# Vantage CNM

*Centralized Network Management*

# *User's Guide*

Version 2.30
1/2007
Edition 1

ZyXEL
www.zyxel.com

# About This User's Guide

✍ The screens in Vantage CNM vary by device type and firmware version. The examples in this User's Guide use one of the most comprehensive examples of each screen, not every variation for each device type and firmware version. If you are unable to find a specific screen or field in this User's Guide, please see the User's Guide for the device for more information.

### Intended Audience

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

### Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up and connecting to your software.
- Web Configurator Online Help

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

✍ It is recommended you use the web configurator to configure the Vantage CNM.

- Device User's Guide

  The User's Guide for each device provides more information about the device, its features, and its configuration.
- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

### User Guide Feedback

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

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

E-mail: techwriters@zyxel.com.tw

# Document Conventions

### Warnings and Notes

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

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

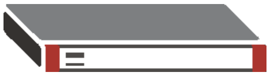
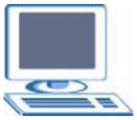
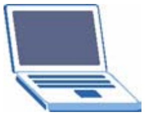
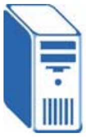
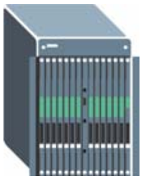
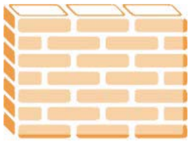
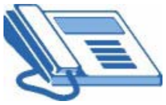
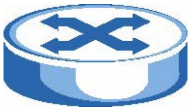
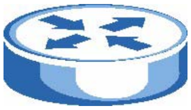
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

### Syntax Conventions

- Vantage CNM may be referred to as "Vantage CNM" or the "product" in this User's Guide.
- Vantage Report may be referred to as "Vantage Report" or "VRPT" in this User's Guide.
- A device that is managed by Vantage CNM may be referred to as the "ZyXEL device," "device," or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

### Icons Used in Figures

Figures in this User's Guide may use the following generic icons. Device icons are not an exact representations of your devices.

| | | |
|---|---|---|
| Device (example)<br> | Computer<br> | Notebook computer<br> |
| Server<br> | DSLAM<br> | Firewall<br> |
| Telephone<br> | Switch<br> | Router<br> |

# Contents Overview

# Table of Contents

# List of Figures

# List of Tables

# PART I
# Introduction

# 1

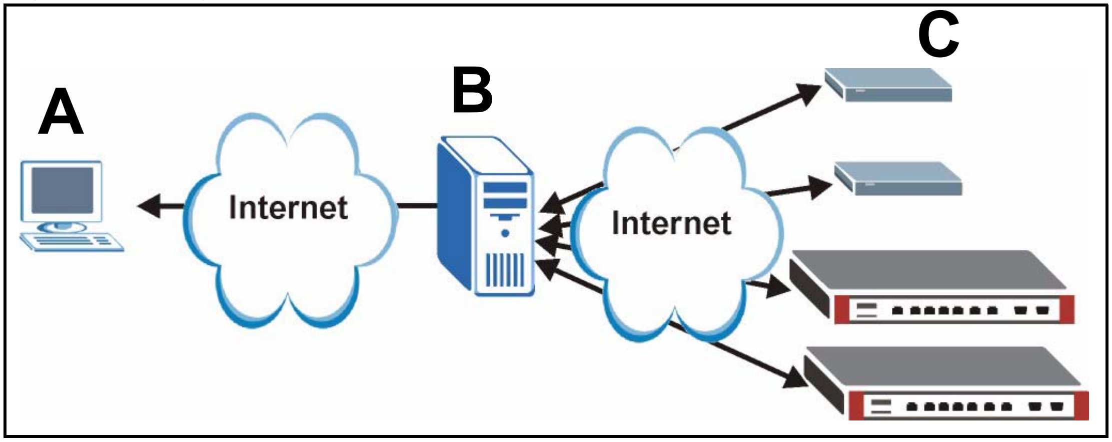
# Introducing Vantage CNM

This chapter introduces the main applications and features of Vantage CNM. It also introduces the ways you can manage Vantage CNM.

## 1.1 Overview

Vantage Centralized Network Management ("Vantage CNM") helps network administrators monitor and manage a distributed network of ZyXEL network devices. A typical application is shown in the following example.

**Figure 1** Vantage CNM Application



In this example, you use the Vantage CNM web configurator (**A**) to access the Vantage CNM server (**B**). The Vantage CNM server is connected to the devices (**C**), and you can

- Monitor all the devices in the network and receive alarms in one place
- Create building blocks to configure one or more devices
- Set up other administrators who are allowed to perform specific functions for specific devices

You can also manage configuration files, upload firmware, and activate subscription services, such as Intrusion Detection and Protection (IDP) and content filtering, on one or more devices. See Appendix A on page 515 for a complete list of features and supported devices.

## 1.2 Ways to Manage Vantage CNM

Use the web configurator to access and manage Vantage CNM. See the Quick Start Guide for instructions to access the web configurator and this User's Guide for more information about the screens.

## 1.3 Good Habits for Managing Vantage CNM

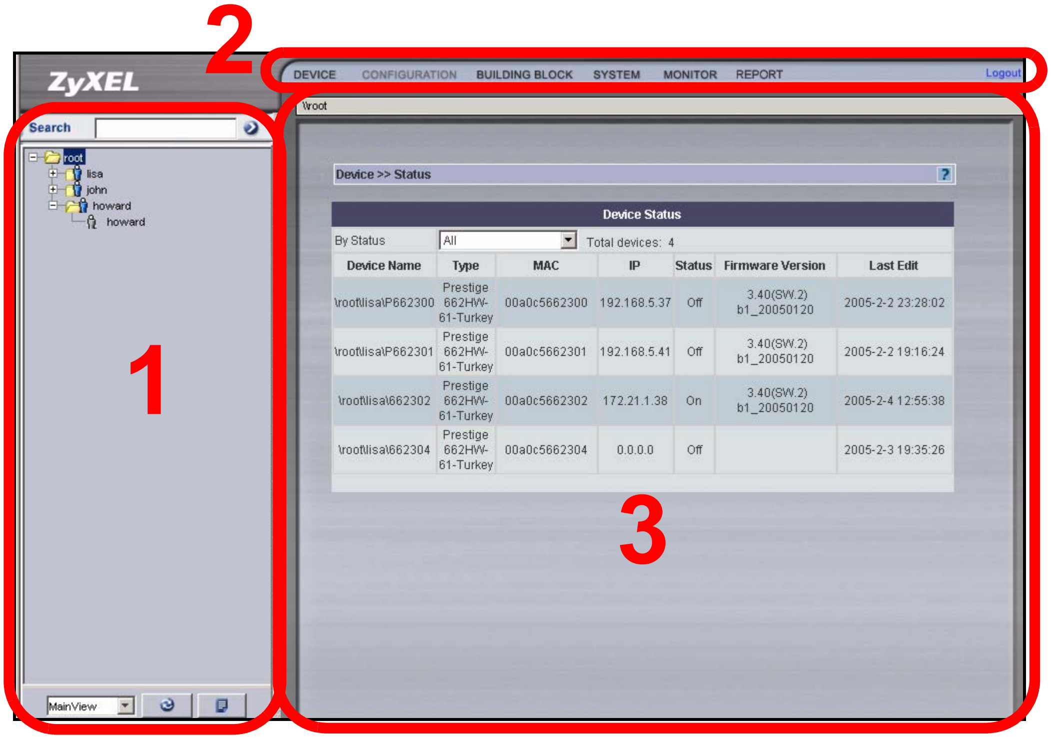
Do the following things regularly to make Vantage CNM more secure and to manage Vantage CNM more effectively.

- Change the **root** password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the **root** password and put it in a safe place. If you forget the **root** password, contact your local vendor.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful or necessary if the system becomes unstable or even crashes. If you have to re-install Vantage CNM, you could simply restore your last configuration afterwards.

# GUI Introduction

See the Quick Start Guide for instructions about installing, setting up, and accessing Vantage CNM. This chapter introduces the Vantage CNM main screen.

**Figure 2** Main Screen



Device >> Status

Device Status

By Status: All

Total devices: 4

| Device Name | Type | MAC | IP | Status | Firmware Version | Last Edit |
|---|---|---|---|---|---|---|
| \root\lisa\P662300 | Prestige 662HW-61-Turkey | 00a0c5662300 | 192.168.5.37 | Off | 3.40(SW.2) b1_20050120 | 2005-2-2 23:28:02 |
| \root\lisa\P662301 | Prestige 662HW-61-Turkey | 00a0c5662301 | 192.168.5.41 | Off | 3.40(SW.2) b1_20050120 | 2005-2-2 19:16:24 |
| \root\lisa\662302 | Prestige 662HW-61-Turkey | 00a0c5662302 | 172.21.1.38 | On | 3.40(SW.2) b1_20050120 | 2005-2-4 12:55:38 |
| \root\lisa\662304 | Prestige 662HW-61-Turkey | 00a0c5662304 | 0.0.0.0 | Off |  | 2005-2-3 19:35:26 |

The main screen consists of three main parts and are numbered in the sequence you typically follow to configure a device.

1 Object pane. Select the folder, device, or administrator you want to configure.

2 Main menu. Select the type of configuration you want to do in the drop-down menu.

3 Content pane. Configure the device or administrator as desired.

Each part is discussed in more detail in the following sections.

## 2.1 Object Pane

Select the folder, device, or administrator you want to configure in this pane.

### 2.1.1 Views

The drop-down box at the bottom of the pane controls the view. In each view, the folders, devices, and/or administrators are displayed in a tree. You can select one of three views: **MainView, TypeView** and **AccountView**.

- In the **MainView**, you can create folders up to seven layers deep (not counting **root**) and add devices and administrators to each one. You can also configure devices and administrators.
- The **TypeView** displays devices by device type. It does not display any administrators. You can configure devices, but you cannot add devices.
- The **AccountView** displays only account folders, and every account folder is shown as a sub-folder of **root**. You can configure devices, but you cannot add devices.

There are a couple icons in the object pane that perform additional functions related to views.

**Table 1** Object Pane: View Icons

| Icon | Description |
|---|---|
| 🔄 | Click this icon to refresh the object tree. |
| 📋 | Click this icon to look at the list of available views. |

### 2.1.2 Folders

A folder is a logical grouping of devices. They are used to organize devices and administrators and can contain devices, administrators, and other folders.

There are two types of folders: group folders and account folders. Both types of folders are similar, except that only account folders appear in the **AccountView**. In the **AccountView**, all the account folders appear on the same level below **root**, so account folders cannot be sub-folders of other account folders.

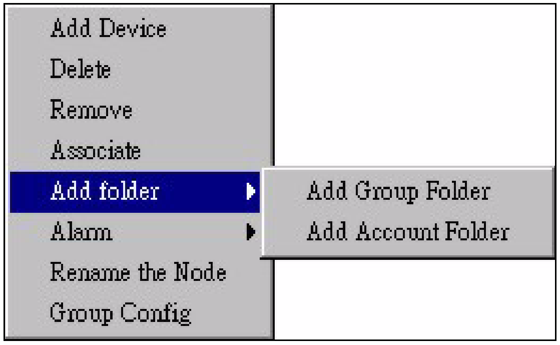
Folders are represented by the following icons in the object pane.

**Table 2** Object Pane: Folder Icons

| Icon | Description |
|---|---|
| 📂👤❗ | This is an account folder where you can see the devices and folders inside and which contain some devices with an alarm. |
| 📂👤 | This is an account folder where you can see the devices and folders inside. |
| 📁👤❗ | This is an account folder where you cannot see the device inside and which contains some devices with an alarm. |
| 📁👤 | This is an account folder where you cannot see the devices inside. |
| 📂❗ | This is an open group folder, which contains some devices and folders with an alarm. |
| 📂 | This is an open group folder. |
| 📁❗ | This is a closed group folder, which contains some devices with an alarm. |
| 📁 | This is a closed group folder. |

In the **MainView**, you can right-click on a folder to see the following menu items. Some folders do not have every menu item.

