represents each level of severity in the graph.
Intrusions	This field displays the number of intrusions of each level of severity.
% of Intrusions	This field displays what percentage of all intrusions are at each level of severity.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the severities above.

9.3.10 Intrusion Hits Severities Drill-Down

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

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

Figure 207 Report > Web Security > Intrusion Hits > By Severity > Drill-Down



Top Intrusions from 2011-04-05 to 2011-04-11 by Severity Informational

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions	View Logs
Window Ping1	🟩	Informational	Buffer Overflow	1057	64.4%	🔍
ICMP PING Windows1	🟦	Informational	Access Control	320	19.5%	🔍
Window Ping2	🟪	Informational	Trojan Horse	33	2%	🔍
Window Ping11	🟧	Informational	IM	33	2%	🔍
Window Ping7	🟪	Informational	Other	33	2%	🔍
Window Ping9	🟨	Informational	IM	33	2%	🔍
Window Ping10	🟦	Informational	IM	33	2%	🔍
Window Ping5	🟩	Informational	Other	33	2%	🔍
Window Ping3	🟨	Informational	Access Control	33	2%	🔍
Window Ping12	🟪	Informational	IM	33	2%	🔍
Total				1641	100%	

Each field is described in the following table.

Table 192 Report > Web Security > Intrusion Hits > By Severity > Drill-Down

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

Table 192 Report > Web Security > Intrusion Hits > By Severity > 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 intrusion signatures above.
Back	Click this to return to the main report.

Security Policy Enforcement

This chapter discusses how you can check reports to look at what users and traffic were allowed or blocked by the application patrol and content filtering policies.

10.1 EPS

These screens display which computers passed or failed endpoint security (EPS) checking.

Endpoint Security (EPS), also known as endpoint control, is used to make sure users' computers comply with defined corporate policies before they can access the network or an SSL Secure Remote Access tunnel. After a successful user authentication, a user's computer must meet the endpoint security object's Operating System (OS) option and security requirements to gain access. You can configure the endpoint security object to require a user's computer to match just one of the endpoint security object's checking criteria or all of them. Configure endpoint security objects to use with the authentication policy and SSL Secure Remote Access features. See the User's Guide of your ZyWALL device for more information.

10.1.1 What Endpoint Security Can Check

The settings endpoint security can check vary depending on the OS of the user's computer. Depending on the OS, EPS can check user computers for the following:

- Operating System (Windows, Linux, Mac OSX, or others)
- Windows version and service pack version
- Windows Auto Update setting and installed security patches
- Personal firewall installation and activation
- Anti-virus installation and activation
- Windows registry settings
- Processes that the endpoint must execute
- Processes that the endpoint cannot execute

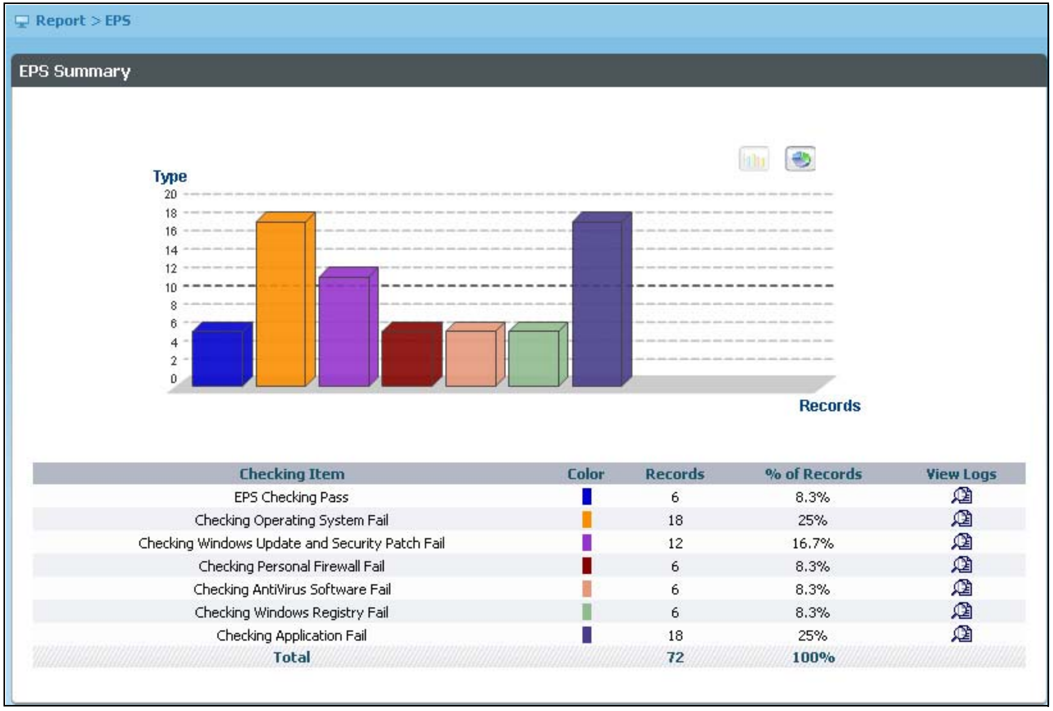
The size and version of specific files

10.1.2 EPS Summary

Use this screen to view statistics about the number of users' computers that passed or failed EPS checking with the reasons for failure displayed in a bar or pie graph.

Select a device in the device window on the left of the main screen and then click **Report** > **Security Policy Enforcement** > **EPS** to open the **EPS Summary** screen.

Figure 208 Report > Security Policy Enforcement > EPS



Checking Item	Color	Records	% of Records	View Logs
EPS Checking Pass	■	6	8.3%	🔍
Checking Operating System Fail	■	18	25%	🔍
Checking Windows Update and Security Patch Fail	■	12	16.7%	🔍
Checking Personal Firewall Fail	■	6	8.3%	🔍
Checking AntiVirus Software Fail	■	6	8.3%	🔍
Checking Windows Registry Fail	■	6	8.3%	🔍
Checking Application Fail	■	18	25%	🔍
Total		72	100%	

Each field is described in the following table.

Table 193 Report > Security Policy Enforcement > EPS

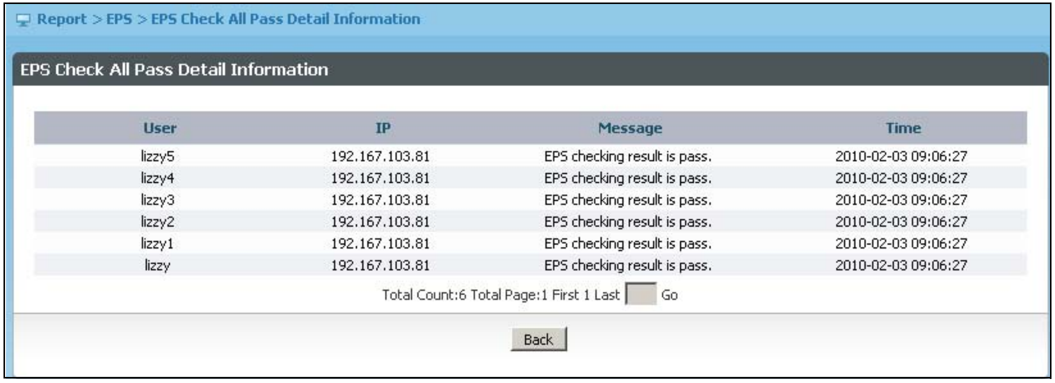
LABEL	DESCRIPTION
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to identify it. • Click on a slice in the pie chart to move it away from the pie chart a little.
Checking Item	This field displays the description about whether users' computers passed all the EPS checking items or failed a specific checking item on the selected device.
Color	This field displays what color represents each EPS checking result in the graph.
Records	This field displays the number of users' computers that passed all the EPS checking items or failed a specific checking item.
% of Records	This field displays what percentage each EPS checking result's number of users' computers makes out of the total number of users' computers that attempted to access the corporate's network.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the EPS rules above.

10.1.3 View Logs

Use this screen to view detailed information about users who passed or failed the EPS checking items defined on the selected ZyWALL device.

Click **View Logs** next to an entry in the **Report** > **Security Policy Enforcement** > **EPS** screen to open the screen.

Figure 209 Report > Security Policy Enforcement > EPS > View Logs



Report > EPS > EPS Check All Pass Detail Information

EPS Check All Pass Detail Information

User	IP	Message	Time
lizzy5	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy4	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy3	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy2	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy1	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27
lizzy	192.167.103.81	EPS checking result is pass.	2010-02-03 09:06:27

Total Count:6 Total Page:1 First 1 Last Go

Each field is described in the following table.

Table 194 Report > Security Policy Enforcement > EPS > View Logs

LABEL	DESCRIPTION
User	This field displays who tried successfully or unsuccessfully to access the protected network.
IP	This field displays the IP address of the user's computer the user used to try to access the protected network.
Message	This field shows whether the user's session passed EPS checking or the reason it failed.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user tried to access the protected network.
Total Count	This field displays how many records there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the records.
First .. Last	Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.
Back	Click this to close this screen.

10.2 Content Filter (All)

These reports look at the number of attempts to access web sites specified in the content filter (blocked, forward and warning) by time interval as well as top allowed sites and hosts.

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

10.2.1 Summary

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

Click **Report > Security Policy Enforcement > Content Filter (All)** > **Summary** to open this screen.

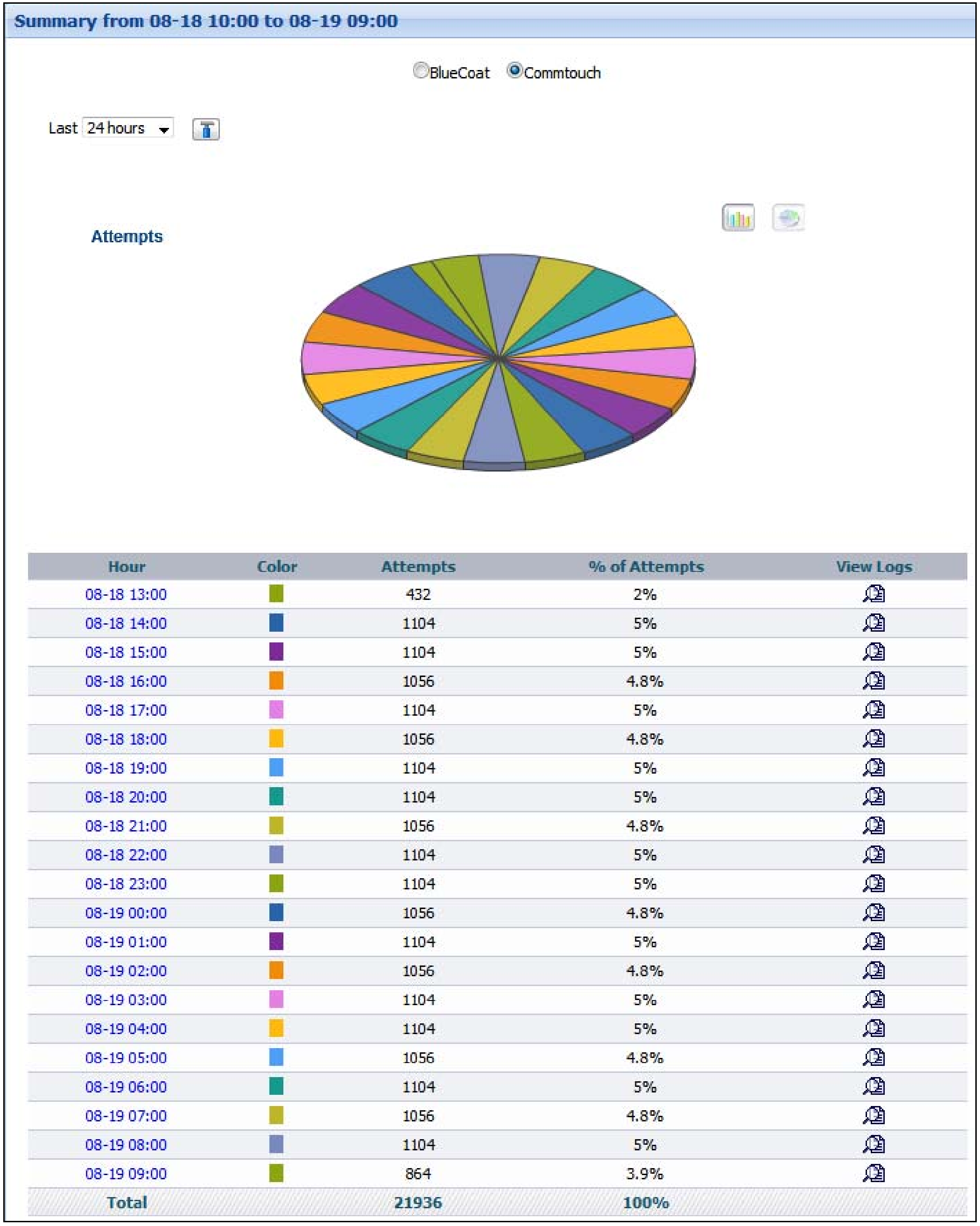


Figure 210 Report > Security Policy Enforcement > Content Filter (All) > Summary

Summary from 08-18 10:00 to 08-19 09:00

○ BlueCoat ● Commtouch

Last 24 hours

Attempts

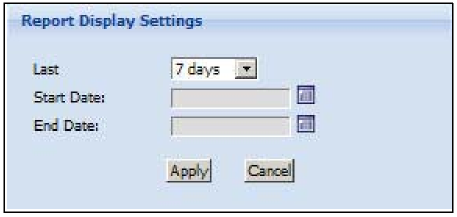
Hour	Color	Attempts	% of Attempts	View Logs
08-18 13:00	🟩	432	2%	🔍
08-18 14:00	🟦	1104	5%	🔍
08-18 15:00	🟪	1104	5%	🔍
08-18 16:00	🟧	1056	4.8%	🔍
08-18 17:00	🟪	1104	5%	🔍
08-18 18:00	🟨	1056	4.8%	🔍
08-18 19:00	🟦	1104	5%	🔍
08-18 20:00	🟩	1104	5%	🔍
08-18 21:00	🟨	1056	4.8%	🔍
08-18 22:00	🟦	1104	5%	🔍
08-18 23:00	🟩	1104	5%	🔍
08-19 00:00	🟦	1056	4.8%	🔍
08-19 01:00	🟪	1104	5%	🔍
08-19 02:00	🟧	1056	4.8%	🔍
08-19 03:00	🟪	1104	5%	🔍
08-19 04:00	🟨	1104	5%	🔍
08-19 05:00	🟦	1056	4.8%	🔍
08-19 06:00	🟩	1104	5%	🔍
08-19 07:00	🟨	1056	4.8%	🔍
08-19 08:00	🟦	1104	5%	🔍
08-19 09:00	🟩	864	3.9%	🔍
Total		21936	100%	

Each field is described in the following table.

Table 195 Report > Security Policy Enforcement > Content Filter (All) > Summary

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.

Table 195 Report > Security Policy Enforcement > Content Filter (All) > Summary

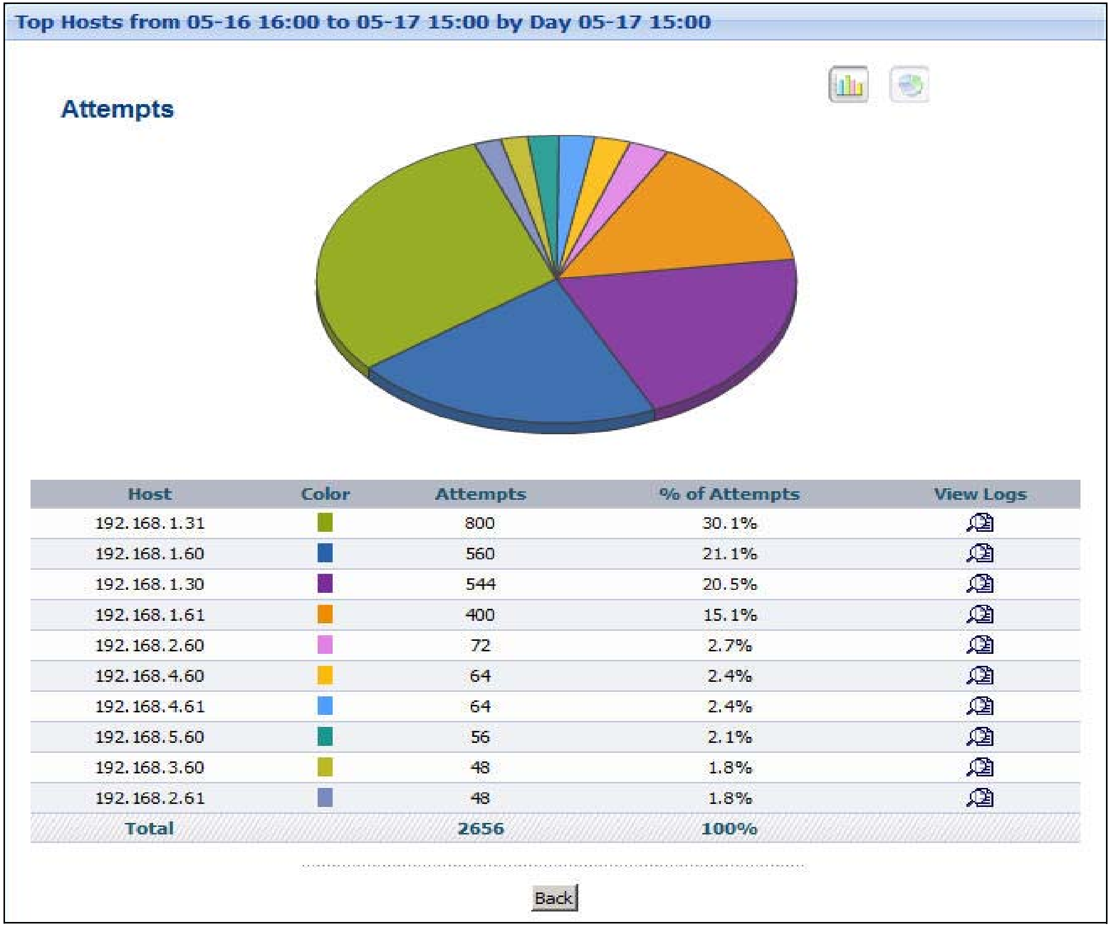
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears. Report Display Settings Last: 7 days Start Date: End Date: 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access specified web sites in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts to access specified web sites in each time interval.
% of Attempts	This field displays the percentage of all attempts in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

10.2.2 Summary Drill-Down

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

Click on a specific time interval in **Report > Security Policy Enforcement > Content Filter (All)** > **Summary** to open this screen.

Figure 211 Report > Security Policy Enforcement > Content Filter (All) > Summary > Drill-Down



Top Hosts from 05-16 16:00 to 05-17 15:00 by Day 05-17 15:00

Attempts

Host	Color	Attempts	% of Attempts	View Logs
192.168.1.31	■	800	30.1%	🔍
192.168.1.60	■	560	21.1%	🔍
192.168.1.30	■	544	20.5%	🔍
192.168.1.61	■	400	15.1%	🔍
192.168.2.60	■	72	2.7%	🔍
192.168.4.60	■	64	2.4%	🔍
192.168.4.61	■	64	2.4%	🔍
192.168.5.60	■	56	2.1%	🔍
192.168.3.60	■	48	1.8%	🔍
192.168.2.61	■	48	1.8%	🔍
Total		2656	100%	

Each field is described in the following table.

Table 196 Report > Security Policy Enforcement > Content Filter (All) > Summary > Drill-Down

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

Table 196 Report > Security Policy Enforcement > Content Filter (All) > Summary > Drill-Down

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

10.2.3 Top Sites

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

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

Click **Report > Security Policy Enforcement > Content Filter (All) > Top Sites** to open this screen.

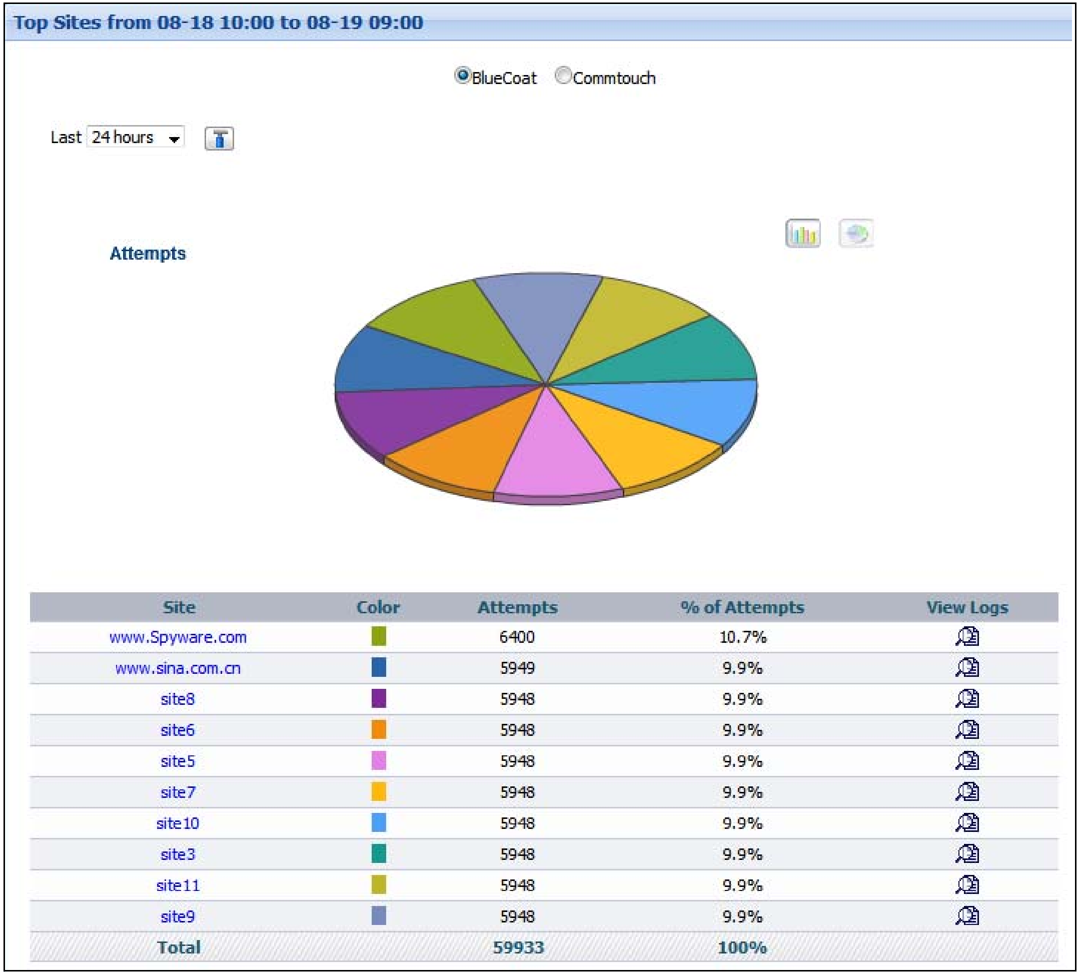


Figure 212 Report > Security Policy Enforcement > Content Filter (All) > Top Sites

Top Sites from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

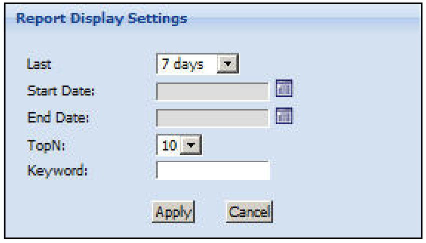
Site	Color	Attempts	% of Attempts	View Logs
www.Spyware.com	■	6400	10.7%	🔍
www.sina.com.cn	■	5949	9.9%	🔍
site8	■	5948	9.9%	🔍
site6	■	5948	9.9%	🔍
site5	■	5948	9.9%	🔍
site7	■	5948	9.9%	🔍
site10	■	5948	9.9%	🔍
site3	■	5948	9.9%	🔍
site11	■	5948	9.9%	🔍
site9	■	5948	9.9%	🔍
Total		59933	100%	

Each field is described in the following table.

Table 197 Report > Security Policy Enforcement > Content Filter (All) > Top Sites

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 197 Report > Security Policy Enforcement > Content Filter (All) > Top Sites

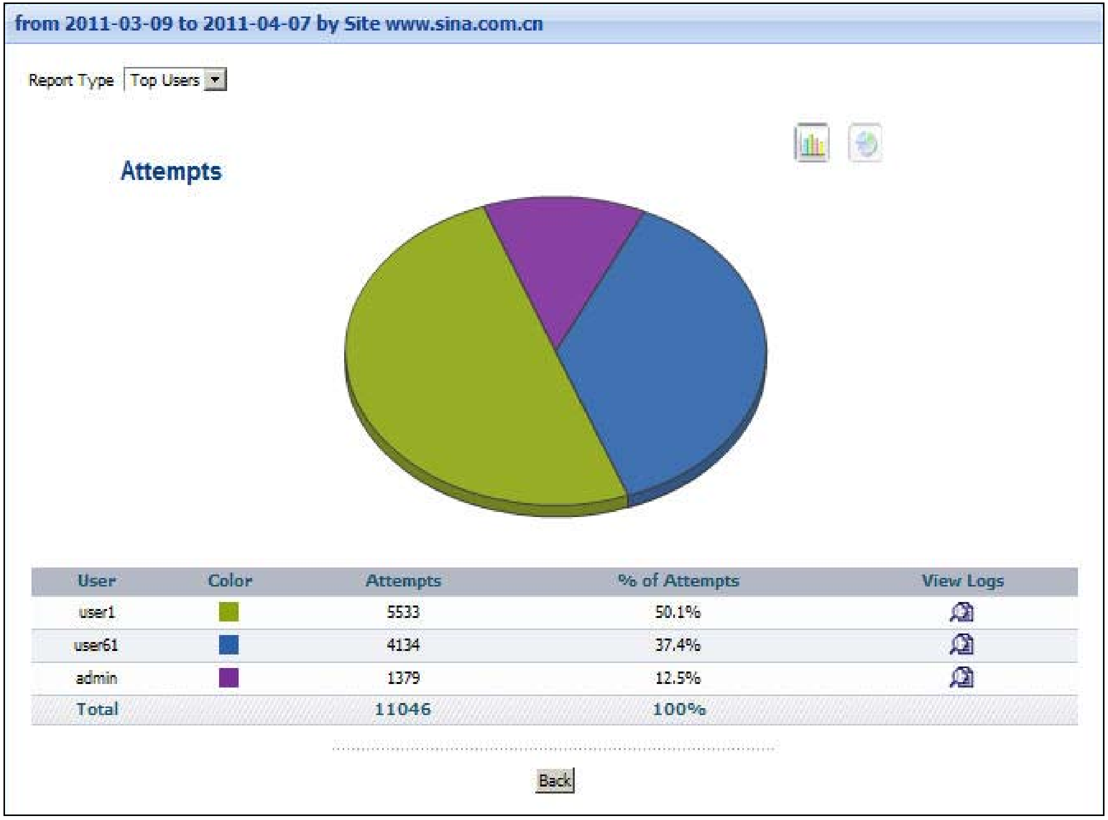
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts for each destination.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

10.2.4 Top Sites Drill-Down

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

Click on a specific destination in **Report > Security Policy Enforcement > Content Filter (All) > Top Sites** to open this screen.

Figure 213 Report > Security Policy Enforcement > Content Filter (All) > Top Sites > Drill-Down



from 2011-03-09 to 2011-04-07 by Site www.sina.com.cn

Report Type: Top Users

User	Color	Attempts	% of Attempts	View Logs
user1	🟩	5533	50.1%	
user61	🟦	4134	37.4%	
admin	🟪	1379	12.5%	
Total		11046	100%	

Each field is described in the following table.

Table 198 Report > Security Policy Enforcement > Content Filter (All) > Top Sites > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Users**, **Top Hosts** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made by each source to the selected destination.
View Logs	Click this icon to see the logs that go with the record.

Table 198 Report > Security Policy Enforcement > Content Filter (All) > Top Sites > Drill-Down

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

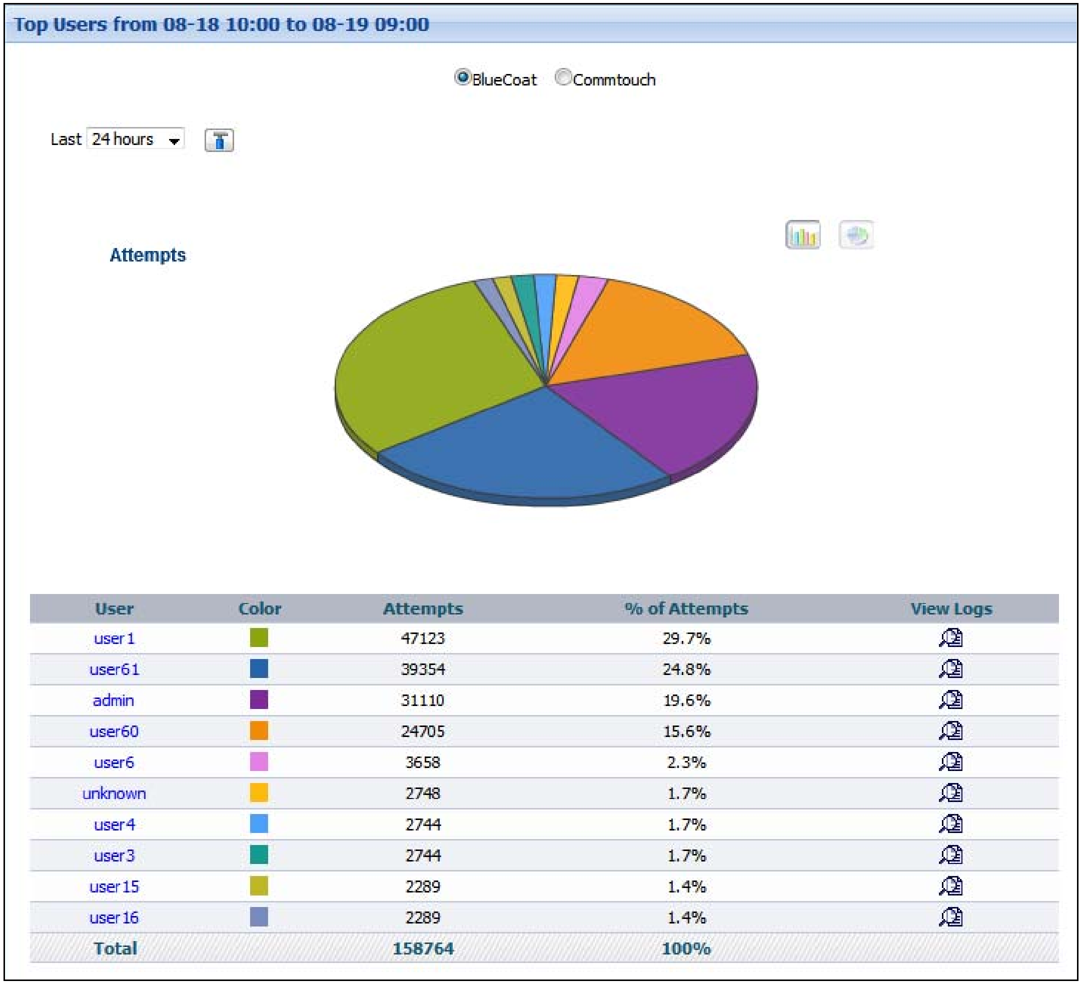
10.2.5 Top Users

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

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

Click **Report > Security Policy Enforcement > Content Filter (All) > Top Users** to open this screen.

Figure 214 Report > Security Policy Enforcement > Content Filter (All) > Top Users



Top Users from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

User	Color	Attempts	% of Attempts	View Logs
user1	🟩	47123	29.7%	🔍
user61	🟦	39354	24.8%	🔍
admin	🟪	31110	19.6%	🔍
user60	🟧	24705	15.6%	🔍
user6	🟪	3658	2.3%	🔍
unknown	🟨	2748	1.7%	🔍
user4	🟦	2744	1.7%	🔍
user3	🟩	2744	1.7%	🔍
user15	🟨	2289	1.4%	🔍
user16	🟦	2289	1.4%	🔍
Total		158764	100%	

Each field is described in the following table.

Table 199 Report > Security Policy Enforcement > Content Filter (All) > Top Users

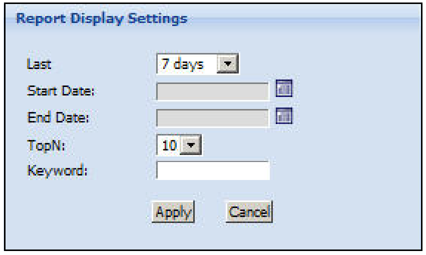
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users of web traffic, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected user.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how many times each user accessed the specified web sites.
% of Attempts	This field displays what percentage of all attempts to access specified web sites was made by each user.

Table 199 Report > Security Policy Enforcement > Content Filter (All) > Top Users

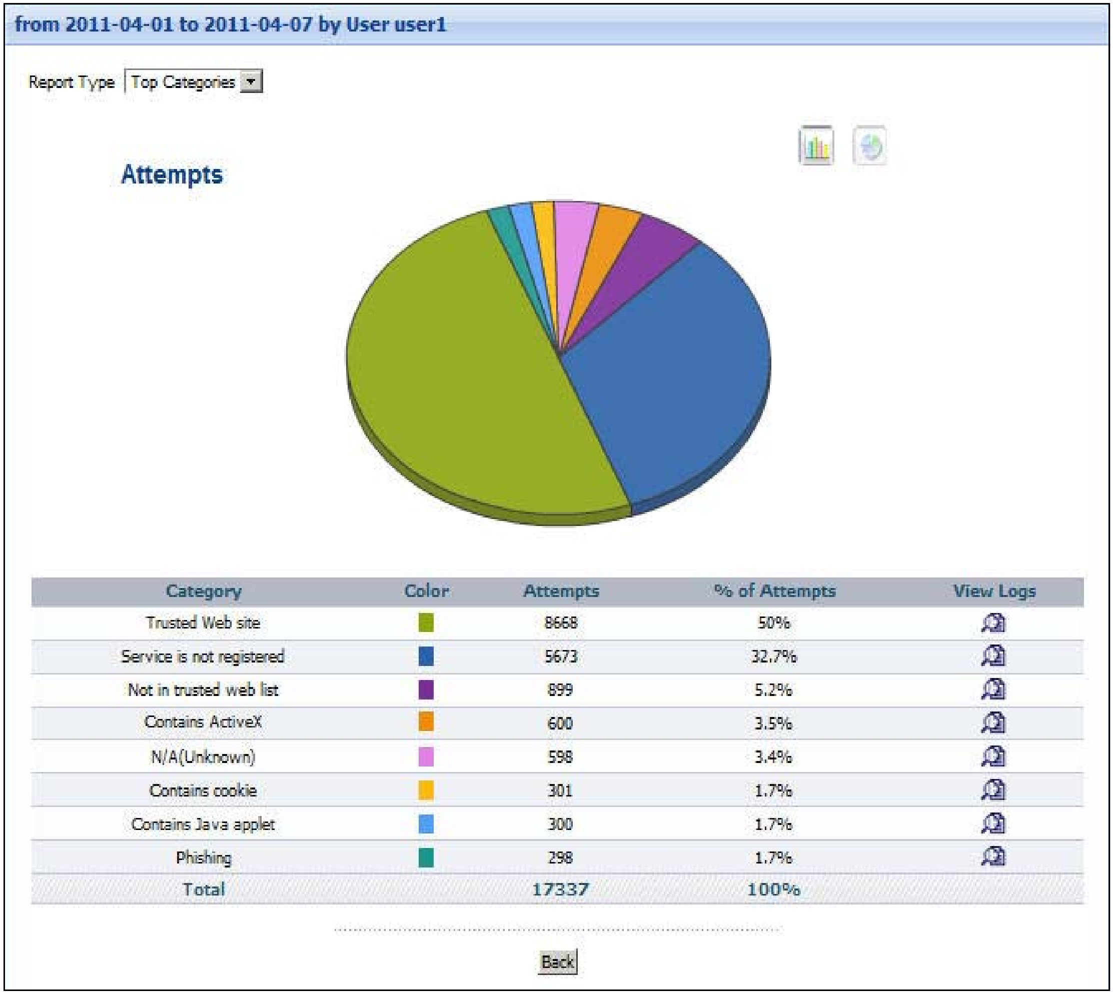
LABEL	DESCRIPTION
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.2.6 Top Users Drill-Down

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

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (All) > Top Users** to open this screen.

Figure 215 Report > Security Policy Enforcement > Content Filter (All) > Top Users > Drill-Down



from 2011-04-01 to 2011-04-07 by User user1

Report Type Top Categories

Category	Color	Attempts	% of Attempts	View Logs
Trusted Web site	■	8668	50%	🔍
Service is not registered	■	5673	32.7%	🔍
Not in trusted web list	■	899	5.2%	🔍
Contains ActiveX	■	600	3.5%	🔍
N/A(Unknown)	■	598	3.4%	🔍
Contains cookie	■	301	1.7%	🔍
Contains Java applet	■	300	1.7%	🔍
Phishing	■	298	1.7%	🔍
Total		17337	100%	

Each field is described in the following table.

Table 200 Report > Security Policy Enforcement > Content Filter (All) > Top Users > Drill-Down

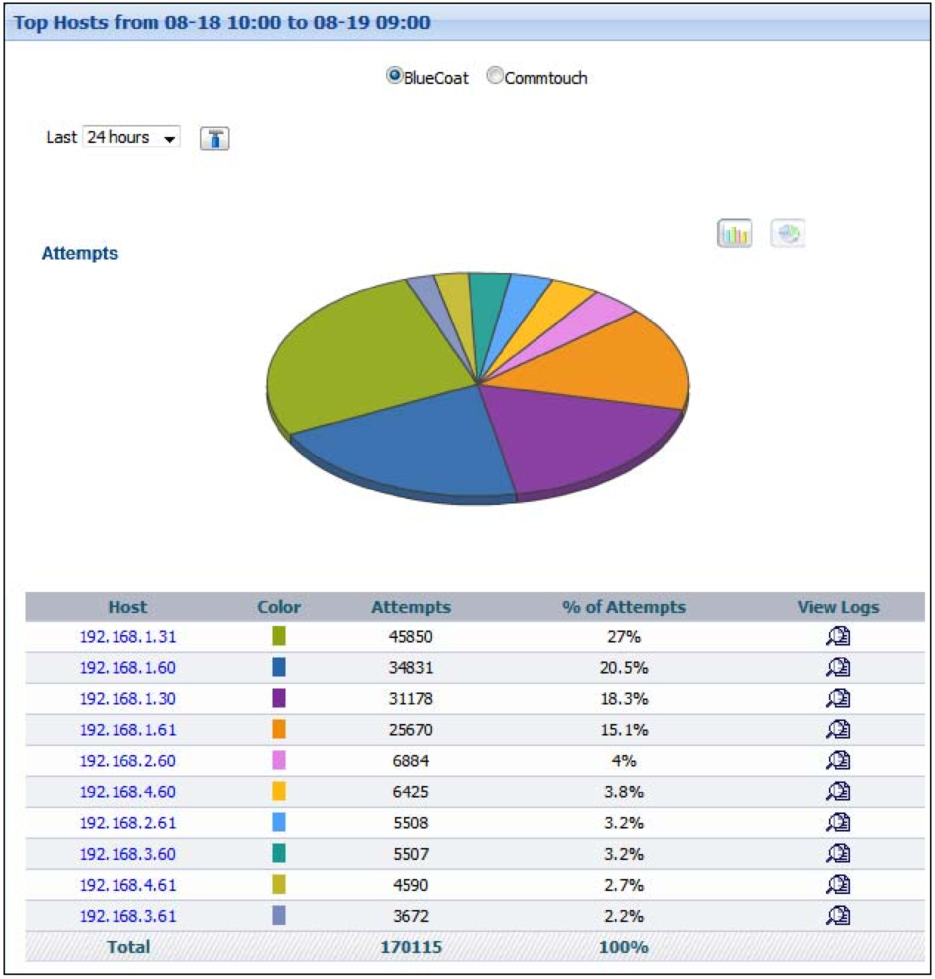
LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Categories**, **Top Sites** or **By Hour** as the content to be displayed.
graph	The graph displays the information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

10.2.7 Top Hosts

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

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

Click **Report > Security Policy Enforcement > Content Filter (All) > Top Hosts** to open this screen.



Top Hosts from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

Host	Color	Attempts	% of Attempts	View Logs
192.168.1.31	■	45850	27%	🔍
192.168.1.60	■	34831	20.5%	🔍
192.168.1.30	■	31178	18.3%	🔍
192.168.1.61	■	25670	15.1%	🔍
192.168.2.60	■	6884	4%	🔍
192.168.4.60	■	6425	3.8%	🔍
192.168.2.61	■	5508	3.2%	🔍
192.168.3.60	■	5507	3.2%	🔍
192.168.4.61	■	4590	2.7%	🔍
192.168.3.61	■	3672	2.2%	🔍
Total		170115	100%	

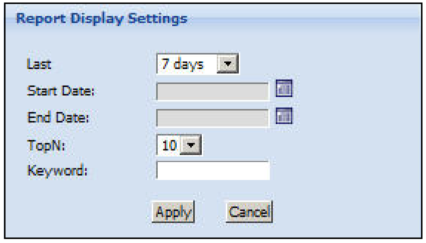
Figure 216 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts

Each field is described in the following table.