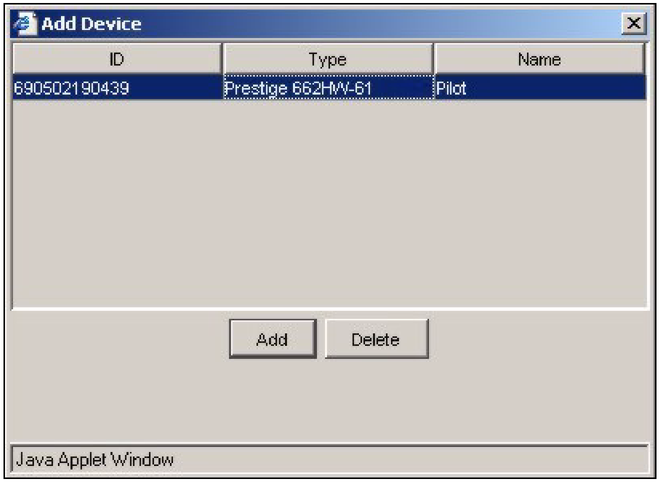
**Figure 3** Folder Right-Click Options



### 2.1.2.1 Add Device

This menu item displays a list of devices that are registered with Vantage CNM but not mapped to any folder. You can add any of these devices to the selected folder or remove them from Vantage CNM.

**Figure 4** Folder > Add Device



| ID | Type | Name |
|---|---|---|
| 690502190439 | Prestige 662HW-61 | Pilot |

### 2.1.2.2 Delete

This menu item deletes the selected folder and un-maps the devices within the folder. These devices are still registered with Vantage CNM and appear in the **Add Device** screen (Figure 4 on page 43).

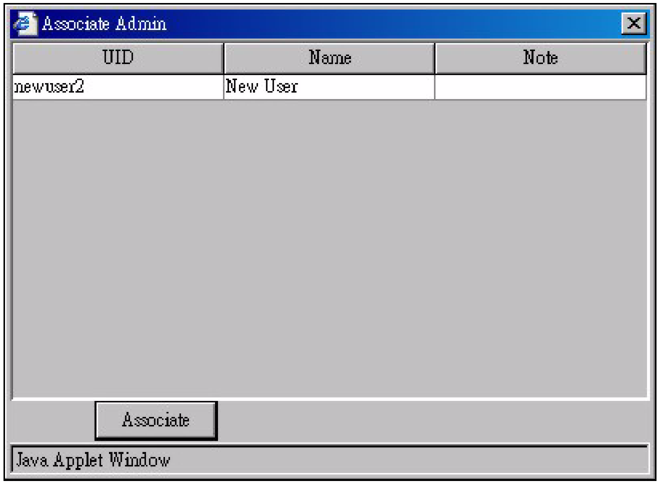
### 2.1.2.3 Remove

This menu item deletes the selected folder and removes the devices in the folder from Vantage CNM. The devices are no longer registered with Vantage CNM. This does not disable Vantage CNM in the device.

### 2.1.2.4 Associate

This menu item links an administrator to this folder. This folder and all sub-folders are then in this administrator’s domain, and the administrator cannot manage or see folders outside this domain. The following screen appears.

**Figure 5** Folder > Associate



| UID | Name | Note |
|---|---|---|
| newuser2 | New User | |

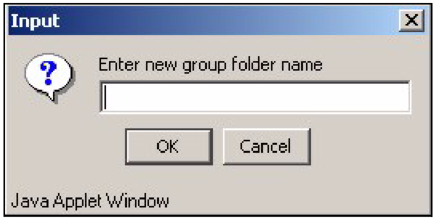
An administrator can only have one domain, so this screen displays only the administrators who are not associated with any domain. Select one or more administrators to associate with this folder, and click **Associate**. An icon for each administrator should appear in the folder.

If you want to change the domain for any administrator, you have to remove the administrator from the current domain first. Right-click on the administrator, and select **UnAssociate**. See Section 2.1.4 on page 48. Then, you can use this menu item to associate the administrator with the new folder.

### 2.1.2.5 Add folder

This menu item creates a new folder as a sub-folder of the selected folder. When you create a folder, you must enter the name of the new folder. The name must contain 1-32 alphanumeric characters, underscores (_), or dashes (-) and is case-sensitive. Spaces are not allowed. The first character must be alphanumeric.

**Figure 6** Folder > Add folder > Add Group Folder



### 2.1.2.6 Alarm > Locate

This menu item finds alarms associated with devices within the selected folder. Alarms are real-time warnings of hardware failure, security breaches, attacks or illegal Vantage CNM login attempts.

### 2.1.2.7 Rename the Node

This menu item lets you rename the folder.

### 2.1.2.8 Group Config

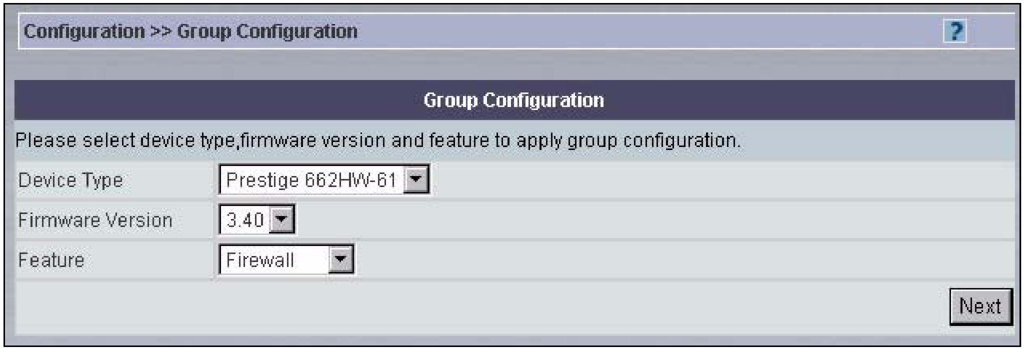
Use this menu item to do one of the following:

- Apply a configuration building block (BB) to one or more devices in the selected folder. You can create the configuration BB during this process, if necessary. See Chapter 24 on page 277 for information about BBs.
- Reset a feature to its default settings in one or more devices.

The first one is illustrated in the following example. An administrator wants to apply an existing firewall BB called "exampleBB1" to a couple P-662HW-61.

First, right-click on a folder that contains both P-662HW-61, and select **Group Config**. The first screen appears.

**Figure 7** Folder > Group Config (Device Type)

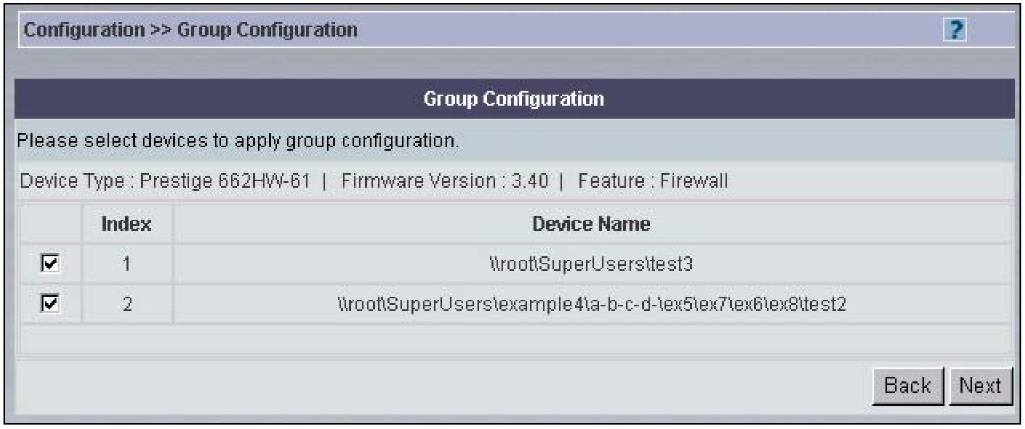


Please select device type,firmware version and feature to apply group configuration.

| | |
|---|---|
| Device Type | Prestige 662HW-61 |
| Firmware Version | 3.40 |
| Feature | Firewall |

Select the device type, firmware version, and feature you want to configure, and click **Next**. The next screen displays a list of registered devices of the specified type in the folder.

**Figure 8** Folder > Group Config (Devices)



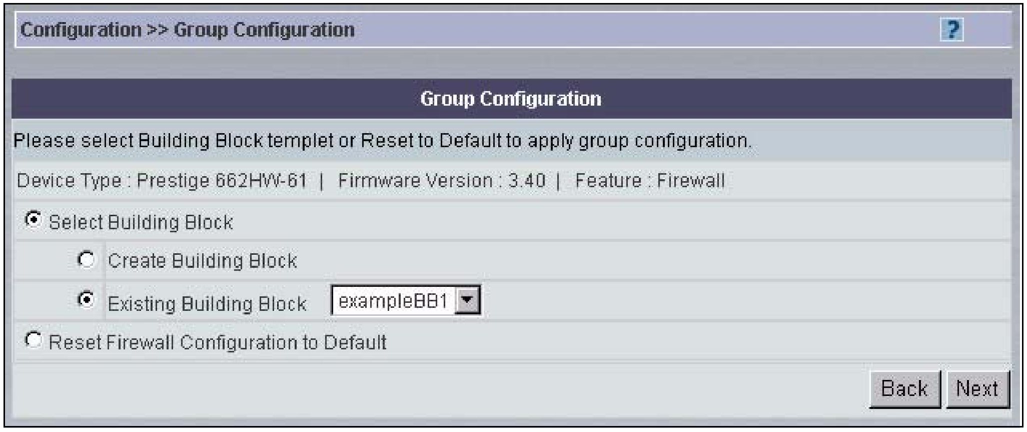
Please select devices to apply group configuration.

Device Type : Prestige 662HW-61 | Firmware Version : 3.40 | Feature : Firewall

| | Index | Device Name |
|---|---|---|
| ☑ | 1 | \\root\SuperUsers\test3 |
| ☑ | 2 | \\root\SuperUsers\example4\a-b-c-d-\ex5\ex7\ex6\ex8\test2 |

Select the devices you want to configure, and click **Next**. The next screen lets you select what you want to do.

**Figure 9** Folder > Group Config (Building Block)



Configuration >> Group Configuration

Group Configuration

Please select Building Block templet or Reset to Default to apply group configuration.

Device Type : Prestige 662HW-61 | Firmware Version : 3.40 | Feature : Firewall

● Select Building Block

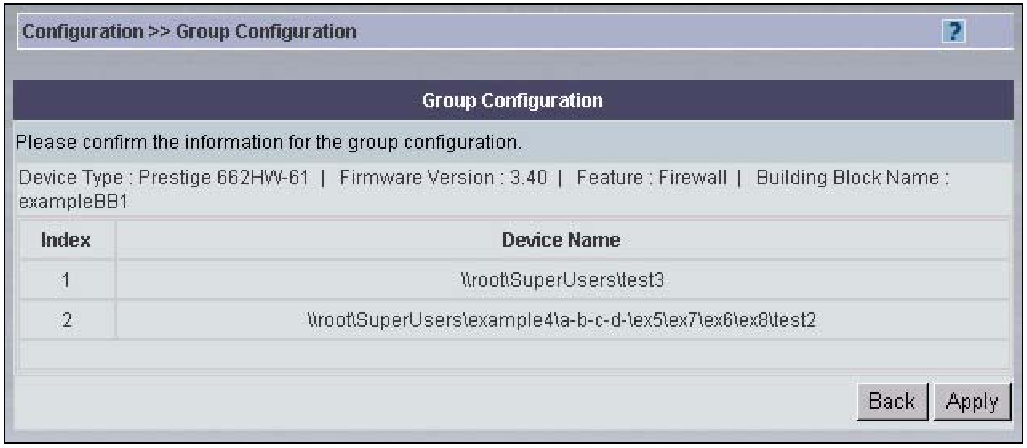
○ Create Building Block

● Existing Building Block exampleBB1

○ Reset Firewall Configuration to Default

Select the building block you want to apply to the devices, create a new building block to apply to the devices, or reset the devices to the default configuration. In this example, select **Existing Building Block**, select **exampleBB1** in the drop-down box, and click **Next**. The last screen is a review screen. If the settings are correct, click **Apply**.

**Figure 10** Folder > Group Config (Confirmation)



Configuration >> Group Configuration

Group Configuration

Please confirm the information for the group configuration.

Device Type : Prestige 662HW-61 | Firmware Version : 3.40 | Feature : Firewall | Building Block Name : exampleBB1

| Index | Device Name |
|---|---|
| 1 | \\root\SuperUsers\test3 |
| 2 | \\root\SuperUsers\example4\a-b-c-d-\ex5\ex7\ex6\ex8\test2 |

You can track the status and look at the results of group configurations in the Group Operation Report. See Section 28.6 on page 327.

## 2.1.3 Devices

A device appears in the object pane if it is registered (Section 3.2 on page 56) and mapped to a folder (Section 2.1.2.1 on page 43).

Devices are represented by the following icons in the object pane.

**Table 3** Object Pane: Device Icons

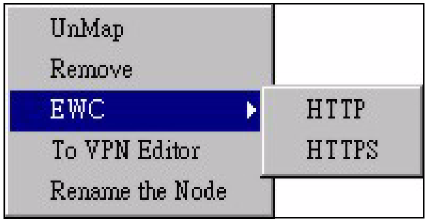
| Icon | Description |
|---|---|
|  | This is a ZyWALL device turned off. |
|  | This is a ZyWALL device that has firmware uploading. |
|  | This is a ZyWALL device that has an alarm that is turned on. |
|  | This is a ZyWALL device turned off with an alarm and will have a firmware upload. |
|  | This is a ZyWALL device turned on. |

**Table 3** Object Pane: Device Icons (continued)

| Icon | Description |
|---|---|
| | This is a ZyWALL device with an alarm. |
| | This is a ZyWALL device turned on with an alarm and has firmware uploading. |
| | This is a ZyWALL device and has firmware uploading. |
| | This is a Prestige device turned off. |
| | This is a Prestige device turned off with an alarm. |
| | This is a Prestige device turned off with an alarm and will have a firmware upload. |
| | This is a Prestige device turned off and will have a firmware upload. |
| | This is a Prestige device that has an alarm that is turned on. |
| | This is a Prestige device with an alarm. |
| | This is a Prestige device with an alarm and has firmware uploading. |
| | This is a Prestige device with firmware uploading. |

In the **MainView**, you can right-click on a device to see the following menu. Some menu items are not available for every device.

**Figure 11** Device Right-Click Options



### 2.1.3.1 UnMap

This menu item un-maps the selected device from the folder and removes the device icon from the object pane. The device is still registered with Vantage CNM and appear in the **Add Device** screen (Figure 4 on page 43).

### 2.1.3.2 Remove

This menu item removes the selected device from Vantage CNM. The device is no longer registered with Vantage CNM. This does not disable Vantage CNM in the device.

### 2.1.3.3 EWC

This menu item opens the web configurator for the selected device in a new window. The new window uses either **HTTP** or **HTTPS**.

If you make changes in the web configurator instead of in Vantage CNM, you might create inconsistencies between the device and Vantage CNM. Click **Device > Synchronize** to resolve them. See Section 3.4 on page 65.

#### 2.1.3.4 To VPN Editor

This menu item opens the VPN editor, where you can click-and-drag VPN tunnels (single-click VPN) and view individual tunnel details. See Section 28.3 on page 322 for more information about the VPN editor.

#### 2.1.3.5 Rename the Node

This menu item lets you rename the device in Vantage CNM. It does not change the configuration of the device.

### 2.1.4 Administrators

An administrator appears in the object pane after you do the following:

1. Create the administrator account. See Chapter 25 on page 281.
2. Associate the administrator with a specific folder. See Section 2.1.2.4 on page 43.

Administrators are represented by the following icons in the object pane.

**Table 4** Object Pane: Administrator Icons

| Icon | Description |
|---|---|
| 👤 | This is an administrator currently logged in. |
| 👤 | This is an administrator that has logged out. |

In the **MainView**, you can right-click on an administrator who is not logged in to see the following menu.

**Figure 12** Administrator Right-Click Options

Select this option if you want to remove the administrator from this domain. Then, you can right-click on a different folder, and associate the administrator with it instead. See Section 2.1.2.4 on page 43.

### 2.1.5 Search

In the **Search** bar, type any part of the name of a node (device, folder, or administrator), and press [ENTER] or click the icon to the right of the field. Vantage CNM looks for the next occurrence of the string in the object pane, starting from the first node after the one currently selected and wrapping around to the top of the tree when necessary. Vantage CNM searches the whole tree, including any parts that may be hidden.

If Vantage CNM finds a match, it automatically selects that node, and the content pane updates automatically. If Vantage CNM does not find a match, it displays a message.

## 2.2 Main Menu

The Vantage CNM main menu consists of the following drop-down menus.

**Table 5** Main Menu Overview

| DEVICE | CONFIGURATION | BUILDING BLOCK |
|---|---|---|
| Status<br>Registration<br>Service Registration<br>Synchronize<br>Firmware Mgmt<br>Firmware Upgrade<br>Scheduler List<br>Configuration File<br>Signature Profile | Select Building Block<br>General<br>Bridge<br>LAN<br>WLAN<br>Wireless Card<br>DMZ<br>WAN<br>NAT<br>Static Route<br>VPN<br>Firewall<br>Port Roles<br>IDP<br>Anti-Virus<br>Anti-Spam<br>Content Filter<br>Device Log<br>ADSL Monitor<br>X Auth<br>Device Alarm<br>DNS<br>Remote MGMT | Configuration BB |
| **SYSTEM** | **MONITOR** | **REPORT** |
| Administrators<br>Status<br>Upgrade<br>License<br>Preferences<br>Maintenance<br>Address Book<br>Logs<br>Certificate Mgmt<br>VRPT Management<br>About | Alarm<br>Firmware Report<br>Status Monitor<br>VPN Editor<br>License Monitor<br>Signature Monitor<br>Group Operation Report | Report |

This section provides some notes about the main menu.

- The **Configuration** menu is only enabled when a device is selected.
- When you open a **Configuration** menu item, the screen shows the current settings for the device.
- If a specific menu item is not supported by a device, then this menu item is grayed out.
- If the administrator does not have permission to use a menu item, it is not displayed.

## 2.3 Content Pane

The content pane displays the selected screen. The screen often depends on what type of device is currently selected.

The content pane also displays the object path for the selected folder or device, such as `\root\zywall2`, and the menu path for the screen that is open, such as `Device >> Status`.

The following table describes some of the widgets that appear in the content pane.

**Table 6** Content Pane: Icons

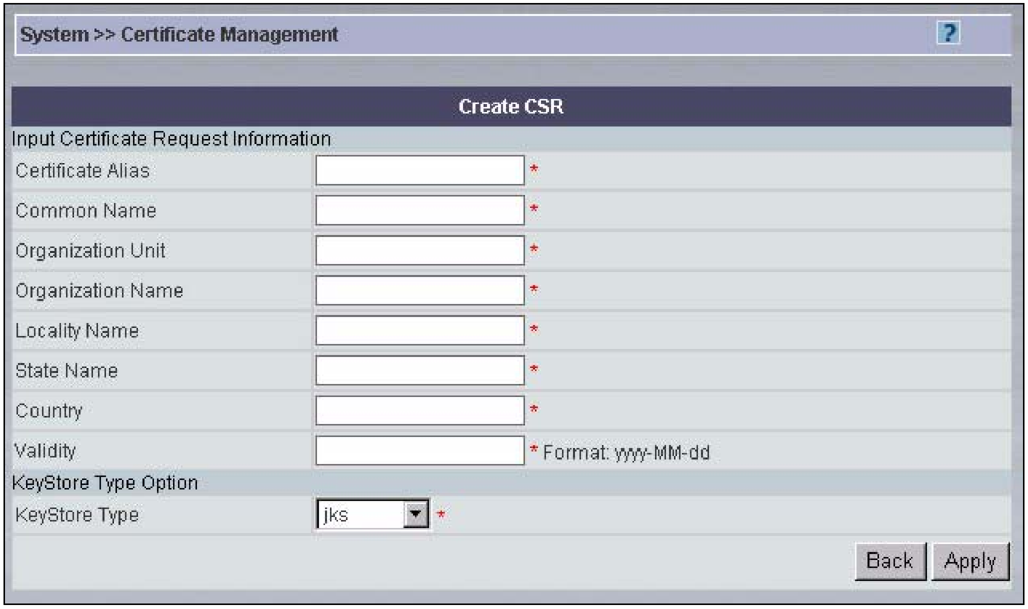
| ICON | DESCRIPTION |
|---|---|
| BB | Click this icon to choose from an existing BB. |
| BB | Click this icon to save a new BB. |
| 💾 | Click this icon to choose from an existing personal profile. |
| 💾 | Click this icon to save as a new personal profile. |
| ☠ | This icon represents a Fatal error. |
| ! | This icon represents a Major error. |
| ! | This icon represents a Minor error. |
| ! | This icon represents a Warning error. |
| ⟳ | Click this icon to refresh the values in this column or screen. |
| 📝 | Click this icon to edit the selected NAT server set. (See Figure 83 on page 157.) |
| ⇅ | Click this icon to move the entry or rule to a different place in the list. |
| ✎ | Click this icon to edit the entry or rule. |
| 📅 | Click this icon to display a calendar from which you can select a date. |
| 🗑 | Click this icon to clear or delete the entry. |
| 🔊 | Click this icon to send the specified notification for the event. |
| 📋 | Click this icon to look at more details about the entry. |
| ? | Click this icon to open online help for the current screen. |

## 2.4 Security Risk Pop-up Messages in Internet Explorer 7.0

The default certificate in Vantage CNM is self-signed, not signed by a trusted CA. As a result, Internet Explorer 7.0 might give you a pop-up message about the security risk. Follow these steps to get rid of this pop-up message.

1. Click **System** > **Certificate Mgmt**.
2. Click **Create CSR**. The following screen appears.

**Figure 13** System > Certificate Management > Create CSR



System >> Certificate Management

Create CSR

Input Certificate Request Information

| | |
|---|---|
| Certificate Alias | * |
| Common Name | * |
| Organization Unit | * |
| Organization Name | * |
| Locality Name | * |
| State Name | * |
| Country | * |
| Validity | * Format: yyyy-MM-dd |

KeyStore Type Option

| | |
|---|---|
| KeyStore Type | jks * |

3 Type the IP address of the Vantage CNM server in the **Common Name** field. This is the IP address you use to log in (http://your IP address:8080/vantage). The value **localhost** cannot be used in the **Common Name** field.

4 Enter the rest of the required information, and click **Apply**. See Section 26.7 on page 302 for more information about these fields.

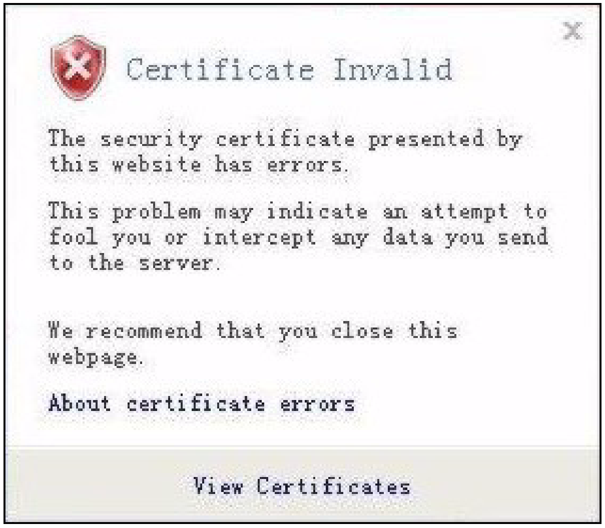
5 Submit the CSR to one of the trusted CAs.

6 Restart the Vantage CNM server.

7 Use the IP address and log in to the Vantage CNM server.

8 In Internet Explorer 7.0, click **View Certificates** when the following screen appears.

**Figure 14** Pop-up Message in Internet Explorer 7.0



Certificate Invalid

The security certificate presented by this website has errors.

This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

9 Install the new certificate.

# PART II
# Device

# 3

# Device

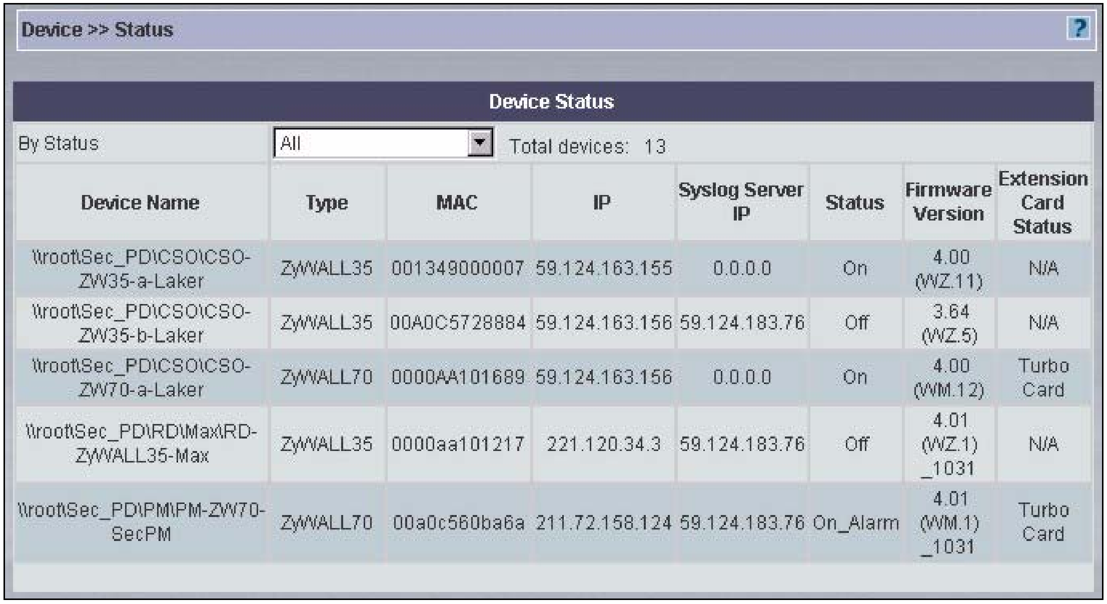
Use the **Device** menu to do the following:

- Check the status of devices
- Register new devices
- Register for subscription services
- Synchronize the configuration between Vantage CNM and devices
- Upload firmware and schedule firmware upgrades
- Back up, manage, and restore configuration files
- Back up, manage, and restore signatures

## 3.1 Status

This screen provides a summary of the selected device or all the devices in the selected folder. To open this screen, select a device or folder, and click **Device > Status**.