Table 201 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 201 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts

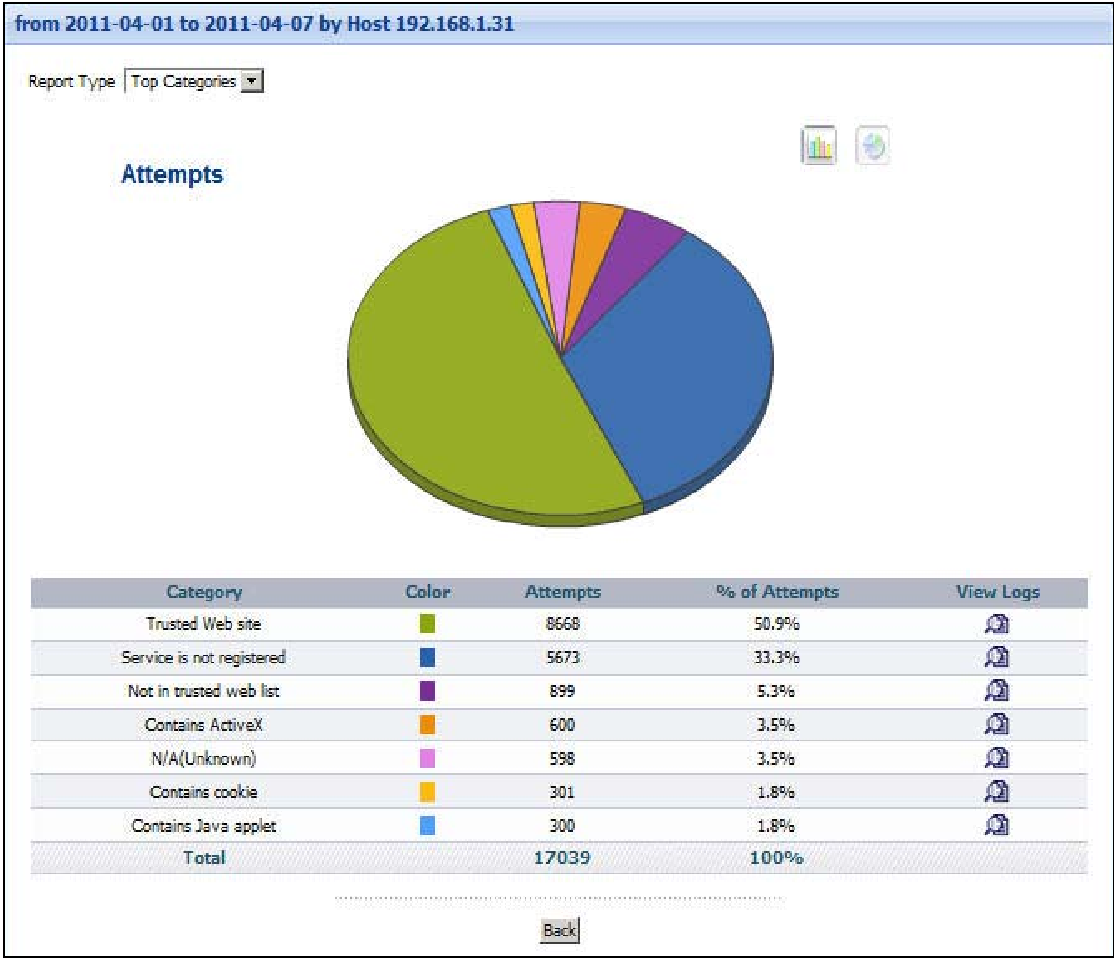
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays how times each source accessed specified web sites.
% of Attempts	This field displays what percentage of all attempts to access allowed web sites was made from each sources.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.2.8 Top Hosts Drill-Down

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

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (All) > Top Hosts** to open this screen.

Figure 217 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts > Drill-Down



from 2011-04-01 to 2011-04-07 by Host 192.168.1.31

Report Type: Top Categories ▾

Attempts

Category	Color	Attempts	% of Attempts	View Logs
Trusted Web site	■	8668	50.9%	🔍
Service is not registered	■	5673	33.3%	🔍
Not in trusted web list	■	899	5.3%	🔍
Contains ActiveX	■	600	3.5%	🔍
N/A(Unknown)	■	598	3.5%	🔍
Contains cookie	■	301	1.8%	🔍
Contains Java applet	■	300	1.8%	🔍
Total		17039	100%	

Back

Each field is described in the following table.

Table 202 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Categories**, **Top Sites** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of web traffic from the selected source, sorted by the number of attempts attributed to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts from the selected source to each destination.

Table 202 Report > Security Policy Enforcement > Content Filter (All) > Top Hosts > Drill-Down

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

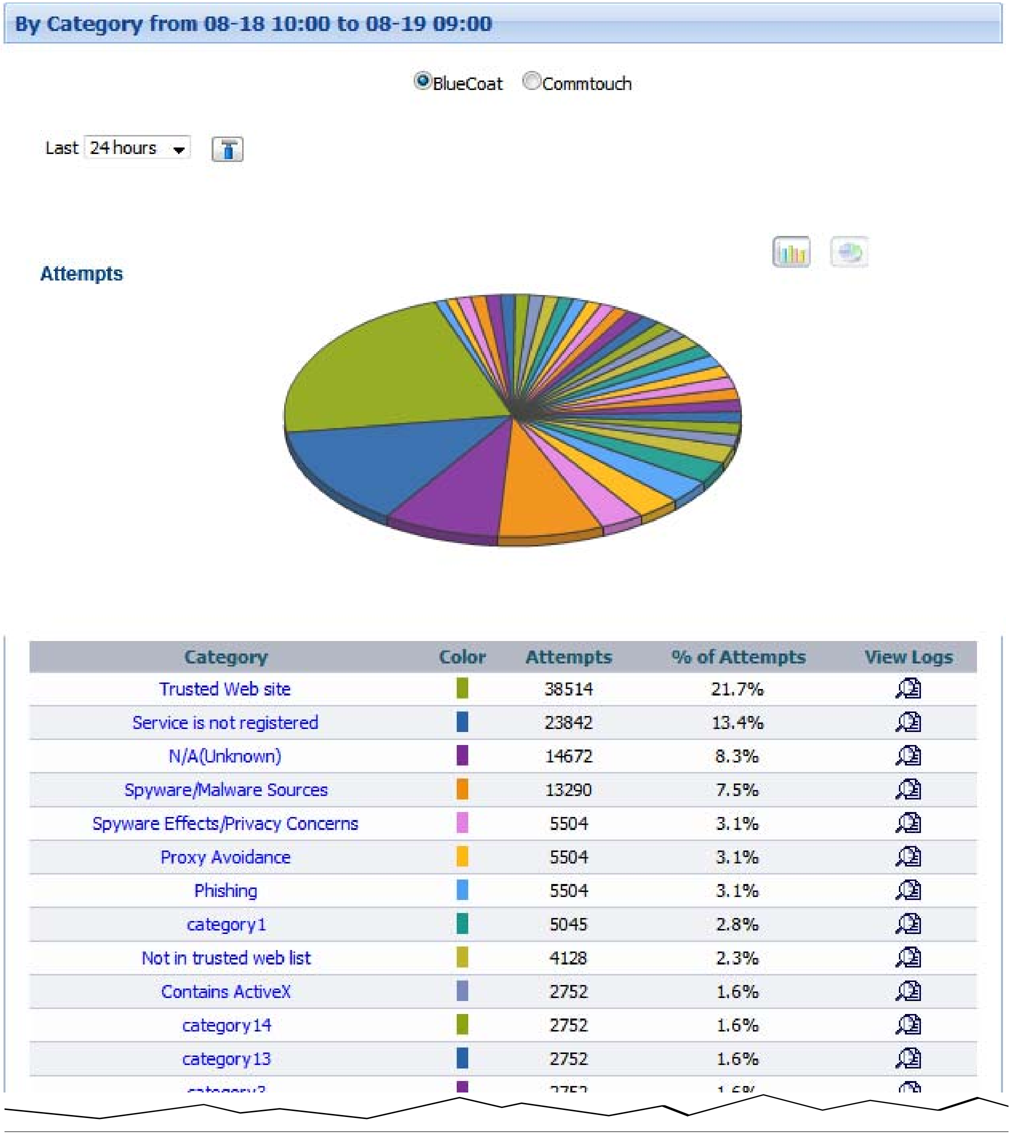
10.2.9 By Category

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

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

Click **Report > Security Policy Enforcement > Content Filter (All) > By Category** to open this screen.

Figure 218 Report > Security Policy Enforcement > Content Filter (All) > By Category



By Category from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

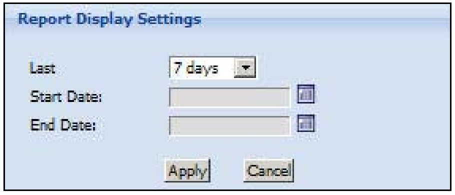
Category	Color	Attempts	% of Attempts	View Logs
Trusted Web site	■	38514	21.7%	
Service is not registered	■	23842	13.4%	
N/A(Unknown)	■	14672	8.3%	
Spyware/Malware Sources	■	13290	7.5%	
Spyware Effects/Privacy Concerns	■	5504	3.1%	
Proxy Avoidance	■	5504	3.1%	
Phishing	■	5504	3.1%	
category1	■	5045	2.8%	
Not in trusted web list	■	4128	2.3%	
Contains ActiveX	■	2752	1.6%	
category14	■	2752	1.6%	
category13	■	2752	1.6%	
category2	■	2752	1.6%	

Each field is described in the following table.

Table 203 Report > Security Policy Enforcement > Content Filter (All) > By Category

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.

Table 203 Report > Security Policy Enforcement > Content Filter (All) > By Category

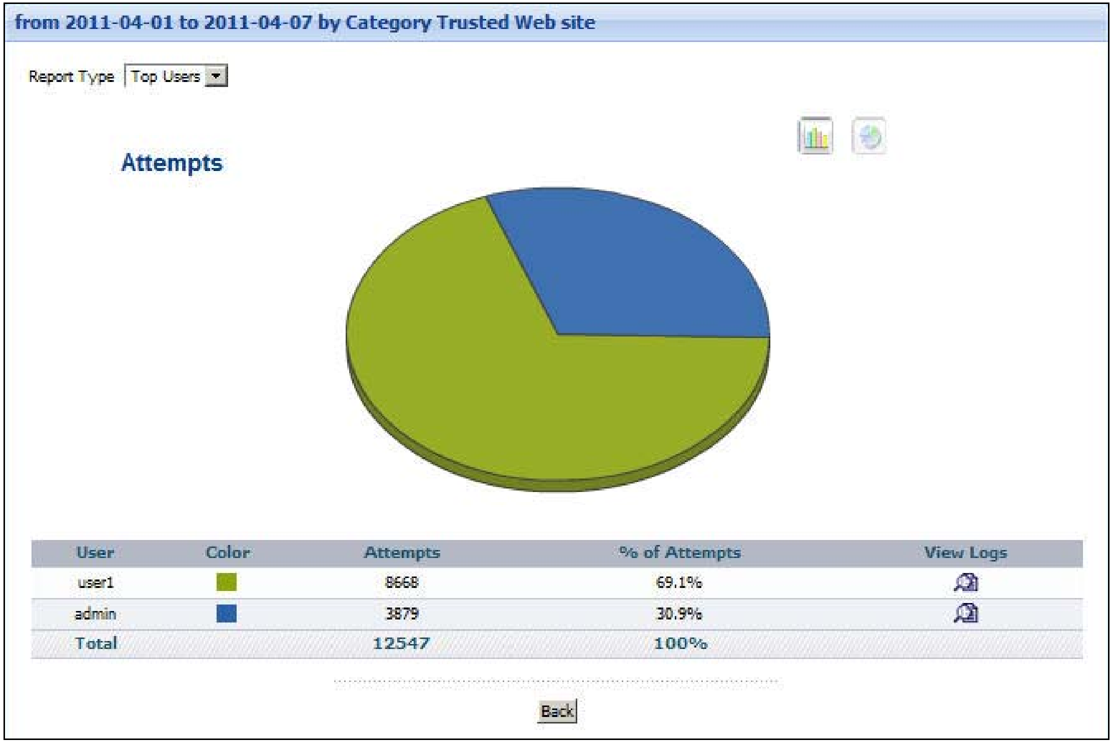
LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access specified web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

10.2.10 By Category Drill-Down

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

Click on a specific category in **Report > Security Policy Enforcement > Content Filter (All) > By Category** to open this screen.

Figure 219 Report > Security Policy Enforcement > Content Filter (All) > By Category > Drill-Down



from 2011-04-01 to 2011-04-07 by Category Trusted Web site

Report Type: Top Users

User	Color	Attempts	% of Attempts	View Logs
user1	🟩	8668	69.1%	🔍
admin	🟦	3879	30.9%	🔍
Total		12547	100%	

Each field is described in the following table.

Table 204 Report > Security Policy Enforcement > By Category > Content Filter (All) > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Users**, **Top Sites**, **Top Hosts** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the destinations of web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts to each destination in the selected category.
% of Attempts	This field displays what percentage of all attempts to access specified web sites in the selected category went to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.
Back	Click this to return to the main report.

10.3 Content Filter (Blocked)

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

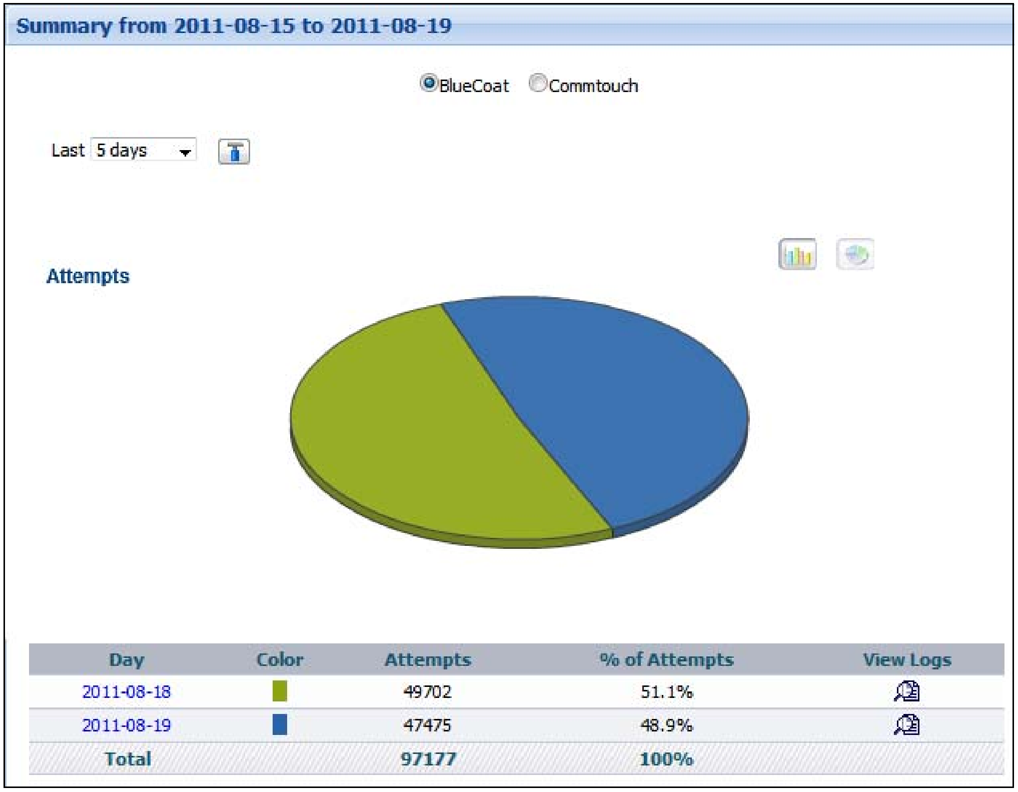
Note: To look at security policy reports, each ZyXEL device must record blocked web packets and blocked web packets in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Blocked Web Sites** is enabled.

10.3.1 Summary

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

Click **Report > Security Policy Enforcement > Content Filter (Blocked)** > **Summary** to open this screen.

Figure 220 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary



Summary from 2011-08-15 to 2011-08-19

● BlueCoat ○ Commtouch

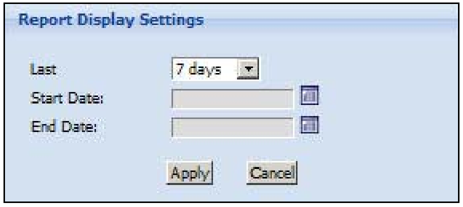
Last 5 days

Attempts

Day	Color	Attempts	% of Attempts	View Logs
2011-08-18	🟩	49702	51.1%	🔍
2011-08-19	🟦	47475	48.9%	🔍
Total		97177	100%	

Each field is described in the following table.

Table 205 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary

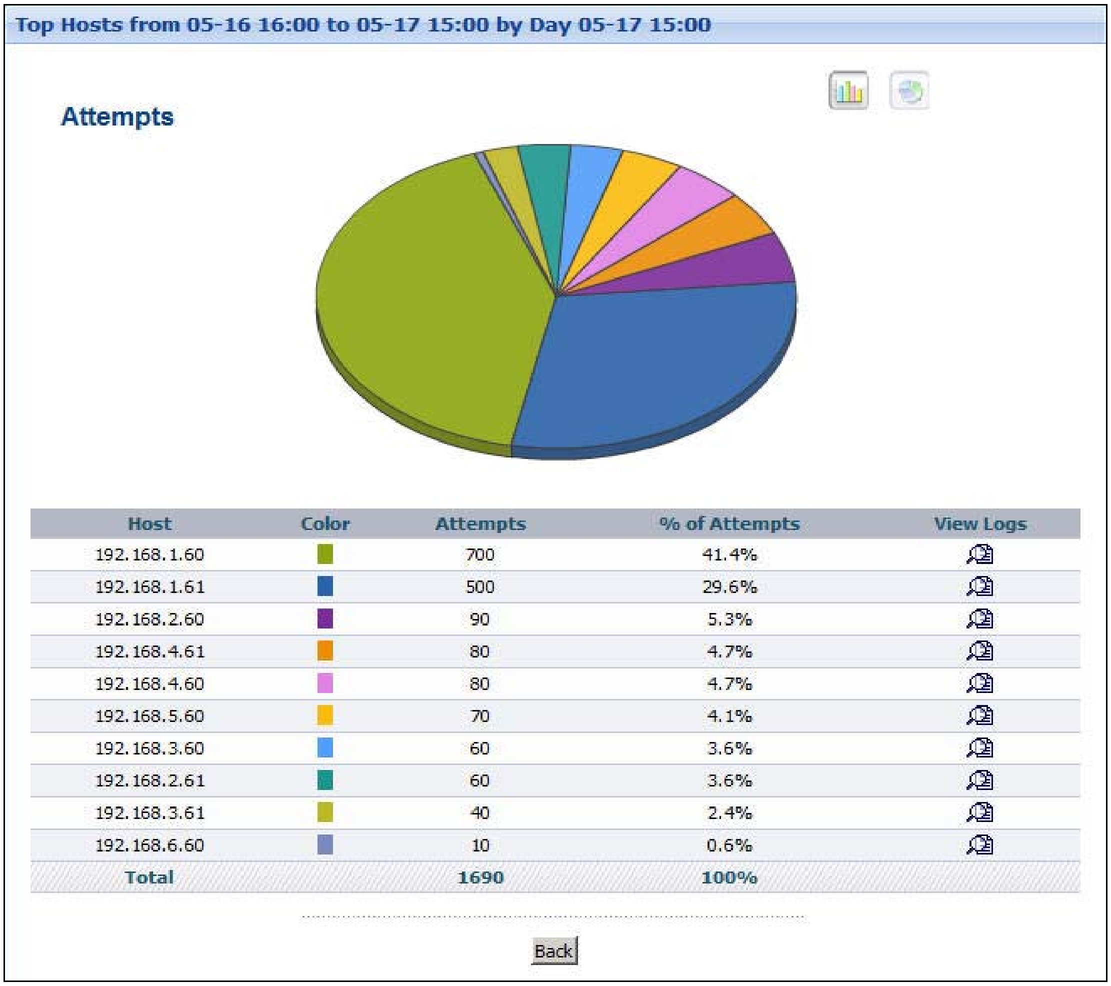
LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: 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** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days. Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval.
Color	This field displays what color represents each time interval in the graph.
Attempts	This field displays the number of attempts by each source to access blocked web sites in the selected time interval.
% of Attempts	This field displays what percentage of all blocked web access attempts was handled in each time interval.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the time intervals above.

10.3.2 Summary Drill-Down

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

Click on a specific time interval in **Report > Security Policy Enforcement > Content Filter (Blocked)** > **Summary** to open this screen.

Figure 221 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary > Drill-Down



Top Hosts from 05-16 16:00 to 05-17 15:00 by Day 05-17 15:00

Host	Color	Attempts	% of Attempts	View Logs
192.168.1.60	🟩	700	41.4%	🔍
192.168.1.61	🟦	500	29.6%	🔍
192.168.2.60	🟪	90	5.3%	🔍
192.168.4.61	🟧	80	4.7%	🔍
192.168.4.60	🟪	80	4.7%	🔍
192.168.5.60	🟨	70	4.1%	🔍
192.168.3.60	🟦	60	3.6%	🔍
192.168.2.61	🟩	60	3.6%	🔍
192.168.3.61	🟨	40	2.4%	🔍
192.168.6.60	🟦	10	0.6%	🔍
Total		1690	100%	

Each field is described in the following table.

Table 206 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
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.

Table 206 Report > Security Policy Enforcement > Content Filter (Blocked) > Summary > Drill-Down

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

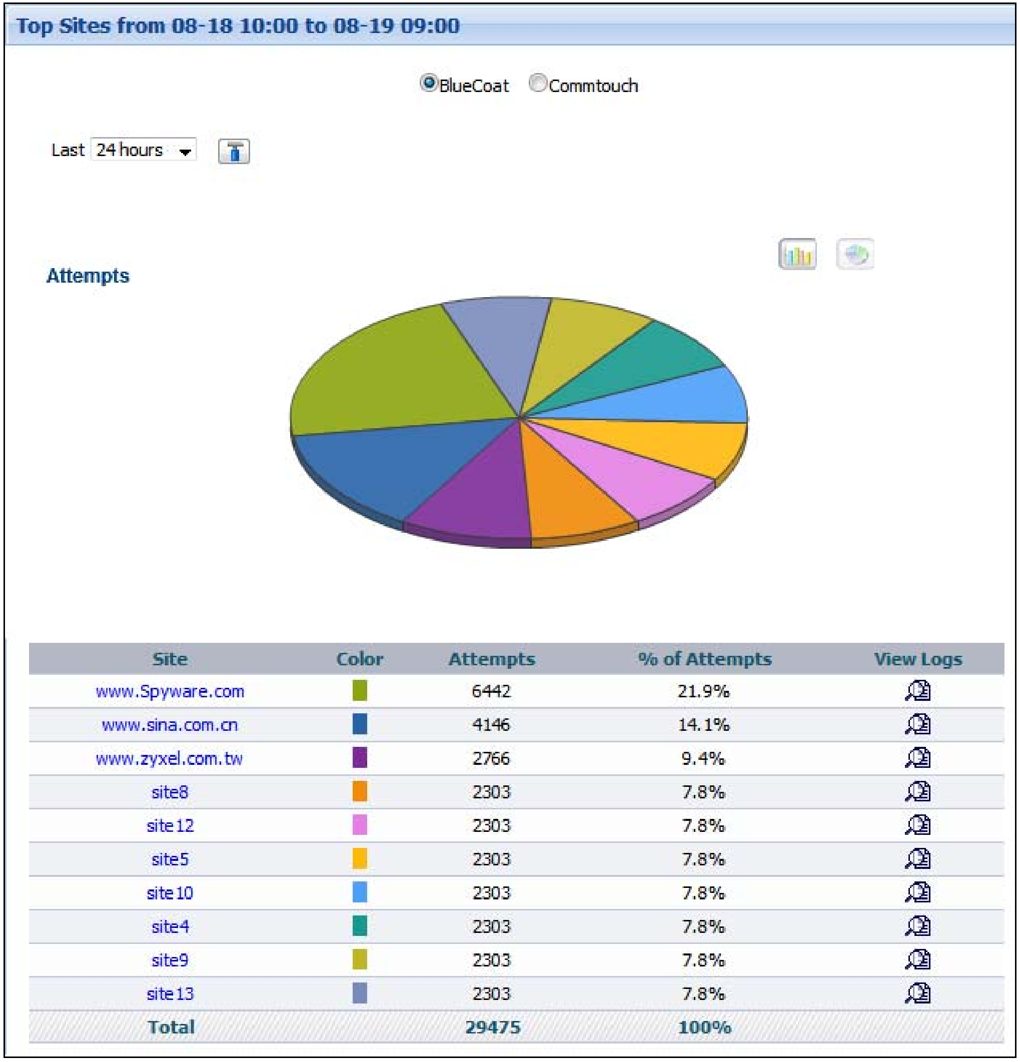
10.3.3 Top Blocked Sites

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

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

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites** to open this screen.

Figure 222 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites



Top Sites from 08-18 10:00 to 08-19 09:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

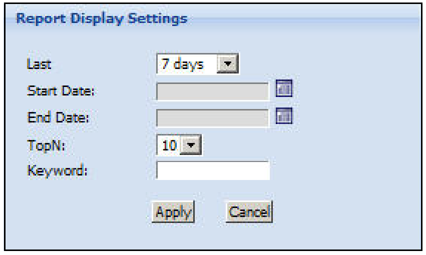
Site	Color	Attempts	% of Attempts	View Logs
www.Spyware.com	■	6442	21.9%	🔍
www.sina.com.cn	■	4146	14.1%	🔍
www.zyxel.com.tw	■	2766	9.4%	🔍
site8	■	2303	7.8%	🔍
site12	■	2303	7.8%	🔍
site5	■	2303	7.8%	🔍
site10	■	2303	7.8%	🔍
site4	■	2303	7.8%	🔍
site9	■	2303	7.8%	🔍
site13	■	2303	7.8%	🔍
Total		29475	100%	

Each field is described in the following table.

Table 207 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 207 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites

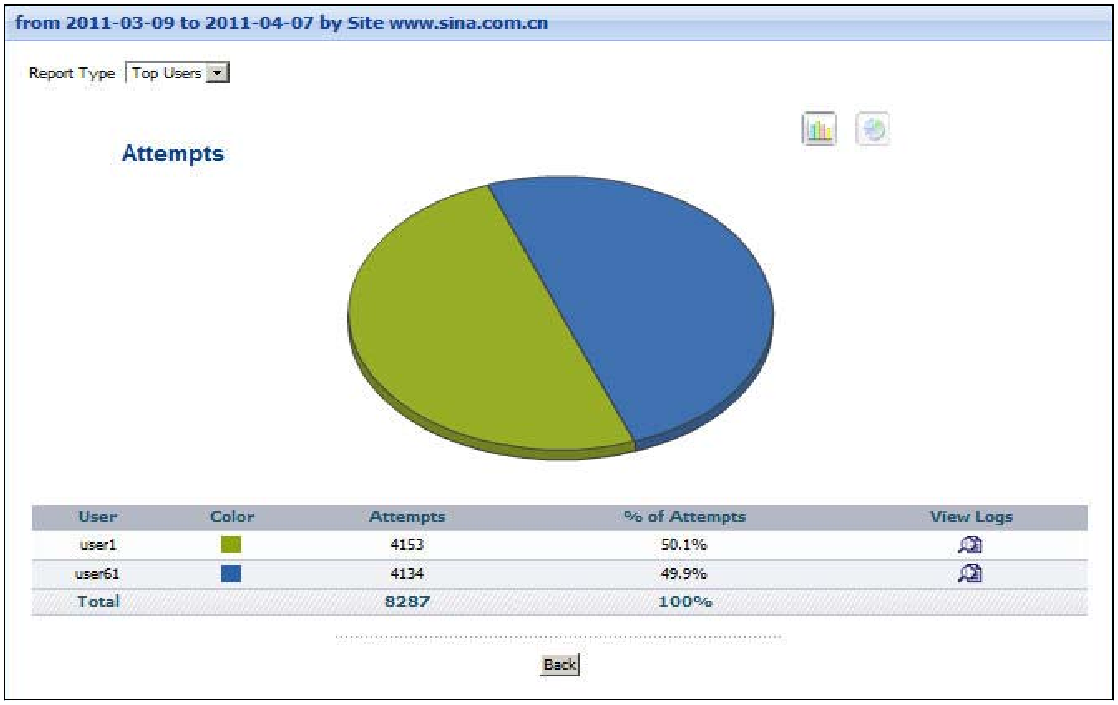
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Site** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the top destinations of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed. Each destination is identified by its domain name. Click on a destination to look at the top sources of blocked web traffic for the selected destination.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays how much traffic (in megabytes) the device handled for each destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.

10.3.4 Top Blocked Sites Drill-Down

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

Click on a specific destination in **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites** to open this screen.

Figure 223 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites > Drill-Down



from 2011-03-09 to 2011-04-07 by Site www.sina.com.cn

Report Type: Top Users

Attempts

User	Color	Attempts	% of Attempts	View Logs
user1	🟩	4153	50.1%	
user61	🟦	4134	49.9%	
Total		8287	100%	

Each field is described in the following table.

Table 208 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Users**, **Top Hosts** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic to the selected destination, sorted by the number of attempts attributed to each one. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of attempts from each source to the selected destination.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made by each source to the selected destination.
View Logs	Click this icon to see the logs that go with the record.

Table 208 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Sites > Drill-Down

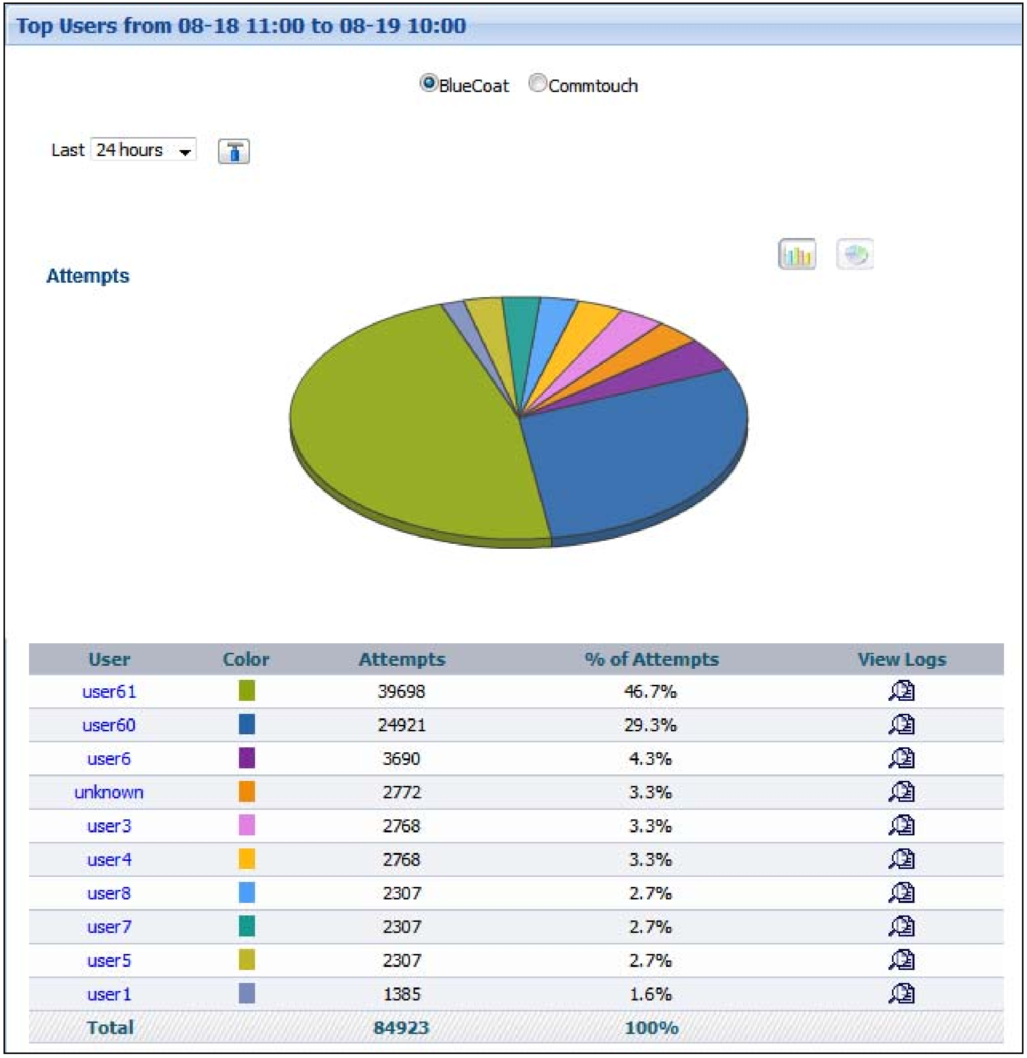
LABEL	DESCRIPTION
Total	This entry displays the totals for the sources above. If the number of sources of attempts to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.
Back	Click this to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

10.3.5 Top Blocked Users

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

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

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users** to open this screen.



Top Users from 08-18 11:00 to 08-19 10:00

● BlueCoat ○ Commtouch

Last 24 hours

User	Color	Attempts	% of Attempts	View Logs
user61	■	39698	46.7%	🔍
user60	■	24921	29.3%	🔍
user6	■	3690	4.3%	🔍
unknown	■	2772	3.3%	🔍
user3	■	2768	3.3%	🔍
user4	■	2768	3.3%	🔍
user8	■	2307	2.7%	🔍
user7	■	2307	2.7%	🔍
user5	■	2307	2.7%	🔍
user1	■	1385	1.6%	🔍
Total		84923	100%	

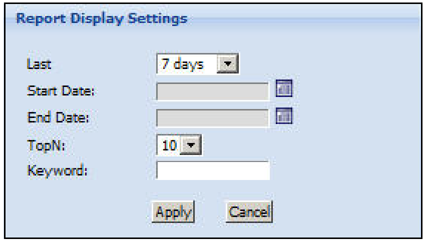
Figure 224 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users

Each field is described in the following table.

Table 209 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 209 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users

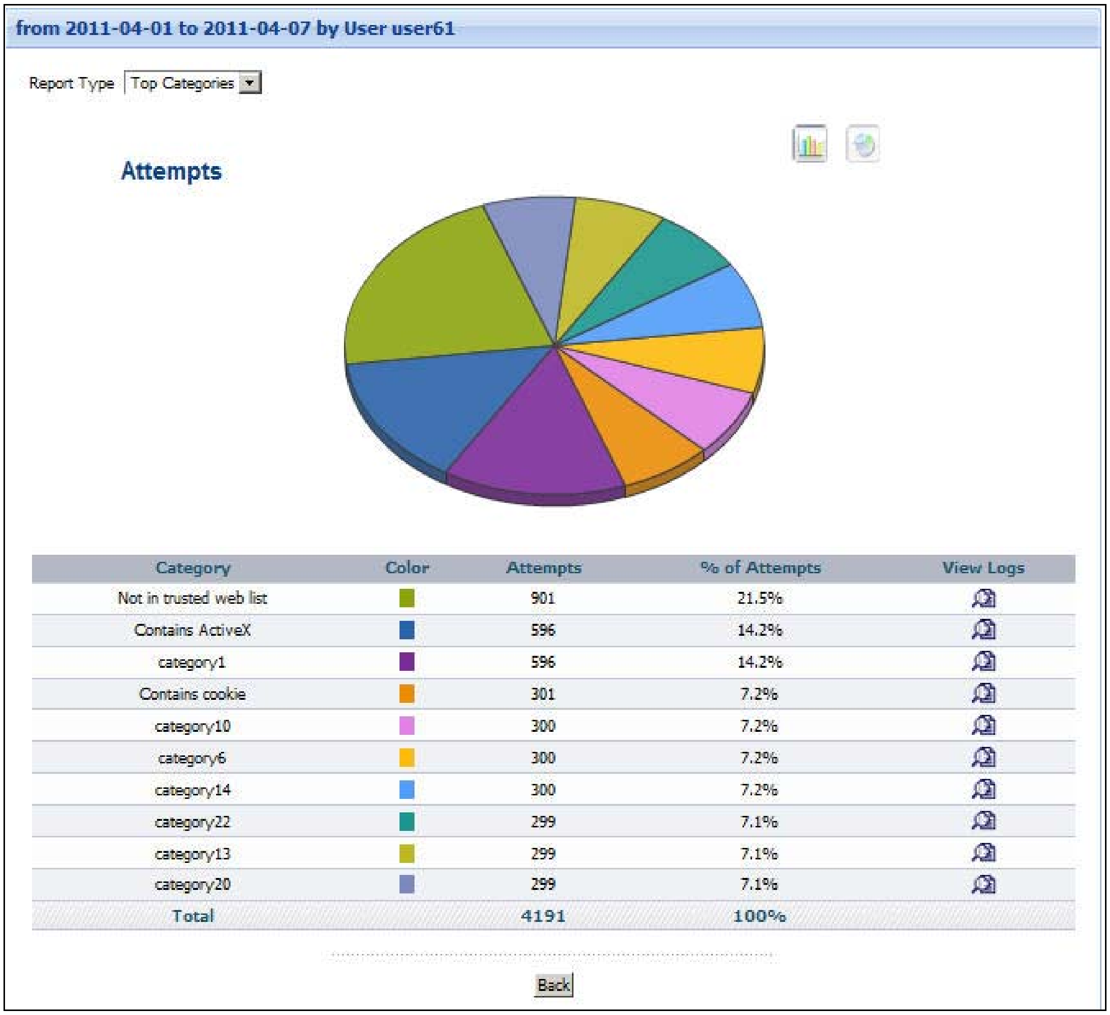
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users for which the device blocked the most web site access attempts, sorted by the number of attempts for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name. Click on a user name to look at the top destinations of web traffic for the selected source.
Color	This field displays what color represents each user in the graph.
Attempts	This field displays the number of web access attempts the device blocked from each user.
% of Attempts	This field displays what percentage the user had of all blocked attempts to access web sites.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.3.6 Top Blocked Users Drill-Down

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

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users** to open this screen.

Figure 225 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users > Drill-Down



from 2011-04-01 to 2011-04-07 by User user61

Report Type: Top Categories

Attempts

Category	Color	Attempts	% of Attempts	View Logs
Not in trusted web list	🟩	901	21.5%	🔍
Contains ActiveX	🟦	596	14.2%	🔍
category1	🟪	596	14.2%	🔍
Contains cookie	🟧	301	7.2%	🔍
category10	🟪	300	7.2%	🔍
category6	🟨	300	7.2%	🔍
category14	🟦	300	7.2%	🔍
category22	🟩	299	7.1%	🔍
category13	🟨	299	7.1%	🔍
category20	🟪	299	7.1%	🔍
Total		4191	100%	

Back

Each field is described in the following table.

Table 210 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Categories**, **Top Sites** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the 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 210 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Users > Drill-Down

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

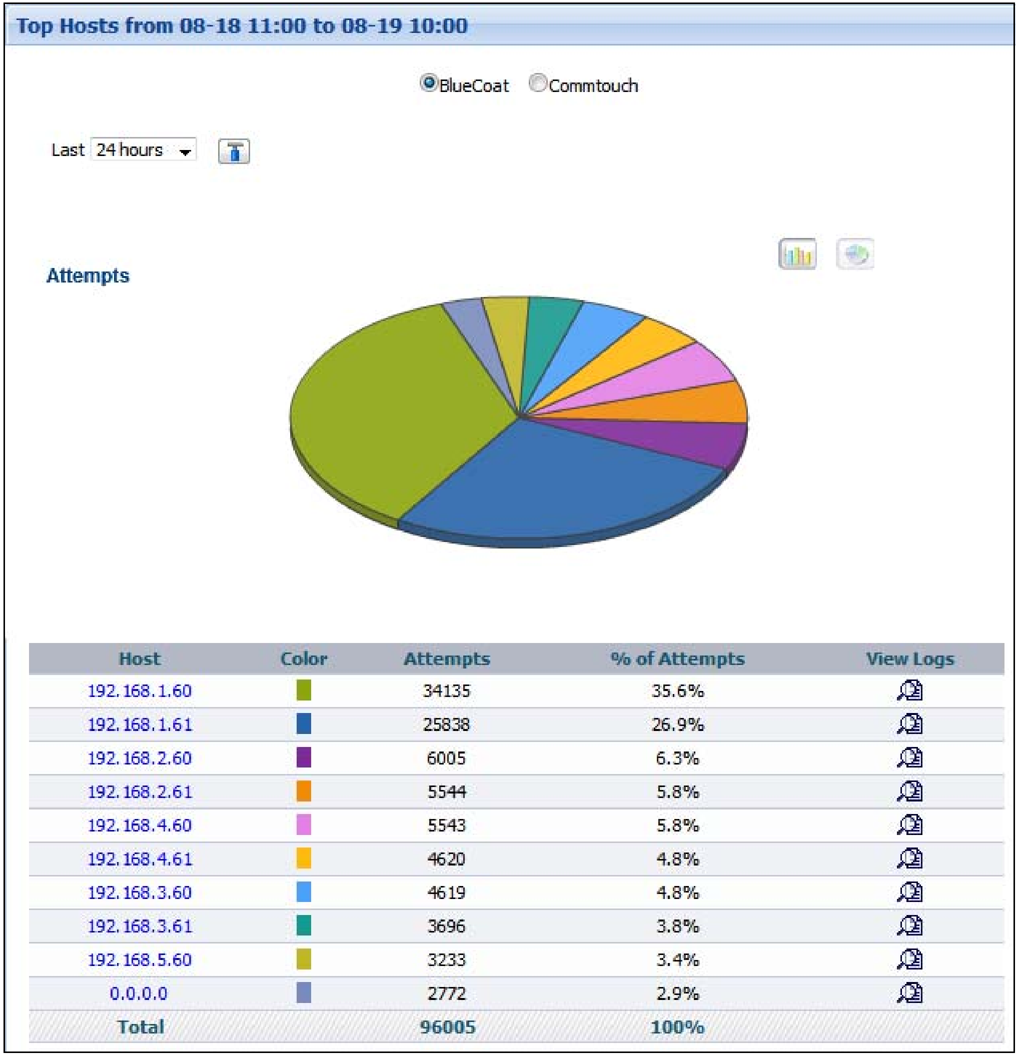
10.3.7 Top Blocked Hosts

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

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

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts** to open this screen.

Figure 226 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts



Top Hosts from 08-18 11:00 to 08-19 10:00

● BlueCoat ○ Commtouch

Last 24 hours

Attempts

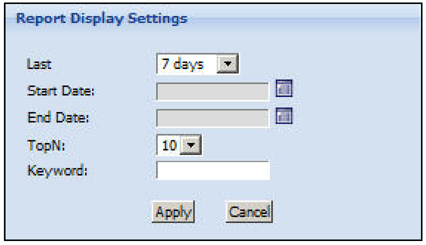
Host	Color	Attempts	% of Attempts	View Logs
192.168.1.60	🟩	34135	35.6%	
192.168.1.61	🟦	25838	26.9%	
192.168.2.60	🟪	6005	6.3%	
192.168.2.61	🟧	5544	5.8%	
192.168.4.60	🟪	5543	5.8%	
192.168.4.61	🟨	4620	4.8%	
192.168.3.60	🟦	4619	4.8%	
192.168.3.61	🟩	3696	3.8%	
192.168.5.60	🟨	3233	3.4%	
0.0.0.0	🟦	2772	2.9%	
Total		96005	100%	

Each field is described in the following table.