**Figure 15** Device > Status



Device >> Status

Device Status

By Status: All

Total devices: 13

| Device Name | Type | MAC | IP | Syslog Server IP | Status | Firmware Version | Extension Card Status |
|---|---|---|---|---|---|---|---|
| \\root\Sec_PD\CSO\CSO-ZW35-a-Laker | ZyWALL35 | 001349000007 | 59.124.163.155 | 0.0.0.0 | On | 4.00 (WZ.11) | N/A |
| \\root\Sec_PD\CSO\CSO-ZW35-b-Laker | ZyWALL35 | 00A0C5728884 | 59.124.163.156 | 59.124.183.76 | Off | 3.64 (WZ.5) | N/A |
| \\root\Sec_PD\CSO\CSO-ZW70-a-Laker | ZyWALL70 | 0000AA101689 | 59.124.163.156 | 0.0.0.0 | On | 4.00 (WM.12) | Turbo Card |
| \\root\Sec_PD\RD\Max\RD-ZyWALL35-Max | ZyWALL35 | 0000aa101217 | 221.120.34.3 | 59.124.183.76 | Off | 4.01 (WZ.1) _1031 | N/A |
| \\root\Sec_PD\PM\PM-ZW70-SecPM | ZyWALL70 | 00a0c560ba6a | 211.72.158.124 | 59.124.183.76 | On_Alarm | 4.01 (WM.1) _1031 | Turbo Card |

The following table describes the fields in this screen.

**Table 7** Device > Status

| LABEL | DESCRIPTION |
|---|---|
| By Status | This field is only available if a folder is selected. Select a filter status from the drop-down list box to choose which devices to view within the folder, or select **All** to look at all devices in the selected folder. |
| Device Name | This field displays the user-defined name, for example, “Dev1”. |
| Type | This field displays the device model. |
| MAC | This field displays the LAN MAC address of the device. |
| IP | This field displays the IP address of the device. |
| Syslog Server IP | This field displays the IP address of the Vantage Report server to which the device sends log messages. See Section 26.8 on page 306. |
| Status | This field displays the operating status of the device. The possible values are.<br>**On**: The device is online, and Vantage CNM is successfully communicating with it.<br>**Off**: The device is offline.<br>**On_Alarm**: The device has an alarm that is turned on.<br>**Off_Alarm**: The device has an alarm that is turned off.<br>**On_Firmware**: The device has firmware uploading.<br>**Off_Firmware**: The device has a scheduled firmware upload. After the device is turned on, Vantage CNM will wait up to twenty minutes to upload the firmware.<br>**On_Alarm_Firmware**: The device has an alarm that is turned on and has firmware uploading.<br>**Off_Alarm_Firmware**: The device has an alarm that is turned off and has a scheduled firmware upload. |
| Firmware Version | This field displays the device firmware network operating system (NOS) version number and date. |
| Extension Card Status | This field displays the type of card that is installed in the device (for example, **Turbo Card** or **Wireless Card**). It displays **N/A** if there is no extension card or if there is no slot for an extension card in the device. |

## 3.2 Registration

Use this menu item to register devices with Vantage CNM and associate them with the selected folder. You can register one device at a time manually, or you can register several devices at a time by importing an XML file.

### 3.2.1 XML Registration File Overview

Create an XML registration file when you want to register multiple devices at one time. Some templates for different types of devices may be found in `<Vantage CNM installed path>\xml\`. You may combine different templates into one XML file and import multiple devices of different types at one time.

- Usually, you must fill in the MAC address, name, type, firmware version, and encryption fields to import a device into Vantage CNM.
- Make sure the device’s name is different from existing devices’ names in that folder.

- Make sure the XML syntax is correct, as there are no validation checks in Vantage CNM. If you import an XML file with incorrect syntax into Vantage CNM, device management might be abnormal.

#### 3.2.1.1 Basic XML Syntax

XML registration files follow these basic syntax rules.

1. You do not have to type a blank value if a device does not contain that configuration.
2. Mandatory fields must be filled in or Vantage CNM will not list that device as a device that can be imported.
3. XML fields must not contain a "return" character. For example, the format below is forbidden:

   ```
   <mac>00a0c544e2fc
   </mac>
   ```

   You must write the field in one line, like this:

   ```
   <mac>00a0c544e2fc</mac>
   ```

4. A field must contain the correct value type. You can't write a string in a field that should contain an integer value. For example, the following is wrong, as <encryptMode> must contain integers only.

   ```
   <encryptMode>abc</encryptMode>
   ```

5. In fields of type string, if the string length is 0, you also need to write zero length field to make import work correctly. For example, both the following zero length string fields are acceptable.

   ```
   <domainName> </domainName>
   ```

   or

   ```
   <domainName/>
   ```

6. If your XML Field contain a special character such as &,', >, <,", you must embrace the character with <![CDATA[and]]>, as shown next:

   ```
   <initString><![CDATA[at&fs0=0]]></initString>
   ```

7. Device configuration fields needn't be in order. For example, you can write a device's LAN configuration fields first and then write the General configuration fields.

For more information about creating XML files for Vantage CNM, see the "Import Device Using XML Reference Manual" at the ZyXEL web site download library.

### 3.2.1.2 XML Registration File Example

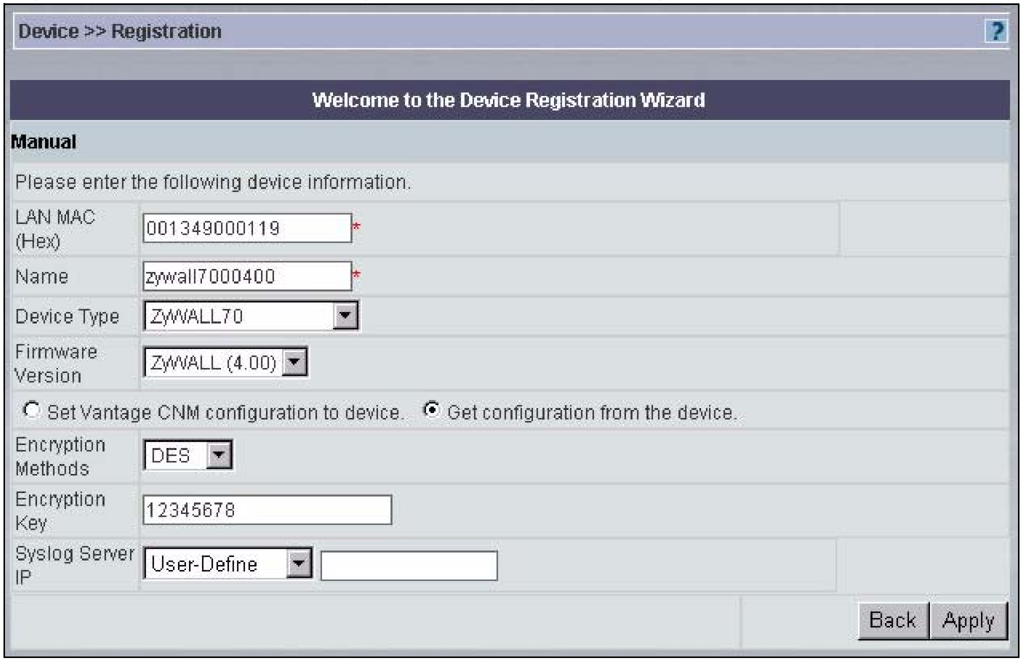
The following figure provides an example of an XML registration file for a ZyWALL 70.

**Figure 16** Example: XML Registration File

```
<zyxel-device>
  <devices>
    <mac>001349000119</mac>
    <name>zywall7000400</name>
    <!--type is device model id. Here is ZyWALL 70 (0X1F55)-->
    <type>8021</type>
    <!--fwid is firmware version id.-->
    <!--CNM 2.3 support firmware version id is: 362, 364, 365, 400, 401.-->
    <fwid>400</fwid>
    <!-- None=0,DES=1,3DES=2 -->
    <encrypt-mode>1</encrypt-mode>
    <!-- if encryptMode = 1, the length of encryptKey is 8;-->
    <!-- if encryptMode = 2, the length of encryptKey is 24.-->
    <encrypt-key>12345678</encrypt-key>
    <!--router is 0,bridge is 1-->
    <!--CNM 2.3 only support router mode-->
    <mode>0</mode>
    <!--Synchronization mode when first time registration-->
    <!--0 means set mode, 1 means get mode-->
    <sync-flag>0</sync-flag>
  </devices>
</zyxel-device>
```

These are the equivalent settings by using the manual device registration wizard screen. Note that the mode and synchronization mode fields in the XML file are not shown in this screen.

**Figure 17** Example: XML Registration File (Equivalent)



Please enter the following device information.

| | |
|---|---|
| LAN MAC (Hex) | 001349000119 * |
| Name | zywall7000400 * |
| Device Type | ZyWALL70 |
| Firmware Version | ZyWALL (4.00) |

○ Set Vantage CNM configuration to device. ● Get configuration from the device.

| | |
|---|---|
| Encryption Methods | DES |
| Encryption Key | 12345678 |
| Syslog Server IP | User-Define |

The syslog server settings for Vantage Report, not shown in Figure 16 on page 58, should be included in the `<log-setting>` section of the XML file.

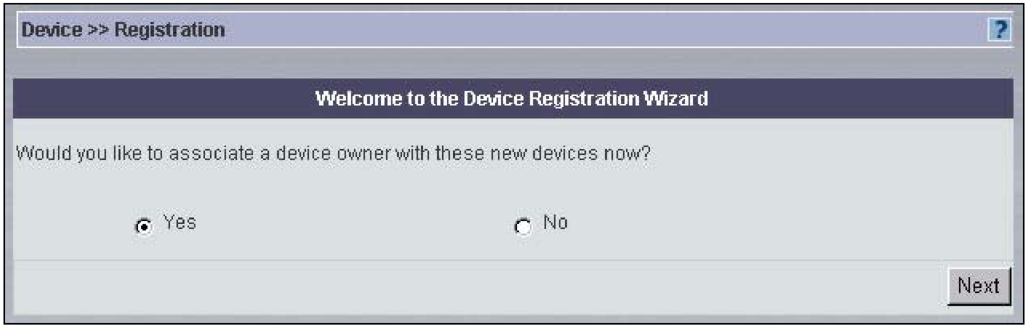
**Figure 18** Example: XML Registration File (Syslog Settings)

```
<device-feature>
  <log-setting>
    <mail-server>asdfasdfasdf</mail-server>
    <mail-sender/>
    <mail-subject/>
    <send-log-to/>
    <send-alerts-to/>
    <syslog-active-flag>false</syslog-active-flag>
    <syslog-server-ip>0.0.0.0</syslog-server-ip>
=================================== SNIP ================================
  </log-setting>
</device-feature>
```

## 3.2.2 Registration Screen

Select a folder in the object tree, and click **Device** > **Registration** to register one or more devices and associate them with the folder.

**Figure 19** Device > Registration



Device >> Registration

Welcome to the Device Registration Wizard

Would you like to associate a device owner with these new devices now?

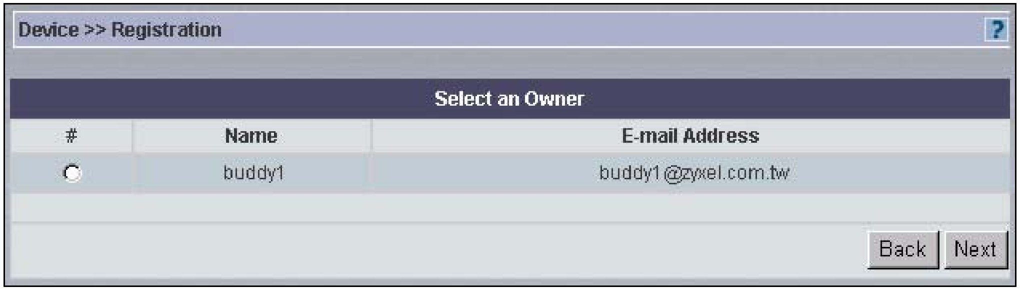
● Yes ○ No

Select **Yes**, and click **Next** to select an owner for the new device(s). The owner must be configured in **System > Address Book**. Go to Section 3.2.3 on page 59. Select **No**, and click **Next** to register the device without selecting an owner. You can set up the owner later. Go to Section 3.2.4 on page 60.