Table 211 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 211 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts

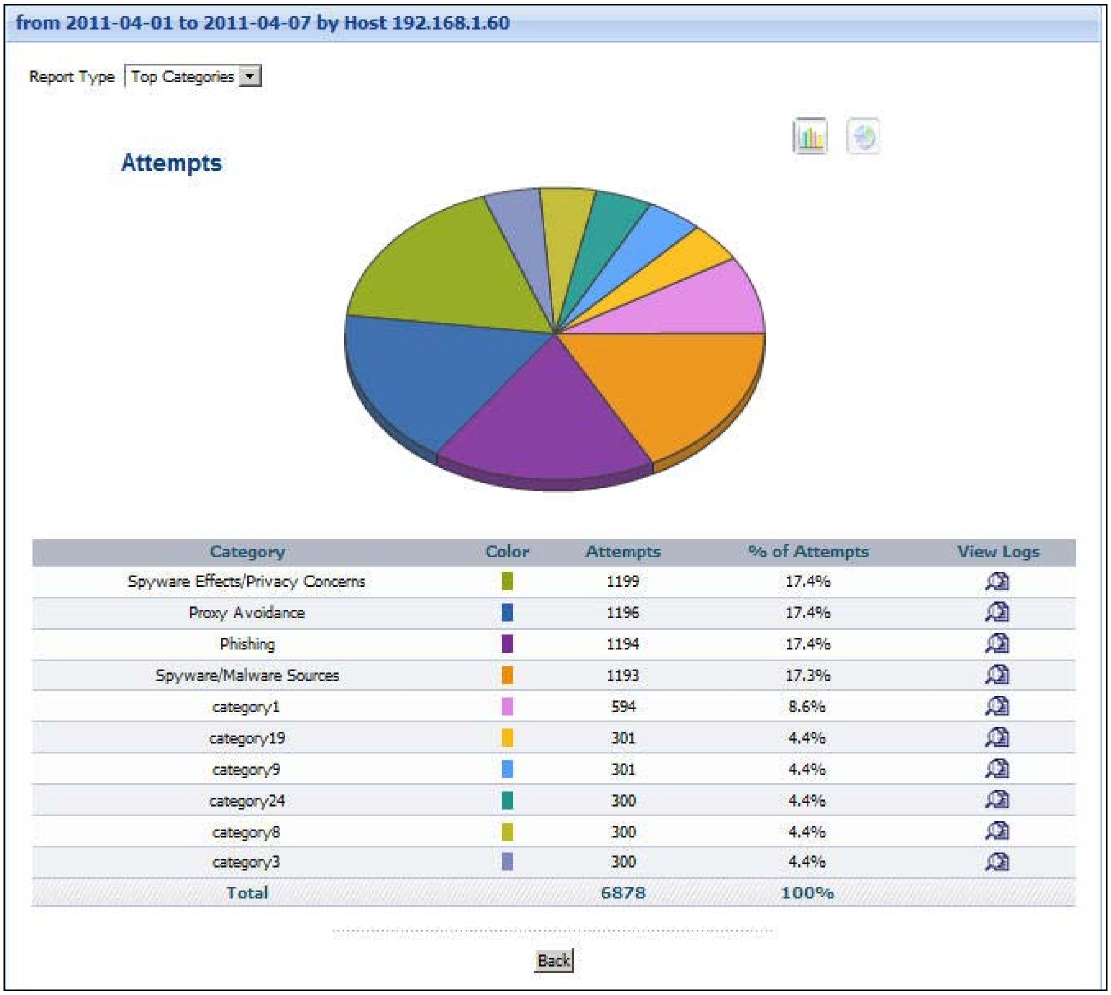
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source.
Color	This field displays what color represents each source in the graph.
Attempts	This field displays the number of web site access attempts the device blocked from each source.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites was made from each source.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

10.3.8 Top Blocked Hosts Drill-Down

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

Click on a specific source in **Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts** to open this screen.

Figure 227 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts > Drill-Down



from 2011-04-01 to 2011-04-07 by Host 192.168.1.60

Report Type: Top Categories

Category	Color	Attempts	% of Attempts	View Logs
Spyware Effects/Privacy Concerns	■	1199	17.4%	🔍
Proxy Avoidance	■	1196	17.4%	🔍
Phishing	■	1194	17.4%	🔍
Spyware/Malware Sources	■	1193	17.3%	🔍
category1	■	594	8.6%	🔍
category19	■	301	4.4%	🔍
category9	■	301	4.4%	🔍
category24	■	300	4.4%	🔍
category8	■	300	4.4%	🔍
category3	■	300	4.4%	🔍
Total		6878	100%	

Each field is described in the following table.

Table 212 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Categories**, **Top Sites** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.

Table 212 Report > Security Policy Enforcement > Content Filter (Blocked) > Top Hosts > Drill-Down

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

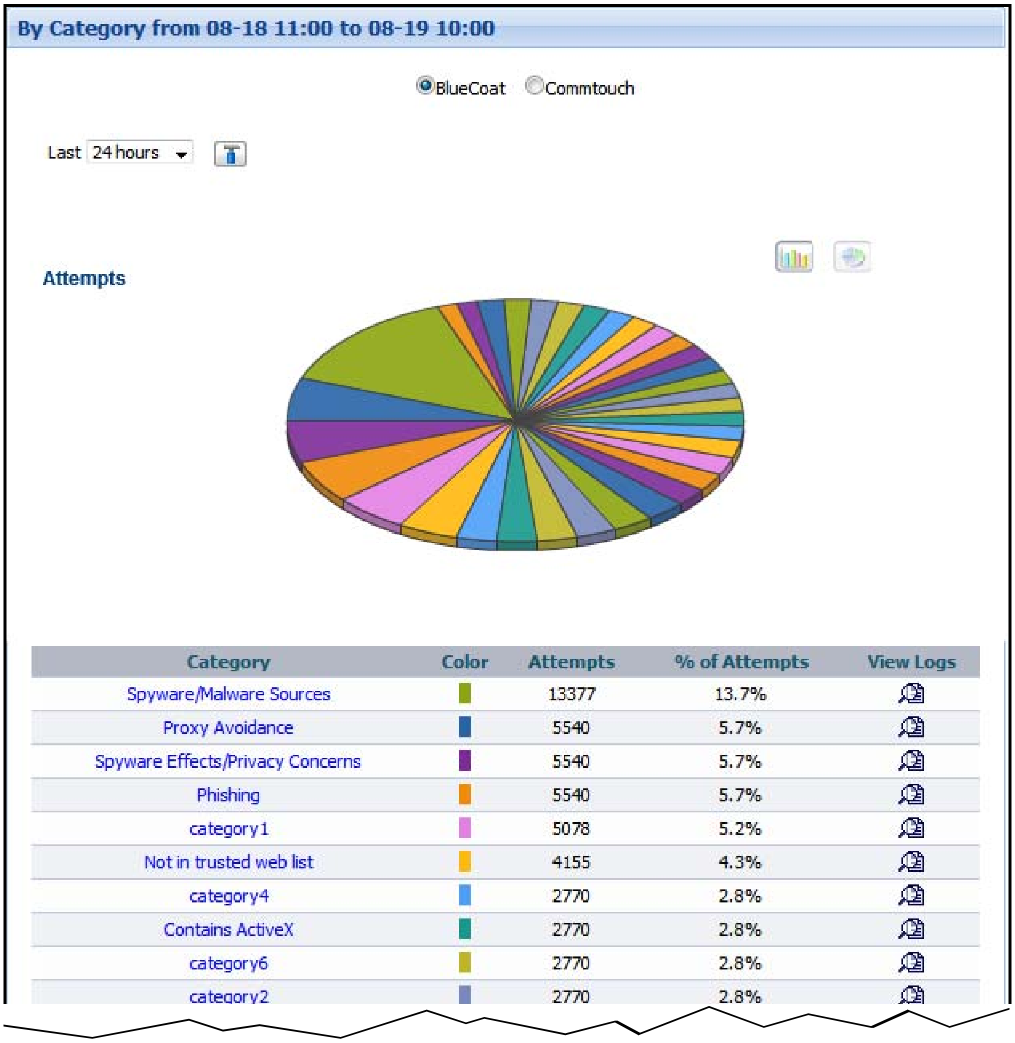
10.3.9 Blocked Web Categories

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

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

Click **Report > Security Policy Enforcement > Content Filter (Blocked) > By Category** to open this screen.

Figure 228 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category



By Category from 08-18 11:00 to 08-19 10:00

● BlueCoat ○ Commtouch

Last 24 hours

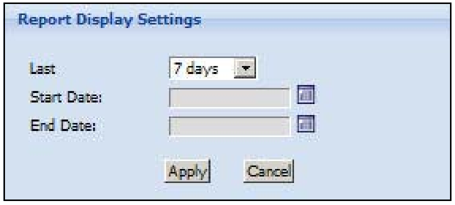
Category	Color	Attempts	% of Attempts	View Logs
Spyware/Malware Sources	■	13377	13.7%	🔍
Proxy Avoidance	■	5540	5.7%	🔍
Spyware Effects/Privacy Concerns	■	5540	5.7%	🔍
Phishing	■	5540	5.7%	🔍
category1	■	5078	5.2%	🔍
Not in trusted web list	■	4155	4.3%	🔍
category4	■	2770	2.8%	🔍
Contains ActiveX	■	2770	2.8%	🔍
category6	■	2770	2.8%	🔍
category2	■	2770	2.8%	🔍

Each field is described in the following table.

Table 213 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
BlueCoat/ Commtouch	Select the content filtering provider the device uses.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.

Table 213 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category

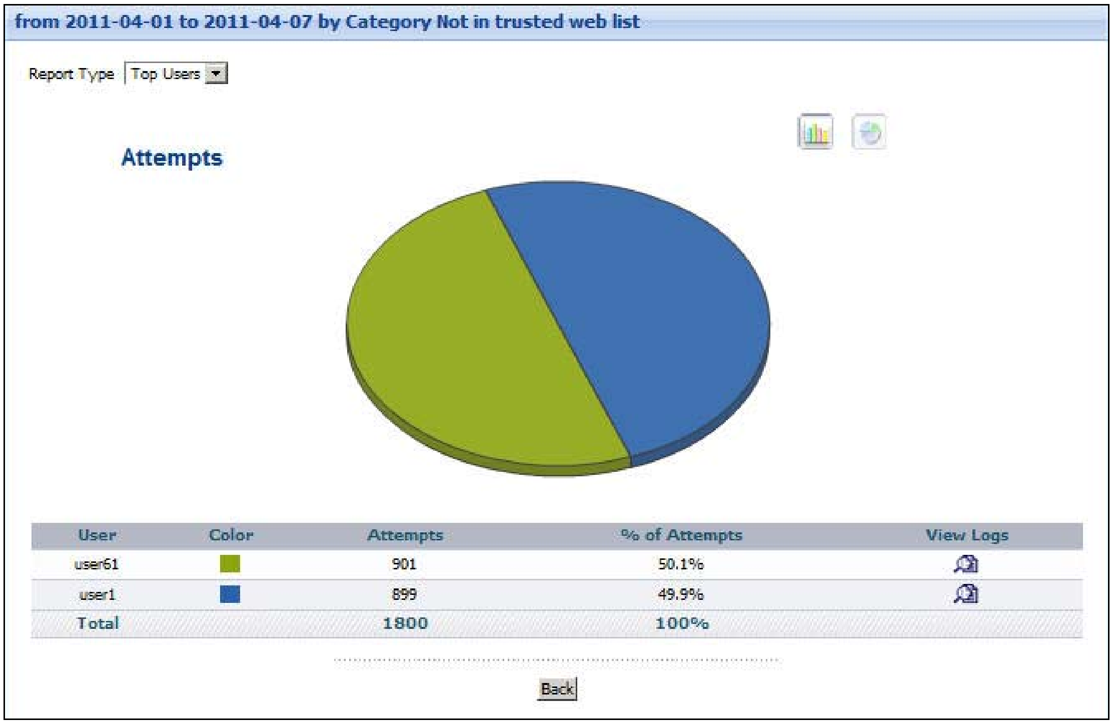
LABEL	DESCRIPTION
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Category	This field displays the categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. Click on a source to look at the destinations of blocked web traffic for the selected category.
Color	This field displays what color represents each category in the graph.
Attempts	This field displays the number of attempts to access allowed web sites in each category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites belong to each category.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the categories above.

10.3.10 Blocked Web Categories Drill-Down

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

Click on a specific category in **Report > Security Policy Enforcement > Content Filter (Blocked) > By Category** to open this screen.

Figure 229 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category > Drill-Down



from 2011-04-01 to 2011-04-07 by Category Not in trusted web list

Report Type: Top Users

Attempts

User	Color	Attempts	% of Attempts	View Logs
user61	🟩	901	50.1%	🔍
user1	🟦	899	49.9%	🔍
Total		1800	100%	

Each field is described in the following table.

Table 214 Report > Security Policy Enforcement > Content Filter (Blocked) > By Category > Drill-Down

LABEL	DESCRIPTION
title	This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields.
Report Type	Specify **Top Users**, **Top Sites**, **Top Hosts** or **By Hour** as the content to be displayed.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Site	This field displays the destinations of blocked web traffic that belongs to the selected category, sorted by the number of attempts to each one. Each destination is identified by its domain name.
Color	This field displays what color represents each destination in the graph.
Attempts	This field displays the number of attempts to each destination in the selected category.
% of Attempts	This field displays what percentage of all attempts to access blocked web sites in the selected category went to each destination.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the destinations above.
Back	Click this to return to the main report.

10.4 Application Access Control

These screens display the most-often blocked applications.

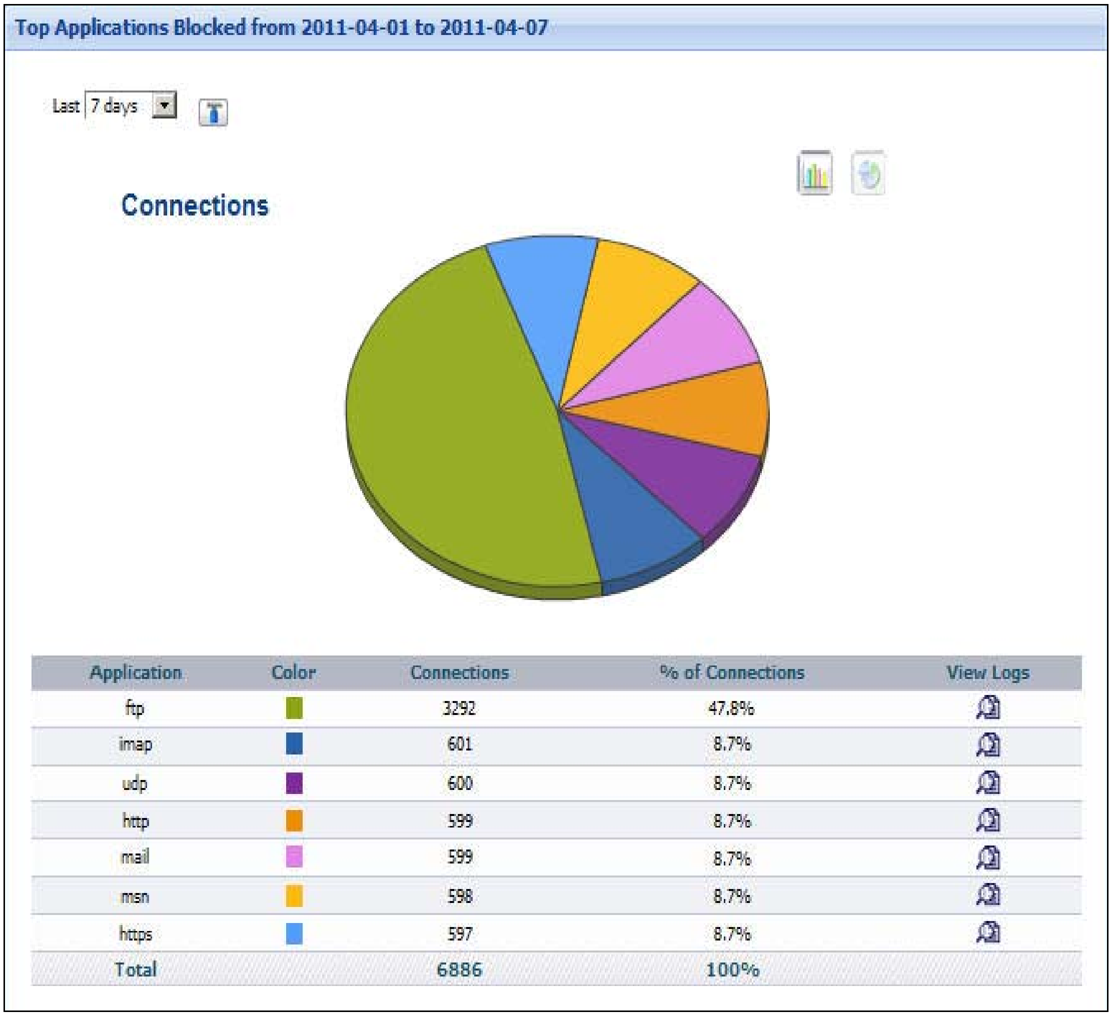
Note: To look at application access control reports, each ZyXEL device must record allowed applications and blocked applications and users in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Application Patrol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

10.4.1 Top Applications Blocked

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

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

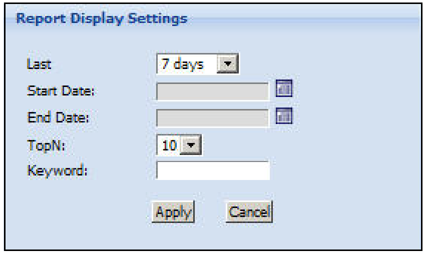
Figure 230 Report > Security Policy Enforcement > Application Access Control > Top Applications Blocked



Application	Color	Connections	% of Connections	View Logs
ftp	🟩	3292	47.8%	🔍
imap	🟦	601	8.7%	🔍
udp	🟪	600	8.7%	🔍
http	🟧	599	8.7%	🔍
mail	🟪	599	8.7%	🔍
msn	🟨	598	8.7%	🔍
https	🟦	597	8.7%	🔍
Total		6886	100%	

Each field is described in the following table.

Table 215 Report > Security Policy Enforcement > Application Access Control > Top Applications Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Application** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the name of the application for which the selected device blocked the most traffic, sorted by the amount of traffic for each one. If the number of applications is less than the maximum number of records displayed in this table, every application is displayed.
Color	This field displays what color represents each application in the graph.
Connections	This field displays the number of traffic events the device blocked for each application.
% of Connections	This field displays what percentage each application’s number of blocked connections makes out of the total number of blocked connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the applications above.

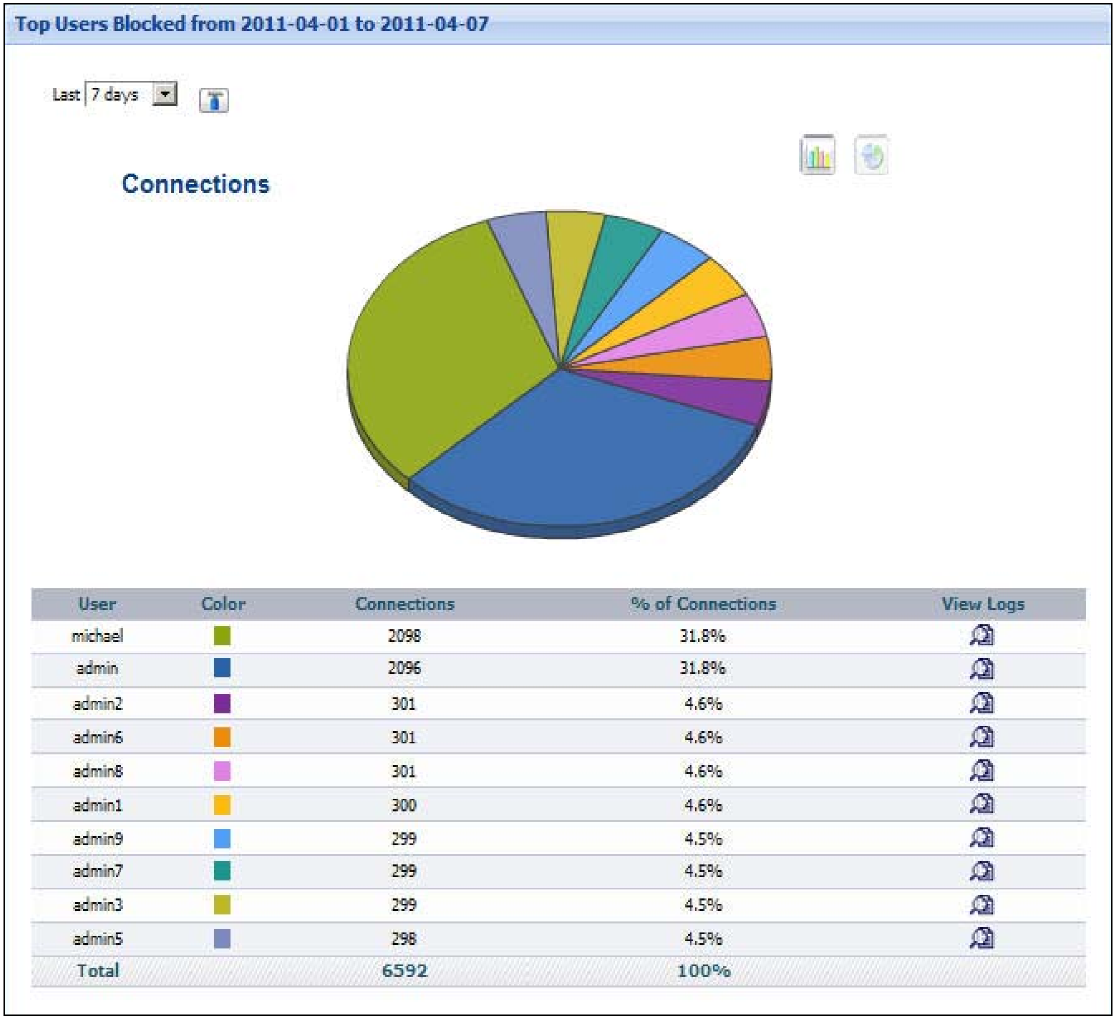
10.4.2 Top Users Blocked

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

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

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

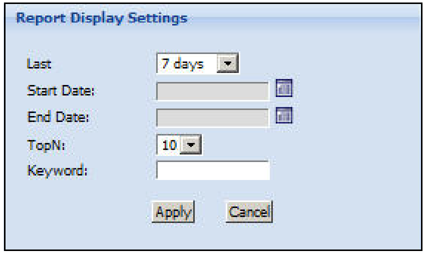
Figure 231 Report > Security Policy Enforcement > Application Access Control > Top Users Blocked



User	Color	Connections	% of Connections	View Logs
michael	🟩	2098	31.8%	🔍
admin	🟦	2096	31.8%	🔍
admin2	🟪	301	4.6%	🔍
admin6	🟧	301	4.6%	🔍
admin8	🟪	301	4.6%	🔍
admin1	🟨	300	4.6%	🔍
admin9	🟦	299	4.5%	🔍
admin7	🟩	299	4.5%	🔍
admin3	🟨	299	4.5%	🔍
admin5	🟪	298	4.5%	🔍
Total		6592	100%	

Each field is described in the following table.

Table 216 Report > Security Policy Enforcement > Application Access Control > Top Users Blocked

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the users from which the selected device’s application patrol blocked the most traffic, sorted by the amount of traffic for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
Color	This field displays what color represents each user in the graph.
Connections	This field displays the number of traffic events the device blocked for each user.
% of Connections	This field displays what percentage each user’s number of blocked connections makes out of the total number of blocked connections that match the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the users above.

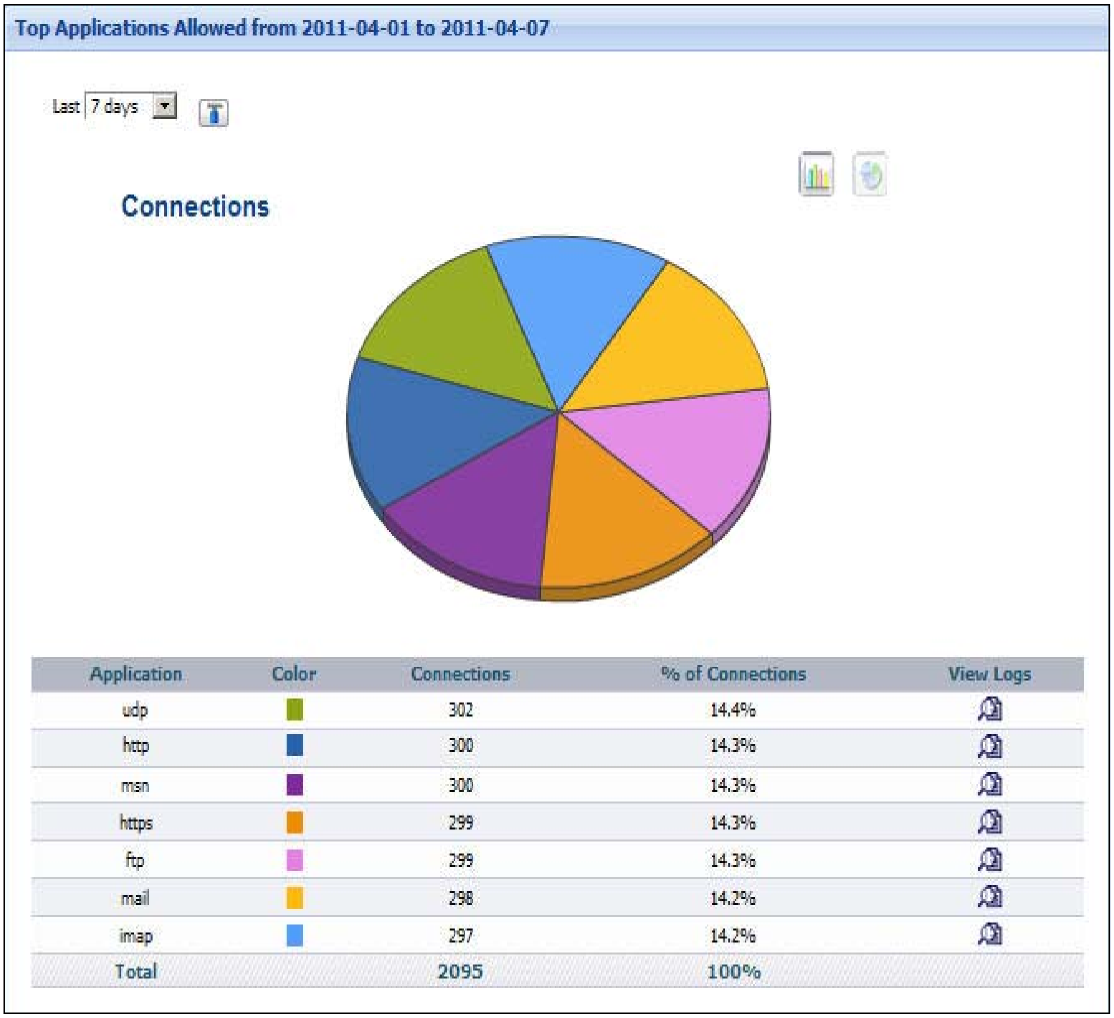
10.4.3 Top Applications Allowed

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

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

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

Figure 232 Report > Security Policy Enforcement > Application Access Control > Top Applications Allowed

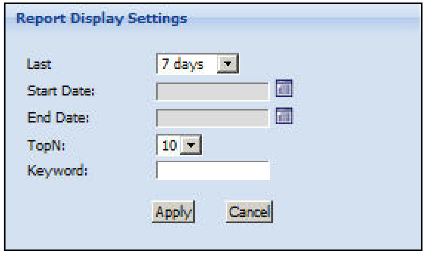


Top Applications Allowed from 2011-04-01 to 2011-04-07

Application	Color	Connections	% of Connections	View Logs
udp	🟩	302	14.4%	🔍
http	🟦	300	14.3%	🔍
msn	🟪	300	14.3%	🔍
https	🟧	299	14.3%	🔍
ftp	🟪	299	14.3%	🔍
mail	🟨	298	14.2%	🔍
imap	🟦	297	14.2%	🔍
Total		2095	100%	

Each field is described in the following table.

Table 217 Report > Security Policy Enforcement > Application Access Control > Top Applications Allowed

LABEL	DESCRIPTION
title	This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select.
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Application** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Application	This field displays the name of the application for which the selected device permitted connections, sorted by the number of connections for each one.
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.

11

Event

Here is how you can check on logins, sessions per host, and DHCP leasing.

11.1 Login

This chapter discusses how you can check who successfully logged into the ZyXEL device or who tried to log in but failed.

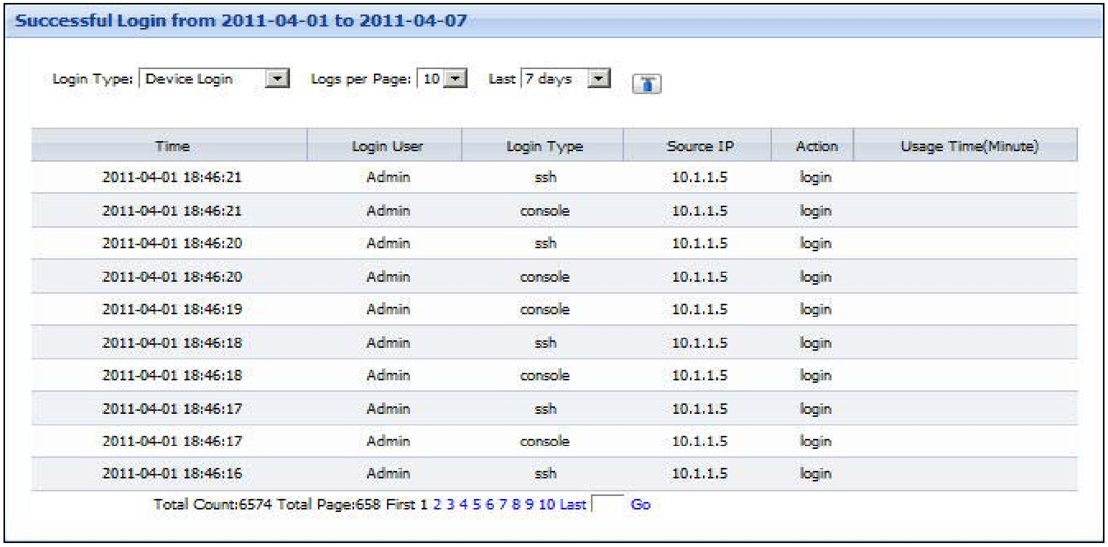
11.1.1 Successful Logins

Use this screen to look at who successfully logged into the ZyXEL device. See Section 2.6 on page 22 for more information about the source data used by the report.

Note: To use the authentication screens, each ZyXEL device must record authentication successes and failures in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **System Maintenance** is enabled.

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

Figure 233 Report > Event > Login > Successful Login



Successful Login from 2011-04-01 to 2011-04-07

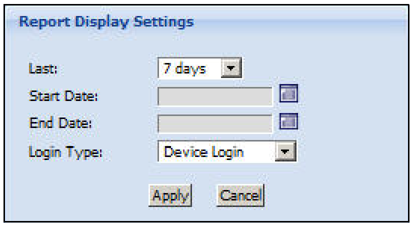
Login Type: Device Login Logs per Page: 10 Last 7 days

Time	Login User	Login Type	Source IP	Action	Usage Time(Minute)
2011-04-01 18:46:21	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:21	Admin	console	10.1.1.5	login	
2011-04-01 18:46:20	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:20	Admin	console	10.1.1.5	login	
2011-04-01 18:46:19	Admin	console	10.1.1.5	login	
2011-04-01 18:46:18	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:18	Admin	console	10.1.1.5	login	
2011-04-01 18:46:17	Admin	ssh	10.1.1.5	login	
2011-04-01 18:46:17	Admin	console	10.1.1.5	login	
2011-04-01 18:46:16	Admin	ssh	10.1.1.5	login	

Total Count:6574 Total Page:658 First 1 2 3 4 5 6 7 8 9 10 Last Go

Each field is described in the following table.

Table 218 Report > Event > Login > Successful Login

LABEL	DESCRIPTION
Login Type	Select **Device Login** to display a list of successful management logins to the ZyXEL device. Select **UserAware Login** to display a list of successful user logins to the ZyXEL device (to use the ZyXEL device's features such as Internet access or Secure Remote Access tunnels). This field is not available with all models.
Last	Select how many more days of information, ending with current information today, you want to look at. Select **1** if you only want to look at today's information.
Settings	Click this if you want to specify the select any **Start Date** and **End Date**. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: Login Type: Device Login Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. The **Login Type** field is the same as in the main screen. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Time	This field displays the time the Vantage Report server received the log entry from the ZyXEL device, not the time the user logged into the device.
Login User	This field displays who logged into the selected device.
Login Type	This field displays what type of connection the user used to log into the device.
Source IP	This field displays the IP address of the computer the user used to log into the selected device.
Action	This field displays if it it is a **login** or **logout** operation.
Usage Time (Minute)	This field displays the time that elapses between the login and logout operation.
Total Count	This field displays how many records there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the records.
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**.

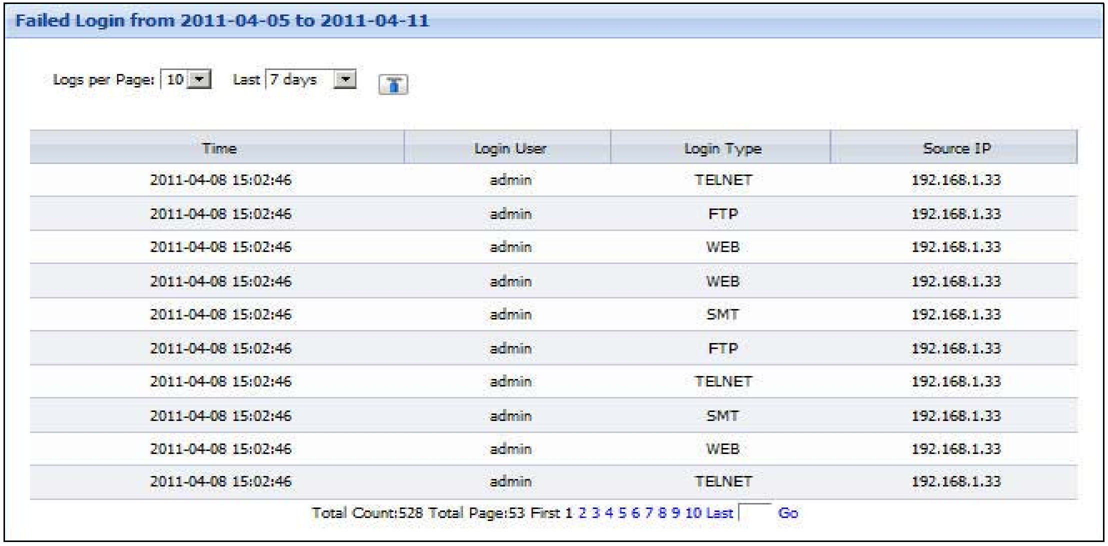
11.1.2 Failed Logins

Use this screen to look at who tried to log in into the ZyXEL device (for management or monitoring purposes) but failed. See Section 2.6 on page 22 for more information about the source data used by the report.

Note: To use the authentication screens, each ZyXEL device must record authentication successes and failures in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **System Maintenance** is enabled.

Click **Report > Event > Login > Failed Login** to open the **Failed Login** screen.

Figure 234 Report > Event > Login > Failed Login



Failed Login from 2011-04-05 to 2011-04-11

Logs per Page: 10 Last 7 days

Time	Login User	Login Type	Source IP
2011-04-08 15:02:46	admin	TELNET	192.168.1.33
2011-04-08 15:02:46	admin	FTP	192.168.1.33
2011-04-08 15:02:46	admin	WEB	192.168.1.33
2011-04-08 15:02:46	admin	WEB	192.168.1.33
2011-04-08 15:02:46	admin	SMT	192.168.1.33
2011-04-08 15:02:46	admin	FTP	192.168.1.33
2011-04-08 15:02:46	admin	TELNET	192.168.1.33
2011-04-08 15:02:46	admin	SMT	192.168.1.33
2011-04-08 15:02:46	admin	WEB	192.168.1.33
2011-04-08 15:02:46	admin	TELNET	192.168.1.33

Total Count:528 Total Page:53 First 1 2 3 4 5 6 7 8 9 10 Last Go

Each field is described in the following table.

Table 219 Report > Event > Device Login > Failed Login

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

11.2 Sessions Per Host

Use these screens to see which hosts and users have most frequently gone over the maximum number of NAT sessions per host.

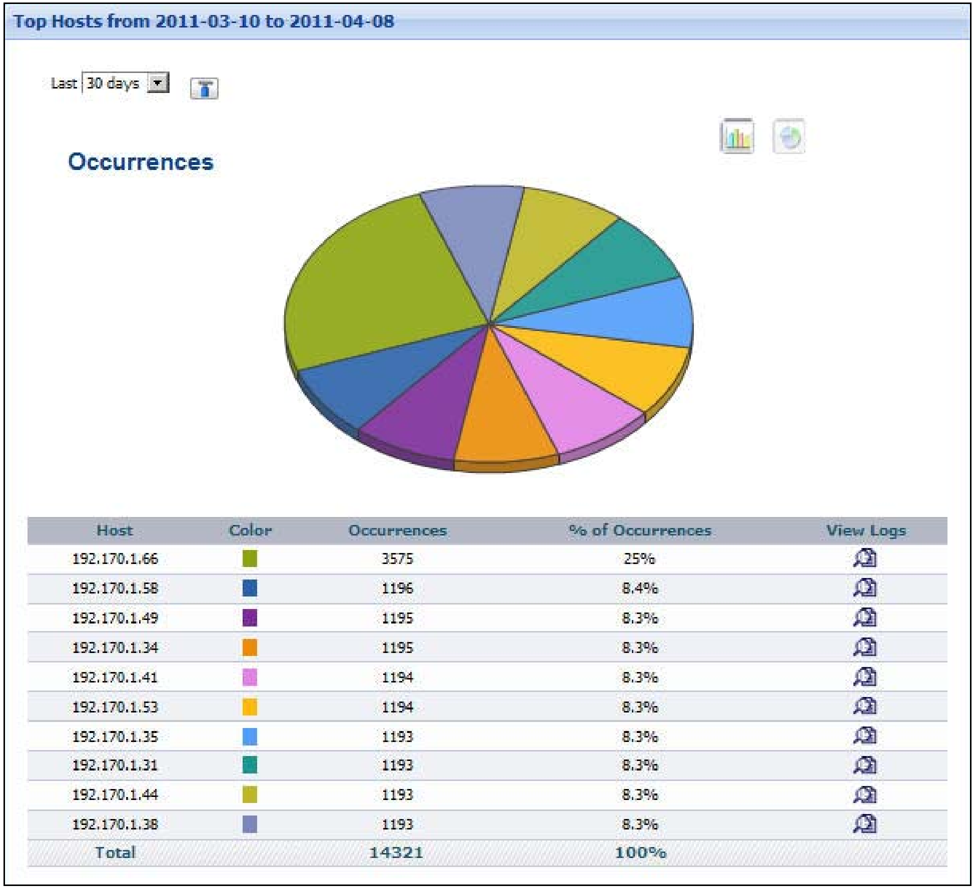
11.2.1 Top Sessions Per Host

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

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

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

Figure 235 Report > Event > Session Per Host > Top Hosts



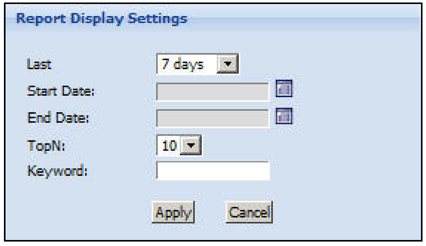
Top Hosts from 2011-03-10 to 2011-04-08

Last 30 days

Host	Color	Occurrences	% of Occurrences	View Logs
192.170.1.66	🟩	3575	25%	🔍
192.170.1.58	🟦	1196	8.4%	🔍
192.170.1.49	🟪	1195	8.3%	🔍
192.170.1.34	🟧	1195	8.3%	🔍
192.170.1.41	🟪	1194	8.3%	🔍
192.170.1.53	🟨	1194	8.3%	🔍
192.170.1.35	🟦	1193	8.3%	🔍
192.170.1.31	🟩	1193	8.3%	🔍
192.170.1.44	🟨	1193	8.3%	🔍
192.170.1.38	🟦	1193	8.3%	🔍
Total		14321	100%	

Each field is described in the following table.

Table 220 Report > Event > Session Per Host > Top Hosts

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources that have gone over the selected device's maximum number of NAT sessions per host, sorted by the number of occurrences for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed. Each source is identified by its IP address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the IP address.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of times each source has gone over the selected device's maximum number of NAT sessions per host.
% of Occurrences	This field displays what percentage each source's number of times it has exceeded the selected device's maximum number of NAT sessions per host makes out of the total number of times that it has occurred within the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

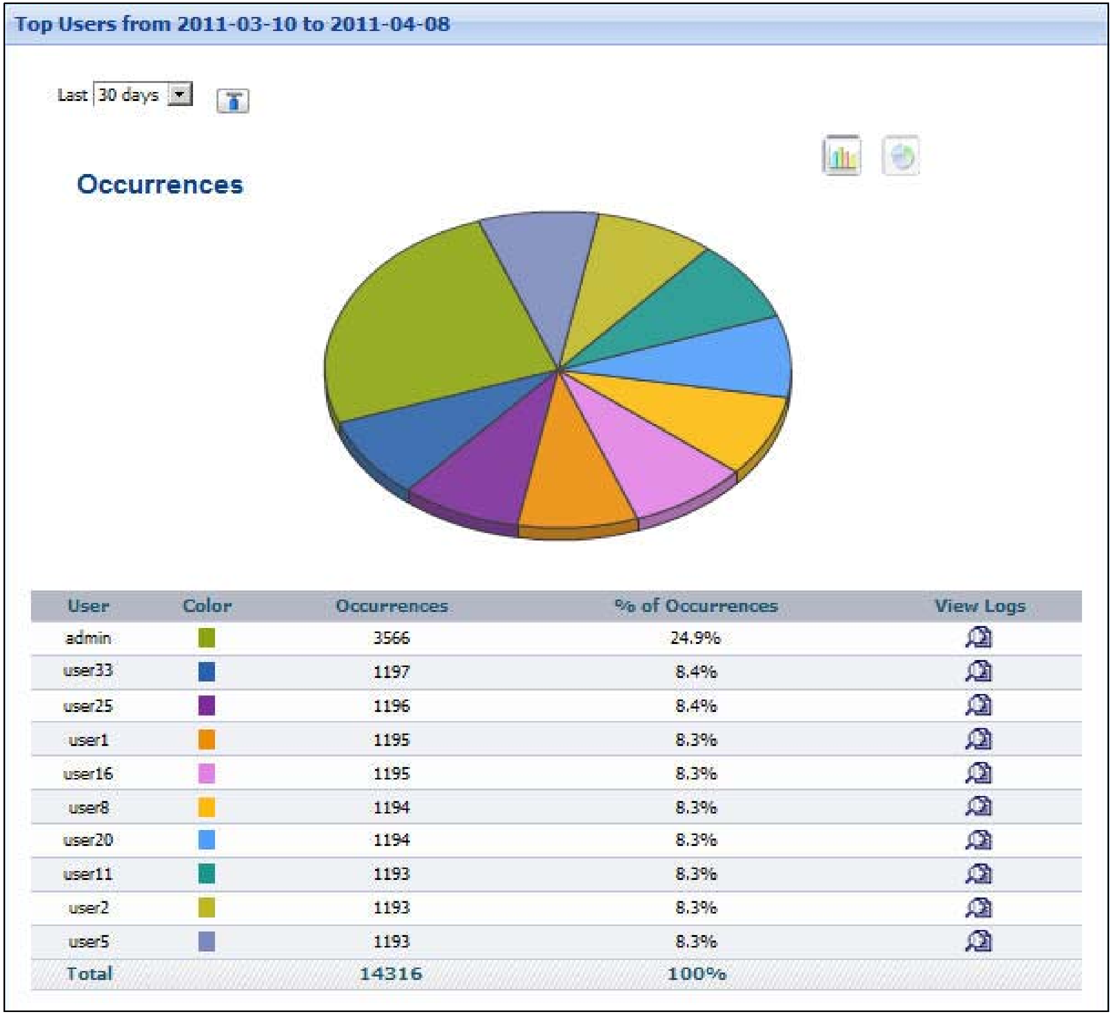
11.3 Top Sessions Per User

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

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

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

Figure 236 Report > Event > Session Per Host > Top Users

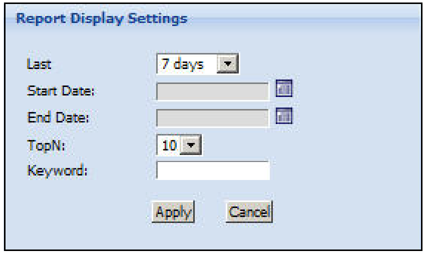


Top Users from 2011-03-10 to 2011-04-08

User	Color	Occurrences	% of Occurrences	View Logs
admin	■	3566	24.9%	🔍
user33	■	1197	8.4%	🔍
user25	■	1196	8.4%	🔍
user1	■	1195	8.3%	🔍
user16	■	1195	8.3%	🔍
user8	■	1194	8.3%	🔍
user20	■	1194	8.3%	🔍
user11	■	1193	8.3%	🔍
user2	■	1193	8.3%	🔍
user5	■	1193	8.3%	🔍
Total		14316	100%	

Each field is described in the following table.

Table 221 Report > Event > Session Per Host > Top Users

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **User** field. You can use any printable ASCII characters except the ’ and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
User	This field displays the top users that have gone over the selected device’s maximum number of NAT sessions per host, sorted by the number of occurrences for each one. If the number of users is less than the maximum number of records displayed in this table, every user is displayed. Each user is identified by user name.
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.

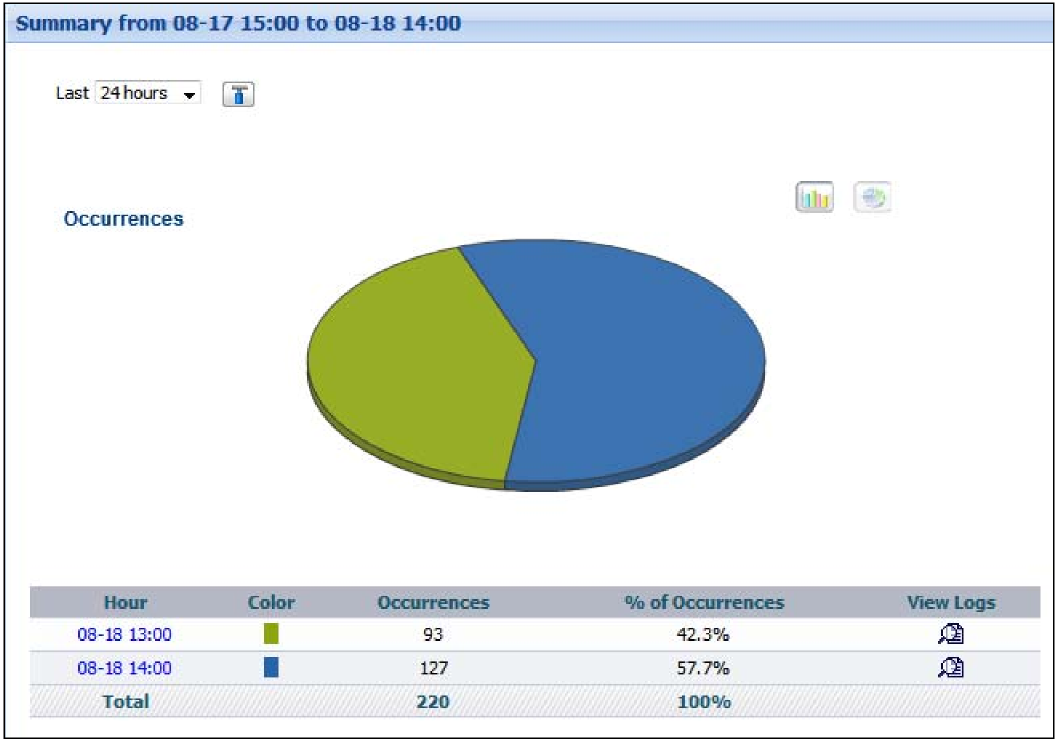
11.4 DHCP Leasing Summary

Use these screens to monitor the number of DHCP requests and the number of DHCP requests from individual computers during a time period.

11.4.1 DHCP Leasing Summary

Click **Report** > **Event > DHCP Leasing > Summary** to open this screen. Use this screen to monitor the number of DHCP requests over a time period. For a given working day, it should normally appear as many DHCP requests in the morning, and fewer throughout the day. If not (if requests are erratic) it may indicate a virus infection.

Figure 237 Report > Event > DHCP Leasing > Summary



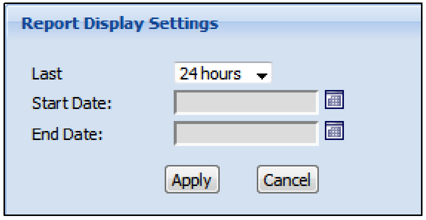
Summary from 08-17 15:00 to 08-18 14:00

Last 24 hours

Hour	Color	Occurrences	% of Occurrences	View Logs
08-18 13:00	🟩	93	42.3%	🔍
08-18 14:00	🟦	127	57.7%	🔍
Total		220	100%	

Each field is described in the following table.

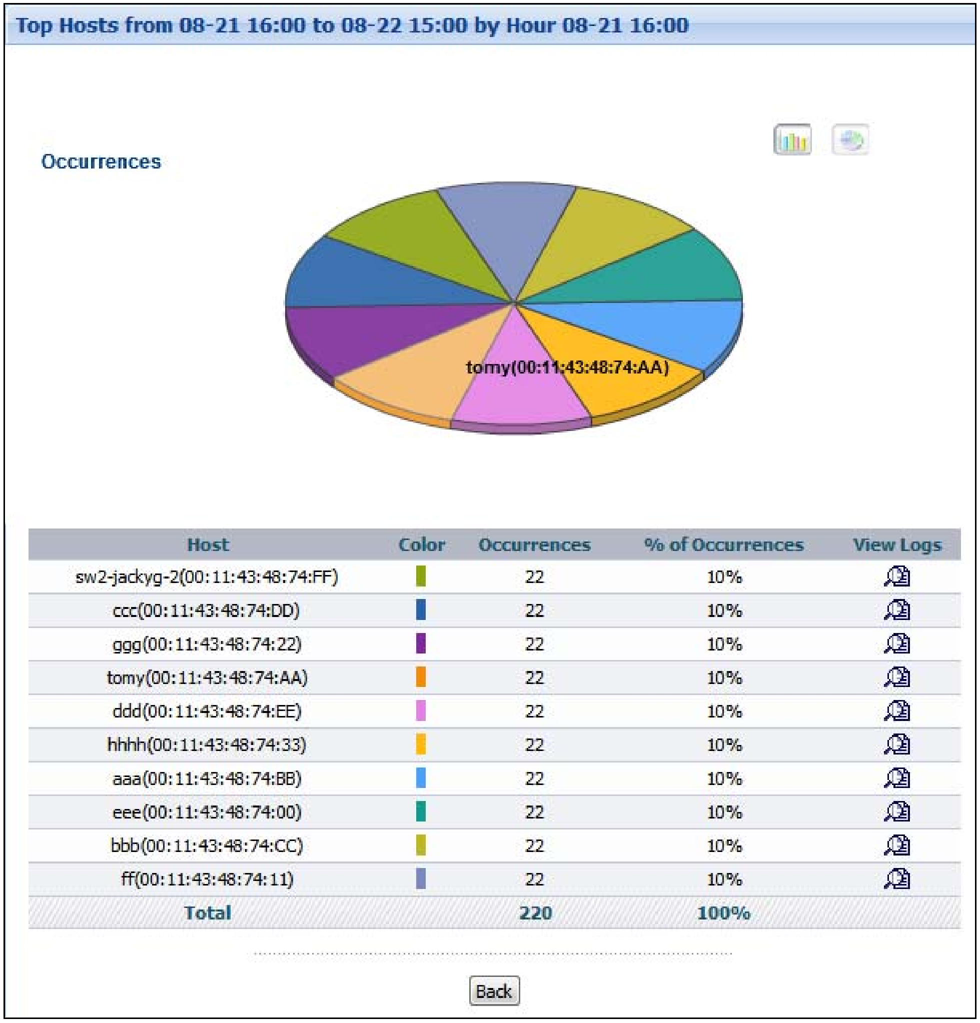
Table 222 Report > Event > DHCP Leasing > Summary

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: 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. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour	This field displays the various 1-hour periods displayed in the graph.
Color	This field displays what color represents each user in the graph.
Occurrences	This field displays the number of DHCP requests detected by the device during the specified hour.
% of Occurrences	This field displays what percentage each hour's number of DHCP requests makes out of the total number of DHCP requests that have 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.

11.4.2 DHCP Leasing Summary Drill-Down

Click on a specific time interval in **Report** > **Event > DHCP Leasing > Summary** to open this screen. Use this screen to see the hosts that sent the most DHCP requests during the time period and how many each sent.

Figure 238 Report > Event > DHCP Leasing > Summary > Drill-Down

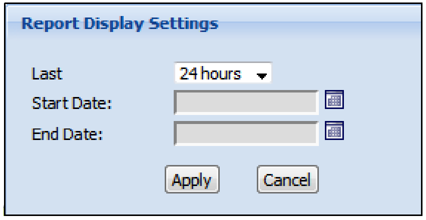


Top Hosts from 08-21 16:00 to 08-22 15:00 by Hour 08-21 16:00

Host	Color	Occurrences	% of Occurrences	View Logs
sw2-jackyg-2(00:11:43:48:74:FF)	🟩	22	10%	🔍
ccc(00:11:43:48:74:DD)	🟦	22	10%	🔍
ggg(00:11:43:48:74:22)	🟪	22	10%	🔍
tomy(00:11:43:48:74:AA)	🟧	22	10%	🔍
ddd(00:11:43:48:74:EE)	🟪	22	10%	🔍
hhhh(00:11:43:48:74:33)	🟨	22	10%	🔍
aaa(00:11:43:48:74:BB)	🟦	22	10%	🔍
eee(00:11:43:48:74:00)	🟩	22	10%	🔍
bbb(00:11:43:48:74:CC)	🟨	22	10%	🔍
ff(00:11:43:48:74:11)	🟦	22	10%	🔍
Total		220	100%	

Each field is described in the following table.

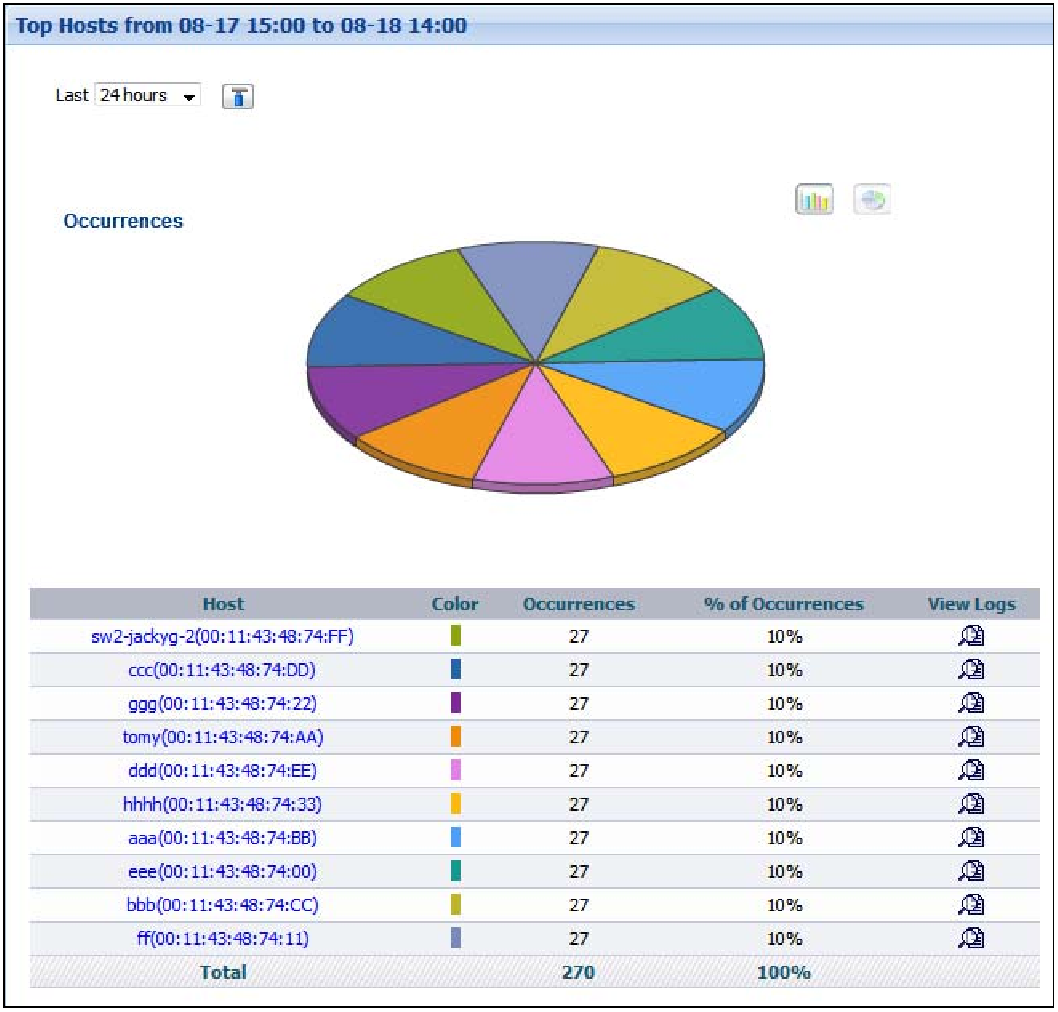
Table 223 Report > Event > DHCP Leasing > Summary > Drill-Down

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 24 hours Start Date: End Date: 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. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of DHCP requests, 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 MAC address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the MAC address.
Color	This field displays what color represents each user in the graph.
Occurrences	This field displays the number of DHCP requests detected by the device during the specified hour.
% of Occurrences	This field displays what percentage each hour's number of DHCP requests makes out of the total number of DHCP requests that have 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.

11.4.3 DHCP Leasing Top Hosts

Click **Report** > **Event > DHCP Leasing > Top Hosts** to open this screen. Use this screen to see the hosts that sent the most DHCP request over a time period.

Figure 239 Report > Event > DHCP Leasing > Top Hosts



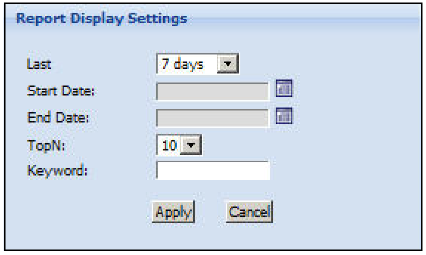
Top Hosts from 08-17 15:00 to 08-18 14:00

Last 24 hours

Host	Color	Occurrences	% of Occurrences	View Logs
sw2-jackyg-2(00:11:43:48:74:FF)	■	27	10%	
ccc(00:11:43:48:74:DD)	■	27	10%	
ggg(00:11:43:48:74:22)	■	27	10%	
tomy(00:11:43:48:74:AA)	■	27	10%	
ddd(00:11:43:48:74:EE)	■	27	10%	
hhhh(00:11:43:48:74:33)	■	27	10%	
aaa(00:11:43:48:74:BB)	■	27	10%	
eee(00:11:43:48:74:00)	■	27	10%	
bbb(00:11:43:48:74:CC)	■	27	10%	
ff(00:11:43:48:74:11)	■	27	10%	
Total		270	100%	

Each field is described in the following table.

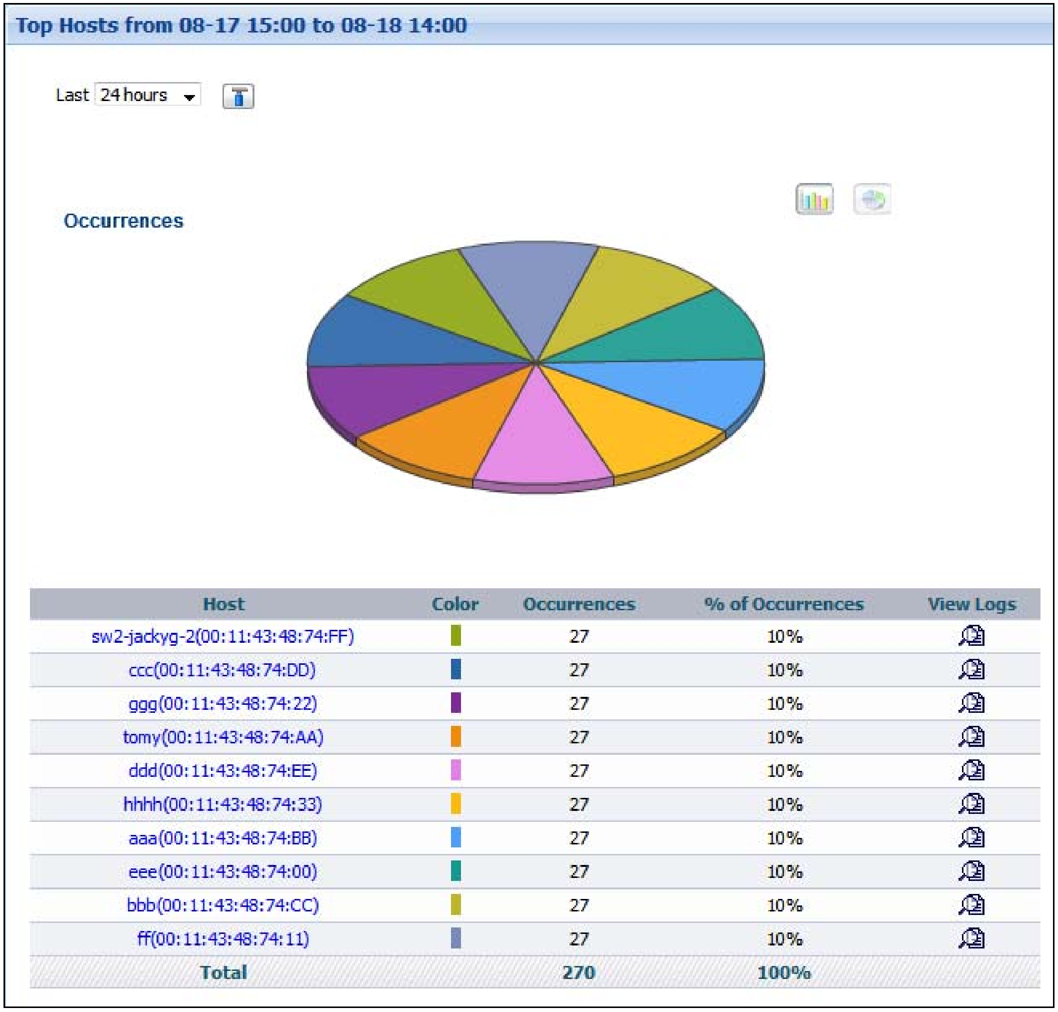
Table 224 Report > Event > DHCP Leasing > Top Hosts

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Host	This field displays the top sources of DHCP requests, 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 MAC address. If **Hostname Reverse** is enabled in **System** > **General Configuration**, the table displays the host name, if identifiable, with the MAC address.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of times each source has sent DHCP requests.
% of Occurrences	This field displays what percentage each source's number of times it has sent DHCP requests makes out of the total number of DHCP requests that have occurred within the settings you displayed in this report.
View Logs	Click this icon to see the logs that go with the record.
Total	This entry displays the totals for the sources above.

11.4.4 DHCP Leasing Top Hosts Drill-Down

Click on a specific host in **Report** > **Event > DHCP Leasing > Top Hosts** to open this screen. Use this screen to see how many DHCP requests the host sent every hour.

Figure 240 Report > Event > DHCP Leasing > Top Hosts > Drill-Down



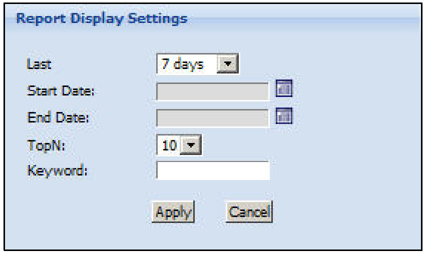
Top Hosts from 08-17 15:00 to 08-18 14:00

Last 24 hours

Host	Color	Occurrences	% of Occurrences	View Logs
sw2-jackyg-2(00:11:43:48:74:FF)	■	27	10%	🔍
ccc(00:11:43:48:74:DD)	■	27	10%	🔍
ggg(00:11:43:48:74:22)	■	27	10%	🔍
tomy(00:11:43:48:74:AA)	■	27	10%	🔍
ddd(00:11:43:48:74:EE)	■	27	10%	🔍
hhhh(00:11:43:48:74:33)	■	27	10%	🔍
aaa(00:11:43:48:74:BB)	■	27	10%	🔍
eee(00:11:43:48:74:00)	■	27	10%	🔍
bbb(00:11:43:48:74:CC)	■	27	10%	🔍
ff(00:11:43:48:74:11)	■	27	10%	🔍
Total		**270**	**100%**	

Each field is described in the following table.

Table 225 Report > Event > DHCP Leasing > Top Hosts > Drill-Down

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Last: 7 days Start Date: End Date: TopN: 10 Keyword: Apply Cancel Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. **TopN**: select the number of records that you want to display. For example, select 10 to display the first 10 records. **Keyword**: enter part or all of any value you want to look for in the **Host** field. You can use any printable ASCII characters except the ' and %. The search is case-insensitive. These fields reset to the default values when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
graph	The graph displays the information in the table visually. • Click the **Pie View** or the **Bar View** icon. You can specify the **Default Chart Type** in **System** > **General Configuration**. • Move your mouse over a slice in the pie chart or a bar in the bar chart to display its identification. • Click on a slice in the pie chart to move it away from the pie chart a little.
Hour	This field displays the various 1-hour periods displayed in the graph.
Color	This field displays what color represents each source in the graph.
Occurrences	This field displays the number of times each source has sent DHCP requests.
% of Occurrences	This field displays what percentage each source's number of times it has sent DHCP requests makes out of the total number of DHCP requests that have 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.

12

Schedule Report

This chapter discusses how you can use the **Report > Schedule Report** screen to set up and maintain daily, weekly, and one-time reports that Vantage Report sends by e-mail. See Section 2.2 on page 20 for more information about e-mail in Vantage Report. Use the template screens to add and edit report templates.

Note: To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 14.2 on page 461 for more information.

Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report saves three days of information, weekly reports only consist of information from these three days, not seven days. See Section 14.1 on page 457 for more information.

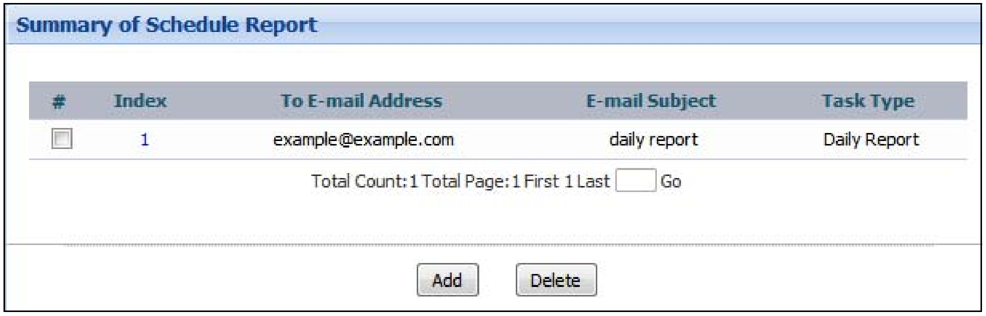
This feature can send e-mail messages with very large attachments (2+ MB). Some SMTP mail servers might not accept such large messages. In this case, there is a way to send e-mail messages without the attachments. See the **E-mail Attached Files** option in any of the **Customize ... Report** screens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

12.1 Scheduled Report Summary Screen

Use this screen to see the list of existing scheduled reports. Use the **Add** button to create new reports.

Click **Report > Schedule Report > Summary**. The following screen appears.

Figure 241 Report > Schedule Report > Summary



Summary of Schedule Report

#	Index	To E-mail Address	E-mail Subject	Task Type
□	1	example@example.com	daily report	Daily Report

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

Each field is described in the following table.

Table 226 Report > Schedule Report > Summary

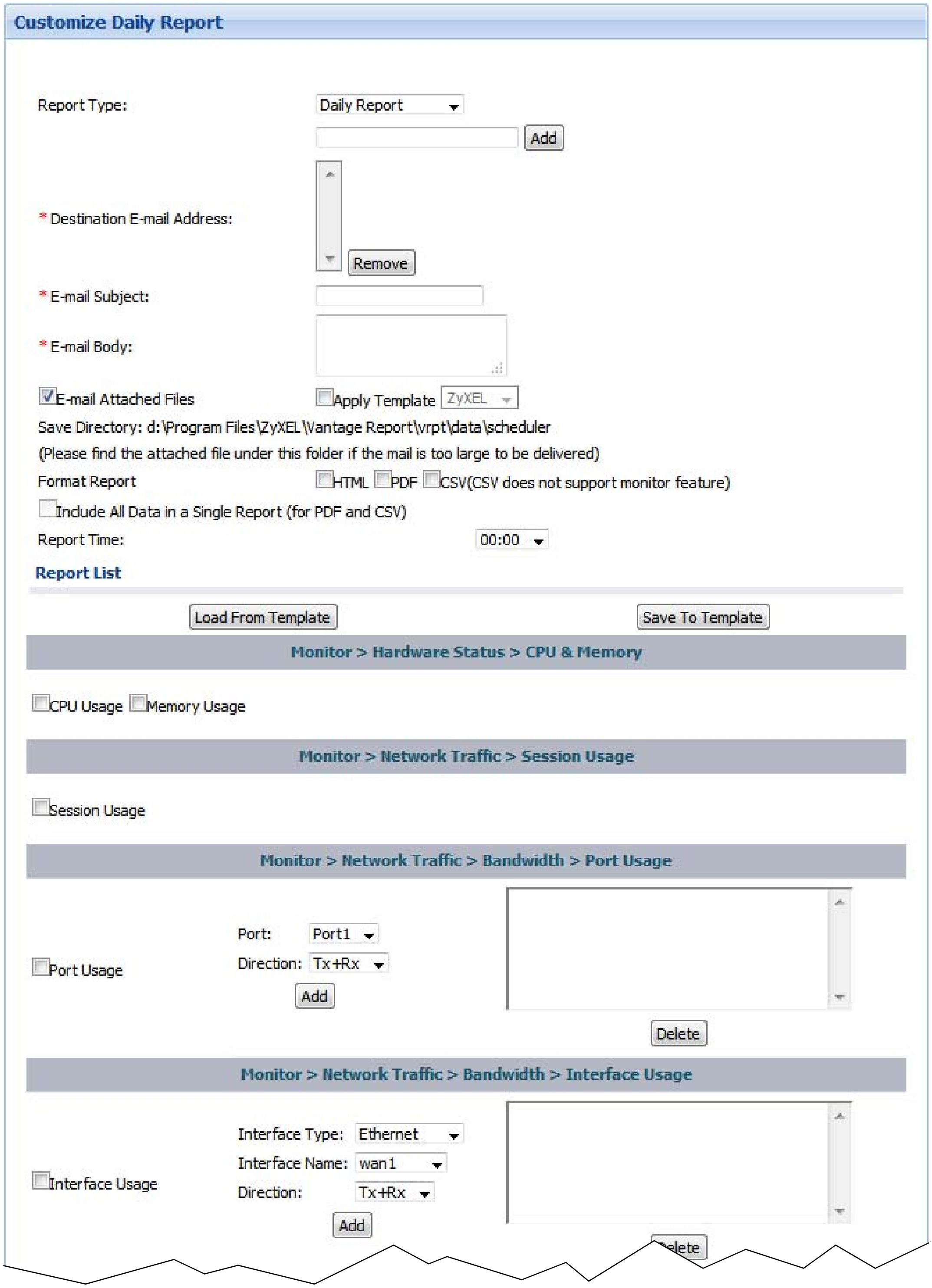
LABEL	DESCRIPTION
#	Select this check box, and click **Delete** to delete the scheduled report.
Index	Click it to edit the scheduled report next to it. The **Customize Scheduled Report** screen appears. Otherwise, this field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
To E-mail Address	This field displays the first e-mail address to which the scheduled report is sent. If there are more, this field displays a couple of punctuation marks at the end.
E-mail Subject	This field displays the subject line in the e-mail message Vantage Report sends.
Task Type	This field displays what type of scheduled report this is.
Total Count	This field displays how many scheduled reports there are.
Total Page	This field displays how many screens it takes to display all the scheduled reports.
First .. Last	Click **First**, **Last**, or a specific page number to look at the scheduled reports on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click **Go**.
Add	Click this to generate and send one or more statistical reports daily, weekly or in a time interval.The **Customize Scheduled Report** screen appears.
Delete	Click this to delete the selected scheduled report.

12.2 Customize Daily Report Screen

Use this screen to configure the Vantage Report to maintain and send daily reports.

Click **Report > Schedule Report > Summary**. Either click on the index number of the entry you want to edit or click **Add.** Choose **Daily Report** in the **Report Type**. The following screen appears.

Figure 242 Report > Schedule Report > Summary > Add (Daily Report)



Customize Daily Report

Report Type: Daily Report

Add

* Destination E-mail Address:

Remove

* E-mail Subject:

* E-mail Body:

☑ E-mail Attached Files □ Apply Template ZyXEL

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

(Please find the attached file under this folder if the mail is too large to be delivered)

Format Report □ HTML □ PDF □ CSV(CSV does not support monitor feature)

□ Include All Data in a Single Report (for PDF and CSV)

Report Time: 00:00

Report List

Load From Template Save To Template

Monitor > Hardware Status > CPU & Memory

□ CPU Usage □ Memory Usage

Monitor > Network Traffic > Session Usage

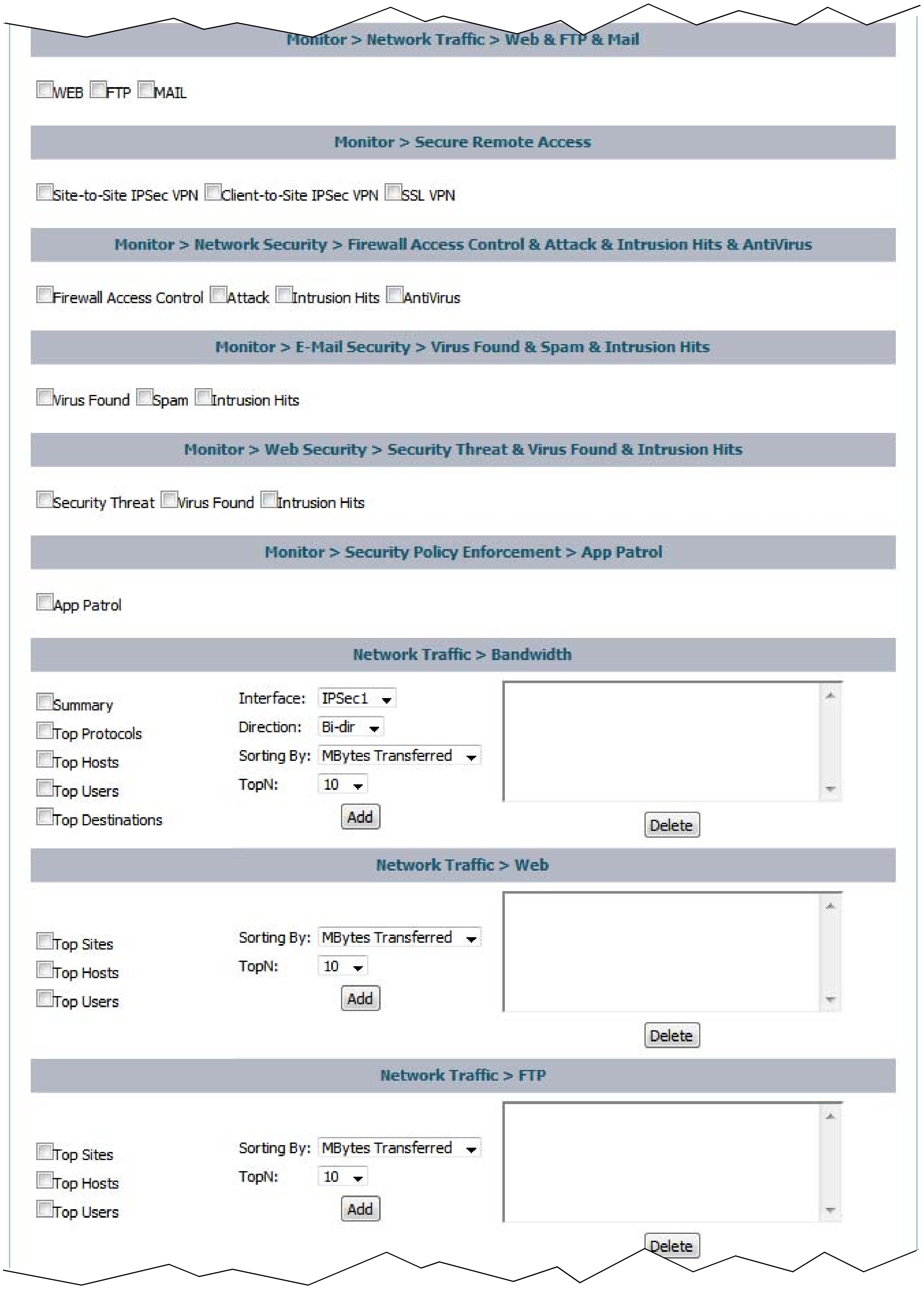
□ Session Usage

Monitor > Network Traffic > Bandwidth > Port Usage

□ Port Usage Port: Port1 Direction: Tx+Rx Add Delete

Monitor > Network Traffic > Bandwidth > Interface Usage

□ Interface Usage Interface Type: Ethernet Interface Name: wan1 Direction: Tx+Rx Add Delete



Monitor > Network Traffic > Web & FTP & Mail

□ WEB □ FTP □ MAIL

Monitor > Secure Remote Access

□ Site-to-Site IPSec VPN □ Client-to-Site IPSec VPN □ SSL VPN

Monitor > Network Security > Firewall Access Control & Attack & Intrusion Hits & AntiVirus

□ Firewall Access Control □ Attack □ Intrusion Hits □ AntiVirus

Monitor > E-Mail Security > Virus Found & Spam & Intrusion Hits

□ Virus Found □ Spam □ Intrusion Hits

Monitor > Web Security > Security Threat & Virus Found & Intrusion Hits

□ Security Threat □ Virus Found □ Intrusion Hits

Monitor > Security Policy Enforcement > App Patrol

□ App Patrol

Network Traffic > Bandwidth

□ Summary
□ Top Protocols
□ Top Hosts
□ Top Users
□ Top Destinations

Interface: IPSec1
Direction: Bi-dir
Sorting By: MBytes Transferred
TopN: 10

Network Traffic > Web

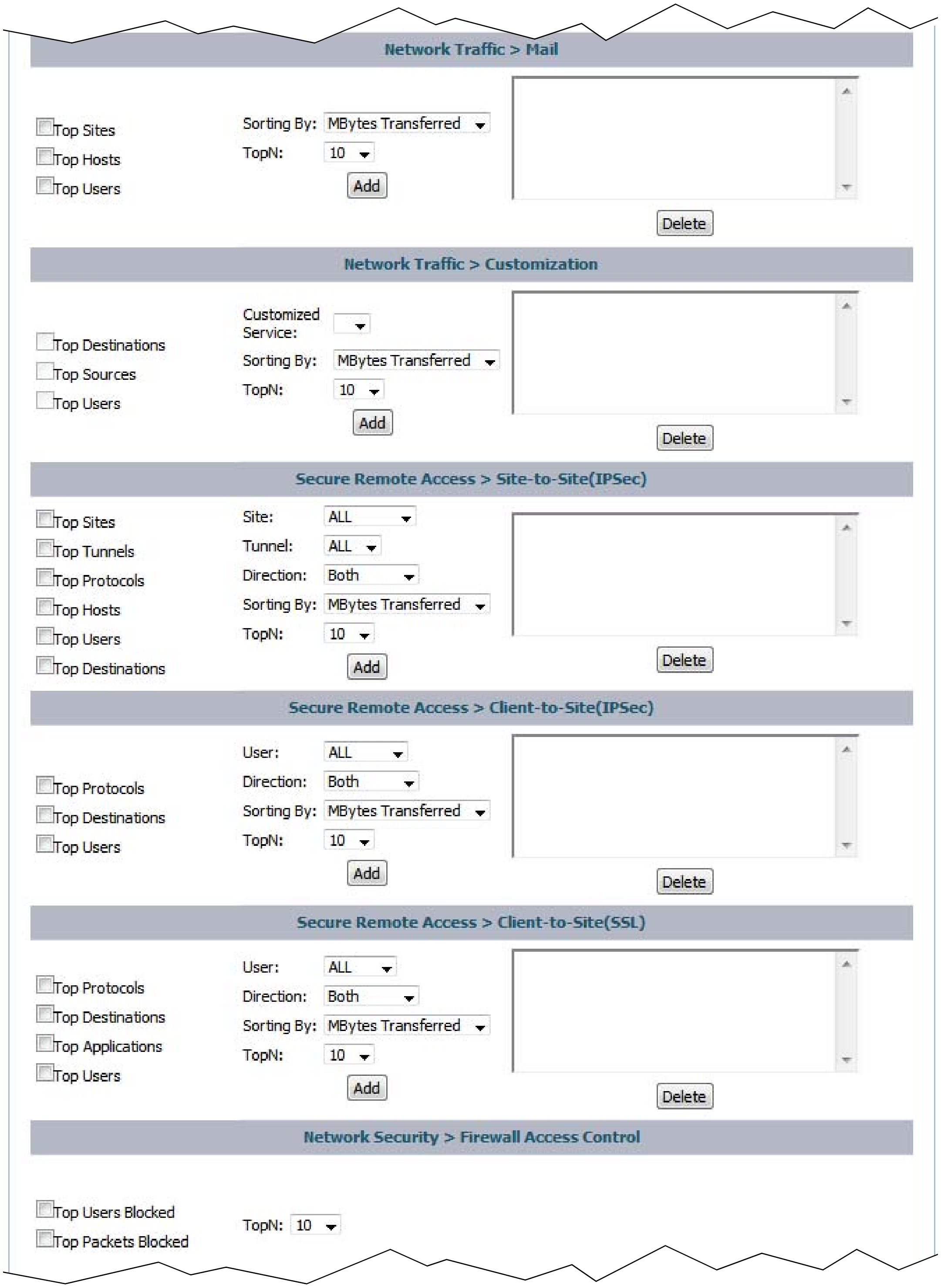
□ Top Sites
□ Top Hosts
□ Top Users

Sorting By: MBytes Transferred
TopN: 10

Network Traffic > FTP

□ Top Sites
□ Top Hosts
□ Top Users

Sorting By: MBytes Transferred
TopN: 10



Network Traffic > Mail

☐ Top Sites
☐ Top Hosts
☐ Top Users

Sorting By: MBytes Transferred
TopN: 10

Network Traffic > Customization

☐ Top Destinations
☐ Top Sources
☐ Top Users

Customized Service:
Sorting By: MBytes Transferred
TopN: 10

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

☐ Top Sites
☐ Top Tunnels
☐ Top Protocols
☐ Top Hosts
☐ Top Users
☐ Top Destinations

Site: ALL
Tunnel: ALL
Direction: Both
Sorting By: MBytes Transferred
TopN: 10

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

☐ Top Protocols
☐ Top Destinations
☐ Top Users

User: ALL
Direction: Both
Sorting By: MBytes Transferred
TopN: 10

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

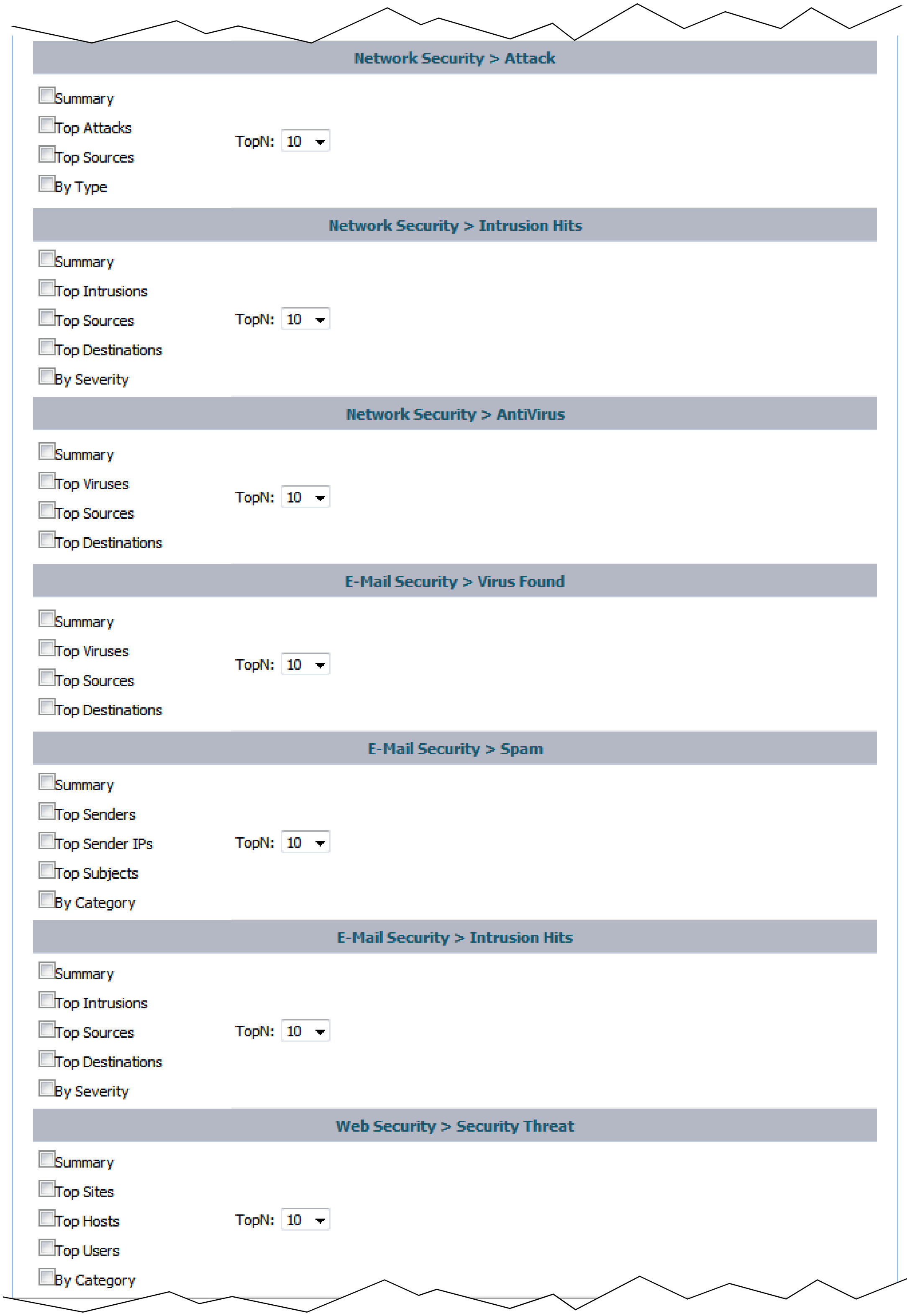
☐ Top Protocols
☐ Top Destinations
☐ Top Applications
☐ Top Users