## 3.2.3 Registration Screen (Select Device Owner)

The following screen appears if you want to select an owner for the new device now.

**Figure 20** Device > Registration (Device Owner)



Device >> Registration

Select an Owner

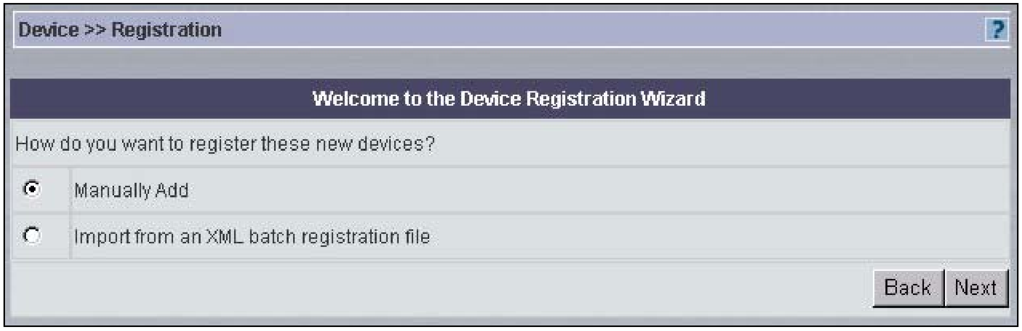
| # | Name | E-mail Address |
|---|---|---|
| ○ | buddy1 | buddy1@zyxel.com.tw |

Select the entry for the device owner, and click **Next** to continue. Go to Section 3.2.4 on page 60.

## 3.2.4 Registration Screen (Method)

The following screen appears regardless of whether or not you select an owner for the new device.

**Figure 21** Device > Registration (Method)



How do you want to register these new devices?

● Manually Add

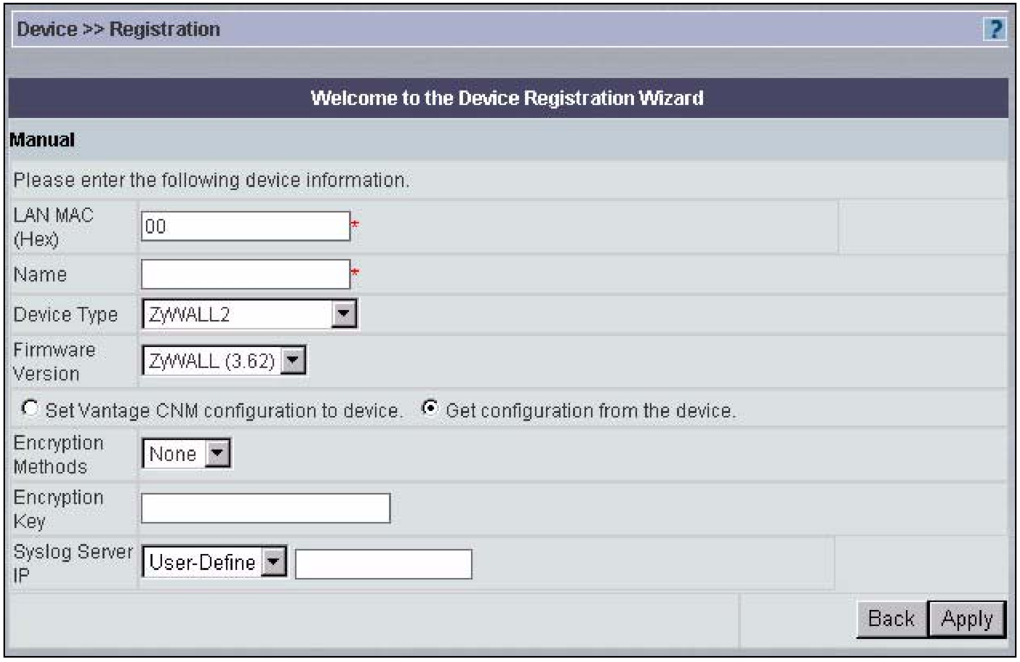
○ Import from an XML batch registration file

Select the method you want to use to register the device(s), and click **Next**. If you select **Manually Add**, go to Section 3.2.5 on page 60. If you select **Import from an XML batch registration file**, go to Section 3.2.6 on page 61.

## 3.2.5 Registration Screen (Manual Registration)

Use this screen to register a device in Vantage CNM manually. You must configure Vantage CNM on the device first. See the Quick Start Guide for instructions. To open this screen, click **Device > Registration**, and select **Manually Add** in Figure 21 on page 60.

**Figure 22** Device > Registration (Manual Registration)



Manual

Please enter the following device information.

| | |
|---|---|
| LAN MAC (Hex) | 00 * |
| Name | * |
| Device Type | ZyWALL2 |
| Firmware Version | ZyWALL (3.62) |

○ Set Vantage CNM configuration to device. ● Get configuration from the device.

| | |
|---|---|
| Encryption Methods | None |
| Encryption Key | |
| Syslog Server IP | User-Define |

The following table describes the fields in this screen.

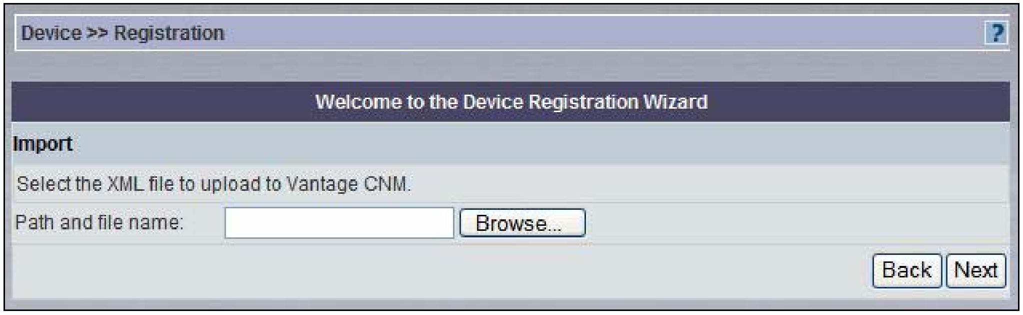
**Table 8** Device > Registration (Manual Registration)

| LABEL | DESCRIPTION |
|---|---|
| LAN MAC (Hex) | Enter the LAN MAC address of the device (without colons) in this field. Vantage CNM uses the MAC address to identify the device, so make sure it is entered correctly. |
| Name | Enter a unique name here for the device for identification purposes. The device name cannot exceed ten characters. |
| Device Type | Select the device type from the pull-down menu. The pull-down menu lists only supported device types. |
| Firmware Version | Select the firmware version the device is currently using. The pull-down menu lists only supported firmware versions. |
| Set Vantage CNM configuration to device | Select this radio button to have Vantage CNM push all current configurations from Vantage CNM to the device. The current device configuration is then reset to the configuration settings that Vantage CNM contains. |
| Get configuration from the device | Select this radio button to have Vantage CNM pull all current device configurations into Vantage CNM. The current device configuration "overwrites" Vantage CNM configurations. |
| Encryption Methods | The encryption options are DES and 3DES. Choose from **None** (no encryption), **DES** or **3DES**. The device must be set to the same encryption mode (and have the same encryption key) as the Vantage CNM server. |
| Encryption Key | Type an eight-character alphanumeric (“0” to “9”, “a” to “z” or "A" to "Z") for DES encryption and a 24-character alphanumeric (“0” to “9”, “a” to “z” or "A" to "Z") for 3DES encryption. |
| Syslog Server IP | Select the IP address of the device’s Vantage Report server, or, if the IP address is not in the drop-down box, select **User-Define** and enter the IP address. Leave the IP address blank if the device does not use a Vantage Report server. See Section 26.8 on page 306. |
| Back | Click this to return to the previous screen. |
| Apply | Click this to register the device. Go to Section 3.2.8 on page 62. |

### 3.2.6 Registration Screen (XML Registration File)

Use this screen to register one or more devices by importing an XML file. You must configure Vantage CNM on the devices first. See the Quick Start Guide for instructions. To open this screen, click **Device** > **Registration**, and select **Import from an XML batch registration file** in Figure 21 on page 60.

**Figure 23** Device > Registration (XML Registration File)


Device >> Registration

Welcome to the Device Registration Wizard

Import

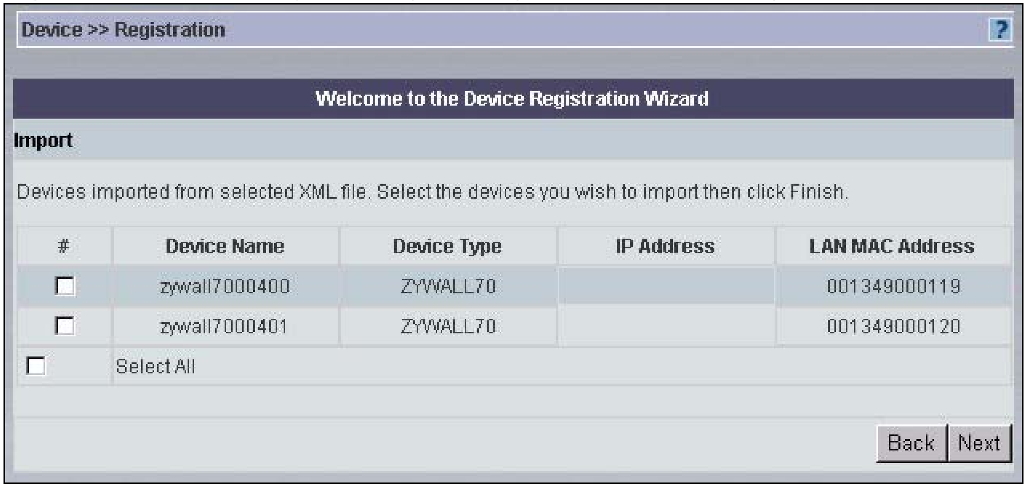
Select the XML file to upload to Vantage CNM.

Enter the path and file name, or click **Browse** to locate it, and then click **Next**. Go to Section 3.2.7 on page 62.

### 3.2.7 Registration Screen (XML File Devices)

The following screen appears.

Figure 24 Device > Registration (XML Registration File Devices)



Welcome to the Device Registration Wizard

Import

Devices imported from selected XML file. Select the devices you wish to import then click Finish.

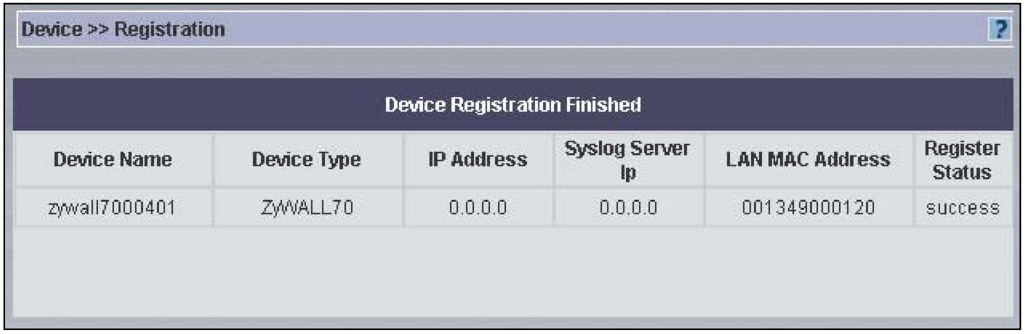
| # | Device Name | Device Type | IP Address | LAN MAC Address |
|---|---|---|---|---|
| □ | zywall7000400 | ZYWALL70 | | 001349000119 |
| □ | zywall7000401 | ZYWALL70 | | 001349000120 |
| □ | Select All | | | |

Vantage CNM lists all the devices in the specified XML registration file. Select which devices you want to import, and click **Next** to import them. It might take Vantage CNM several minutes to import the devices, depending on how many devices you have in your XML file. Go to Section 3.2.8 on page 62.

### 3.2.8 Registration Screen (Finish)

This screen displays the device(s) you tried to register and whether or not registration was successful.

Figure 25 Device > Registration (Finish)



Device Registration Finished

| Device Name | Device Type | IP Address | Syslog Server Ip | LAN MAC Address | Register Status |
|---|---|---|---|---|---|
| zywall7000401 | ZYWALL70 | 0.0.0.0 | 0.0.0.0 | 001349000120 | success |

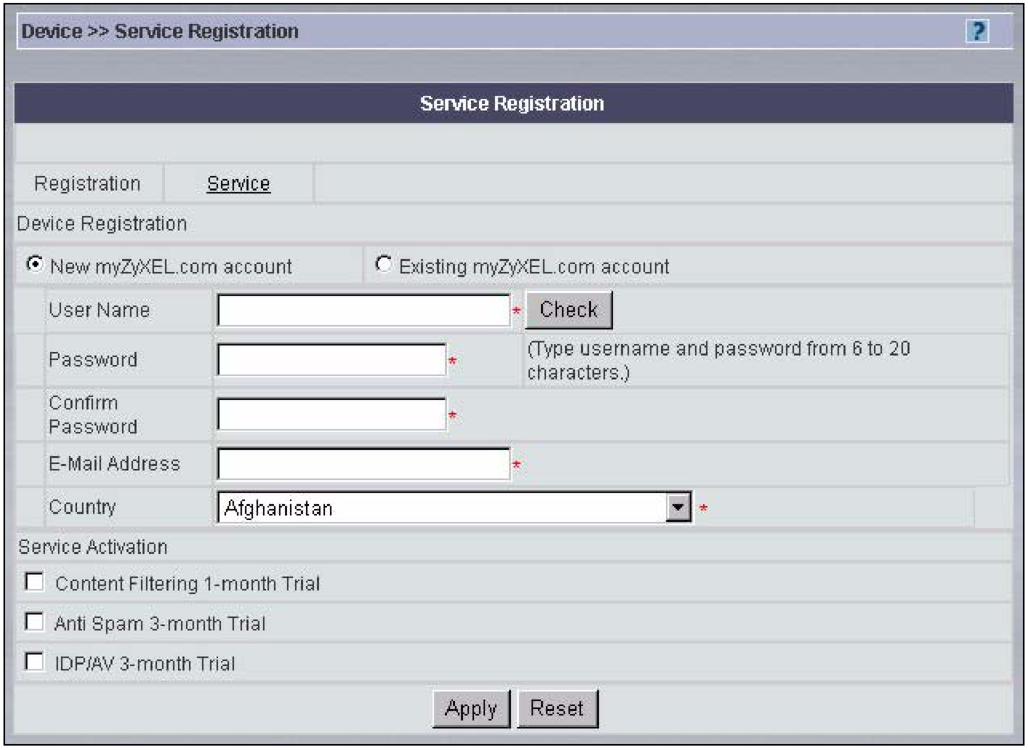
## 3.3 Service Registration

Use this menu item to register the selected device and to activate subscription services.

## 3.3.1 Registration

Use this screen to register the selected device on www.myzyxel.com and to activate free trials for subscription services, such as IDP and content filtering. The Vantage CNM server must be connected to the Internet and have access to www.myzyxel.com.

**Figure 26** Device > Service Registration > Registration



Device >> Service Registration

Service Registration

Registration | Service

Device Registration

● New myZyXEL.com account ○ Existing myZyXEL.com account

| | | |
|---|---|---|
| User Name | * | Check |
| Password | * | (Type username and password from 6 to 20 characters.) |
| Confirm Password | * | |
| E-Mail Address | * | |
| Country | Afghanistan * | |

Service Activation

□ Content Filtering 1-month Trial

□ Anti Spam 3-month Trial

□ IDP/AV 3-month Trial

The following table describes the labels in this screen.

**Table 9** Device > Service Registration > Registration

| LABEL | DESCRIPTION |
|---|---|
| Device Registration | If you select **Existing myZyXEL.com account**, only the **User Name** and **Password** fields are available. |
| New myZyXEL.com account | If you haven’t created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your device. |
| Existing myZyXEL.com account | If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your device. |
| User Name | Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Check | Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used. |
| Password | Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Confirm Password | Enter the password again for confirmation. |
| E-Mail Address | Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces. |
| Country | Select your country from the drop-down box list. |

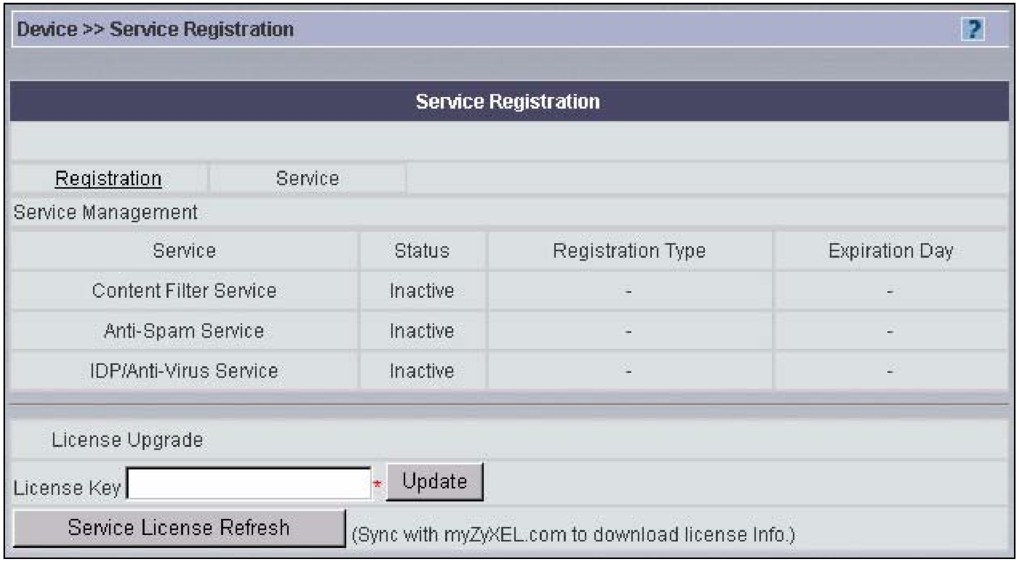
**Table 9** Device > Service Registration > Registration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service Activation | These are trial service subscriptions. After the trial expires, you can buy an iCard and enter the license key in the **Device > Service Registration > Service** screen to extend the service. |
| Content Filtering 1-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| Anti Spam 3-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| IDP/AV 3-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 3.3.2 Service

Use this screen to look at or update the current status of subscription services, such as IDP and content filtering, in the selected device. The Vantage CNM server must be connected to the Internet and have access to www.myzyxel.com to update the current status.

**Figure 27** Device > Service Registration > Service



Device >> Service Registration

Service Registration

Service Management

| Service | Status | Registration Type | Expiration Day |
|---|---|---|---|
| Content Filter Service | Inactive | - | - |
| Anti-Spam Service | Inactive | - | - |
| IDP/Anti-Virus Service | Inactive | - | - |

License Upgrade

License Key *

(Sync with myZyXEL.com to download license Info.)

The following table describes the labels in this screen.

**Table 10** Device > Service Registration > Service

| LABEL | DESCRIPTION |
|---|---|
| Service Management | |
| Service | This field displays the service name available on the device. |
| Status | This field displays whether a service is activated (**Active**) or not (**Inactive**). |
| Registration Type | This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). |
| Expiration Day | This field displays the date your service expires. |
| License Upgrade | |

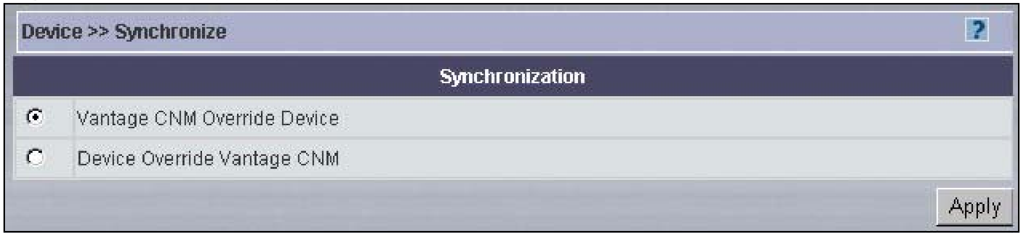
**Table 10** Device > Service Registration > Service (continued)

| LABEL | DESCRIPTION |
|---|---|
| License Key | Enter your iCard's PIN number and click **Update** to activate or extend a standard service subscription.<br>If a standard service subscription runs out, you need to buy a new iCard (specific to your device) and enter the new PIN number to extend the service. |
| Service License Refresh | Click this button to renew service license information, such as the license key, registration status and expiration day. You might do this if you restore the device to the default configuration file or upload a different configuration file after you register the device on www.myzyxel.com. |

## 3.4 Synchronize

Data inconsistencies may occur if device configurations are made directly to the device instead of in Vantage CNM. Use this screen to resolve any data inconsistencies between the selected device and Vantage CNM. To use this screen, select a device, and click **Device** > **Synchronize**.

**Figure 28** Device > Synchronize



Select **Vantage CNM Override Device** if you want Vantage CNM to push all current configurations from Vantage CNM to the device. The current device configuration is then reset to the configuration settings in Vantage CNM.

Select **Device Override Vantage CNM** if you want Vantage CNM to pull all current device configurations into Vantage CNM. The current device configuration "overwrites" Vantage CNM configurations.

If you are not sure how to resolve inconsistencies between the device and Vantage CNM, you might access the device's web configurator and compare the settings in the web configurator to the settings in Vantage CNM before you use this function.

## 3.5 Firmware Mgmt

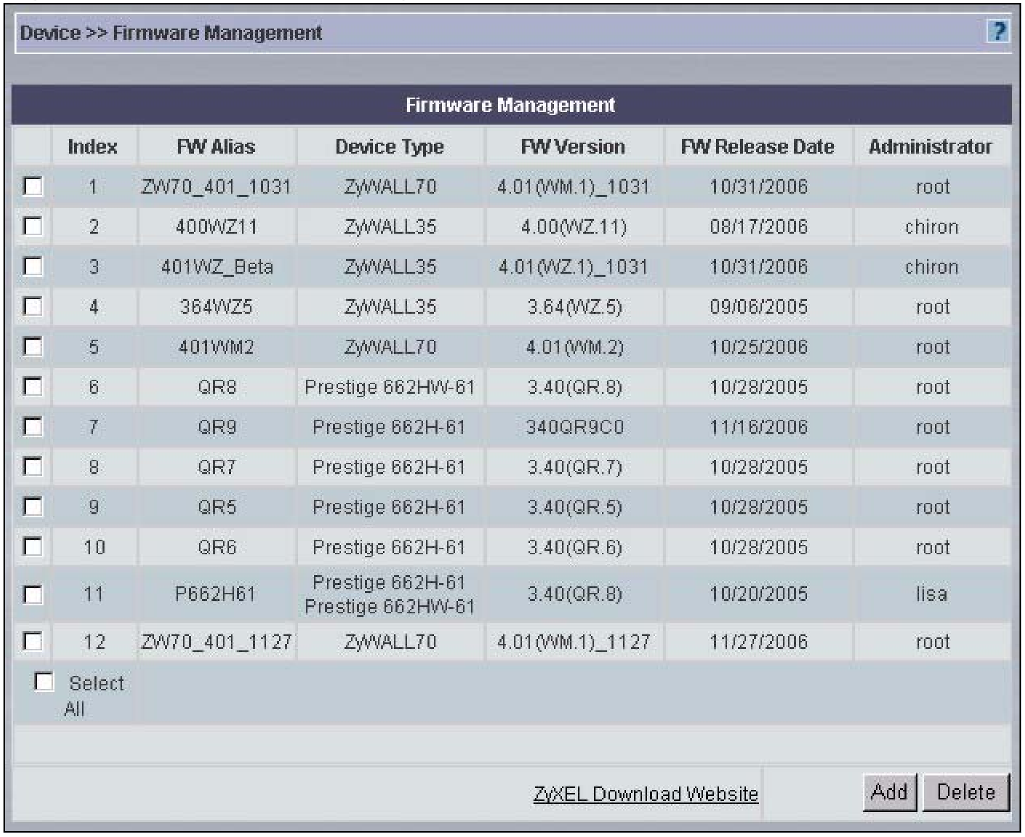
Use this screen to upload device firmware to Vantage CNM. Administrators should subscribe to the ZyXEL mailing lists to be regularly informed of new firmware versions.

All firmware is downloaded to one repository within Vantage CNM. All firmware is available to every administrator, regardless of domain.

After you download firmware to Vantage CNM, you can use the **Device** > **Firmware Upgrade** menu item to upload it from Vantage CNM to one or more devices. See Section 3.6 on page 67.

Click **Device** > **Firmware Mgmt** to display the next screen.