User: ALL
Direction: Both
Sorting By: MBytes Transferred
TopN: 10

Network Security > Firewall Access Control

☐ Top Users Blocked
☐ Top Packets Blocked

TopN: 10



Network Security > Attack

□ Summary
□ Top Attacks
□ Top Sources
□ By Type

TopN: 10

Network Security > Intrusion Hits

□ Summary
□ Top Intrusions
□ Top Sources
□ Top Destinations
□ By Severity

TopN: 10

Network Security > AntiVirus

□ Summary
□ Top Viruses
□ Top Sources
□ Top Destinations

TopN: 10

E-Mail Security > Virus Found

□ Summary
□ Top Viruses
□ Top Sources
□ Top Destinations

TopN: 10

E-Mail Security > Spam

□ Summary
□ Top Senders
□ Top Sender IPs
□ Top Subjects
□ By Category

TopN: 10

E-Mail Security > Intrusion Hits

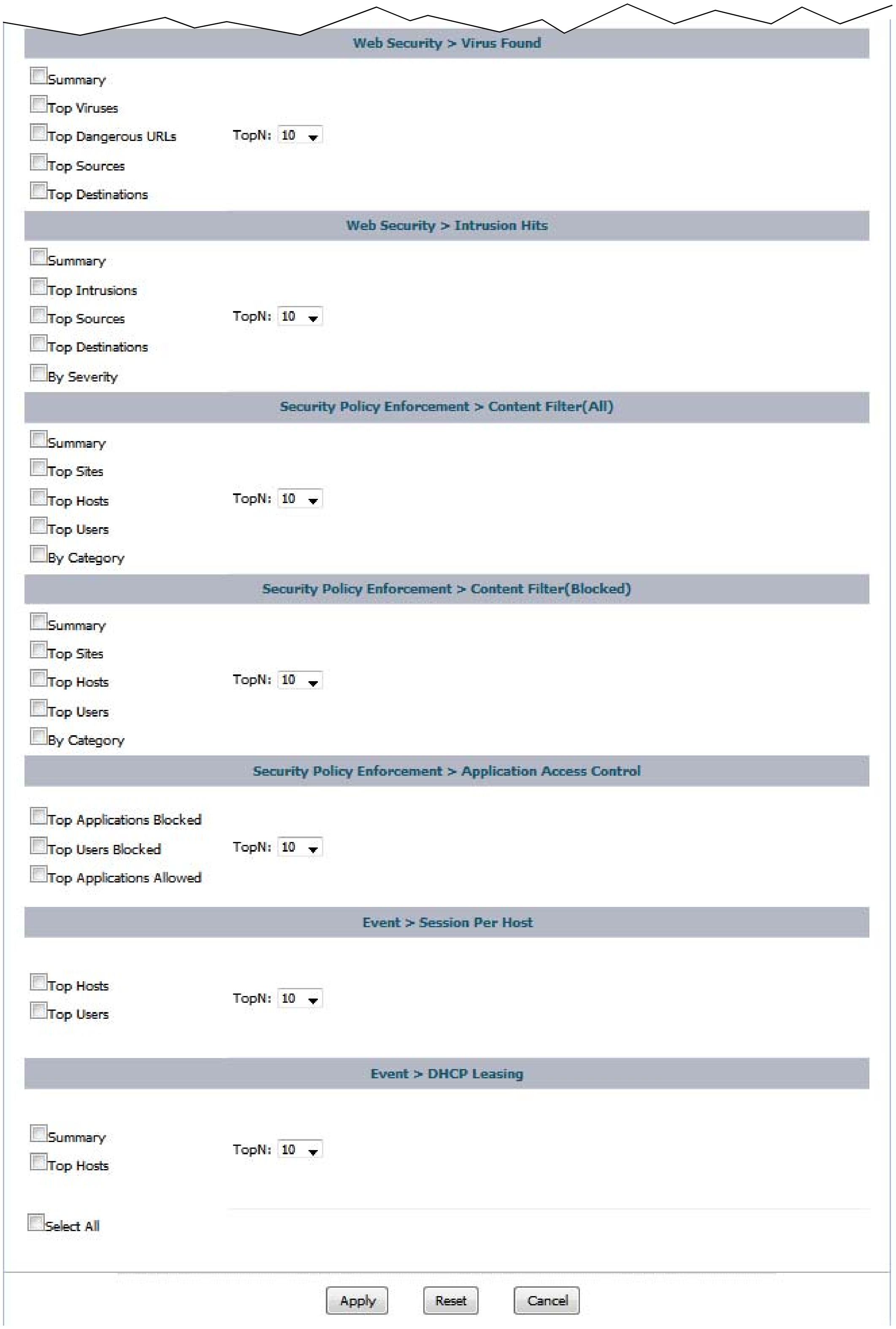
□ Summary
□ Top Intrusions
□ Top Sources
□ Top Destinations
□ By Severity

TopN: 10

Web Security > Security Threat

□ Summary
□ Top Sites
□ Top Hosts
□ Top Users
□ By Category

TopN: 10



Web Security > Virus Found

□ Summary
□ Top Viruses
□ Top Dangerous URLs
□ Top Sources
□ Top Destinations

TopN: 10

Web Security > Intrusion Hits

□ Summary
□ Top Intrusions
□ Top Sources
□ Top Destinations
□ By Severity

TopN: 10

Security Policy Enforcement > Content Filter(All)

□ Summary
□ Top Sites
□ Top Hosts
□ Top Users
□ By Category

TopN: 10

Security Policy Enforcement > Content Filter(Blocked)

□ Summary
□ Top Sites
□ Top Hosts
□ Top Users
□ By Category

TopN: 10

Security Policy Enforcement > Application Access Control

□ Top Applications Blocked
□ Top Users Blocked
□ Top Applications Allowed

TopN: 10

Event > Session Per Host

□ Top Hosts
□ Top Users

TopN: 10

Event > DHCP Leasing

□ Summary
□ Top Hosts

TopN: 10

□ Select All

Each field is described in the following table.

Table 227 Report > Schedule Report > Summary > Add

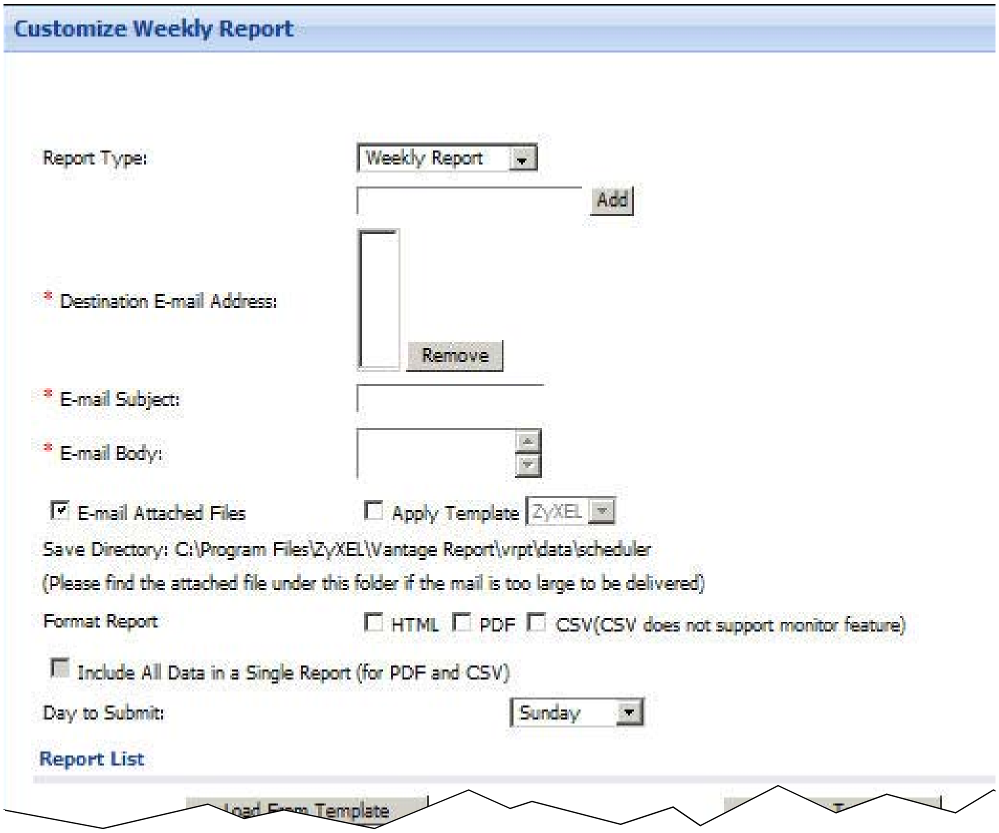
LABEL	DESCRIPTION
Report Type	Choose **Daily Report** in this field.
Add	Enter the e-mail address(es) to which Vantage Report sends the selected report(s). Use a comma to separate each e-mail address and click **Add**. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Destination E-mail Address	The list of e-mail addresses you enter appears here. Select one and click **Remove** to delete that e-mail address from the list.
E-mail Subject	Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
E-mail Body	Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long.
E-mail Attached Files	Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. These report(s) are stored in `data\scheduler` in the Vantage Report installation directory.
Apply Template	Select the check box and a template if you want to use a customized report format.
Save Directory	This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is.
Format Report	Select the format(s) of the selected report(s). HTML format looks like the statistical reports you can see online.
Include All Data in a Single Report	This field is enabled if you selected PDF format. Select this if you want to combine all the selected report(s) into one file.
Report Time	Select the hour to start generating the report. Vantage Report sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having Vantage Report generate too many reports at the same time can affect performance. It is recommended that you vary the times for your reports.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report.
Load From Template	Click this to select a preconfigured template for a scheduled report.
Save To Template	Click this to save the daily report configuration as a template for future use.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.3 Customize Weekly Report Screen

Use this screen to configure the Vantage Report to maintain and send weekly reports.

Click **Report > Schedule Report > Summary**. Either click on the index number of the entry you want to edit or click **Add**. Choose **Weekly Report** in the **Report Type**. The following screen appears.

Figure 243 Report > Schedule Report > Summary > Add (Weekly Report)



Customize Weekly Report

Report Type: Weekly Report

* Destination E-mail Address:

* E-mail Subject:

* E-mail Body:

☑ E-mail Attached Files ☐ Apply Template ZyXEL

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

(Please find the attached file under this folder if the mail is too large to be delivered)

Format Report ☐ HTML ☐ PDF ☐ CSV(CSV does not support monitor feature)

☐ Include All Data in a Single Report (for PDF and CSV)

Day to Submit: Sunday

Report List

Each field is described in the following table.

Table 228 Report > Schedule Report > Summary > Add (Weekly Report)

LABEL	DESCRIPTION
Report Type	Choose **Weekly Report** in this field.
Add	Enter the e-mail address(es) to which Vantage Report sends the selected report(s) and click **Add**. Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Destination E-mail Address	The list of e-mail addresses you enter appear here. Select one and click **Remove** to delete that e-mail address from the list.

Table 228 Report > Schedule Report > Summary > Add (Weekly Report)

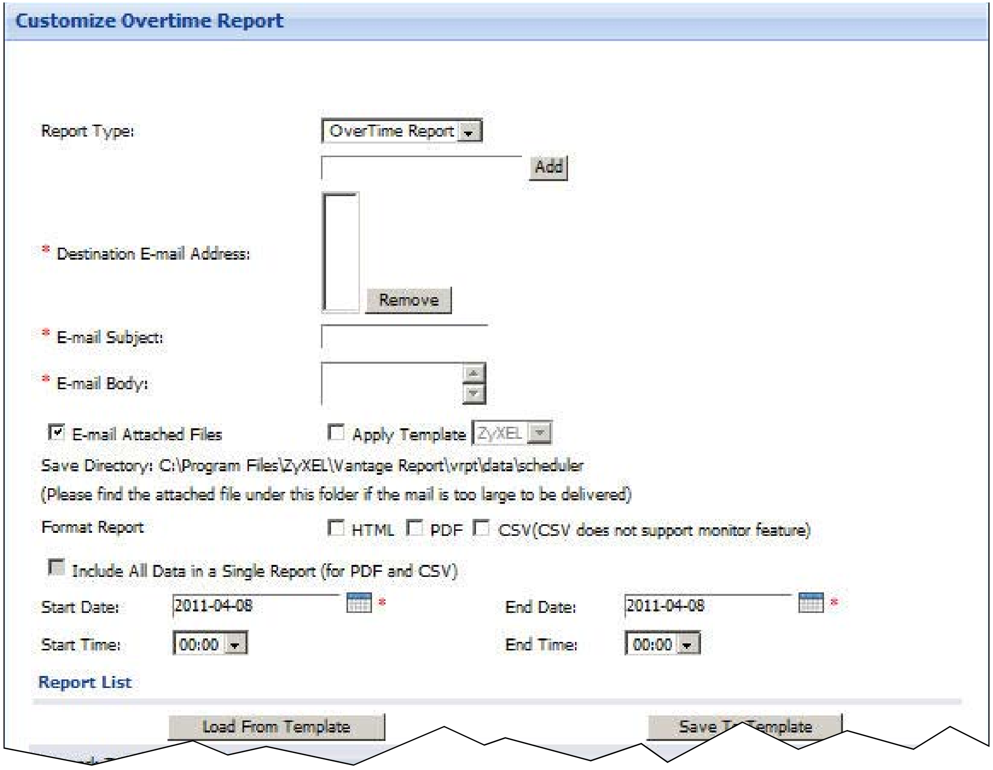
LABEL	DESCRIPTION
E-mail Subject	Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
E-mail Body	Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long.
E-mail Attached Files	Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. These report(s) are stored in `data\scheduler` in the Vantage Report installation directory.
Apply Template	Select the check box and a template if you want to use a customized report format.
Save Directory	This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is.
Day to Submit	Select the day of the week to generate and send the selected report(s).
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report. Refer to Figure 242 on page 426 for the full view of Report List.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.4 Customize Overtime Report Screen

Use this screen to configure the Vantage Report to maintain and send reports during a specified period of time.

Click **Report > Schedule Report > Summary**. Either click on the index number of the entry you want to edit or click **Add.** Choose **OverTime Report** in the **Report Type**. The following screen appears.

Figure 244 Report > Schedule Report > Summary > Add (Overtime Report)



Customize Overtime Report

Report Type: OverTime Report

Add

* Destination E-mail Address:

Remove

* E-mail Subject:

* E-mail Body:

☑ E-mail Attached Files □ Apply Template ZyXEL

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

(Please find the attached file under this folder if the mail is too large to be delivered)

Format Report □ HTML □ PDF □ CSV(CSV does not support monitor feature)

□ Include All Data in a Single Report (for PDF and CSV)

Start Date: 2011-04-08 * End Date: 2011-04-08 *

Start Time: 00:00 End Time: 00:00

Report List

Load From Template Save To Template

Each field is described in the following table.

Table 229 Report > Schedule Report > Summary > Add (Overtime Report)

LABEL	DESCRIPTION
Report Type	Choose **OverTime Report** in this field.
Add	Enter the e-mail address(es) to which Vantage Report sends the selected report(s) and click **Add**. Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want. Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value.
Destination E-mail Address	The list of e-mail addresses you enter appear here. Select one and click **Remove** to delete that e-mail address from the list.
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 229 Report > Schedule Report > Summary > Add (Overtime Report)

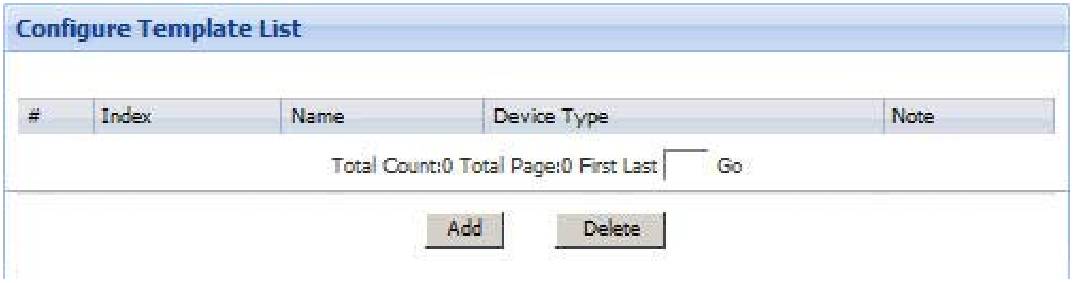
LABEL	DESCRIPTION
E-mail Attached Files	Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. These report(s) are stored in `data\scheduler` in the Vantage Report installation directory.
Apply Template	Select the check box and a template if you want to use a customized report format.
Save Directory	This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is.
Start Date	Select the day to start collecting information for the selected report(s).
End Date	Select the day to stop collecting information for the selected report(s).
Start Time	Select the hour to start collecting information for the selected report(s). Vantage Report starts collecting information at the beginning of this hour.
End Time	Select the hour to stop collecting information for the selected report(s). Vantage Report stops collecting information at the end of this hour and generates the report. Vantage Report sends the report after it finishes generating it. The report generation time depends on the amount of information in the report. Having Vantage Report generate too many reports at the same time can affect performance.
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report. Refer to Figure 242 on page 426 for the full view of Report List.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.5 Configure Template List

Use this screen to see a list of report templates that provides what kind of details are available in reports.

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

Figure 245 Report > Schedule Report > Configure Template



Configure Template List

#	Index	Name	Device Type	Note

Total Count:0 Total Page:0 First Last [ ] Go

Each field is described in the following table.

Table 230 Report > Schedule Report > Configure Template

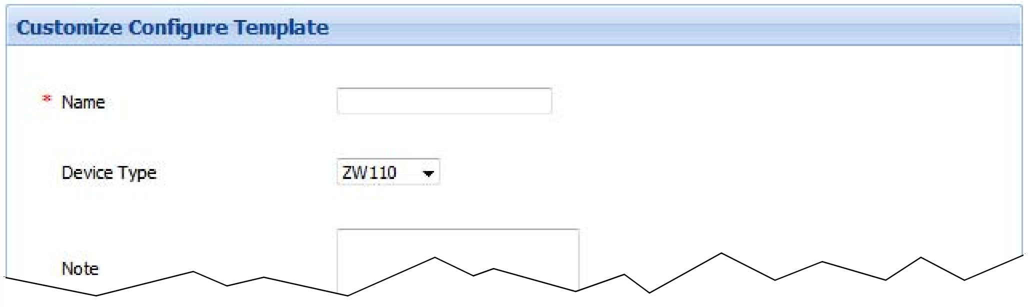
LABEL	DESCRIPTION
#	Select this check box, and click **Delete** to delete the report template.
Index	This is the number of this template in the list. This field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered.
Name	This is the name that identifies the template inside Vantage Report. Click it to edit the template.
Device Type	This field displays which device this template can be generated for.
Note	This is a short description of the template.
Total Count	This field displays how many report templates there are.
Total Page	This field displays how many screens it takes to display all the scheduled reports.
First .. Last	Click **First**, **Last**, or a specific page number to look at the scheduled reports on that page. Some choices are not available, depending on the number of pages.s
Go	Enter the page number you want to see, and click **Go**.
Add	Click this to go to another screen to create a new report template.
Delete	Select the check box next to a template and click delete to remove the report template.

12.6 Template Add/Edit

Use this screen to customize a scheduled report template for a particular ZyXEL Device.

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

Figure 246 Report > Schedule Report > Configure Template > Add



Each field is described in the following table.

Table 231 Report > Schedule Report > Configure Template > Add

LABEL	DESCRIPTION
Name	Enter a name to identify the template inside Vantage Report. Numbers (0-9), letters (a-z A-Z), periods (.) and the underscore (_) are allowed. Spaces are not allowed. The name must start with a number or letter. Use up to 28 characters.
Device Type	Select the ZyXEL Device you would like to associate with the scheduled report template.
Note	Write a short description to identity the scheduled report template.

Table 231 Report > Schedule Report > Configure Template > Add

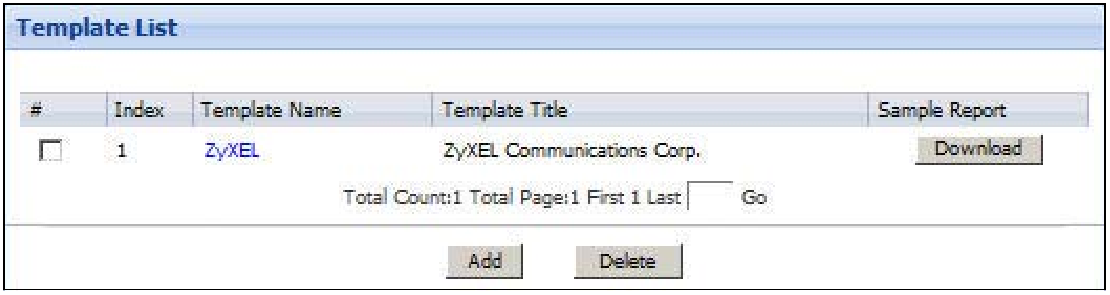
LABEL	DESCRIPTION
Report List	Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. Use the **Select All** check box at the bottom to select every report. Refer to Figure 242 on page 426 for the full view of Report List.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to close the screen without saving any changes.

12.7 Logo Template

Use this screen to see the list of existing logo templates.

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

Figure 247 Report > Schedule Report > Logo Template



Template List

#	Index	Template Name	Template Title	Sample Report
□	1	ZyXEL	ZyXEL Communications Corp.	Download

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

Each field is described in the following table.

Table 232 Report > Schedule Report > Logo Template

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

Table 232 Report > Schedule Report > Logo Template

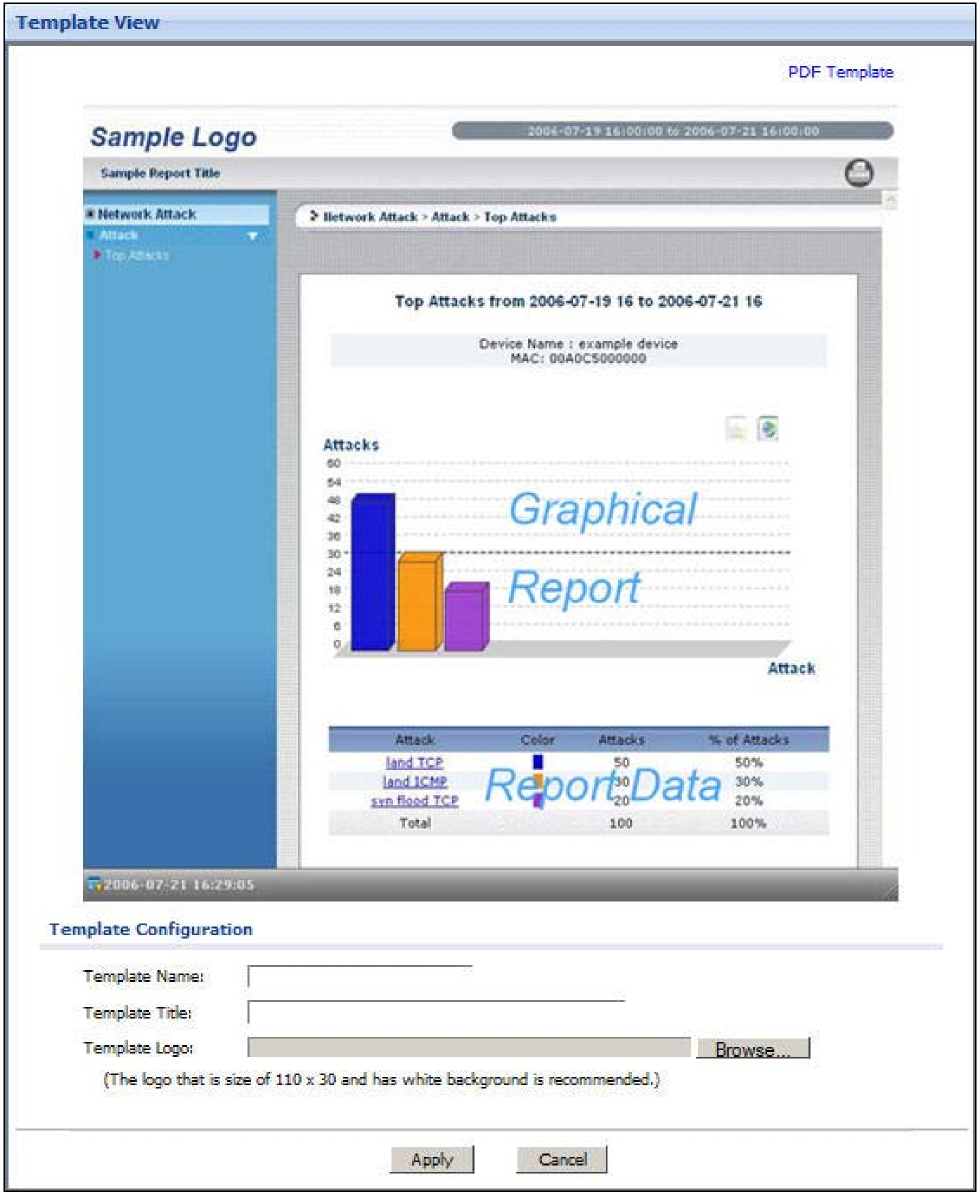
LABEL	DESCRIPTION
Add	Click this to go to another screen to create a new report template.
Delete	Select the check box next to a template and click delete to remove the report template.

12.8 Logo Template Add/Edit

Use this screen to add or edit logo templates.

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

Figure 248 Report > Schedule Report > Logo Template > Add



Template View

PDF Template

Sample Logo

2006-07-19 16:00:00 to 2006-07-21 16:00:00

Sample Report Title

Top Attacks from 2006-07-19 16 to 2006-07-21 16

Device Name : example device
MAC: 00A0C5000000

Attack	Color	Attacks	% of Attacks
land TCP	🟦	50	50%
land ICMP	🟧	30	30%
syn flood TCP	🟪	20	20%
Total		100	100%

Template Configuration

Template Name:

Template Title:

Template Logo: Browse...

(The logo that is size of 110 x 30 and has white background is recommended.)

Each field is described in the following table.

Table 233 Report > Schedule Report > Logo Template > Add

LABEL	DESCRIPTION
Template View	This section of the screen displays a sample of the report layout.
PDF Template	Click this button to view a sample of a report in PDF format.
Template Configuration	Use this section of the screen to configure the template's name and the report title and upload a logo to display on the reports.
Template Name	Enter a name to identify the template inside Vantage Report. Numbers (0-9), letters (a-z, A-Z), periods (.) and the underscore (_) are allowed. Spaces are not allowed. The name must start with a number or letter. Use up to 28 characters.
Template Title	Enter the title that you want to appear at the top of the reports generated using this template. Use up to 50 ASCII characters. Spaces are allowed.
Template Logo	Type the location of the file that you want to display as the logo in the report or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. The template logo file must be .gif or .jpg.
Apply	Click this to save your settings and close the screen.
Cancel	Click this to close the screen without saving any changes.

13

Logs

These screens provide information for all log entries for devices being monitored by Vantage Report.

Note: The logs screens, fields and menus can vary according to which device the logs are collected for.

Vantage Report consolidates log entries. See Appendix A on page 491 for information on the logs.

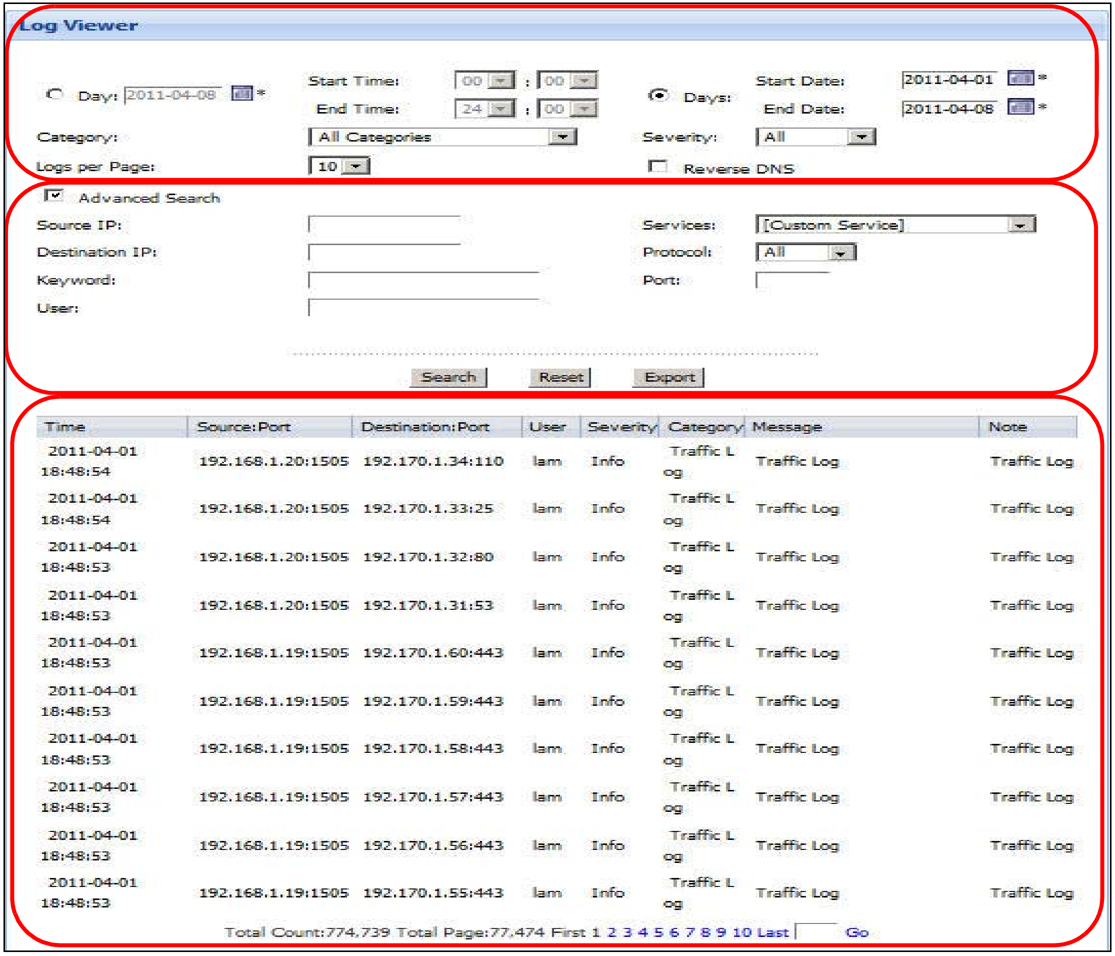
13.1 Log Viewer

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

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

See Section 2.3 on page 20 for more information about update frequencies for log entries. See Section 2.6 on page 22 for more information about the source data used by the report.

Figure 249 Logs > Log Viewer > All Logs



Log Viewer

○ Day: 2011-04-08 *	Start Time: 00 : 00 End Time: 24 : 00	● Days:	Start Date: 2011-04-01 * End Date: 2011-04-08 *
Category:	All Categories	Severity:	All
Logs per Page:	10	□ Reverse DNS	

☑ Advanced Search

Source IP:		Services:	[Custom Service]
Destination IP:		Protocol:	All
Keyword:		Port:	
User:			

Time	Source:Port	Destination:Port	User	Severity	Category	Message	Note
2011-04-01 18:48:54	192.168.1.20:1505	192.170.1.34:110	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:54	192.168.1.20:1505	192.170.1.33:25	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.20:1505	192.170.1.32:80	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.20:1505	192.170.1.31:53	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.60:443	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.59:443	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.58:443	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.57:443	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.56:443	Iam	Info	Traffic Log	Traffic Log	Traffic Log
2011-04-01 18:48:53	192.168.1.19:1505	192.170.1.55:443	Iam	Info	Traffic Log	Traffic Log	Traffic Log

Total Count:774,739 Total Page:77,474 First 1 2 3 4 5 6 7 8 9 10 Last Go

The fields in the first three rows (and **Search** and **Reset**) appear when you open the report. The fields in the next two rows (above **Search**, **Reset** and **Export**) appear if you do not select **All Categories** in the **Category** field and select **Advanced Search**. The table of log entries appears after you click **Search**, even if there are no log entries for your search criteria. Each field is described in the following table.

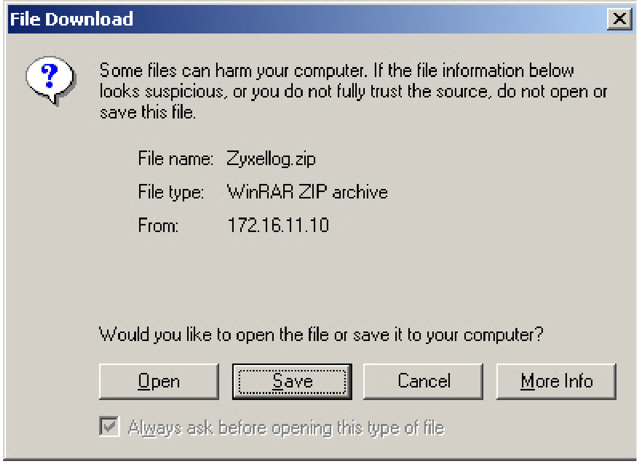
Table 234 Logs > Log Viewer > All Logs

LABEL	DESCRIPTION
Day	Select this if you want to look at log entries from one day or part of one day. You cannot select a date earlier than the number of previous days that you configured in the **System Setting** > **General Configuration** screen. You can also click the **Calendar** icon to specify the date.
Start Time	Enter the time of the earliest log entries you want to see, if you select **Day**.
End Time	Enter the time of the latest log entries you want to see, if you select **Day**.
Days	Select this if you want to look at log entries for a specific range of days.
Start Date	This field is enabled and required if you select **Days**. Enter the date of the earliest log entries you want to see. You cannot enter a date earlier than the number of previous days that you configured in the **System Setting** > **General Configuration** screen. You can also click the **Calendar** icon to specify the date.

Table 234 Logs > Log Viewer > All Logs

LABEL	DESCRIPTION
End Date	This field is enabled and required if you select **Days**. Enter the date of the latest log entries you want to see. You cannot enter a date earlier than **Start Date** or later than today. You can also click the **Calendar** icon to specify the date.
Category	This field can vary according to which device the logs are collected for.Vantage Report. Select what type of log entries you want to see. You can also select **All Categories**.
Severity	This field depends on the logs received by Vantage Report from the selected ZyXEL device. Select what type of log entries you want to see. You can also select **All**. Severity ranking follows RFC 3164 of the SYSLOG protocol and is defined as follows. • **Emergent** - System is unusable • **Alert** - Action must be taken immediately • **Critical** - Critical conditions • **Error** - Error conditions • **Warning** - Warning conditions • **Notice** - Normal but significant condition • **Info** - Informational messages • **Debug** - Debug-level messages
Reverse DNS	Select this to display logs with the domain name of hosts instead of their IP addresses. If you select this and Vantage Report does not find the domain name of a host, it will display the IP address. This feature might increase the amount of time it takes to display log entries, however.
Advanced Search	This field is disabled if **Category** is **All Categories**. Select this if you want to use other search criteria to look at log entries.
Source IP	Enter the source IP address in the event that generated the log entry.
Services	Select the service whose log entries you want to see. If you select **[Custom Service]**, you have to specify the **Protocol** and **Port** too.
Destination IP	Enter the destination IP address in the event that generated the log entry.
Protocol	This field is enabled if **Services** is **[Custom Service]**. Select the protocol whose log entries you want to see.
Keyword	Enter part or all of any value you want to look for in the **Message** field. You can use any printable ASCII character. The search is not case-sensitive.
Port	This field is enabled if **Services** is **[Custom Service]**. Select the destination port number whose log entries you want to see.
User	Enter a user’s name (or part of the name) who is associated with the log entries that you want to see. This field is case insensitive.
Search	Click this to display the log entries based on the current search criteria.
Reset	Click this to set the search criteria to the values they had the last time you clicked **Search**. If you have not clicked **Search** yet, the search criteria return to their default values.

Table 234 Logs > Log Viewer > All Logs

LABEL	DESCRIPTION
Export	This button is available when there are logs that matched your search criteria. Click this to export the results to a zip file. The screen pops up as shown next. **Figure 250** Export Logs  File Download Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file. File name: Zyxellog.zip File type: WinRAR ZIP archive From: 172.16.11.10 Would you like to open the file or save it to your computer? Open Save Cancel More Info ☑ Always ask before opening this type of file • Click **Open** to open the zip file directly. • Click **Save** to save the zip file to the computer that you are currently using to access the Vantage Report server, then exit this screen. • Click **Cancel** to exit this screen without saving any changes. • Click **More Info** to view an on-line help page about downloading files.
Time	This field displays the time the Vantage Report server received the log entry, not the time the log entry was generated.
Source:Port	This field displays the source IP address and port (if any) of the event that generated the entry.
Destination:Port	This field displays the destination IP address and port (if any) of the event that generated the entry.
Category	This field displays the type of log entry.
Message	This field displays the reason the log entry was generated.
Note	This field displays additional information about the log entry.
Total Count	This field displays how many log entries there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the log entries.
First .. Last	Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.

Note: The following screens are available only to the root account or accounts in the 'super' group. Otherwise, these menus are not shown.

13.2 Log Receiver

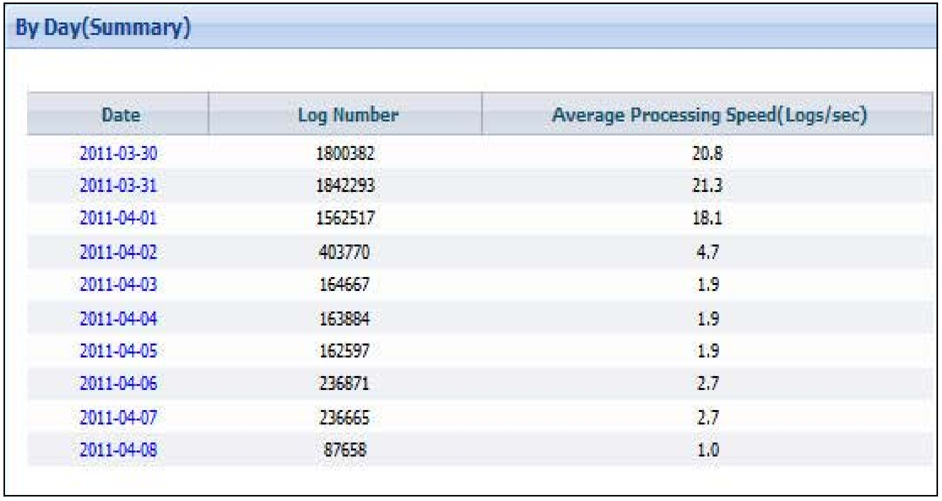
These screens show the total number of logs that Vantage Report received from all registered devices by day and how many logs Vantage Report processed per second. It also shows the number of logs that Vantage Report received from each device over a selected range of days.

13.2.1 By Day (Summary)

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

Click **Logs > Log Receiver** > **By Day (Summary)**. The following screen displays.

Figure 251 Logs > Log Receiver > By Day (Summary)



By Day(Summary)

Date	Log Number	Average Processing Speed(Logs/sec)
2011-03-30	1800382	20.8
2011-03-31	1842293	21.3
2011-04-01	1562517	18.1
2011-04-02	403770	4.7
2011-04-03	164667	1.9
2011-04-04	163884	1.9
2011-04-05	162597	1.9
2011-04-06	236871	2.7
2011-04-07	236665	2.7
2011-04-08	87658	1.0

Each field is described in the following table.

Table 235 Logs > Log Receiver > By Day (Summary)

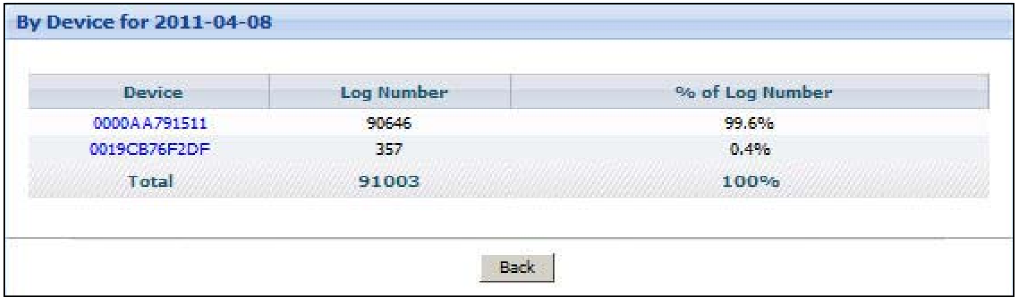
LABEL	DESCRIPTION
Date	This field displays the day for which the logs were collected. Click the date to go to a screen that lists how many logs were received from each device on that day.
Log Number	This field displays how many logs were received on each day.
Average Processing Speed (Logs/sec)	This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

13.2.1.1 Log Receiver > By Day (Summary) > By Device Screen

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

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

Figure 252 Logs > Log Receiver > By Day (Summary) > By Device



By Device for 2011-04-08

Device	Log Number	% of Log Number
0000AA791511	90646	99.6%
0019CB76F2DF	357	0.4%
Total	91003	100%

All the fields are described in the following table.

Table 236 Logs > Log Receiver > By Day (Summary) > By Device

LABEL	DESCRIPTION
Device	This field displays the MAC addresses of the registered devices that sent logs on the day you clicked. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected day.
Log Number	This field displays how many logs were received from each device on the day you clicked.
% of Log Number	This field displays what percent of the day's total logs came from each device.

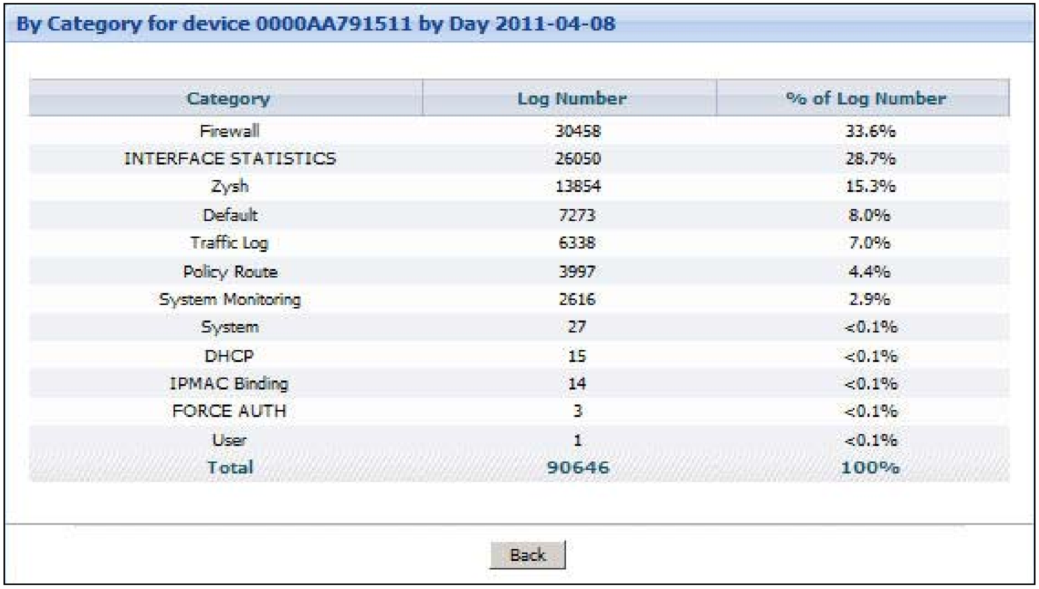
13.2.1.1.1 Log Receiver By Day (Summary) > By Device > By Category Screen

Use this screen to look at the number of logs that Vantage Report received according to the category of log (the log type such as Login, Traffic log, etc.) from an individual device on a particular day.