**Figure 29** Device > Firmware Mgmt



Device >> Firmware Management

Firmware Management

| | Index | FW Alias | Device Type | FW Version | FW Release Date | Administrator |
|---|---|---|---|---|---|---|
| □ | 1 | ZW70_401_1031 | ZyWALL70 | 4.01(WM.1)_1031 | 10/31/2006 | root |
| □ | 2 | 400WZ11 | ZyWALL35 | 4.00(WZ.11) | 08/17/2006 | chiron |
| □ | 3 | 401WZ_Beta | ZyWALL35 | 4.01(WZ.1)_1031 | 10/31/2006 | chiron |
| □ | 4 | 364WZ5 | ZyWALL35 | 3.64(WZ.5) | 09/06/2005 | root |
| □ | 5 | 401WM2 | ZyWALL70 | 4.01(WM.2) | 10/25/2006 | root |
| □ | 6 | QR8 | Prestige 662HW-61 | 3.40(QR.8) | 10/28/2005 | root |
| □ | 7 | QR9 | Prestige 662H-61 | 340QR9C0 | 11/16/2006 | root |
| □ | 8 | QR7 | Prestige 662H-61 | 3.40(QR.7) | 10/28/2005 | root |
| □ | 9 | QR5 | Prestige 662H-61 | 3.40(QR.5) | 10/28/2005 | root |
| □ | 10 | QR6 | Prestige 662H-61 | 3.40(QR.6) | 10/28/2005 | root |
| □ | 11 | P662H61 | Prestige 662H-61<br>Prestige 662HW-61 | 3.40(QR.8) | 10/20/2005 | lisa |
| □ | 12 | ZW70_401_1127 | ZyWALL70 | 4.01(WM.1)_1127 | 11/27/2006 | root |

□ Select All

The following table describes the fields in this screen.

**Table 11** Device > Firmware Mgmt

| TYPE | DESCRIPTION |
|---|---|
| Index | This is the file list number. |
| FW Alias | This is a descriptive name for the firmware. This is specified when the firmware is uploaded. See Section 3.5.1 on page 67. |
| Device Type | This field displays the model. You must upload firmware to the correct model. Vantage CNM should automatically detect firmware for the device selected. Uploading incorrect firmware may damage the device. |
| FW Version | This field displays ZyNOS (ZyXEL Network Operating System) firmware version. |
| FW Release Date | This field displays the date the firmware was created. |
| Administrator | This field displays the administrator who downloaded this firmware file to Vantage CNM. |
| ZyXEL Download Website | Click this hyperlink to go to the ZyXEL Website and download firmware to your computer.<br>Firmware is uploaded to your device in the following manner:<br>• Download from the web site to your computer.<br>• Upload from your computer to the Vantage CNM (**Device > Firmware Mgmt**).<br>• Upload from Vantage CNM to your selected device (**Device > Firmware Upgrade**). |

**Table 11** Device > Firmware Mgmt (continued)

| TYPE | DESCRIPTION |
|---|---|
| Add | Click **Add** to proceed to the next screen. |
| Delete | Click to delete a selected firmware from your Vantage CNM firmware management. |

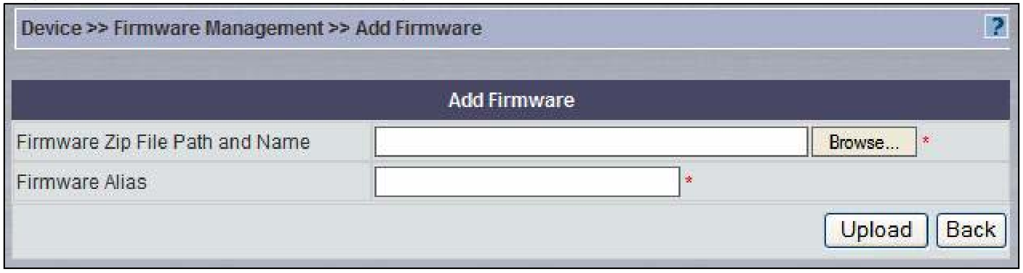
### 3.5.1 Add Firmware

Use this screen to select the firmware you want to upload to Vantage CNM. To open this screen, click **Add** in **Device > Firmware Mgmt**.

You must upload the whole firmware zip file, which contains the following:

- The device firmware (bin file extension). Only this firmware file is actually downloaded to the device.
- The device default configuration file (config file extension).
- Device firmware release notes (doc file extension) highlighting.
- Boot module with bm file extension.
- A file with XML file extension. Vantage CNM uses the XML file to gather the device type, firmware version and release date information.

**Figure 30** Device > Firmware Mgmt > Add



Device >> Firmware Management >> Add Firmware

Add Firmware

| | |
|---|---|
| Firmware Zip File Path and Name | * |
| Firmware Alias | * |

Type the file name and path of the firmware zip file, or click **Browse** to locate it. You may also create an alias that appears in the previous screen. Click **Upload** to load the firmware zip file to Vantage CNM. Then, click **Device > Firmware Upgrade** if you want to upload the firmware to one or more devices. See Section 3.6 on page 67.

## 3.6 Firmware Upgrade

Use this menu item to upload ZyXEL device firmware from Vantage CNM to one or more devices. You have to use the **Device > Firmware Mgmt** menu item to upload firmware from the ZyXEL FTP site (or other source) to Vantage CNM first. See Section 3.5 on page 65.

Consider the following when you decide to upgrade firmware.

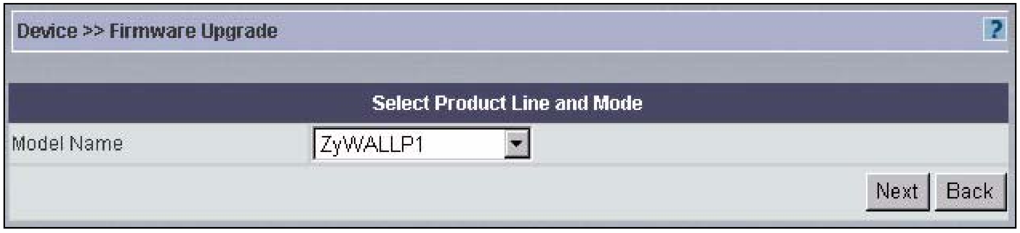
- It is advisable to upgrade firmware during periods of low network activity, since each device must restart after firmware upload.
- You should also notify device owners before you begin the upload. See the **System > Preferences > Notifications** screen.

The first screen depends on whether a folder or a device is currently selected in the object pane.

### 3.6.1 Folder

Use this screen to select what type of devices to which you want to download firmware. To open this screen, select a folder, and click **Device** > **Firmware Upgrade**.

**Figure 31** Device > Firmware Upgrade (Folder)



Device >> Firmware Upgrade

Select Product Line and Mode

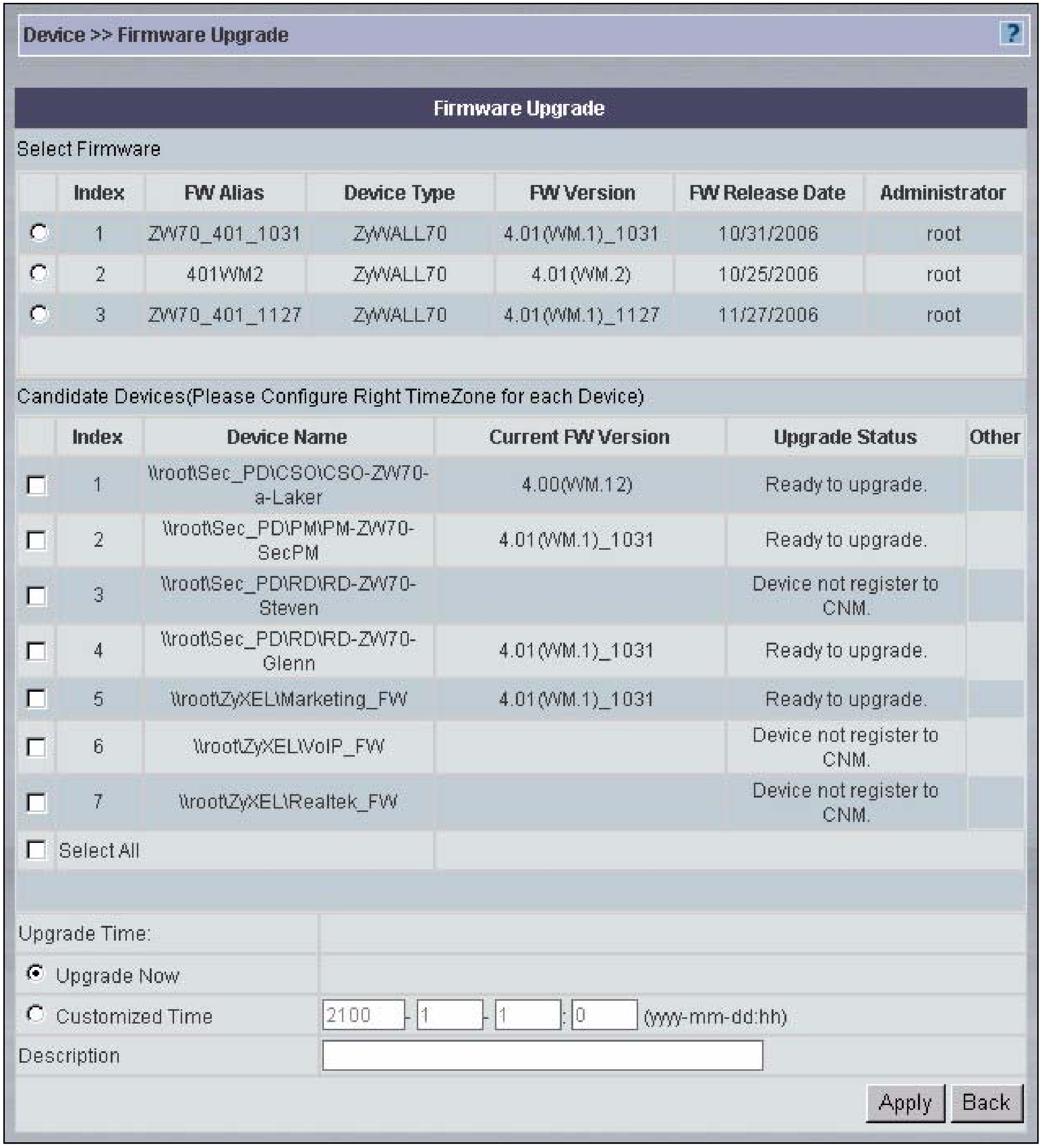
Model Name: ZyWALLP1

Pick a model name, and click **Next**. This opens a screen like the one in Section 3.6.2 on page 68. Click **Back** to look at a summary of firmware upgrades currently scheduled. See Section 3.7 on page 70.

### 3.6.2 Device

Use this screen to select the new firmware and the device(s) to which to upload it. To open this screen, select a model in the **Device** > **Firmware Upgrade** screen, and click **Next**. Alternatively, select a device in any view or a folder in **TypeView**, and click **Device** > **Firmware Upgrade**.

**Figure 32** Device > Firmware Upgrade (Device)



Device >> Firmware Upgrade

Firmware Upgrade

Select Firmware

| | Index | FW Alias | Device Type | FW Version | FW Release Date | Administrator |
|---|---|---|---|---|---|---|
| ○ | 1 | ZW70_401_1031 | ZyWALL70 | 4.01(WM.1)_1031 | 10/31/2006 | root |
| ○ | 2 | 401WM2 | ZyWALL70 | 4.01(WM.2) | 10/25/2006 | root |
| ○ | 3 | ZW70_401_1127 | ZyWALL70 | 4.01(WM.1)_1127 | 11/27/2006 | root |

Candidate Devices(Please Configure Right TimeZone for each Device)

| | Index | Device Name | Current FW Version | Upgrade Status | Other |
|---|---|---|---|---|---|
| □ | 1 | \\root\Sec_PD\CSO\CSO-ZW70-a-Laker | 4.00(WM.12) | Ready to upgrade. | |
| □ | 2 | \\root\Sec_PD\PM\PM-ZW70-SecPM | 4.01(WM.1)_1031 | Ready to upgrade. | |
| □ | 3 | \\root\Sec_PD\RD\RD-ZW70-Steven | | Device not register to CNM. | |
| □ | 4 | \\root\Sec_PD\RD\RD-ZW70-Glenn | 4.01(WM.1)_1031 | Ready to upgrade. | |
| □ | 5 | \\root\ZyXEL\Marketing_FW | 4.01(WM.1)_1031 | Ready to upgrade. | |
| □ | 6 | \\root\ZyXEL\VoIP_FW | | Device not register to CNM. | |
| □ | 7 | \\root\ZyXEL\Realtek_FW | | Device not register to CNM. | |

□ Select All

Upgrade Time:

● Upgrade Now

○ Customized Time 2100 - 1 - 1 : 0 (yyyy-mm-dd:hh)

Description

The following table describes the fields in this screen.