Note that log categories vary according to the type of device selected.

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

Figure 253 Logs > Log Receiver > By Day (Summary) > By Device > By Category



By Category for device 0000AA791511 by Day 2011-04-08

Category	Log Number	% of Log Number
Firewall	30458	33.6%
INTERFACE STATISTICS	26050	28.7%
Zysh	13854	15.3%
Default	7273	8.0%
Traffic Log	6338	7.0%
Policy Route	3997	4.4%
System Monitoring	2616	2.9%
System	27	<0.1%
DHCP	15	<0.1%
IPMAC Binding	14	<0.1%
FORCE AUTH	3	<0.1%
User	1	<0.1%
Total	90646	100%

All the fields are described in the following table.

Table 237 Logs > Log Receiver > By Day (Summary) > By Device > By Category

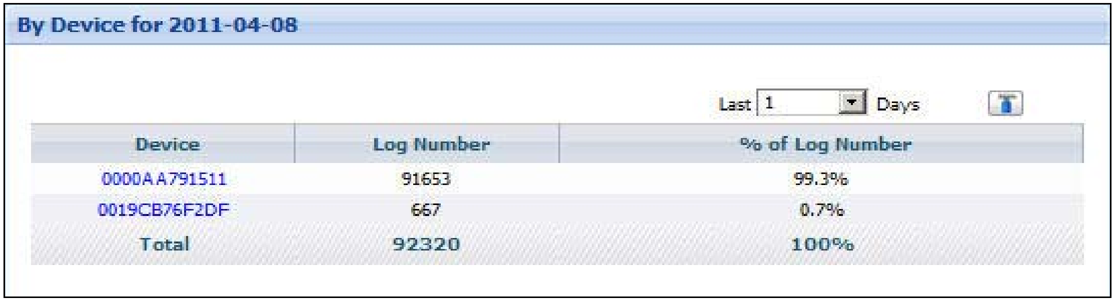
LABEL	DESCRIPTION
Category	This field displays the types of logs that the device sent to Vantage Report during the day selected from the previous screen.
Log Number	This field displays how many of the device's logs belonged to each category.
% of Log Number	This field displays what percent of the day's total logs came from each category.

13.3 By Device

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

Click **Logs > Log Receiver**> **By Device**. The following screen displays. Logs > Log Receiver > By Device. The following screen displays.

Figure 254 Logs > Log Receiver > By Device

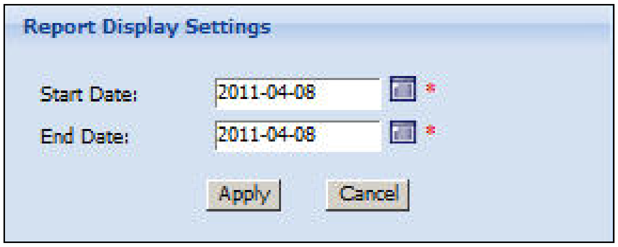


By Device for 2011-04-08

Device	Log Number	% of Log Number
0000AA791511	91653	99.3%
0019CB76F2DF	667	0.7%
Total	92320	100%

Each field is described in the following table.

Table 238 Logs > Log Receiver > By Device

LABEL	DESCRIPTION
Last	Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include. When you change this field, the report updates automatically. You can see the current date range in the title. This field resets to its default value when you click a menu item in the menu panel (including the menu item for the same report). It does not reset when you open or close drill-down reports.
Settings	Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.  Report Display Settings Start Date: 2011-04-08 * End Date: 2011-04-08 * Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.
Device	This field displays the MAC addresses of the devices that sent logs on the days you selected. They are sorted according to the number of logs received by each, in descending order. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected days.
Log Number	This field displays how many logs Vantage Report received from each device.
% of Log Number	This field displays what percent of the selected time period's total logs came from each category.

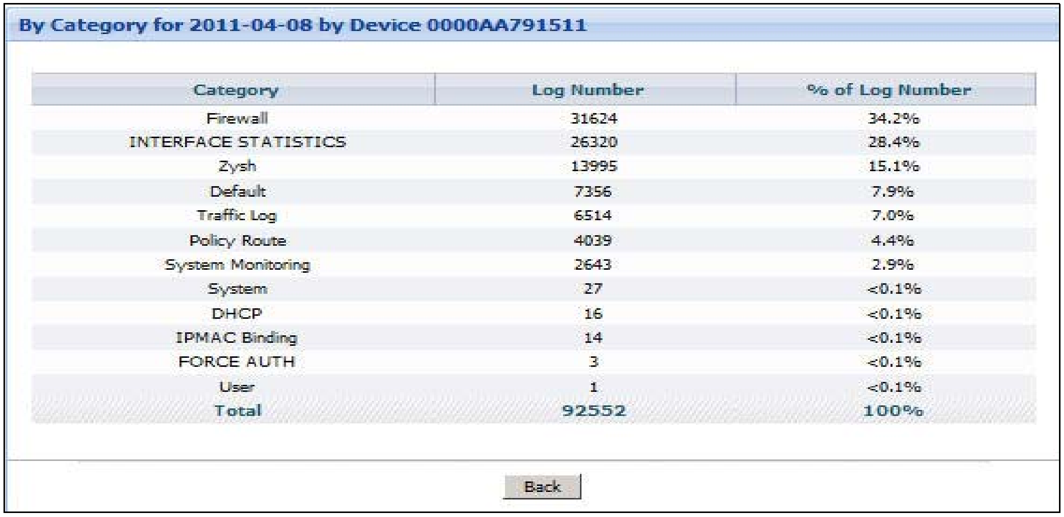
13.3.1 Log Receiver > By Device > By Category Screen

Use this screen to look at the number of logs that Vantage Report received according to the category of log (the log type such as Login, Traffic log, etc.) from an individual device over a selected range of days.

Note that the categories vary according to the type of device selected.

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

Figure 255 Logs > Log Receiver > By Device > By Category



By Category for 2011-04-08 by Device 0000AA791511

Category	Log Number	% of Log Number
Firewall	31624	34.2%
INTERFACE STATISTICS	26320	28.4%
Zysh	13995	15.1%
Default	7356	7.9%
Traffic Log	6514	7.0%
Policy Route	4039	4.4%
System Monitoring	2643	2.9%
System	27	<0.1%
DHCP	16	<0.1%
IPMAC Binding	14	<0.1%
FORCE AUTH	3	<0.1%
User	1	<0.1%
Total	92552	100%

All the fields are described in the following table.

Table 239 System > Log Receiver > By Device > By Category

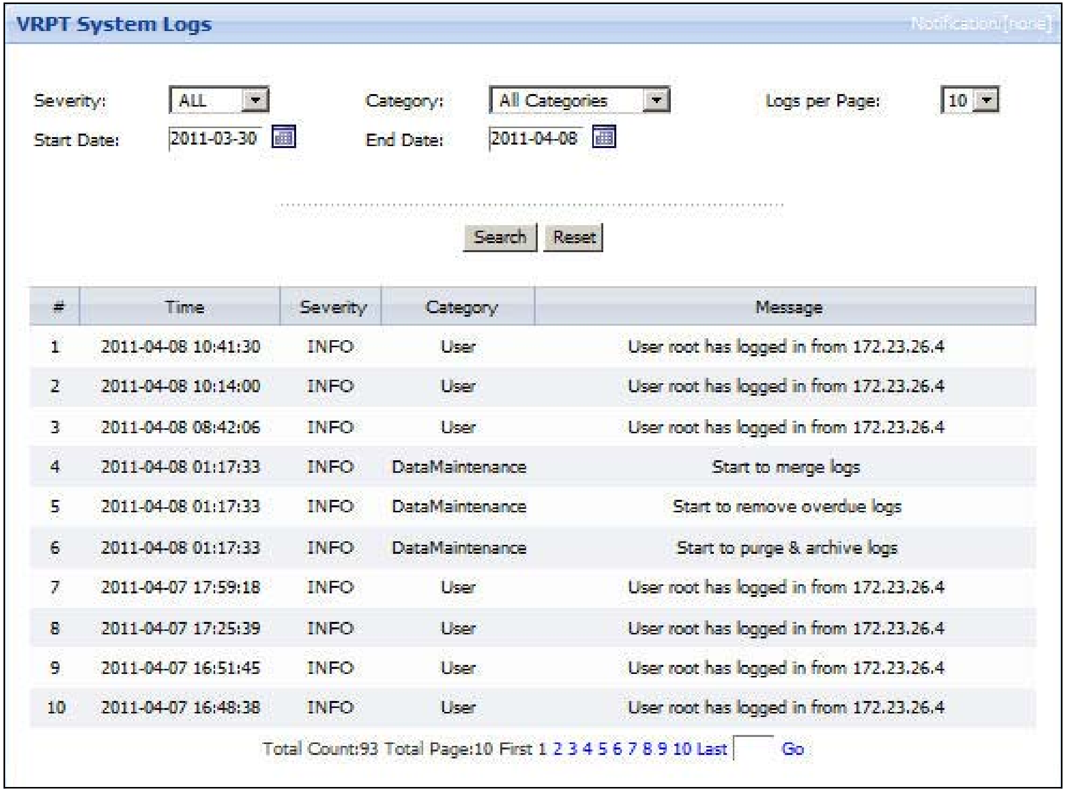
LABEL	DESCRIPTION
Category	This field displays the types of logs that the device sent to Vantage Report during the selected day.
Log Number	This field displays how many logs Vantage Report received from the device during the selected time period.
% of Log Number	This field displays what percent of the device's logs came from each category.

13.4 VRPT System Logs

Use this screen to view system, device and user information, events, scheduled reports and data maintenance records related to Vantage Report.

Click **Logs > Log Viewer** > **VRPT System Logs**. The following screen displays.

Figure 256 Logs > VRPT System Logs



Severity: ALL

Category: All Categories

Logs per Page: 10

Start Date: 2011-03-30

End Date: 2011-04-08

#	Time	Severity	Category	Message
1	2011-04-08 10:41:30	INFO	User	User root has logged in from 172.23.26.4
2	2011-04-08 10:14:00	INFO	User	User root has logged in from 172.23.26.4
3	2011-04-08 08:42:06	INFO	User	User root has logged in from 172.23.26.4
4	2011-04-08 01:17:33	INFO	DataMaintenance	Start to merge logs
5	2011-04-08 01:17:33	INFO	DataMaintenance	Start to remove overdue logs
6	2011-04-08 01:17:33	INFO	DataMaintenance	Start to purge & archive logs
7	2011-04-07 17:59:18	INFO	User	User root has logged in from 172.23.26.4
8	2011-04-07 17:25:39	INFO	User	User root has logged in from 172.23.26.4
9	2011-04-07 16:51:45	INFO	User	User root has logged in from 172.23.26.4
10	2011-04-07 16:48:38	INFO	User	User root has logged in from 172.23.26.4

Total Count:93 Total Page:10 First 1 2 3 4 5 6 7 8 9 10 Last Go

Each field is described in the following table.

Table 240 Logs > VRPT System Logs

LABEL	DESCRIPTION
Severity	Select what type of log entries in terms of severity you want to see. You can also select **All**. Severity ranking is as follows: • **Fatal** - System is unusable. • **Error** - Error conditions • **Warn -** Warning conditions • **Info -** Informational messages
Category	Select what category type of log entries you want to see. You can also select **All Categories**. The categories are as follows: • **System** - See information about Vantage Report's disk space. • **Device** - Check which devices were added, edited or removed in the Vantage Report. • **Alert** - Select this to see logs pertaining to rule-based alerts. See Chapter 14 on page 469 for more details. • **User** - See a list of users who logged in or logged out. • **Schedule Report -** Select this to see logs pertaining to scheduled reports. See Chapter 12 on page 423 for more details. • **Data Maintenance** - Check if logs have been purged, removed, archived or merged.
Logs per Page	Specify how many log entries you want to view per page.
Start Date	Enter the time of the earliest log entry you want to see.
End Date	Enter the time of the latest log entry you want to see.
Search	Click this to display the log entries based on the current search criteria.

Table 240 Logs > VRPT System Logs

LABEL	DESCRIPTION
Reset	Click this to set the search criteria to the values they had the last time you clicked **Search**. If you have not clicked **Search** yet, the search criteria return to their default values.
#	This is the number identifying the entry, with the number 1 entry being the latest event to be logged.
Time	This is the time when the event was logged by the Vantage Report.
Severity	This is the severity of the system log entry.
Category	This is the category where the event belongs to.
Message	This is the log message for the specific entry. See Appendix A on page 491 for information on the logs.
Total Count	This field displays how many log entries there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the log entries.
First .. Last	Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.

13.5 Log Archiving

These screens allow you to archive past logs to a preferred location (local directory, FTP or network server) as a ZIP file. You can set the day(s) or time interval when Vantage Report performs this task.

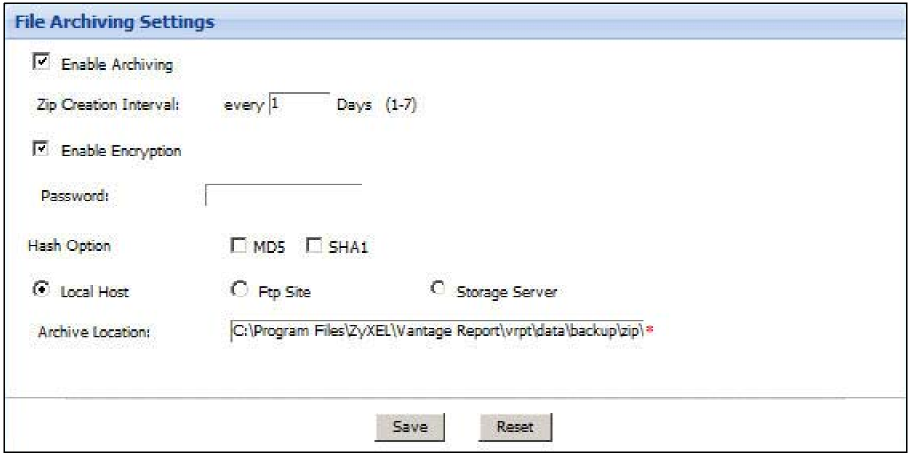
You can view, import/export, or delete log archives for a particular device.

Note: If the storage space is not enough for the size of the log archive, Vantage Report sends out an alert e-mail and generates a system log.

13.5.1 File Archiving Settings

Use this screen to archive past logs to a preferred location (local directory or FTP/storage server) as a ZIP file.

Click **Logs > Log Archiving** > **File Archiving Settings**. The screen display varies according to your storage location preference.



File Archiving Settings

☑ Enable Archiving

Zip Creation Interval: every 1 Days (1-7)

☑ Enable Encryption

Password:

Hash Option □ MD5 □ SHA1

● Local Host ○ Ftp Site ○ Storage Server

Archive Location: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\backup\zip\ *

Figure 257 Logs > Log Archiving > File Archiving Settings

Each field is described in the following table.

Table 241 Logs > Log Archiving > File Archiving Settings

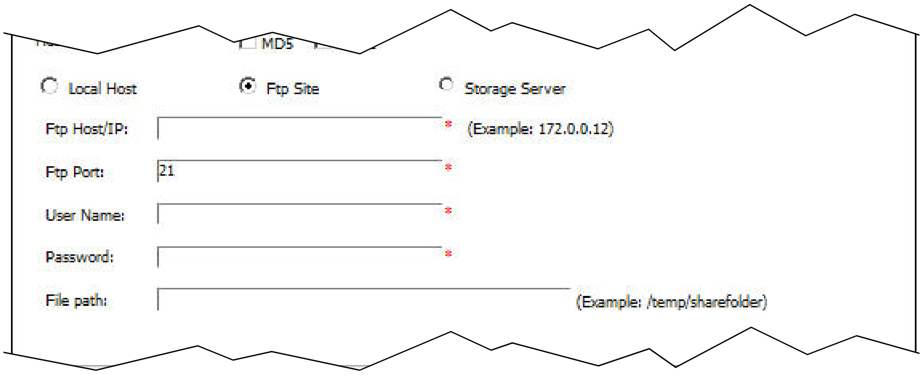
LABEL	DESCRIPTION
Enable Archiving	Click this to enable Vantage Report to archive log files.
Zip Creation Interval: every... Days (1-7)	Set every which day or the time interval the Vantage Report archives the generated log files for record keeping.
Enable Encryption	Select this if you want to encrypt archive files.
Password	This field is available when you select **Enable Encryption**. Enter up to 20 alphanumeric characters for the key used for file encryption. You have to use the same password to decrypt the file when you want to view the archived logs.
Hash Option	Select which hash algorithm to use for verifying the integrity of log data in archives. **SHA1** (Secure Hash Algorithm) is generally considered stronger than **MD5** (Message Digest 5), but it is also slower.
Local Host	Select this to store the archive to a local folder in the computer where the Vantage Report is installed. This is the default storage setting for the Vantage Report.
FTP Site	Select this to store the archive to an FTP site. Additional fields appear when you choose this option. See Section 13.5.1.1 on page 452 for more details.
Storage Server	Select this to store the archive to a storage server. Additional fields appear when you choose this option. See Section 13.5.1.2 on page 452 for more details.
Archive Location	Specify where you want Vantage Report to store log archives. The fields vary according to your preferred storage location. • Select **Local Host** to store archives in the local directory of the Vantage Report. • Select **FTP Site** to store the archives in an FTP server. Make sure you know the **FTP Host/IP address**, **User Name** and **Password**. • Select **Storage Server** to store the archives on a storage server, such as a Network Attached Storage (NAS) server. Make sure you know the **Network Folder** server location, **User Name** and **Password**.
Save	Click this to save your settings.
Reset	Click this to change the settings in this screen to the last-saved values.

13.5.1.1 File Transfer Protocol

Use this screen to store archive files on a File Transfer Protocol (FTP) server.

Click **Logs** > **Log Archiving** > **File Archiving Settings**. Choose **Ftp Site** to display the following fields.

Figure 258 Logs > Log Archiving > File Archiving Settings > Ftp Site



□ MD5

○ Local Host ● Ftp Site ○ Storage Server

Ftp Host/IP: * (Example: 172.0.0.12)

Ftp Port: 21 *

User Name: *

Password: *

File path: (Example: /temp/sharefolder)

Each field is described in the following table.

Table 242 Logs > Log Archiving > File Archiving Settings > FTP Site

LABEL	DESCRIPTION
Ftp Host/IP	Enter the location of the File Transfer Protocol (FTP) server you want to use in the **Ftp Host/IP** field.
Ftp Port	Enter the port number the FTP server uses for the service.
User Name	Enter the **User Name** for your FTP account.
Password	Enter the **Password** for your FTP account.
File path	You can specify in which FTP folder you want to store the archive in the **File Path** field (optional).

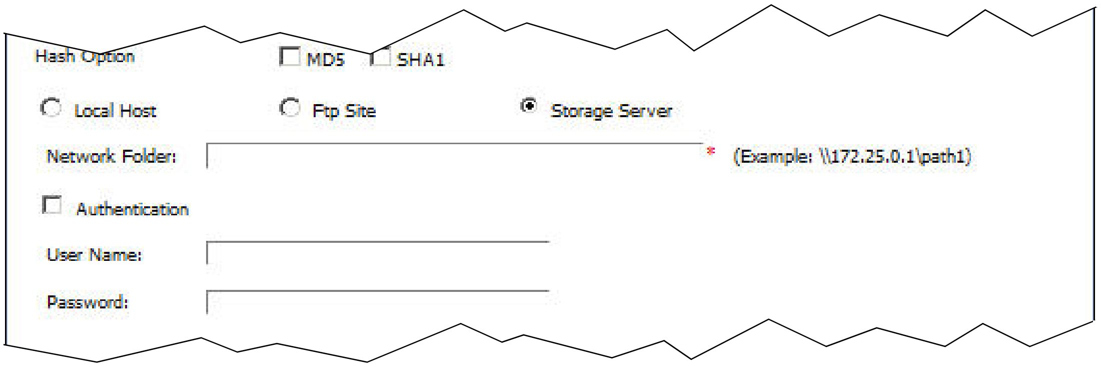
See Figure 259 on page 453 for descriptions of other table fields found in this screen.

13.5.1.2 Storage Server

Use this screen to store archive files on a storage server, such as a Network Attached Storage (NAS) server.

Click **Logs > Log Archiving** > **File Archiving Settings**. Choose **Storage Server** to display the following fields.

Figure 259 Logs > Log Archiving > File Archiving Settings > Storage Server



Hash Option □ MD5 □ SHA1

○ Local Host ○ Ftp Site ● Storage Server

Network Folder: * (Example: \\172.25.0.1\path1)

□ Authentication

User Name:

Password:

Each field is described in the following table.

Table 243 Logs > Log Archiving > File Archiving Settings > Storage

LABEL	DESCRIPTION
Network Folder	Enter the server location where you want to store the archive in the **Network Folder** field.
Authentication	Click **Authentication** if your server prompts for identification before allowing access.
User Name	Enter the **User Name** for server login if authentication is required.
Password	Enter the corresponding **Password** for server login if authentication is required.

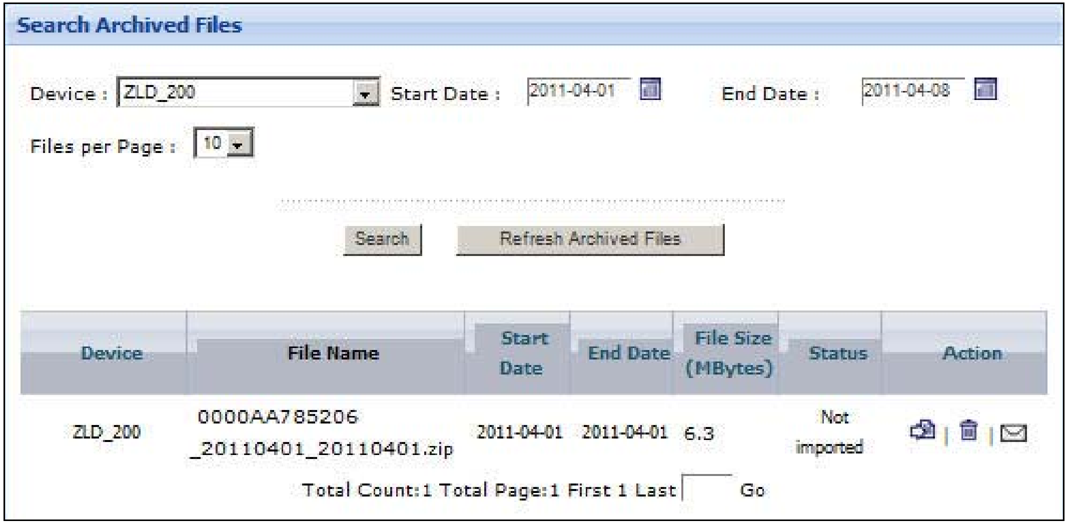
See Figure 260 on page 454 for descriptions of other table fields found in this screen.

13.5.2 View Archived Files

Use this screen to view archived logs for a particular day or range of days. Vantage Report imports the archived logs from the location where they are stored and enables you to view them in the web browser.

Click **Logs > Log Viewer** > **View Archived Files**. The following screen displays.

Figure 260 Logs > Log Archiving > View Archived Files



Search Archived Files

Device : ZLD_200 Start Date : 2011-04-01 End Date : 2011-04-08

Files per Page : 10

Device	File Name	Start Date	End Date	File Size (MBytes)	Status	Action
ZLD_200	0000AA785206 _20110401_20110401.zip	2011-04-01	2011-04-01	6.3	Not imported	

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

Each field is described in the following table.

Table 244 Logs > Log Archiving > View Archived Files

LABEL	DESCRIPTION
Device	This field displays the name of the devices that have archived logs on Vantage Report. You can also select **All**.
Start Date	Enter the date of the earliest log entries you want to see. You can also click the **Calendar** icon to specify the date.
End Date	Enter the date of the latest log entries you want to see. You cannot enter a date earlier than **Start Date**. You can also click the **Calendar** icon to specify the date.
Files per page	Select the number of archived files to view on each page.
Search	Click this to see the archives in the date range you specified.
Refresh Archive Files	Click this to update the screen and see the latest log files immediately.
Device	This refers to the ZyXEL Device the logs are generated for.
File Name	This is the file name of the log archive.
Start Date	This is the date of the earliest log entry in the archive.
End Date	This is the date of the latest log entry in the archive.
File Size (MBytes)	This is the size of the log archive.
Hash	Click **MD5** or **SHA1** to view the corresponding hash value produced using the MD5 or SHA1 algorithm while the archive file is generated. You can make sure the data integrity if this value is the same as the one produced from the same archive file you downloaded using the same hash generation tool.
Status	This column shows whether the archive is **Imported** or **Not Imported**. If it is imported, you can view the logs in the web browser. You can click on the icons in the **Action** column to set the status for each log archive.
Action	Select whether to **Export**, **Import**, **Delete** or **Transfer** an archive. Click on the corresponding icon of the action you want to apply.
Total Count	This field displays how many log entries there are for the specified search criteria.
Total Page	This field displays how many screens it takes to display all the log entries.

Table 244 Logs > Log Archiving > View Archived Files

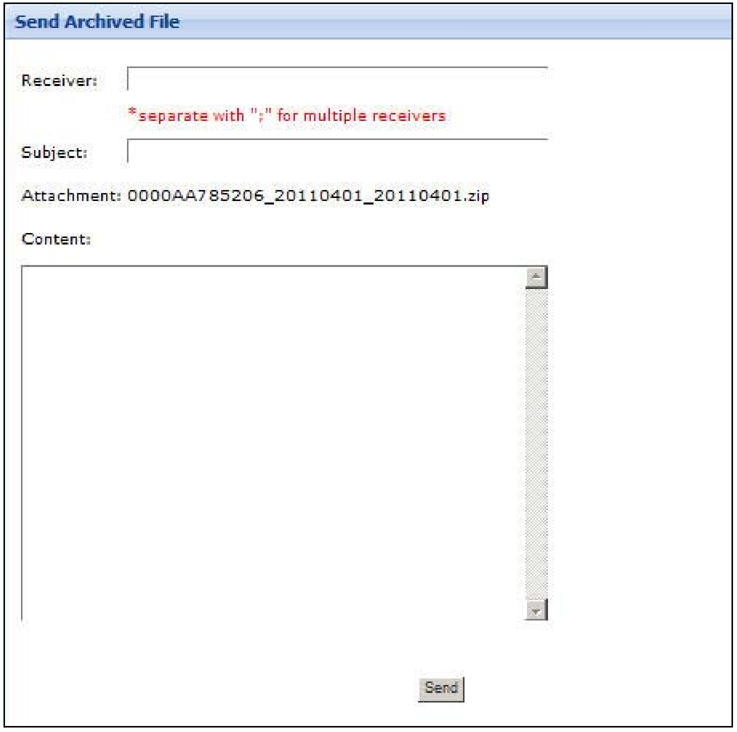
LABEL	DESCRIPTION
First .. Last	Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.

13.5.3 Log Transfer

Use this screen to send an archived file to one or multiple people using e-mail. You can also configure the mail subject and content in this screen.

Click a **Transfer** icon next to an archive entry in the **Logs > Log Archiving** > **View Archived Files** screen. The following screen displays.

Figure 261 Logs > Log Archiving > View Archived Files



Send Archived File

Receiver:

*separate with ";" for multiple receivers

Subject:

Attachment: 0000AA785206_20110401_20110401.zip

Content:

Each field is described in the following table.

Table 245 Logs > Log Archiving > View Archived Files

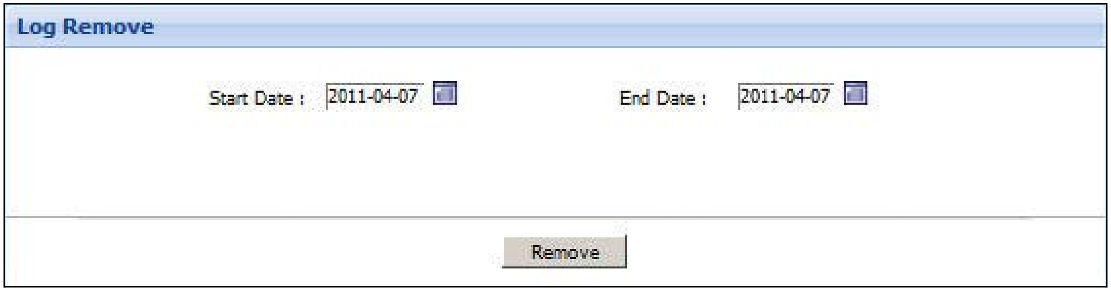
LABEL	DESCRIPTION
Receiver	Type the e-mail address(es) of people to whom you want to forward the archive file. Use a semicolon (;) to separate multiple e-mail addresses. You can type up to 100 characters in this field.
Subject	Type a short description for this mail.
Attachment	This field displays the name of the selected archive file.
Content	Type the descriptive information for this mail.
Send	Click this to send this mail to the specified e-mail addresses.

13.6 Log Remove

Use this screen to purge logs collected over a specified period of time. This helps clear up space in Vantage Report.

Click **Logs > Log Remove**. The following screen displays.

Figure 262 Logs > Log Remove



Log Remove

Start Date : 2011-04-07

End Date : 2011-04-07

Each field is described in the following table.

Table 246 Logs > Log Remove

LABEL	DESCRIPTION
Start Date	Enter the date of the earliest log entries you want to remove. You can also click the **Calendar** icon to specify the date.
End Date	Enter the date of the latest log entries you want to remove. You cannot enter a date earlier than **Start Date**. You can also click the **Calendar** icon to specify the date.
Remove	Click this to remove the said log records.

14

System Setting

The root account or the accounts in the 'super' group can use the system screens to:

- Maintain global reporting settings, such as how many days of logs to keep and default chart type
- Maintain mail server settings
- Add, remove, or edit groups and users who can access Vantage Report
- Backup the current configuration and restore a different configuration
- Export the current device panel to XML and import devices from XML
- Upgrade to a new software release of Vantage Report
- Register Vantage Report (You have to register Vantage Report if you want to get the trial version, upgrade to the full version, or increase the number of devices Vantage Report supports.)
- Monitor the number of logs received by time or by device
- Get basic information about Vantage Report

Other users can use the system screens to

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

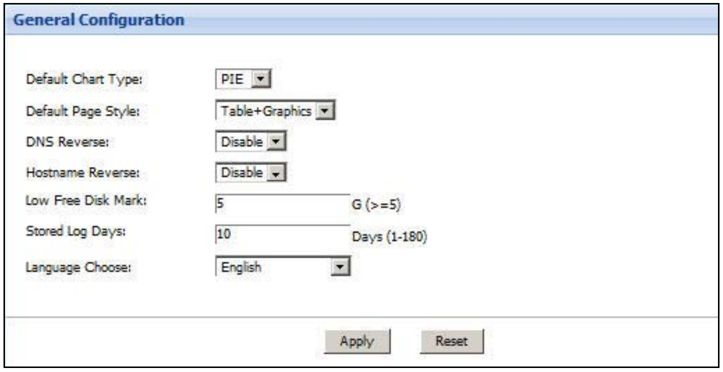
14.1 General Configuration Screen

Note: Only the root account or accounts in the 'super' group can open this screen.

Use this screen to maintain global reporting settings, such as how many days of logs to keep and default chart type.

Click **System Setting > General Configuration** to open the **General Configuration** screen.

Figure 263 System Setting > General Configuration



General Configuration

Default Chart Type:	PIE
Default Page Style:	Table+Graphics
DNS Reverse:	Disable
Hostname Reverse:	Disable
Low Free Disk Mark:	5 G (>=5)
Stored Log Days:	10 Days (1-180)
Language Choose:	English

Each field is described in the following table.

Table 247 System Setting > General Configuration

LABEL	DESCRIPTION
Default Chart Type	Select the default chart type in statistical report screens.
Default Page Style	Select the default page style in statistical report screens.
DNS Reverse	Select **Enable** if you want Vantage Report to do reverse DNS lookups in statistical reports. It has no effect in **Log Viewer**. In reverse DNS lookups, Vantage Report looks for the domain name associated with IP addresses that it displays. If Vantage Report finds the domain name, it displays the domain name and the IP address in the field. If it does not find the domain name, it only displays the IP address. This feature might increase the amount of time it takes to display statistical reports, however.
Hostname Reverse	Select **Enable** if you want Vantage Report to display the host names for local computers instead of IP addresses. It has no effect in **Log Viewer**. In hostname reverse lookups, Vantage Report looks for the host name associated with local IP addresses that it displays. If Vantage Report finds the host name, it displays the host name and the IP address in the field. If it does not find the host name, it only displays the IP address. This feature might increase the amount of time it takes to display statistical reports, however. You also need to configure the host computers and ZyXEL device (see Section 14.1.1 on page 458).
Low Free Disk Mark	When the amount of available disk space falls below this number of gigabytes, Vantage Report sends a notification to the e-mail address (if any) for the `root` user account.
Stored Log Days	Enter the number of days you want to store logs in Vantage Report before removing them.
Language Choose	Choose the language for the Vantage Report.
Apply	Click this to save your settings.
Reset	Click this to change the settings in this screen to the last-saved values.

14.1.1 Configuring for Hostname Reverse

Besides enabling hostname, do the following to allow the hostname reverse function to work.

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

14.1.1.1 Enabling the Default NetBIOS Setting in Host Computers

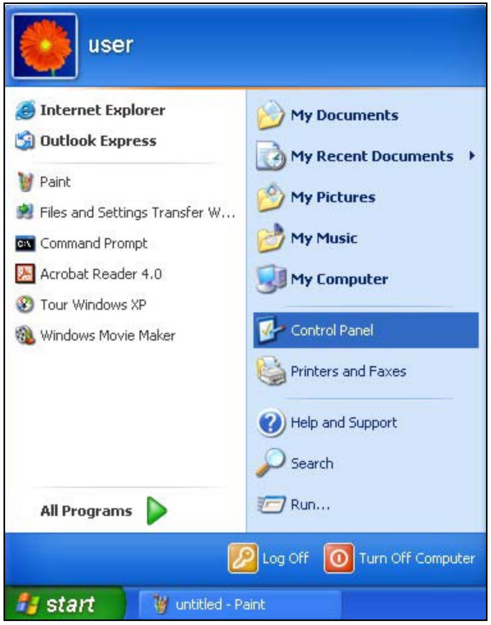
The following procedure gives an example of how to enable the default NetBIOS settings in host computers using Windows 2000, XP, Vista or 7.

1 For Windows XP, click **Start** > **Control Panel**.

For Windows 2000, click **Start** > **Settings** > **Control Panel**.

For Windows Vista/7, click **Start** > **Control Panel**.

Figure 264 Windows XP: Start Menu

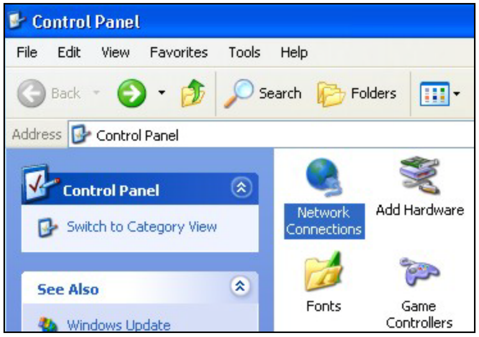


2 For Windows XP, click **Network Connections**.

For Windows 2000, click **Network and Dial-up Connections** and then **Local Area Connection**.

For Windows Vista/7, double click **Network and Sharing Center**.

Figure 265 Windows XP: Control Panel



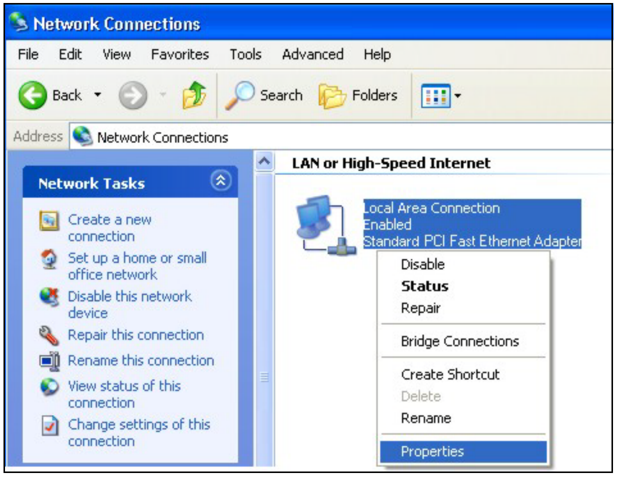
3 For Windows XP, right-click **Local Area Connection** and then click **Properties**.

For Windows 2000, the **Local Area Connection Status** window appears. click **Properties**.

For Windows Vista, click **View status** next to the **Connection** field. A screen appears and then click **Properties**.

For Windows 7, click **Local Area Connection** and then click **Properties**.

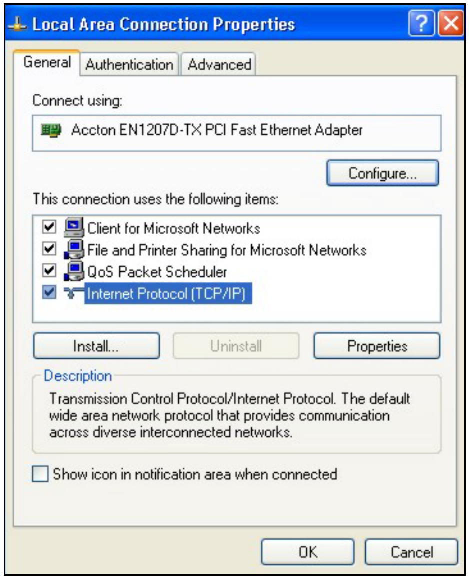
Figure 266 Windows XP: Control Panel: Network Connections: Properties



4 For Windows XP/2000, select **Internet Protocol (TCP/IP)** (under the **General** tab) and click **Properties**.

For Windows Vista/7, select **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.

Figure 267 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
□ Show icon in notification area when connected
OK
Cancel

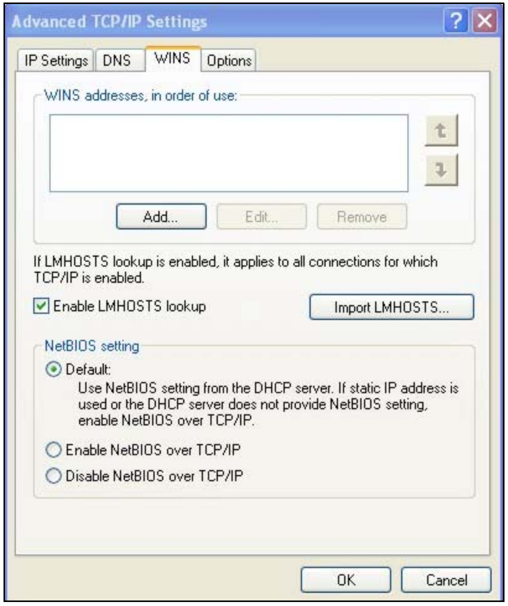
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5 For Windows XP, the **Internet Protocol TCP/IP Properties** window opens. Click the **WINS** tab.

For Windows 2000, the **Internet Protocol TCP/IP Properties** window opens. Click **Advanced** and then the **WINS** tab.

In Windows Vista/7, The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens, click **Advanced** and then the **WINS** tab.

Figure 268 Windows XP: Advanced TCP/IP Settings: WINS



If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

● Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

6 For Windows XP/Vista/7, select the **Default** NetBIOS setting and click **OK**.

For Windows 2000, select **Use NetBIOS setting from the DHCP server** and click **OK**.

7 Click **OK** (and **Close**) to close the previously opened windows.

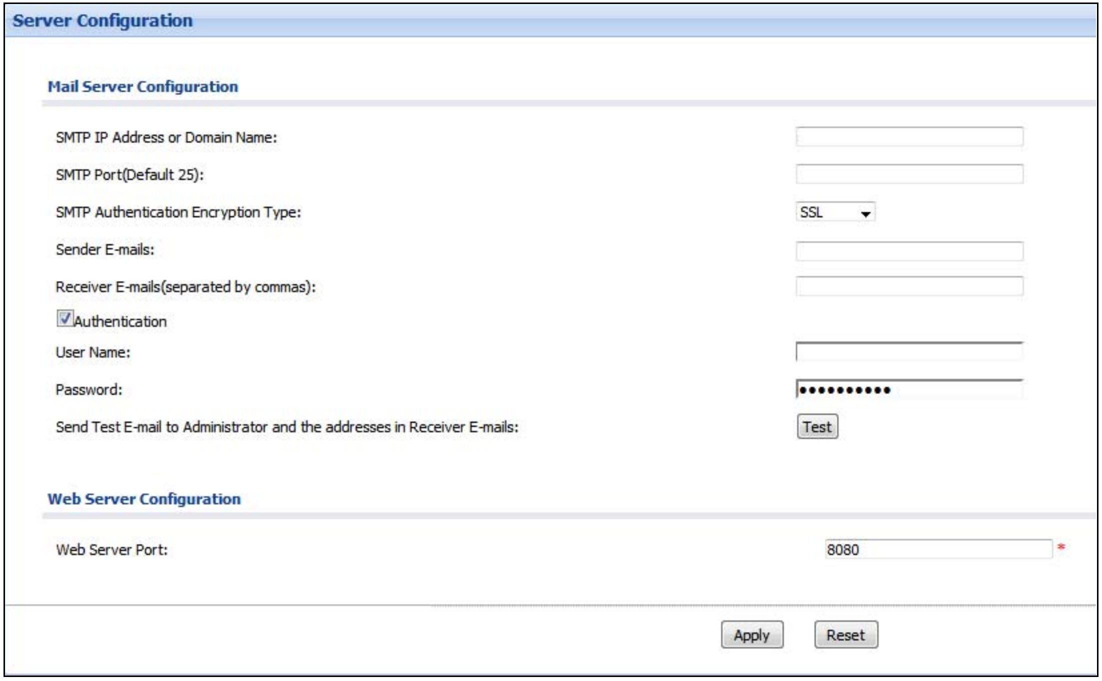
8 Turn on your ZyXEL device and restart your computer (if prompted).

14.2 Server Configuration Screen

Note: Only the root account or accounts in the 'super' group can open this screen.

Use the **Server Configuration** screen to set up mail server and web server configuration for Vantage Report. See Section 2.2 on page 20 for more information. Click **System Setting > Server Configuration** to open the **Server Configuration** screen.

Figure 269 System Setting > Server Configuration



Server Configuration

Mail Server Configuration

SMTP IP Address or Domain Name:

SMTP Port(Default 25):

SMTP Authentication Encryption Type: SSL

Sender E-mails:

Receiver E-mails(separated by commas):

☑ Authentication

User Name:

Password: •••••••••••

Send Test E-mail to Administrator and the addresses in Receiver E-mails:

Web Server Configuration

Web Server Port: 8080 *

Each field is described in the following table.

Table 248 System Setting > Server Configuration

LABEL	DESCRIPTION
Mail Server Configuration	Use this part of the screen to set up the SMTP mail server that Vantage Report uses for notifications and scheduled reports.
SMTP IP Address or Domain Name	Enter the IP address or domain name of the SMTP mail server on which Vantage Report has an account to send e-mail messages.
SMTP Port	Enter the port number upon which the SMTP mail server receives mail. Leave this blank if you were not given a specific number to use.
SMTP Authentication Encryption Type	Select the type of encryption the SMTP mail server uses during authentication. The options are **Default**, **TLS**, **SSL**. Default means no encryption. Leave this set to default if you do not know which one to use.
Sender E-mails	Enter the complete e-mail address for the Vantage Report account.
Receiver E-mails (seperated by commas)	Enter the e-mail address you want to be the receiver when Vantage Report sends e-mail. This is the e-mail address to which Vantage Report e-mail appears to be sent.
Authentication	Check this to supply your credentials to the SMTP server you want to use.
User Name	Enter the user name for the email account. If the user name is not required, leave this field blank.
Password	Enter the password for the email account. If the password is not required, leave this field blank.

Table 248 System Setting > 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.

14.3 Data Maintenance Screens

Note: Only the root account or accounts in the 'super' group can open these screens.

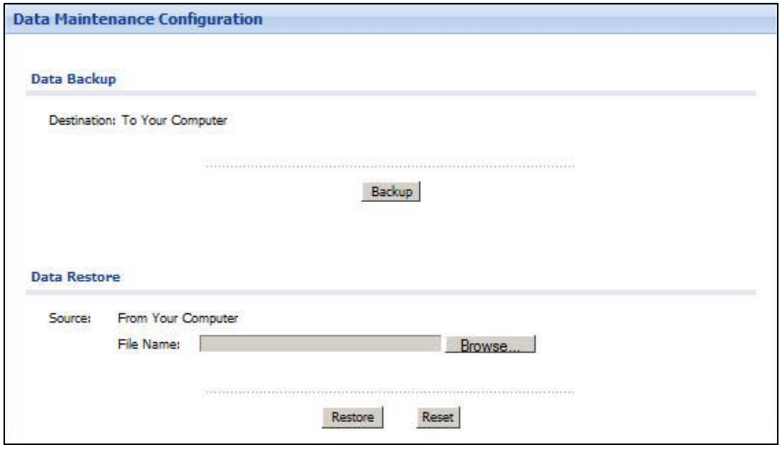
Use the data maintenance screens to backup the current configuration, restore a different configuration, export the device panel, or import a different device panel.

14.3.1 Data Backup and Data Restore Screen

Note: Only the root account or accounts in the 'super' group can open this screen.

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

Figure 270 System Setting > Data Maintenance > Configuration



Data Maintenance Configuration

Data Backup

Destination: To Your Computer

Data Restore

Source: From Your Computer

File Name:

Each field is described in the following table.

Table 249 System Setting > Data Maintenance > Configuration

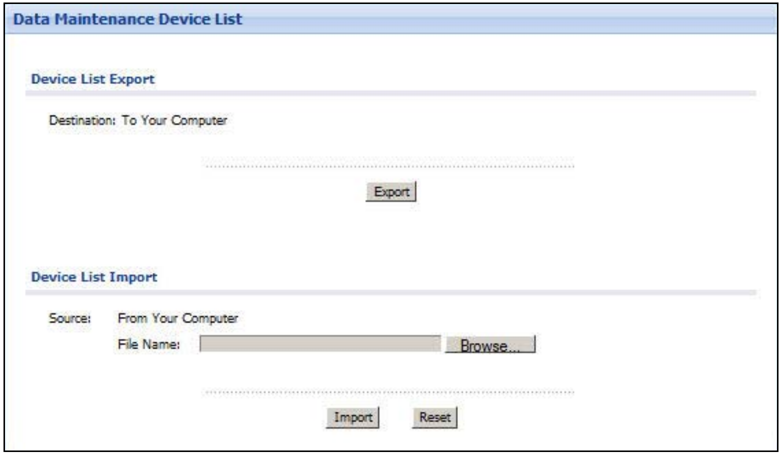
LABEL	DESCRIPTION
Backup	Click this to look at or save the current settings in the **General Configuration**, **Server Configuration**, **User Management**, and **Device List** screens. Vantage Report saves the current settings in XML format.
File Name / Browse	Enter the XML file name that contains the settings you want to restore. You can also click **Browse**.
Restore	Click this to load the settings in the specified file name.
Reset	Click this to clear the fields in this screen.

14.3.2 Device List Screen

Note: Only the root account or accounts in the 'super' group can open this screen.

You can use this screen to export the current device panel to an XML file, or you can add devices stored in XML format to Vantage Report. To access this screen, click **System Setting > Data Maintenance > Device List**.

Figure 271 System Setting > Data Maintenance > Device List


Data Maintenance Device List
Device List Export
Destination: To Your Computer
Export
Device List Import
Source: From Your Computer
File Name:
Browse...
Import
Reset

Each field is described in the following table.

Table 250 System Setting > Data Maintenance > Device List

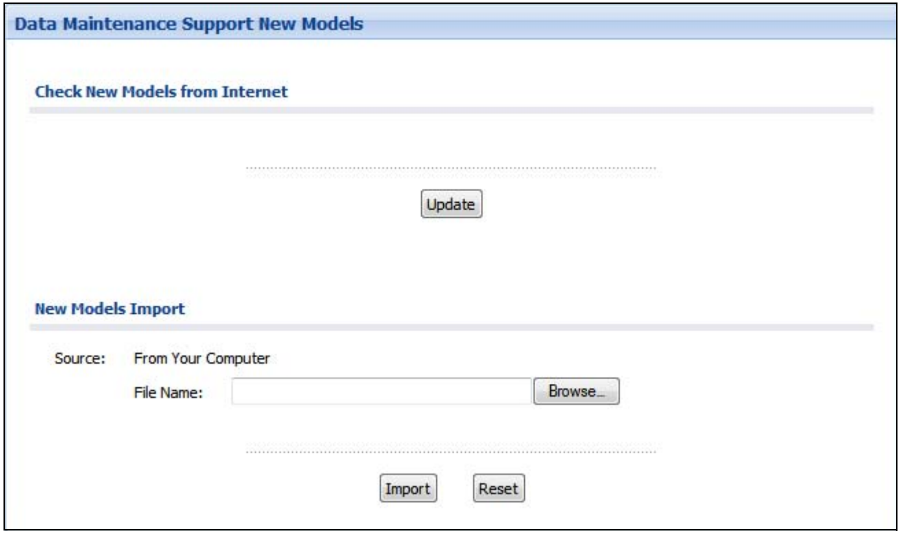
LABEL	DESCRIPTION
Export	Click this to look at or save the current device panel in XML format.
File Name / Browse	Enter the XML file name that contains the devices you want to add. You can also click **Browse**.
Import	Click this to add the devices in the specified file name. You cannot add any of the devices in the XML file if the total number of devices (current device panel + devices in XML file) is more than your license allows.
Reset	Click this to clear the fields in this screen.

14.3.3 Support New Models Screen

Note: Only the root account or accounts in the 'super' group can open this screen.

Use this screen to add support for new device models. To access this screen, click **System Setting > Data Maintenance > Support New Models**.

Figure 272 System Setting > Data Maintenance > Support New Models



Each field is described in the following table.

Table 251 System Setting > Data Maintenance > Support New Models

LABEL	DESCRIPTION
Check New Models from Internet	Click **Update** to check ZyXEL’s server for any new models you can add.
New Models Import	Use this section if you have already downloaded the Vantage Report new model support file from the ZyXEL website. See the Vantage Report product page for a supported models list. Use **File Name** to enter the Vantage Report new model support file path or click **Browse** and look for it. Click **Import** to load the selected Vantage Report new model support file into Vantage Report.
Reset	Click this to clear the fields in this screen.

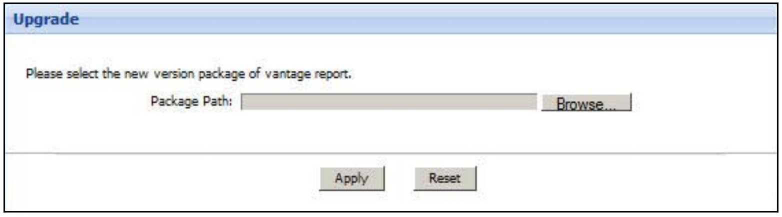
14.4 Upgrade Screen

Note: Only the root account or accounts in the 'super' group can open this screen.

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

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

Figure 273 System Setting > Upgrade



Upgrade

Please select the new version package of vantage report.

Package Path:

Each field is described in the following table.

Table 252 System Setting > Upgrade

LABEL	DESCRIPTION
Package Path / Browse	Enter the path to the release of Vantage Report that you want to install. You can also click **Browse**.
Apply	Click this to install the selected release. Follow the prompts.
Reset	Click this to clear the fields in this screen.

14.5 Registration Screens

Note: Only the root account or accounts in the 'super' group can open these screens.

Use these screens to

- Upgrade to the full version of Vantage Report; or
- Increase the number of devices you can manage with the full version.

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

The following information may be required for registration.

Table 253 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

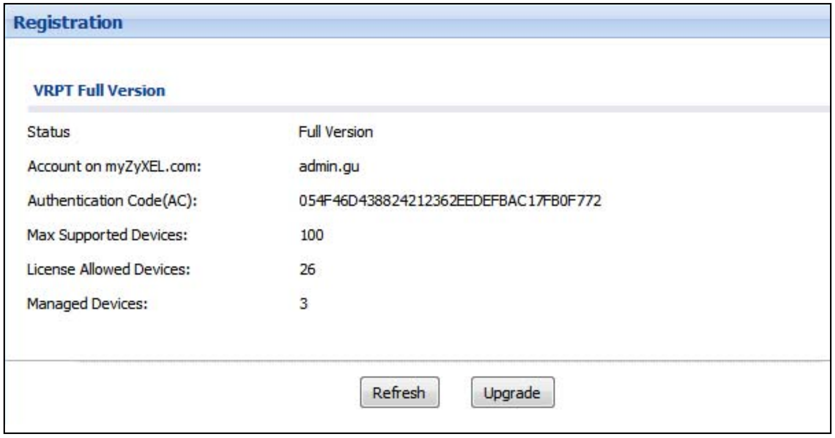
Table 254 Information for Upgrading the Version or Number of Devices

To add more devices for the full version, you need your...
• license key (E-Vantage Report)

14.5.1 Registration Summary Screen

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

Figure 274 System Setting > Registration



Registration

VRPT Full Version

Status	Full Version
Account on myZyXEL.com:	admin.gu
Authentication Code(AC):	054F46D438824212362EEDEFBAC17FB0F772
Max Supported Devices:	100
License Allowed Devices:	26
Managed Devices:	3

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 255 System Setting > Registration

LABEL	DESCRIPTION
Status	This field displays what type of registration this installation of Vantage Report has. When you first install Vantage Report you get the trial version with full management authority for one device for 30 days. The days remaining also displays for the trial version. After the trial version expires you have a basic version with only limited management authority for one device. Purchase license keys to use the full version with full management authority for more devices.
Account on myZyXEL.com	This field appears if you have used the registration screens to log into myZyXEL.com before. It displays the user name of your myZyXEL.com account.
Authentication Code (AC)	This field displays the authentication code for Vantage Report. You have to enter this number in myZyXEL.com if you log in to myZyXEL.com directly.
Max Supported Devices	This field appears if you have the full version. It displays the maximum number of devices Vantage Report can currently support, regardless of the number of licenses you purchase. You can never increase the number of devices in Vantage Report higher than this value, regardless of how many licenses you have. In other words, this is the maximum value of **License Allowed Devices**.
License Allowed Devices	This field appears if you have the full version. It displays the number of devices you can add in Vantage Report based on your current license(s).
Managed Devices	This field appears if you have the full version. It displays the number of devices you currently have added in Vantage Report.
Refresh	Click this to update the information in this screen.

Table 255 System Setting > Registration

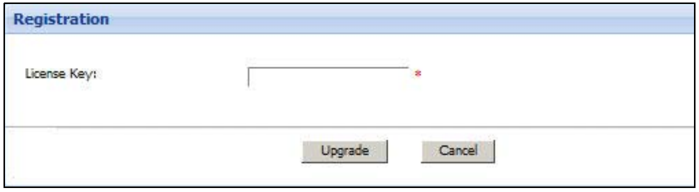
LABEL	DESCRIPTION
Trial	This appears if you have the basic version and if you have not installed the trial version yet. Click this to get the trial version of Vantage Report. The **Registration** screen appears.
Upgrade	Click this to upgrade to the full version of Vantage Report or to increase the number of devices in Vantage Report. If you cannot upgrade Vantage Report further (in other words, if you can already add the maximum number of devices in Vantage Report), an error message is displayed. Otherwise, the **Registration** screen appears.

14.5.2 Registration > Upgrade Screen

Note: The Vantage Report server must be connected to the Internet to use this screen.

To access this screen, click **Trial** or **Upgrade** in **System Setting > Registration**.

Figure 275 System Setting > Registration > Upgrade Screen



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

Table 256 System Setting > Registration > Upgrade Screen

LABEL	DESCRIPTION
License Key	Enter the E-Vantage Report license key if you are adding more devices for the full version.
New myZyXEL.com account	Select this if you want Vantage Report to create a new myZyXEL.com account for you.
Existing myZyXEL.com account	Select this if you want to use an existing myZyXEL.com account.
User Name	If you are creating a new myZyXEL.com account, enter the user name that you would like to use. Your user name must be 6 - 20 alphanumeric characters and/or underscores(_) long. If you are using an existing myZyXEL.com account, enter the user name for that account.
Password	If you are creating a new myZyXEL.com account, enter the password that you would like to use. Your password must be 6 - 20 alphanumeric characters and/or underscores(_) long. If you are using an existing myZyXEL.com account, enter the password for that account.
Confirm Password	This field appears if you are creating a new myZyXEL.com account. Retype your password.
E-mail Address	This field appears if you are creating a new myZyXEL.com account. Enter the e-mail address where you would like to be notified about your new myZyXEL.com account.

Table 256 System Setting > Registration > Upgrade Screen

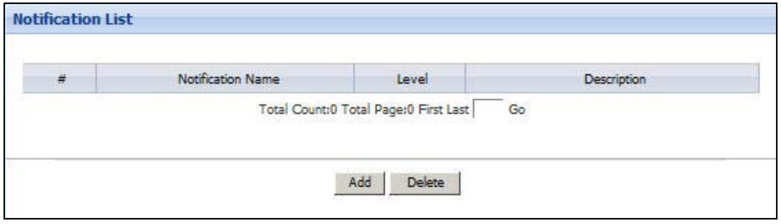
LABEL	DESCRIPTION
Country	This field appears if you are creating a new myZyXEL.com account. Select the country where you work.
Upgrade	Click this to get the trial version, upgrade to the full version, or increase the number of devices in Vantage Report.
Cancel	Click this to return to the **Registration** summary screen without registering.

14.6 Notification

Use this screen to manage your Vantage Report notifications. Based on the monitoring data collected and the notifications you set, Vantage Report can send e-mail, E-mail SMS, and/or Web SMS notifications to you when events happen in monitored devices.

Click **System Setting > Notification** to display the following screen.

Figure 276 System Setting > Notification



The fields are described in the following table.

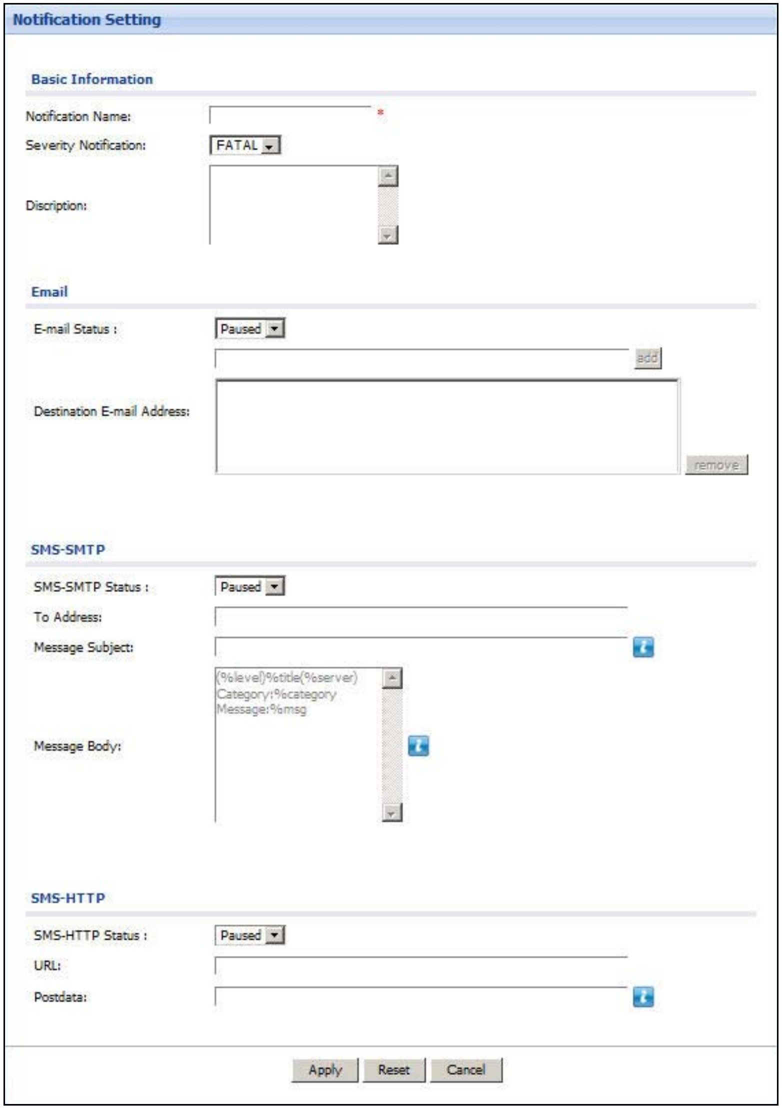
Table 257 System Setting > Notification

LABEL	DESCRIPTION
#	This is the index number of a notification.
Notification Name	This is the name identifying the notification. You can edit the settings of this notification by clicking this link. See Section 14.6.1 on page 470 to see the **Add/Edit** screen for notifications.
Level	This specifies the severity of the notification, which may be the following: • **FATAL** - System is unusable • **WARN** - Warning conditions • **INFO** - Informational messages Severity labels are user-defined. You can determine how the severity labels apply to each type of event when you are setting the parameters for the notification file. You can set this in the **Add/Edit** screen (see Section 14.6.1 on page 470).
Description	This shows the basic information for the notification.
Total Count	This field displays how many rules are recorded.
Total Page	This field displays how many screens it takes to display all the rules.
First .. Last	Click **First**, **Last**, or a specific page number to look at the rules on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.
Add	Click this to add the rule to the Vantage Report.
Delete	Select the check box(es) of the rule(s) you want to delete and then click this button. Click **OK** in the confirmation dialog box.

14.6.1 Add/Edit a Notification

Use this screen to create or edit a notification. Click **Add** or click a notification's name in the **System Setting > Notification** screen to open the following screen.

Figure 277 System Setting > Notification > Add/Edit



Notification Setting

Basic Information

Notification Name: *

Severity Notification: FATAL

Discription:

Email

E-mail Status : Paused

Destination E-mail Address:

SMS-SMTP

SMS-SMTP Status : Paused

To Address:

Message Subject:

Message Body: (%level)%title(%server)
Category:%category
Message:%msg

SMS-HTTP

SMS-HTTP Status : Paused

URL:

Postdata:

The fields are described in the following table.

Table 258 System Setting > Notification > Add/Edit

LABEL	DESCRIPTION
Notification Name	Type up to 30 alphanumeric characters for the name of the notification. Underscores (_) are allowed.
Severity Notification	Select the severity of the notification. The available options are: • **FATAL** - System is unusable • **WARN** - Warning conditions • **INFO** - Informational messages
Description	This shows the basic information for the notification.

Table 258 System Setting > Notification > Add/Edit

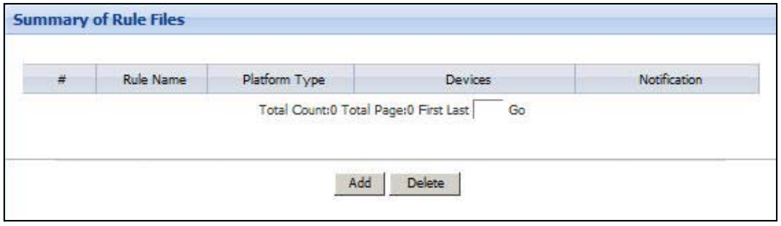
LABEL	DESCRIPTION
Email	
Email Status	Select **Active** to enable the Vantage Report to send this type of notification to the configured e-mail address(es) in the **Destination E-mail Address** field. Alternatively, select **Paused** to disable it.
add	Type a valid e-mail address and click this to add it to the **Destination E-mail Address** list. Repeat to add more than one e-mail addresses.
Destination E-mail Address	This is a list of receiver e-mail addresses. You can select an e-mail address and then click **remove** to delete it from the list.
SMS-SMTP	
SMS-SMTP Status	Select **Active** to enable the Vantage Report to send this type of notification to the configured address(es) below using E-mail Short Message Service (SMS). Alternatively, select **Paused** to disable it.
To Address	Type one or more valid SMS addresses. Use a comma (,) to separate multiple addresses. An SMS address is usually your cell phone number plus an '@' and your SMS service provider's domain name. For example, 1234567890@abcdefg.com. Check your service provider if you are not sure about this.
Message Subject	Type up to 50 printable characters for the mail subject. Spaces are allowed. Mouse over the information icon to see what variables you can use for the mail subject. The available variables are: **%msg**: Use this to show the content of the notification. **%level**: Use this to show the severity level of the notification. **%server**: Use this to show the IP address of the mail server used to send the notification. **%title**: Use this to show the title of the notification. **%category**: Use this to show the category of the notification.
Message Body	Type up to 160 printable characters for the mail content. Spaces are allowed. Mouse over the information icon to see what variables you can use for the mail content. The available variables are: **%msg**: Use this to show the content of the notification. **%level**: Use this to show the severity level of the notification. **%server**: Use this to show the IP address of the mail server used to send the notification. **%title**: Use this to show the title of the notification. **%category**: Use this to show the category of the notification.
SMS-HTTP	
SMS-HTTP Status	Select **Active** to enable the Vantage Report to send this type of notification to the configured URL(s) below using Web SMS. Alternatively, select **Paused** to disable it.
URL	Type up to 539 characters for the address of a web site that provides the Web SMS service.
Postdata	Enter any POST parameters for the HTTP request. A POST request sends additional data after the URL to the web server. Leave this empty for a GET request or you are not sure about it.
Apply	Click this to save the changes to the Vantage Report.
Reset	Click this to reset all field values back to the previous settings in this screen.
Cancel	Click this to exit this screen without saving any changes.

14.7 Rule-Based Alert

Use this screen to manage your Vantage Report alert system. Based on the monitoring data collected and the rules you set, Vantage Report can send e-mail notifications and keep you in the loop on events happening in monitored devices.

Click **System Setting > Rule-based Alert** to display the following screen.

Figure 278 System Setting > Rule-based Alert



Summary of Rule Files

#	Rule Name	Platform Type	Devices	Notification

Total Count:0 Total Page:0 First Last Go

The fields are described in the following table.

Table 259 System Setting > Rule-based Alert

LABEL	DESCRIPTION
#	This is the index number of a rule.
Rule Name	This is the name identifying the rule. You can edit the parameters of this rule by clicking on this link. See Section 14.7.1 on page 472 to see the **Add/Edit** screen for rules.
Level	This specifies the severity of the alert, which may be the following. • **FATAL** - System is unusable • **WARN** - Warning conditions • **INFO** - Informational messages Note that severity labels are user-defined. You can determine how the severity labels apply to each type of event when you are setting the parameters for the rule file. You can set this in the **Add/Edit** screen (see Section 14.7.1 on page 472).
Platform Type	This specifies what firmware platform the rule applies to. Firmware platform can be **ZLD**.
Devices	This field specifies in which monitored devices the rule applies.
To E-mail Address	This shows the e-mail address where you would like to be notified of alerts.
Total Count	This field displays how many rules are recorded.
Total Page	This field displays how many screens it takes to display all the rules.
First .. Last	Click **First**, **Last**, or a specific page number to look at the rules on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.
Add	Click this to add the rule to the Vantage Report.
Delete	Select the check box(es) of the rule(s) you want to delete and then click this button. Click **OK** in the confirmation dialog box.

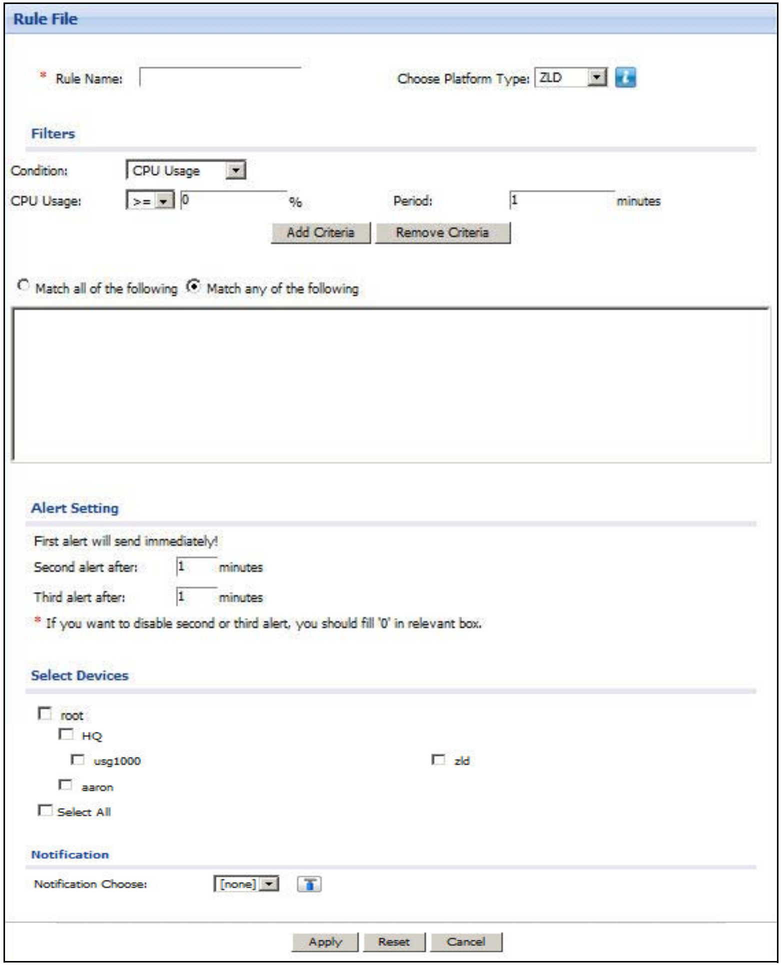
14.7.1 Add/Edit a Rule-based Alert

These screens allow you to add a new rule file or edit an existing one.

Click **System Setting > Rule-based Alert**. To edit an existing rule click the link of the existing **Rule Name**. To add a new rule, click **Add**.

The following screen displays.

Figure 279 System Setting > Rule-based Alert > Add/Edit > CPU/Memory/Session Usage



Rule File

* Rule Name:

Choose Platform Type: ZLD

Filters

Condition: CPU Usage

CPU Usage: >= 0 %

Period: 1 minutes

○ Match all of the following ● Match any of the following

Alert Setting

First alert will send immediately!

Second alert after: 1 minutes

Third alert after: 1 minutes

* If you want to disable second or third alert, you should fill '0' in relevant box.

Select Devices

□ root

□ HQ

□ usg1000

□ zld

□ aaron

□ Select All

Notification

Notification Choose: [none]

The fields in this screen are described in Table 260 on page 474.

The following sections describe the **System Setting > Rule-based Alert > Add/Edit** screens according to the **Condition** filter selected.

The fields under **Filters** vary according to the **Condition** filter you want to set the rule for.

14.7.1.1 CPU, Memory and Session Usage

Note: These condition filters only apply to the ZLD platform type.

In case you want to know how much of the system resources are being used by the monitored devices, use this screen to configure a rule for CPU, memory and session usage conditions.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **CPU Usage, Memory Usage** or **Session Usage** in the **Condition** field.

The fields are described in the following table.

Table 260 System Setting > Rule-based Alert > Add/Edit > CPU/Memory/Session Usage

LABEL	DESCRIPTION
Rule Name	This is the name identifying the rule. If you are adding a new rule, you can enter up to 28 alphanumeric characters for the rule name. If you are editing a rule, this field cannot be changed.
Choose Platform Type	This specifies what firmware platform the rule applies to. Select **ZLD**.
Information icon	Click this for a quick look of which devices belong to which platform type.
Filters	Set the criteria for the alert-based rule in this section.
Condition	Select **CPU Usage**, **Memory Usage** or **Session Usage** in this field.
(CPU/Memory/ Session) Usage.. %	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • **>=** - Select this if you want to be alerted when a device uses resources greater than or equal to the percentage value you set. • **<=** - Select this if you want to be alerted when a device uses resources less than or equal to the percentage value you set. • **<** - Select this if you want to be alerted when a device uses resources greater than the percentage value you set. • **>** - Select this if you want to be alerted when a device uses resources less than the percentage value you set. For example, choose **CPU Usage**, select **>=** and set the percentage value to 75. This means Vantage Report sends an alert once a monitored device uses or exceeds usage of 75% of CPU resource allocation for a set time (see **Period.. minutes** field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device uses or exceeds usage of 75% of CPU resource allocation for 5 minutes, Vantage Report sends out an alert.
Add Criteria	Click this to add the set criteria to the list box.
Remove Criteria	Select a criteria from the list box and click **Remove** to delete this criteria.
Match all of the following	Click this if you want all criteria to apply before Vantage Report sends out a notification.
Match any of the following	Click this if you want Vantage Report to send out a notification even if only one criteria has been met.
Alert Setting	Vantage Report sends out a notification immediately as soon as conditions set in the rule are detected. Set when you want Vantage Report to send out the second and third notifications in this section.
Second Alert after.. minutes	Specify when you want Vantage Report to send a second e-mail notification. Enter the number of minutes between 1 to 60. Enter **0** to disable this.
Third alert after.. minutes	Specify when you want Vantage Report to send a third e-mail notification. Enter the number of minutes between 1 to 60. Enter **0** to disable this.
Select Devices	Check which devices the rule applies to. Click **Select All** if you want the conditions you set to be monitored for all devices.
Notification	
Notification Choose	Select a notification profile that applies to this rule. Click the **Setting** icon to take you to the **System Setting** > **Notification** screen (see Section 14.6 on page 469) for managing notification profiles.
Apply	Click this to add the rule or apply the edits to an existing rule.

Table 260 System Setting > Rule-based Alert > Add/Edit > CPU/Memory/Session Usage

LABEL	DESCRIPTION
Reset	Click this to leave all the fields blank or back to the original values if you are editing a previous configuration.
Cancel	Click this to go back to the **Rule-Based Alert** screen.

14.7.1.2 Port Usage

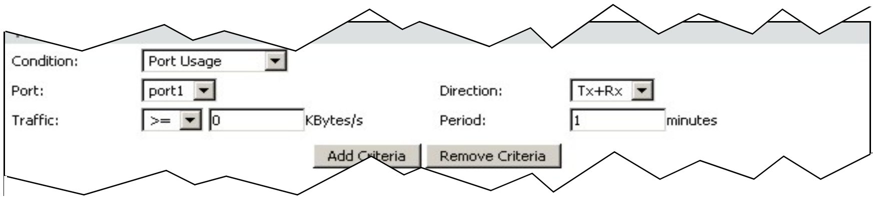
Use this screen to configure an alert rule for port usage.

Note: This condition filter only applies to the ZLD platform type.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Port Usage** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 280 System Setting > Rule-based Alert > Add/Edit > Port Usage



Condition: Port Usage
Port: port1
Direction: Tx+Rx
Traffic: >= 0 KBytes/s
Period: 1 minutes

The fields above are described in the following table.

Table 261 System Setting > Rule-based Alert > Add/Edit > Port Usage

LABEL	DESCRIPTION
Condition	Select **Port Usage** in this field.
Port	Select which port in the device you want to monitor.
Direction	Select if you want to check outgoing (**Tx**) or incoming (**Rx**) traffic. You can also choose both (**Tx+Rx**).
Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • **>=** - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • **<=** - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • **<** - Select this if you want to be alerted when a device uses resources greater than the value you set. • **>** - Select this if you want to be alerted when a device uses resources less than the value you set. For example, choose **Port1** port and **Tx** direction, select **>=** and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes/s outgoing traffic on port 1 for a set time (see **Period.. minutes** field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of outgoing port traffic for 5 minutes, Vantage Report sends out an alert.

See Section Table 260 on page 474 for descriptions of other table fields found in this screen.

14.7.1.3 Interface Usage

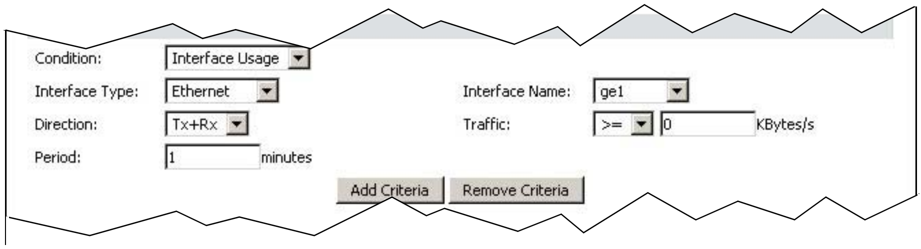
Use this screen to configure an alert rule for interface type (such as **Ethernet**, **VLAN** or **Bridge**) used by the selected device(s).

Note: This condition filter only applies to the ZLD platform type.

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Interface Usage** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 281 System Setting > Rule-based Alert > Add/Edit > Interface Usage



Condition: Interface Usage
Interface Type: Ethernet
Interface Name: ge1
Direction: Tx+Rx
Traffic: >= 0 KBytes/s
Period: 1 minutes

The fields above are described in the following table.

Table 262 System Setting > Rule-based Alert > Add/Edit > Interface Usage

LABEL	DESCRIPTION
Condition	Select **Interface Usage** in this field.
Interface Type	Select which interface mode you want to monitor. Interface refers to the connectivity implementation of the device to the network or other devices. Choose one of the following. • **Ethernet** • **VLAN** • **PPP** (stands for Point-to-Point Protocol) • **Bridge** • **Dial-backup** • **3G** (stands for 3rd Generation) • **wireless**
Interface Name	Select the specific name for devices that can have multiple interface profiles.
Direction	Select if you want to check outgoing (**Tx**) or incoming (**Rx**) traffic. You can also choose both (**Tx+Rx**).

Table 262 System Setting > Rule-based Alert > Add/Edit > Interface Usage

LABEL	DESCRIPTION
Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • **>=** - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • **<=** - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • **<** - Select this if you want to be alerted when a device uses resources greater than the value you set. • **>** - Select this if you want to be alerted when a device uses resources less than the value you set. For example, choose **Ethernet**, specifying **lan1** interface and **Tx** direction, select **>=** and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes/s outgoing traffic on lan1 of the Ethernet interface for a set time (see **Period.. minutes** field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of interface traffic for 5 minutes, Vantage Report sends out an alert.

See Section Table 260 on page 474 for descriptions of other table fields found in this screen.

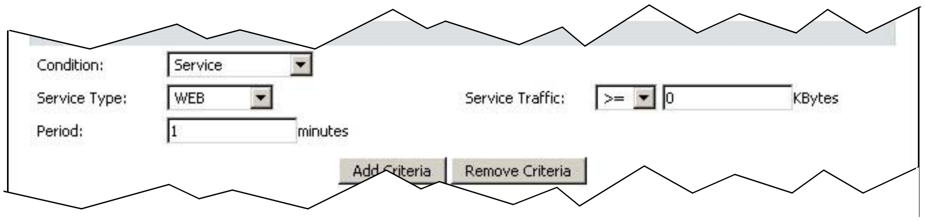
14.7.1.4 Service

Use this screen to configure an alert rule based on a service (such as **Web**, **Mail** or **FTP**) used by the selected device(s).

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select **Service** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 282 System Setting > Rule-based Alert > Add/Edit > Service



Condition: Service

Service Type: WEB

Service Traffic: >= 0 KBytes

Period: 1 minutes

The fields above are described in the following table.

Table 263 System Setting > Rule-based Alert > Add/Edit > Service

LABEL	DESCRIPTION
Condition	Select **Service** in this field.
Interface Type	Select which service type you want to monitor. Choose one of the following. • **WEB** • **FTP** • **MAIL** • **IPSec VPN** • **SSL VPN**

Table 263 System Setting > Rule-based Alert > Add/Edit > Service

LABEL	DESCRIPTION
Service Traffic.. KBytes/s	Set your filters according to how much system resources are being consumed by monitored devices. The following parameters can be used. • **>=** - Select this if you want to be alerted when a device uses resources greater than or equal to the value you set. • **<=** - Select this if you want to be alerted when a device uses resources less than or equal to the value you set. • **<** - Select this if you want to be alerted when a device uses resources greater than the value you set. • **>** - Select this if you want to be alerted when a device uses resources less than the value you set. For example, choose **MAIL**, select **>=** and set the percentage value to 100 KByte/s. This means Vantage Report sends an alert once a monitored device uses or exceeds 100 KBytes for mail for a set time (see **Period.. minutes** field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device reaches or exceeds 100 KByte/s of mail traffic for 5 minutes, Vantage Report sends out an alert.

See Section Table 260 on page 474 for descriptions of other table fields found in this screen.

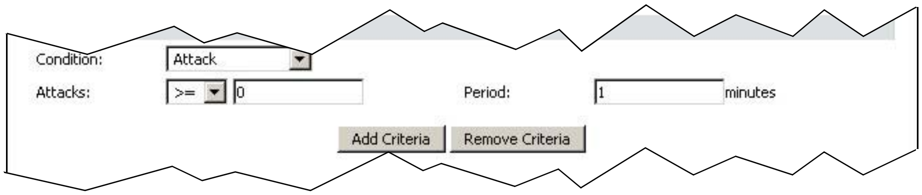
14.7.1.5 Attack/Intrusion/Antivirus/Antispam

Use this screen to configure an alert rule for the number of attacks, intrusions, virus and spam detected on the selected device(s).

Click **System Setting > Rule-based Alert** then either click on the link of the existing **Rule Name** or click **Add**. Select either **Attack**, **Intrusion**, **Antivirus** or **Antispam** in the **Condition** field.

The fields in the **Filter** section change to the following.

Figure 283 System Setting > Rule-based Alert > Add/Edit > Attack/Intrusion/Antivirus/Antispam



Condition: Attack

Attacks: >= 0

Period: 1 minutes

The fields above are described in the following table.

Table 264 System Setting > Rule-based Alert > Add/Edit > Attack/Intrusion/Antivirus/Antispam

LABEL	DESCRIPTION
Condition	Select either **Attack**, **Intrusion**, **Antivirus** or **Antispam** in this field.
Attacks	Set your filters according to how many attacks, intrusions, virus and spam are detected on a device. The following parameters can be used. • **>=** - Select this if you want to be alerted when number of encounters is greater than or equal to the value you set. • **<=** - Select this if you want to be alerted when number of encounters is less than or equal to the value you set. • **<** - Select this if you want to be alerted when number of encounters is greater than the value you set. • **>** - Select this if you want to be alerted when number of encounters is less than the value you set. For example, choose **Attack**, select **>=** and set the percentage value to 5. This means Vantage Report sends an alert once a monitored device receives 5 attacks for a set time (see **Period.. minutes** field below).
Period.. minutes	Set this to the number of minutes the condition persists before Vantage Report sends out an alert. Using the previous example, you can set the period to 5 minutes. This means that if the device received 5 attacks within 5 minutes, Vantage Report sends out an alert.

See Section Table 260 on page 474 for descriptions of other table fields found in this screen.

15

User Management

The **root** account or accounts in the 'super' group can use these screens to view, add, edit, or remove Vantage Report groups and users. Other users can only use these screens to look at and edit their user settings, including their password. The screens are the same except where noted below.

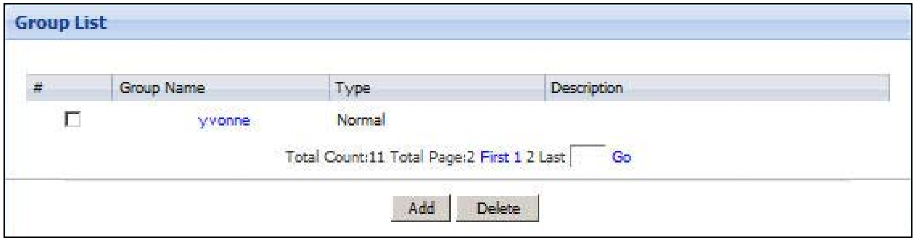
15.1 Group Screen

Use the **Group** screen to set up user group for Vantage Report.

Click **User Management > Group** to open the **Group** screen.

Note: Only the root account or accounts in the 'super' group can open this screen.

Figure 284 User Management > Group



Group List

#	Group Name	Type	Description
□	yvonne	Normal	

Total Count:11 Total Page:2 First 1 2 Last Go

Each field is described in the following table.

Table 265 User Management > Group

LABEL	DESCRIPTION
#	Select the check box next to a user group, and click **Delete** to remove the group. This does not apply to the **super** group since you cannot delete it.
Group Name	This field displays the name of the user group. You can also click this to edit the group settings. The **Add/Edit Group** screen appears.
Type	This field displays the type of the user group. • **Super** displays if the group has read/write/execute permissions for all Vantage Report screens. • **Normal** displays if the group has read/write permissions for the **Monitor**, **Report** and **Logs > Log Reviewer** screens. • **Read-Only** displays if the group has read permissions only for the **Monitor**, **Report** and **Logs > Log Reviewer** screens.
Description	This field displays the description for the group.
Total Count	This field displays how many groups there are.
Total Page	This field displays how many screens it takes to display all the groups.
First .. Last	Click **First**, **Last**, or a specific page number to look at the groups on that page. Some choices are not available, depending on the number of pages.s

Table 265 User Management > Group

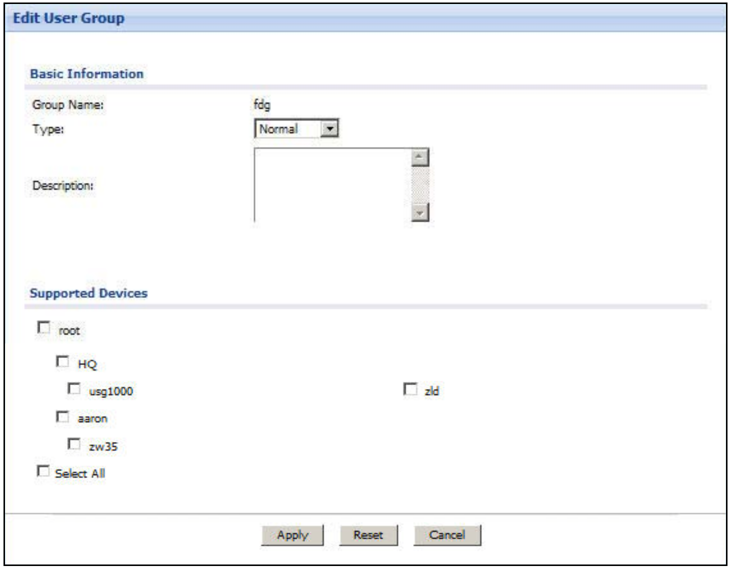
LABEL	DESCRIPTION
Go	Enter the page number you want to see, and click **Go**.
Add	Click this to create a new group. The **Add/Edit Group** screen appears.
Delete	Click this to delete the groups that are selected in Index field. You cannot to delete a group if it still contains any users.

15.1.1 Group > Add/Edit Group Screen

Use this screen to add or edit a user group.

Click the link in an entry in **User Management > Group** to access this screen.

Figure 285 User Management > Group > Add/Edit Group



Edit User Group

Basic Information

Group Name: fdg

Type: Normal

Description:

Supported Devices

□ root

□ HQ

□ usg1000 □ zld

□ aaron

□ zw35

□ Select All

All the fields are described in the following table.

Table 266 User Management > Group > Add/Edit Group

LABEL	DESCRIPTION
Basic Information	Use this part of the screen to view the group name you selected and to modify the description.
Group Name	If you are editing an existing group, this field is read-only. It displays the name of the user. If you are creating a new group, enter the user name for the new account. The user name must be 1-28 alphanumeric characters and/or underscores(_) long, and it must begin with a letter or underscore.
Type	Select the user group type. If you select **Normal**, the members of this group can access the **Monitor**, **Report** and **Logs** screens with read/write permissions. If you select **Read-Only**, the members of this group can access the **Monitor**, **Report** and **Logs** screens with read permissions only.
Description	Enter the description for the user group.

Table 266 User Management > Group > Add/Edit Group

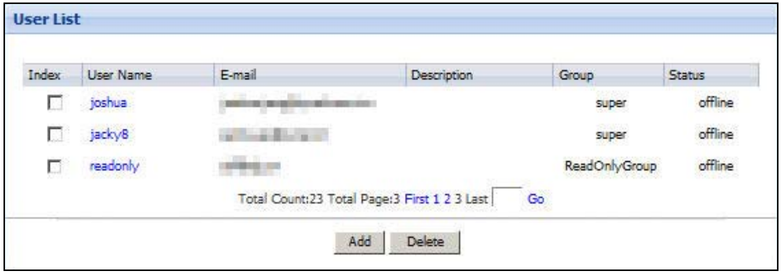
LABEL	DESCRIPTION
Supported Devices	Use this part of the screen to select the devices the user group can view. The available folders and devices are listed, select individual devices or a folder to select all devices under it. Select the Select All to select all folders and devices.
Apply	Click this to save your settings and close the screen.
Reset	Click this to change the settings in this screen to the last-saved values.
Cancel	Click this to return to the previous screen without saving any changes.

15.2 Account Screen

Use the **Account** screen to manage user accounts for Vantage Report.

Click **User Management > Account** to open the **Account** screen.

Figure 286 User Management > Account



User List

Index	User Name	E-mail	Description	Group	Status
□	joshua	[redacted]		super	offline
□	jacky8	[redacted]		super	offline
□	readonly	[redacted]		ReadOnlyGroup	offline

Total Count:23 Total Page:3 First 1 2 3 Last [ ] Go

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

Table 267 User Management > Account

LABEL	DESCRIPTION
Index	Select the check box next to a user account, and click **Delete** to remove the account. This does not apply to the **root** account since you cannot delete it.
User Name	This field displays the user name used to log in. You can also click this to edit the account settings. The **Add/Edit User Account** screen appears.
E-mail	This field displays the e-mail address associated with the user account. This address is used for notifications (**root** only) and forgotten passwords.
Description	This field displays the description for the user account.
Group	This field displays the group the user account belongs to.
Status	This field displays whether or not the user is logged in to Vantage Report. **off line** - this user is not currently logged in **on line** - this user is currently logged in
Total Count	This field displays how many accounts there are.
Total Page	This field displays how many screens it takes to display all the accounts.
First .. Last	Click **First**, **Last**, or a specific page number to look at the accounts on that page. Some choices are not available, depending on the number of pages.
Go	Enter the page number you want to see, and click **Go**.

Table 267 User Management > Account

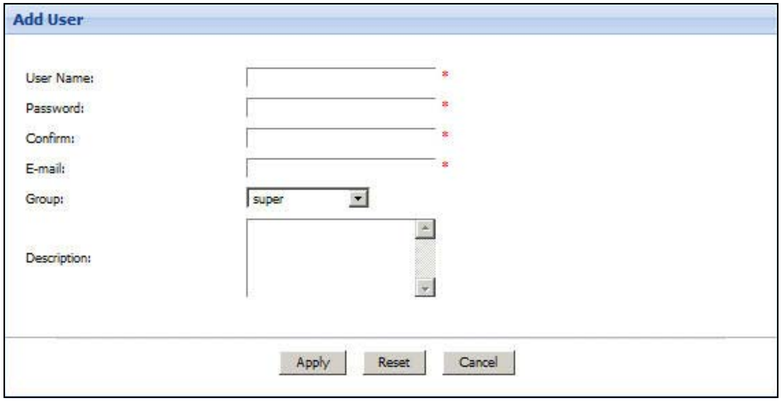
LABEL	DESCRIPTION
Add	Click this to create a new user account. The **Add/Edit User Account** screen appears.
Delete	Click this to delete the user accounts that are selected in **Index** field. If a user is currently logged in, the user is kicked out of the system the next time the session accesses the Vantage Report server.

15.2.1 Account > Add/Edit User Account Screen

Use this screen to add or edit a user account.

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

Figure 287 User Management > Account > Add/Edit User Account



Add User

User Name: *

Password: *

Confirm: *

E-mail: *

Group: super

Description:

Each field is described in the following table.

Table 268 User Management > Account > Add/Edit User Account

LABEL	DESCRIPTION
User Name	If you are editing an existing account, this field is read-only. It displays the user name used to log in. If you are creating a new account, enter the user name for the new account. The user name must be 1-28 alphanumeric characters and/or underscores(_) long, and it must begin with a letter or underscore.
Password	If you are editing an existing account, this field displays the same number of asterisks, regardless of the current password. You can change the password. If you are creating a new account or changing the password of an existing account, enter the password for the new account. The password must be 4-30 alphanumeric characters and/or underscores(_) long.
Confirm	Type the password again to verify it, if you are creating a new account or changing the password of an existing account.
E-mail	Enter the e-mail address associated with the user account. This address is used for notifications (**root** only) and forgotten passwords.
Group	Select the group for the user account. The ‘super’ group can view all devices, just like the **root** account.
Description	Enter the description for the user account.
Apply	Click this to save your settings and close the screen.

Table 268 User Management > Account > Add/Edit User Account

LABEL	DESCRIPTION
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.

16

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

I cannot start the Vantage Report server.

1 Make sure the following system variables are defined.

```
PATH=%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem
```

Do the following to check these variables in different operating systems.

- In Windows 2000, click **Start** > **Settings** > **Control Panel** > **System** > **Advanced** > **Environment Variables**.
- In Windows XP, click **Start** > **Control Panel** > **System** > **Advanced** > **Environment Variables**.
- In Windows Vista/7, click **Start** > **Control Panel** > **System** > **Advanced system settings** > **Advanced > Environment Variables**.

Make sure the variables are in the **System Variables** box.

2 If the problem continues, follow these steps to collect logs.

- Edit the file `<Installed directory>\vrpt\conf\log4j.properties`.

  Change the following:

  log4j.logger.com.zyxel.vantage.vrpt = INFO

  log4j.logger.com.zyxel.vantage.web = INFO

  To:

  log4j.logger.com.zyxel.vantage.vrpt = DEBUG

  log4j.logger.com.zyxel.vantage.web = DEBUG
- Restart the Vantage Report server.
- Get the log files from the `<Installed directory>\vrpt\log` folder and send them to your local vendor.

There is no information in any report for my device.

1 If you just added the device, wait. See Table 3 on page 20 for the amount of time it takes for information to appear in each report.

2 Look for the device’s MAC address in `<Installed directory>\vrpt\log\LogRecord.log` in the Vantage Report installation directory. This file keeps track of all the log entries received by the syslog server in Vantage Report, including log entries for devices that are not set up in Vantage Report.

- If the MAC address is in the file, Vantage Report is receiving information from the device. Wait. If the **Attribute** is **Unregistered**, however, the MAC address is not set up correctly in Vantage Report. See section 3.4.
- If the MAC address is not in the file, Vantage Report is not receiving information from the device. Make sure you have configured the ZyXEL devices correctly. See section 2.6.

3 Make sure packets on TCP port 3316, UDP port 514, and the port number you specified during installation are forwarded to the Vantage Report server, especially if the Vantage Report server runs behind a NAT or firewall.

4 Check the amount of available disk space on the Vantage Report server. If it is less than the minimum amount of free disk space required to run Vantage Report, the Vantage Report server stops receiving log entries.

5 Make sure your ZyXEL devices support Vantage Report. Check the release notes for the current firmware version.

6 Check the connections between the ZyXEL devices and Vantage Report server.

7 Make sure the system times on the Vantage Report server and the managed devices are configured correctly.

If the problem continues, contact your local vendor.

There is information in some reports, but there is no information in others.

1 Make sure your ZyXEL devices support these reports. Check the release notes for the current firmware version.

2 Make sure you have configured the ZyXEL devices correctly. See section 2.6.

3 Make sure there are log entries or traffic statistics for the report dates you selected. For example, if there were no attacks yesterday, yesterday’s attack report is empty.

If the problem continues, contact your local vendor.

My web configurator screens still show information from the previous version (like the old version number) after a successful upgrade.

1 Clear the browser’s cache on your computer.

- In Internet Explorer, click **Tools** > **Internet Option** > **Delete Cookies** > **Delete files**.
- In Firefox, click **Tools** > **Options** > **Privacy** > **Cache** > **Clear Cache Now**.
- In Mozilla, click **Edit** > **Preferences** > **Privacy** > **Cache** > **Clear**.

2 Close your browser and open a new web configurator session. The version number should be updated.

ZyWALL Log Descriptions

This appendix provides descriptions of example log messages.

Table 269 AV Logs

LOG MESSAGE	DESCRIPTION
`%s Virus infected[%s] - ID:%s,%s,%s.`	The device detected a virus of the specified severity {High|Medium|Low}; {Protocol} Virus infected - ID:{Virus ID}, {Virus Name}, {Name of the Infected File}
`Dangerous URL:[%s], virus detected!`	The device detected a virus in a URL a user tried to access; %s is the URL link.

Table 270 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 271 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 272 Blocked Web Site Logs

LOG MESSAGE	DESCRIPTION
`%s :%s`	The rating server responded that the web site is in a specified category and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
`%s: Unrated`	The rating server responded that the web site cannot be categorized and access was blocked according to a content filter profile. %s: website host
`%s: Service is unavailable`	Content filter rating service is temporarily unavailable and access to the web site was blocked due to: 1. Can't resolve rating server IP (No DNS) 2. Invalid service license 4. Rating service is restarting 5. Can't connect to rating server 6. Query failed 7. Query timeout 8. Too many queries 9. Unknown reason %s: website host
`%s: %s(cache hit)`	The web site's category exists in the device's local cache and access was blocked according to a content filter profile. 1st %s: website host 2nd %s: website category
`%s: Not in trusted web list`	The web site is not a trusted host/domain, and the device blocks all traffic except for trusted web sites. %s: website host
`%s: Contains ActiveX`	The web site contains ActiveX and access was blocked according to a profile. %s: website host
`%s: Contains Java applet`	The web site contains Java applet and access was blocked according to a profile. %s: website host
`%s: Contains cookie`	The web site contains a cookie and access was blocked according to a profile. %s: website host
`%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

Table 272 Blocked Web Site Logs (continued)

LOG MESSAGE	DESCRIPTION
`%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 273 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.

Table 273 User Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 274 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

Table 274 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
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.

Table 274 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.
`Update has failed. Because of lack must fields.`	The device received an incomplete response from the update server and it caused a parsing error for the device.
`Update server is busy now. File download after %d seconds.`	The update server was busy so the device will wait for the specified number of seconds and send the download request to the update server again.
`Device has latest file. No need to update.`	The device already has the latest version of the file so no update is needed.
`Device has latest signature file; no need to update`	The device already has the latest version of the signature file so no update is needed.
`Connect to update server has failed.`	The device cannot connect to the update server.
`Wrong format for packets received.`	The device cannot parse the response returned by the server. Maybe some required fields are missing.
`Server setting error. Update stop.`	The device could not resolve the update server's FQDN to an IP address through gethostbyname(). The update process stopped.
`Build query message failed.`	Some information was missing in the packets that the device sent to the server.
`Starting signature update.`	The device started an IDP signature update.
`Signature download has succeeded.`	The device successfully downloaded a signature file.
`Signature update has succeeded.`	The device successfully downloaded and applied an IDP signature file.
`Signature update has failed:%s.`	The signature update signature failed, an error message returned by the update server will be appended to this log. %s: error message returned by update server
`Signature download has failed.`	The device still can't download the IDP signature after 3 retries.
`Signature update has failed. Do %d retry.`	The IDP signature update failed, so the device will process 3 retries. %d: retry times (1~3)
`Resolve server IP has failed.`	The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname().
`Connect to MyZyXEL.com server has failed.`	The device could not connect to the MyZyXEL.com server.

Table 274 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`Build query message has failed.`	Some information was missing in the packets that the device sent to the server.
`Verify server's certificate has failed.`	The device could not process an HTTPS connection because it could not verify the server's certificate.
`Get server response has failed.`	The device sent packets to the server, but did not receive a response. The root cause may be that the connection is abnormal.
`Expiration daily-check has failed:%s.`	The daily check for service expiration failed, an error message returned by the MyZyXEL.com server will be appended to this log. %s: error message returned by myZyXEL.com server
`Do expiration daily-check has failed. Because of lack must fields.`	The device received an incomplete response to the daily service expiration check and the packets caused a parsing error for the device.
`Server setting error.`	The device could not retrieve the server's IP address or FQDN from local.
`Do expiration daily-check has failed.`	The daily check for service expiration failed.
`Do expiration daily-check has succeeded.`	The daily check for service expiration was successful.
`Expiration daily-check will trigger PPP interface. Do self-check.`	Before the device sends an expiration day check packet, it needs to check whether or not it will trigger a PPP connection.
`System bootup. Do expiration daily-check.`	The device processes a service expiration day check immediately after it starts up.
`After register. Do expiration daily-check immediately.`	The device processes a service expiration day check immediately after device registration.
`Time is up. Do expiration daily-check.`	The processes a service expiration day check every 24 hrs.
`Read MyZyXEL.com storage has failed.`	Read data from EEPROM has failed.
`Open /proc/MRD has failed.`	This error message is shown when getting MAC address.
`IDP service has expired.`	The IDP service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count.
`Content-Filter service has expired.`	The content filtering service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count.
`Unknown TLS/SSL version: %d.`	The device only supports SSLv3 protocol. %d: SSL version assigned by client.
`Load trusted root certificates has failed.`	The device needs to load the trusted root certificate before the device can verify a server's certificate. This log displays if the device failed to load it.
`Certificate has expired.`	Verification of a server's certificate failed because it has expired.
`Self signed certificate.`	Verification of a server's certificate failed because it is self-signed.
`Self signed certificate in certificate chain.`	Verification of a server's certificate failed because there is a self-signed certificate in the server's certificate chain.

Table 274 myZyXEL.com Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 275 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.
`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.

Table 275 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
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.

Table 275 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 process failed. IDP activation failed.
`[type=`*`<type>`*`] `*`<message>`*`, Action: `*`<action>,`*` Severity: `*`<severity>`*	IDP triggered event log. <*type*> = {sig(<*id*>) | scan-detection(<*attack*>) | flood-detection(<*attack*>) | http-inspection(<*attack*>) | tcp-decoder(<*attack*>) | udp-decoder(<*attack*>) | icmp-decoder(<*attack*>) }, <*attack*> = attack type. <severity> = {very low | low | medium | high | severe}
`Program DFA failed.`	IDP program DFA to hardware search engine failed.
`IDP signature update failed. Fail to create temporary directory`	IDP signature update failed. Create /tmp/sig directory failed
`IDP signature update failed. Fail to extract temporary file.`	IDP signature update failed. Extract signature package to /tmp/sig failed.
`IDP signature update failed. Invalid IDP config file.`	IDP signature update failed. Sig_check_update check failed.
`IDP signature update failed. Invalid signature content.`	IDP signature update failed. Sig_query check signature content failed.

Table 275 IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 276 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.
`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.

Table 276 Application Patrol Logs (continued)

LOG MESSAGE	DESCRIPTION
`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
`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 277 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.
`[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.

Table 277 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`[SA] : Tunnel [%s] Phase 1 negotiation mode mismatch`	%s is the tunnel name. When negotiating Phase-1, the negotiation mode did not match.
`[SA] : Tunnel [%s] Phase 2 authentication algorithm mismatch`	%s is the tunnel name. When negotiating Phase-2, the authentication algorithm did not match.
`[SA] : Tunnel [%s] Phase 2 encapsulation mismatch`	%s is the tunnel name. When negotiating Phase-2, the encapsulation did not match.
`[SA] : Tunnel [%s] Phase 2 encryption algorithm mismatch`	%s is the tunnel name. When negotiating Phase-2, the encryption algorithm did not match.
`[SA] : Tunnel [%s] Phase 2 pfs mismatch`	%s is the tunnel name. When negotiating Phase-2, the PFS specified did not match.
`[SA] : Tunnel [%s] Phase 2 pfs unsupported: %d`	%s is the tunnel name. When negotiating Phase-2, this device does not support the PFS specified.
`[SA] : Tunnel [%s] Phase 2 SA encapsulation mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA encapsulation did not match.
`[SA] : Tunnel [%s] Phase 2 SA protocol mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA protocol did not match.
`[SA] : Tunnel [%s] SA sequence size mismatch`	%s is the tunnel name. When negotiating Phase-2, the SA sequence size did not match.
`[XCHG] exchange type is not IP, AGGR, or INFO`	This device is the responder and this is the initiator’s first packet, but exchange type is not IP, AGGR, or INFO and the packet is ignored.
`Cannot resolve My IP Addr %s for Tunnel [%s]`	1st %s is my ip address. 2nd %s is the tunnel name. When selecting a matched proposal in phase-1, the engine could not get My-IP address.
`Cannot resolve Secure Gateway Addr %s for Tunnel [%s]`	1st %s is my ip address. 2nd %s is the tunnel name; When selecting a matched proposal in phase-1, the engine could not get the correct secure gateway address.
`Could not dial dynamic tunnel "%s"`	%s is the tunnel name. The tunnel is a dynamic tunnel and the device cannot dial it.
`Could not dial incomplete tunnel "%s"`	%s is the tunnel name. The tunnel setting is not complete.
`Could not dial manual key tunnel "%s"`	%s is the tunnel name. The manual key tunnel cannot be dialed.
`DPD response with invalid ID`	When receiving a DPD response with invalid ID ignored.
`DPD response with no active request`	When receiving a DPD response with no active query.
`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.

Table 277 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Recv:[SA]%s[KE]%s[ID]%s[CERT]%s[CR]%s[HASH]%s[SIG]%s[NONCE]%s[DEL]%s[VID]%s[ATTR]%s	This is a combined message for incoming IKE packets.
Send Main Mode request to [%s]	%s is the remote name. The device sent a request to enter Main Mode.
Send Aggressive Mode request to [%s]	%s is the remote name. The device sent a request to enter Aggressive Mode.
Send DPD request to "%s:%s"	%s:%s is peer IP:Port. The device sent a Dead Peer Detection request to the peer.
Send DPD response to "%s:%s"	%s:%s is peer IP:Port. The device sent a DPD response sent to the peer.
Send:[ID]%s[SA]%s[KE]%s[ID]%s[CERT]%s[CR]%s[HASH]%s[SIG]%s[NONCE]%s[DEL]%s[VID]%s[ATTR]%s[	This is a combined message for outgoing IKE packets.
Start Phase 2: Quick Mode	Indicates the beginning of phase 2 using quick mode.
The cookie pair is : 0x%08x%08x / 0x%08x%08x	Indicates the initiator/responder cookie pair.
The IPSec tunnel "%s" is already established	%s is the tunnel name. When dialing a tunnel, the tunnel is already dialed.
Tunnel [%s] built successfully	%s is the tunnel name. The phase-2 tunnel negotiation is complete.
Tunnel [%s] Phase 1 pre-shared key mismatch	%s is the tunnel name. When negotiating phase-1, the pre-shared key did not match.
Tunnel [%s] Recving IKE request	%s is the tunnel name. The device received an IKE request.
Tunnel [%s] Sending IKE request	%s is the tunnel name. The device sent an IKE request.
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 277 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 278 IPSec Logs

LOG MESSAGE	DESCRIPTION
`Corrupt packet, Inbound transform operation fail`	The device received corrupt IPsec packets and could not process them.
`Encapsulated packet too big with length`	An outgoing packet needed to be transformed but was longer than 65535.
`Get inbound transform fail`	When performing inbound processing for incoming IPSEC packets and ICMPs related to them, the engine cannot obtain the transform context.
`Get outbound transform fail`	When outgoing packet need to be transformed, the engine cannot obtain the transform context.
`Inbound transform operation fail`	After encryption or hardware accelerated processing, HWAccel dropped packet (resource shortage, corrupt packet, invalid MAC, and so on).
`Outbound transform operation fail`	After encryption or hardware accelerated processing, Hwaccel dropped packet (e.g., resource overflow, corrupt packet, and so on).
`Packet too big with Fragment Off`	An outgoing packet needed to be transformed, but the fragment flag was off and the packet was too big.
`SPI:0x%x SEQ:0x%x Execute transform step fail, ret=%d`	The variables represent the SPI, sequence number and the error number. When trying to perform transforming, the engine returned an error.
`SPI:0x%x SEQ:0x%x No rule found, Dropping packet`	The variables represent the SPI and the sequence number. The packet did not match the tunnel policy and was dropped.
`SPI:0x%x SEQ:0x%x Packet Anti-Replay detected`	The variables represent the SPI and the sequence number. The device received a packet again (that it had already received).
`VPN connection %s was disabled.`	%s is the VPN connection name. An administrator disabled the VPN connection.
`VPN connection %s was enabled.`	%s is the VPN connection name. An administrator enabled the VPN connection.

Table 279 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 280 Sessions Limit Logs

LOG MESSAGE	DESCRIPTION
`Maximum sessions per host (%d) was exceeded.`	%d is maximum sessions per host.

Table 281 Policy Route Logs

LOG MESSAGE	DESCRIPTION
`Can't open bwm_entries`	Policy routing can't activate BWM feature.
`Can'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.

Table 281 Policy Route Logs (continued)

LOG MESSAGE	DESCRIPTION
`mblock: allocate memory failed!`	Allocating policy routing rule fails: insufficient memory.
`pt: allocate memory failed!`	Allocating policy routing rule fails: insufficient memory.
`To send message to policy route daemon failed!`	Failed to send control message to policy routing manager.
`The policy route %d allocates memory fail!`	Allocating policy routing rule fails: insufficient memory. %d: the policy route rule number
`The policy route %d uses empty user group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty source address group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty destination address group!`	Use an empty object group. %d: the policy route rule number
`The policy route %d uses empty service group`	Use an empty object group. %d: the policy route rule number
`Policy-route rule %d was inserted.`	Rules is inserted into system. %d: the policy route rule number
`Policy-route rule %d was appended.`	Rules is appended into system. %d: the policy route rule number
`Policy-route rule %d was modified.`	Rule is modified. %d: the policy route rule number
`Policy-route rule %d was moved to %d.`	Rule is moved. 1st %d: the original policy route rule number 2nd %d: the new policy route rule number
`Policy-route rule %d was deleted.`	Rule is deleted. %d: the policy route rule number
`Policy-route rules were flushed.`	Policy routing rules are cleared.

Table 282 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).

Table 282 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`HTTP port has changed to port %s.`	An administrator changed the port number for HTTP. %s is port number assigned by user
`HTTP port has changed to default port.`	An administrator changed the port number for HTTP back to the default (80).
`SSH port has been changed to port %s.`	An administrator changed the port number for SSH. %s is port number assigned by user
`SSH port has been changed to default port.`	An administrator changed the port number for SSH back to the default (22).
`SSH certificate:%s does not exist. SSH service will not work.`	An administrator assigned a nonexistent certificate to SSH. %s is certificate name assigned by user
`SSH certificate:%s format is wrong. SSH service will not work.`	After an administrator assigns a certificate for SSH, the device needs to convert it to a key used for SSH. %s is certificate name assigned by user
`TELNET port has been changed to port %s.`	An administrator changed the port number for TELNET. %s is port number assigned by user
`TELNET port has been changed to default port.`	An administrator changed the port number for TELNET back to the default (23).
`FTP certificate:%s does not exist.`	An administrator assigned a nonexistent certificate to FTP. %s is certificate name assigned by user
`FTP port has been changed to port %s.`	An administrator changed the port number for FTP. %s is port number assigned by user
`FTP port has been changed to default port.`	An administrator changed the port number for FTP back to the default (21).
`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

Table 282 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`Set timezone to %s.`	An administrator changed the time zone. %s is time zone value
`Set timezone to default.`	An administrator changed the time zone back to the default (0).
`Enable daylight saving.`	An administrator turned on daylight saving.
`Disable daylight saving.`	An administrator turned off daylight saving.
`DNS access control rules have been reached the maximum number.`	An administrator tried to add more than the maximum number of DNS access control rules (64).
`DNS access control rule %u of DNS has been appended.`	An administrator added a new rule. %u is rule number
`DNS access control rule %u has been inserted.`	An administrator inserted a new rule. %u is rule number
`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

Table 282 Built-in Services Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.
`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 283 System Logs

LOG MESSAGE	DESCRIPTION
`Port %d is up!!`	When LINK is up, %d is the port number.
`Port %d is down!!`	When LINK is down, %d is the port number.
`%s is dead at %s`	A daemon (process) is gone (was killed by the operating system). 1st %s: Daemon Name, 2nd %s: date+time
`%s process count is incorrect at %s`	The count of the listed process is incorrect. 1st %s: Daemon Name, 2nd %s: date+time

Table 283 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`%s becomes Zombie at %s`	A process is present but not functioning. 1st %s: Daemon Name, 2nd %s: date+time When memory usage exceed threshold-max, memory usage reaches %d%% :mem-threshold-max. When disk usage exceeds threshold-max, %s: Partition name file system usage reaches %d%%: disk-threshold-max. When memory usage drops below threshold-min, System Memory usage drops below the threshold of %d%%: mem-threshold-min. When disk usage drops below threshold-min, %s: partition_name file system drops below the threshold of %d%%: disk-threshold-min.
`DHCP Server executed with cautious mode enabled`	DHCP Server executed with cautious mode enabled.
`DHCP Server executed with cautious mode disabled`	DHCP Server executed with cautious mode disabled.
`Received packet is not an ARP response packet`	A packet was received but it is not an ARP response packet.
`Receive an ARP response`	The device received an ARP response.
`Receive ARP response from %s (%s)`	The device received an ARP response from the listed source.
`The request IP is: %s, sent from %s`	The device accepted a request.
`Received ARP response NOT for the request IP address`	The device received an ARP response that is NOT for the requested IP address.
`Receive an ARP response from the client issuing the DHCP request`	The device received an ARP response from the client issuing the DHCP request.
`Receive an ARP response from an unknown client`	The device received an ARP response from an unknown client.
`In total, received %d arp response packets for the requested IP address`	The device received the specified total number of ARP response packets for the requested IP address.
`Clear arp cache successfully.`	The ARP cache was cleared successfully.
`Client MAC address is not an Ethernet address`	A client MAC address is not an Ethernet address.
`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.

Table 283 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`NTP update successful, current time is %s`	The device successfully synchronized with a NTP time server. %s is the time format.
`NTP update failed`	The device was not able to synchronize with the NTP time server successfully.
`Device is rebooted by administrator!`	An administrator restarted the device.
`Insufficient memory.`	Cannot allocate system memory.
`Connect to dyndns server has failed.`	Cannot connect to members.dyndns.org to update DDNS.
`Update the profile %s has failed because of strange server response.`	Update profile failed because the response was strange, %s is the profile name.
`Update the profile %s has succeeded because the IP address of FQDN %s was not changed.`	Update profile succeeded, because the IP address of profile is unchanged, %s is the profile name.
`Update the profile %s has succeeded.`	Update profile succeeded, %s is the profile name.
`Update the profile %s has failed because the FQDN %s is invalid.`	Update profile failed because FQDN for the profile is invalid for DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s is malformed.`	The FQDN format is malformed for DynDNS server, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s is not under your control.`	The owner of this FQDN is not the user, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because the FQDN %s was blocked for abuse.`	The FQDN is blocked by DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile.
`Update the profile %s has failed because of authentication fail.`	Try to update profile, but failed, because of authentication fail, %s is the profile name.
`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.

Table 283 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`Update the profile %s has failed because of dyndns internal error`	Update profile failed because of a dyndns internal error, %s is the profile name.
`Update the profile %s has failed because the feature requested is only available to donators.`	Update profile failed because the feature requested is only available to donators, %s is the profile name.
`Update the profile %s has failed because of error response.`	Update profile failed because the response is incorrect, %s is the profile name.
`Update the profile %s has failed because %s.`	Update profile failed, and show the response message, 1st %s is the profile name, 2nd %s is the reason.
`Update the profile %s has failed because of unknown error.`	Update profile failed because unknown error. Sometimes, the force authentication will result in this error, 1st %s is the profile name.
`Update the profile %s has failed because Username was empty.`	DDNS profile needs username, %s is the profile name.
`Update the profile %s has failed because Password was empty.`	DDNS profile needs password, %s is the profile name.
`Update the profile %s has failed because Domain name was empty.`	DDNS profile needs domain name, %s is the profile name.
`Update the profile %s has failed because Custom IP was empty.`	The DDNS profile's IP select type is custom, and a custom IP was not defined, %s is the profile name.
`Update the profile %s has failed because WAN interface was empty.`	If the DDNS profile's IP select type is iface, it needs a WAN iface, %s is the profile name.
`The profile %s has been paused because the VRRP status of WAN interface was standby.`	The profile is paused by device-HA, because the VRRP status of that iface is standby, %s is the profile name.
`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.

Table 283 System Logs (continued)

LOG MESSAGE	DESCRIPTION
`Update the profile %s has failed because ping-check of WAN interface has failed.`	DDNS profile cannot be updated because the ping-check for WAN iface failed , %s is the profile name.
`The profile %s has been paused because the HA interface of VRRP status was standby.`	The profile is paused by Device-HA, because the VRRP status of that HA iface is standby, %s is the profile name.
`Update the profile %s has failed because HA interface was link-down.`	DDNS profile cannot be updated for HA IP address because HA iface is link-down, %s is the profile name.
`Update the profile %s has failed because the HA interface was not connected.`	DDNS profile cannot be updated for HA IP address because HA iface is PPP and not connected, %s is the profile name.
`Update the profile %s has failed because IP address of HA interface was empty.`	DDNS profile cannot be updated because the IP address of HA iface is 0.0.0.0, %s is the profile name.
`Update the profile %s has failed because ping-check of HA interface has failed.`	DDNS profile cannot be updated because the fail of ping-check for HA iface, %s is the profile name
`DDNS has been disabled by Device-HA.`	DDNS is disabled by Device-HA, because all VRRP groups are standby.
`DDNS has been enabled by Device-HA.`	DDNS is enabled by Device-HA, because one of VRRP groups is active.
`Disable DDNS has succeeded.`	Disable DDNS.
`Enable DDNS has succeeded.`	Enable DDNS.
`DDNS profile %s has been renamed as %s.`	Rename DDNS profile, 1st %s is the original profile name, 2nd %s is the new profile name.
`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 284 Connectivity Check Logs

LOG MESSAGE	DESCRIPTION
`Can’t open link_up2`	Can not recover routing status which is link-down.
`Can not open %s.pid`	Can not open connectivity check process ID file. %s: interface name

Table 284 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
`Can not open %s.arg`	Can not open configuration file for connectivity check process. %s: interface name
`The connectivity-check is activate for %s interface`	The link status of interface is still activate after check of connectivity check process. %s: interface name
`The connectivity-check is fail for %s interface`	The link status of interface is fail after check of connectivity check process. %s: interface name
`Can't get gateway IP of %s interface`	The connectivity check process can't get the gateway IP address for the specified interface. %s: interface name
`Can't alloc memory`	The connectivity check process can't get memory from OS.
`Can't load %s module`	The connectivity check process can't load module for check link-status. %s: the connectivity module, currently only ICMP available.
`Can't handle 'isalive' function of %s module`	The connectivity check process can't execute 'isalive' function from module for check link-status. %s: the connectivity module, currently only ICMP available.
`Create socket error`	The connectivity check process can't get socket to send packet.
`Can't get IP address of %s interface`	The connectivity check process can't get IP address of interface. %s: interface name.
`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.

Table 284 Connectivity Check Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 285 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, 2nd %s: %s: the name of VRRP group.
`Device HA syncing from %s starts.`	Device HA Syncing from Master starts when user click "Sync Now" using Auto Sync, %s: The IP of FQDN of Master.
`%s has no file to sync, Skip syncing it for %s.`	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2nd %s: The feature name for the syncing object.
`Master configuration is the same with Backup. Skip updating it.`	The System Startup configuration file synchronized from the Master is the same with the one in the Backup, so the configuration does not have to be updated.
`%s file not existed, Skip syncing it for %s`	There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2nd %s: The feature name for the syncing object.
`Master firmware version can not be recognized. Stop syncing from Master.`	Synchronizing stopped because the firmware version file was not found in the Master. A Backup device only synchronizes from the Master if the firmware versions are the same between the Master and the Backup.
`Device HA Sync has failed when syncing %s for %s due to bad \"Sync Password\".`	The synchronization password was incorrect when attempting to synchronize a certain object (AV/AS/IDP/Certificate/System Configuration). 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
`Device HA Sync has failed when syncing %s for %s due to bad \"Sync From\" or \"Sync Port\".`	The Sync From IP address or Sync Port may be incorrect when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration).
`Device HA Sync has failed when syncing %s for %s.`	Synchronization failed when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration) due to an unknown reason, 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.

Table 285 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
Sync Failed: Cannot connect to Master when syncing %s for %s.	Synchronization failed because the Backup could not connect to the Master. The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Backup firmware version can not be recognized. Stop syncing from Master.	The firmware version on the Backup cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Sync failed: Remote Firmware Version Unknown	The firmware version on the Master cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Master firmware version should be the same with Backup.	The Backup and Master have different firmware versions. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions.
Update %s for %s has failed.	Updating a certain object failed when updating (AS/AV/IDP/Certificate/ System Configuration). 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Update %s for %s has failed: %s.	Updating a certain object failed when updating (AS/AV/IDP/Certificate/ System Configuration) due to some reason. 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized.
Device HA has skipped syncing %s since %s is %s.	A certain service has no license or the license is expired, so it was not synchronized from the Master. 1st %s: The object to be synchronized, 2nd %s: The feature name for the object to be synchronized, 3rd %s: unlicensed or license expired.
Device HA authentication type for VRRP group %s maybe wrong.	A VRRP group's Authentication Type (Md5 or IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group.
Device HA 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, 2nd %s: The feature name for the object to be synchronized, %d: the retry count.
Recovering to Backup original state for %s has failed.	An update failed. The device will try to recover the failed update feature to the original state before Device HA synchronizes the specified object.
Recovering to Backup original state for %s has succeeded.	Recovery succeeded when an update for the specified object failed.
One of VRRP groups has became active. Device HA Sync has aborted from Master %s.	%s: IP or FQDN of Master
Master configuration file does not exist. Skip updating ZySH Startup Configuration.	

Table 285 Device HA Logs (continued)

LOG MESSAGE	DESCRIPTION
`System internal error: %s. Skip updating %s.`	1st %s: error string, 2ed %s: the syncing object
`Master configuration file is empty. Skip updating ZySH Startup Configuration.`	
`Device HA Sync has failed when syncing %s for %s due to transmission timeout.`	1st %s: the syncing object, 2ed %s: the feature name for the syncing object

Table 286 Routing Protocol Logs

LOG MESSAGE	DESCRIPTION
`RIP on interface %s has been stopped because Device-HA binds this interface.`	Device-HA is currently running on the interface %s, so all the local service have to be stopped including RIP. %s: Interface Name
`RIP on all interfaces have been stopped`	Got the CLI command 'no router rip' to shut down RIP on all interfaces
`Invalid RIP md5 authentication`	RIP md5 authentication has been set without setting md5 authentication id and key first
`Invalid RIP text authentication.`	RIP text authentication has been set without setting authentication key first
`RIP on interface %s has been activated.`	RIP on interface %s has been activated. %s: Interface Name
`RIP direction on interface %s has been changed to In-Only.`	RIP direction on interface %s has been changed to In-Only. %s: Interface Name
`RIP direction on interface %s has been changed to Out-Only.`	RIP direction on interface %s has been changed to Out-Only. %s: Interface Name
`RIP authentication mode has been changed to %s.`	RIP authentication mode has been changed to text or md5.
`RIP text authentication key has been changed.`	RIP text authentication key has been changed.
`RIP md5 authentication id and key have been changed.`	RIP md5 authentication id and key have been changed.
`RIP global version has been changed to %s.`	RIP global version has been changed to version 1 or 2.
`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

Table 286 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
`RIP authentication has been disabled.`	RIP text or md5 authentication has been disabled.
`RIP text authentication key has been deleted.`	RIP text authentication key has been deleted.
`RIP md5 authentication id and key have been deleted.`	RIP md5 authentication id and key have been deleted.
`RIP global version has been deleted.`	RIP global version has been deleted.
`RIP redistribute OSPF routes has been disabled.`	RIP redistribute OSPF routes has been disabled.
`RIP redistribute static routes has been disabled.`	RIP redistribute static routes has been disabled.
`RIP v2-broadcast on interface %s has been enabled.`	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
`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

Table 286 Routing Protocol Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 287 NAT Logs

LOG MESSAGE	DESCRIPTION
`The NAT range is full`	The NAT mapping table is full.
`%s FTP ALG has succeeded.`	The FTP Application Layer Gateway (ALG) has been turned on or off. %s: Enable or Disable
`Extra signal port of FTP ALG has been modified.`	Extra FTP ALG port has been changed.
`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 288 PKI Logs

LOG MESSAGE	DESCRIPTION
`Generate X509certifiate "%s" successfully`	The router created an X509 format certificate with the specified name.
`Generate X509 certificate "%s" failed, errno %d`	The router was not able to create an X509 format certificate with the specified name. See Table 289 on page 523 for details about the error number.
`Generate certificate request "%s" successfully`	The router created a certificate request with the specified name.
`Generate certificate request "%s" failed, errno %d`	The router was not able to create a certificate request with the specified name. See Table 289 on page 523 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 289 on page 523 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.
`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

Table 288 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 289 on page 523), %s is the certificate subject.

Table 289 Certificate Path Verification Failure Reason Codes

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

Table 289 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
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 290 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.
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.

Table 290 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.
`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.

Table 290 Interface Logs (continued)

LOG MESSAGE	DESCRIPTION
`Interface %s is disconnected.`	A PPP or AUX interface disconnected successfully. %s: interface name.
`Interface %s connect failed: Peer not responding.`	The interface's connection will be terminated because the server did not send any LCP packets.
`Interface %s connect failed: PAP authentication failed.`	PAP authentication failed (the server must support PAP and verify verify that the authentication failed, this does not include cases where the server does not support PAP). %s: PPP interface name.
`Interface %s connect failed: Connect timeout.`	A PPPOE connection timed out due to a lack of response from the PPPOE server. %s: PPP interface name.
`Interface %s create failed because has no member.`	A bridge interface has no member. %s: bridge interface name.
`Interface %s has been renamed from '%s' to '%s'`	An interface was renamed. 1st %s: the interface's system name (gex), 2nd %s: current interface name, 3rd %s: new interface name.

Table 291 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 292 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 293 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 294 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.

Table 295 EPS Logs

LOG MESSAGE	DESCRIPTION
`'EPS' signature data of Auth. policy %d has been updated.`	EPS profile settings were changed and have been re-applied to the associated authentication policy. %d is the authentication profile name.
`'EPS' signature data of SSL policy %d has been updated.`	EPS profile settings were changed and have been re-applied to the associated SSL VPN rule. %d is the SSL VPN rule name.
`EPS profile %s has been modified.`	An EPS pofile was modified. %s is the EPS profile name.
`'EPS' signature file is replaced with default one.`	An administrator reset EPS signatures back to the factory defaults.
`Missing EPS signature default tools, ret = %d.`	An error occurred when reloading the factory default EPS signatures.
`Windows service pack check fail in %s`	A user’s computer failed to pass an EPS checking item, the failed item is about the Windows service pack version.
`'Windows auto update check fail in %s`	A user’s computer failed to pass an EPS checking item, the failed item is about Windows Auto Update settings.
`Windows security patch check fail in %s`	A user’s computer failed to pass an EPS checking item about Windows service patches.
`Antivirus check fail in %s`	A user’s computer failed to pass an EPS checking item about anti-virus installation and activation.
`Personal firewall check fail in %s`	A user’s computer failed to pass an EPS checking item about personal firewall installation and activation.
`Windows registry check fail in  %s`	A user’s computer failed to pass an EPS checking item about Windows registry settings.
`Trusted process check fail in %s`	A user’s computer failed to pass an EPS checking item about processes that the user’s computer must execute.
`Forbidden process check fail in  %s`	A user’s computer failed to pass an EPS checking item about processes that the user’s computer cannot execute.
`Files information check fail in %s`	A user’s computer failed to pass an EPS checking item about the size and version of specific files.
`OS type check fail in %s`	A user’s computer failed to pass an EPS checking item about the Operating System.
`Windows version check fail in %s`	A user’s computer failed to pass an EPS checking item about the Windows version.
`EPS checking result is pass.`	A user’s computer passed all the EPS checking items.

Legal Information

Copyright

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

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

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.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index