**Table 12** Device > Firmware Upgrade (Device)

| TYPE | DESCRIPTION |
|---|---|
| Select Firmware | Select the firmware you want to upload to one or more devices. Use the **Device > Firmware Mgmt** screens to upload firmware in this section. See Table 11 on page 66 for field descriptions in this section. |
| Candidate Devices | Select the device(s) to which you want to upload the selected firmware. You can also select **Select All** to upload the selected firmware to all devices on this page to upload the selected firmware to all devices of the appropriate type including those not shown on the current screen. |
| Index | This field displays the device number. |
| Device Name | This field displays the full path and name of the device in Vantage CNM. |

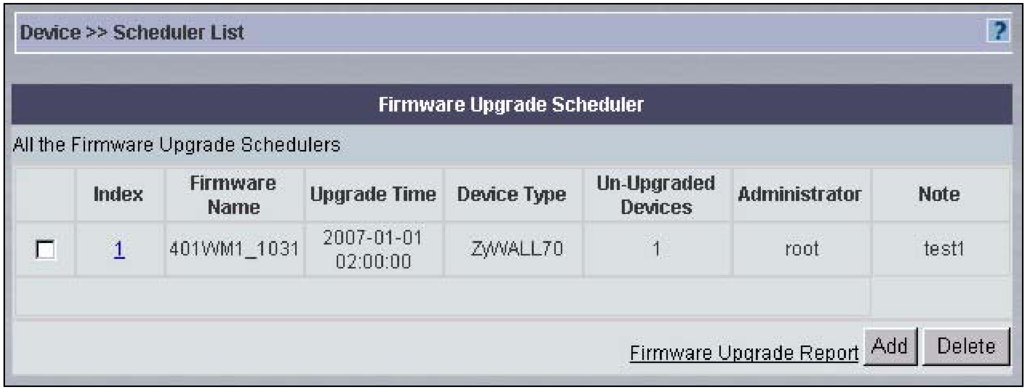
**Table 12** Device > Firmware Upgrade (Device) (continued)

| TYPE | DESCRIPTION |
|---|---|
| Current FW Version | This field displays ZyNOS (ZyXEL network operating System) firmware version. It is blank if the device has not been registered. |
| Upgrade Status | This field displays the current status of the device with respect to firmware upgrades.<br>**Ready to upgrade**: The device is available for upgrading.<br>**Device is scheduled**: The device is already scheduled for an upgrade.<br>**Upgrading**: The device is upgrading right now.<br>**Device is offline**: The device is offline.<br>**Device not register to CNM**: The device has not been registered in Vantage CNM. |
| Other | If the **Upgrade Status** is **Device is scheduled**, this field provides a Remove button to remove the device from the scheduled upgrade. Otherwise, this field is blank. |
| Upgrade Time | Select **Upgrade Now** if you want to upgrade the firmware immediately or **Customized Time** if you want to upgrade the firmware at a specified day and time in the future. |
| Description | Enter any information you want to appear in the Scheduler List screen before the upgrade is completed and in the Firmware Upgrade Report when the upgrade is completed. See Section 3.7 on page 70 and Section 28.1 on page 321, respectively, for more information about these screens and reports. |
| Apply | Click **Apply** to save your changes. If you selected **Upgrade Now**, the firmware upgrade begins immediately. If you selected **Customized Time**, the scheduled firmware upgrade is added to the **Device > Scheduler List** screen. See Section 3.7 on page 70 for more information about this screen. |
| Back | Click **Back** to return to the previous screen. |

## 3.7 Scheduler List

Use this screen to look at and maintain the list of scheduled firmware upgrades in Vantage CNM. Once an upgrade is complete, Vantage CNM removes the upgrade from this screen and adds it to the **Firmware Upgrade Report** (Section 28.1 on page 321). To open this screen, click **Device > Scheduler List**. You can also click **Device > Firmware Upgrade**, and click **Back**.

**Figure 33** Device > Scheduler List



Device >> Scheduler List

Firmware Upgrade Scheduler

All the Firmware Upgrade Schedulers

| | Index | Firmware Name | Upgrade Time | Device Type | Un-Upgraded Devices | Administrator | Note |
|---|---|---|---|---|---|---|---|
| □ | 1 | 401WM1_1031 | 2007-01-01 02:00:00 | ZyWALL70 | 1 | root | test1 |

The following table describes the fields in this screen.

**Table 13** Device > Scheduler List

| TYPE | DESCRIPTION |
|---|---|
| Index | This field displays the firmware upgrade list number. Click this to edit the scheduled firmware upgrade. This opens a screen similar to the **Device > Firmware Upgrade** screen shown in Figure 32 on page 69. |
| Firmware Name | This field displays the ZyNOS (ZyXEL network operating System) firmware version that is scheduled to be uploaded. |
| Upgrade Time | This field displays the time the upgrade is scheduled to occur. |
| Device Type | This field displays the type of device that is going to be upgraded. |
| Un-Upgraded Devices | This field displays the number of devices that are going to be upgraded. |
| Administrator | This field displays the administrator who scheduled this upgrade. |
| Note | This field displays any additional information the administrator provided when setting up this upgrade. This information is specified in the **Description** field in Figure 32 on page 69. |
| Firmware Upgrade Report | Click this to look at information about completed firmware upgrades. See Section 28.1 on page 321 for more information. |
| Add | Click this to set up a firmware upgrade. Vantage CNM returns to the screen in Figure 31 on page 68. |
| Delete | Click to cancel or delete the selected upgrade(s) from Vantage CNM. |

## 3.8 Configuration File

Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Use this menu item to manage, back up and restore configuration files for specific devices or for multiple devices in a specific folder. If you back up multiple devices in a specific folder, you can manage and restore the configuration files at the folder level or individually by device.

You can back up configuration files to Vantage CNM or to your computer. If you back up a configuration file to Vantage CNM, you can only restore that configuration file to that device, even if other devices are the same model and are running the same firmware.

Before you restore a configuration file, make sure the new configuration does not prevent you from managing the device remotely, unless that is desired.

Make sure you restore a configuration file to an appropriate model. Otherwise, you may damage the device or lock yourself out.

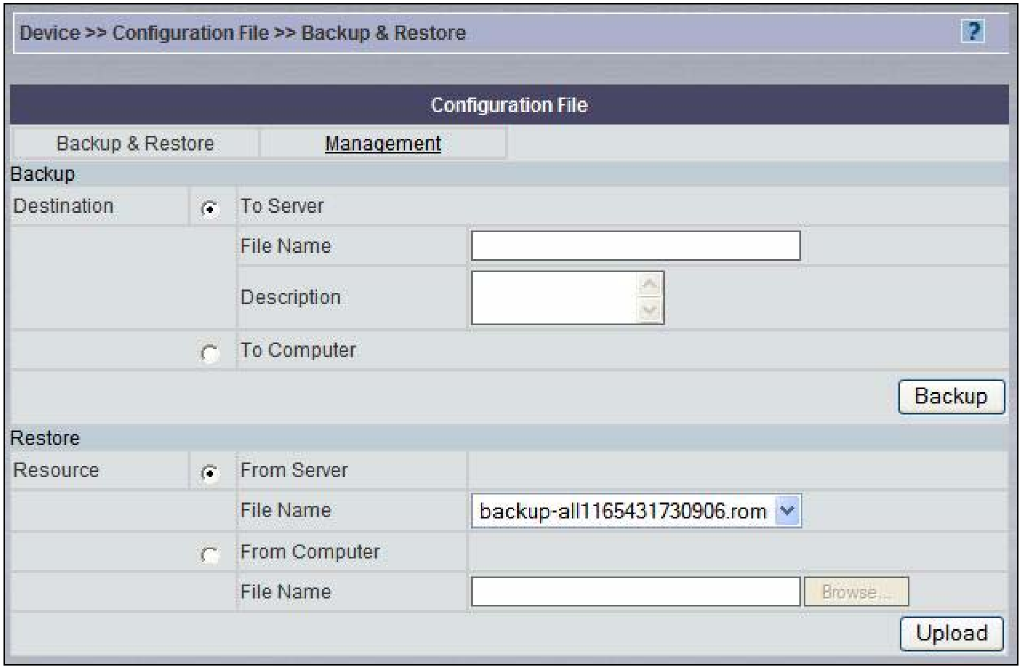
You can create your own configuration file alias in Vantage CNM. This may make it easier to distinguish between configuration files.

The menu item displays different screens depending on whether you selected a device or a folder before you clicked this menu item.

## 3.8.1 Backup & Restore (Device)

Use this screen to back up and restore configuration files for a specific device. The configuration files may be stored in the Vantage CNM server or on the computer from which you access Vantage CNM. To open this screen, select a device, and then click **Device > Configuration File > Backup & Restore**.

**Figure 34** Device > Configuration File > Backup & Restore (Device)



Device >> Configuration File >> Backup & Restore

Configuration File

Backup & Restore | Management

Backup

Destination ● To Server

File Name

Description

○ To Computer

Backup

Restore

Resource ● From Server

File Name backup-all1165431730906.rom

○ From Computer

File Name

The following table describes the fields in this screen.

**Table 14** Device > Configuration File > Backup & Restore (Device)

| TYPE | DESCRIPTION |
|---|---|
| Backup | |
| To Server | Select the radio button to save the configuration file on the Vantage CNM server. |
| File Name | Type in the name of the configuration file you want to create. The name must be 1-20 characters long, and you cannot use spaces or the \ / : * ? < > \| “ characters. Vantage CNM automatically appends a string of numbers followed by “.rom” to this name. |
| Description | Type a description of the file backup. This description is displayed in the **Device > Configuration > Management** screen (see Figure 35 on page 73). |
| To Computer | Select the radio button to save the configuration file to your computer. If you select this and click **Backup**, you will be prompted where to save the file on your computer. |
| Backup | Click this to save the specified configuration file. |

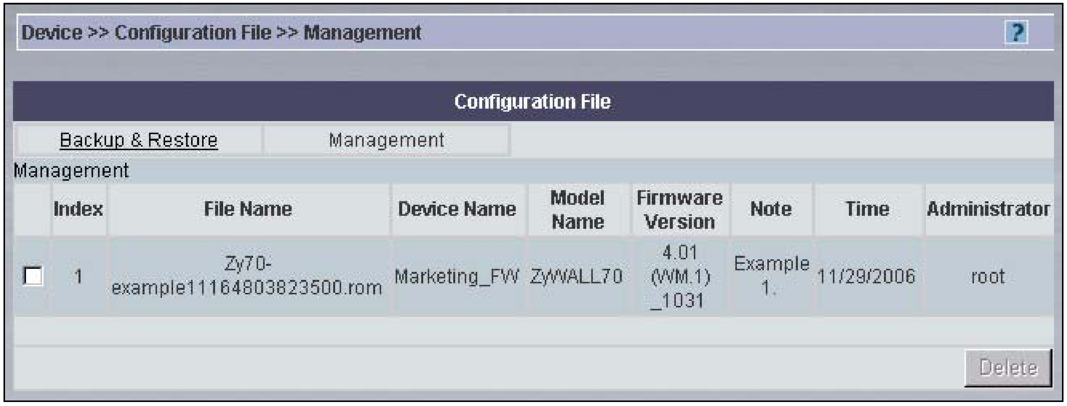
**Table 14** Device > Configuration File > Backup & Restore (Device) (continued)

| TYPE | DESCRIPTION |
|---|---|
| Restore | |
| From Server | Select this radio button to upload a configuration file from the Vantage CNM server. |
| File Name | Select the configuration file you want to upload to the selected device. |
| From Computer | Select this radio button to upload a configuration file from your computer. |
| File Path and Name | Type in the name and location of the file you want to upload, or click **Browse...** to find it. |
| Upload | Click **Upload** to begin the upload process. |

## 3.8.2 Management (Device)

Use this screen to manage configuration files uploaded to Vantage CNM for the selected device. To open this screen, select the device, and click **Device** > **Configuration File** > **Management**.

**Figure 35** Device > Configuration File > Management (Device)



Device >> Configuration File >> Management

Configuration File

Backup & Restore | Management

Management

| | Index | File Name | Device Name | Model Name | Firmware Version | Note | Time | Administrator |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | Zy70-example11164803823500.rom | Marketing_FW | ZyWALL70 | 4.01 (WM.1) _1031 | Example 1. | 11/29/2006 | root |

The following table describes the fields in this screen

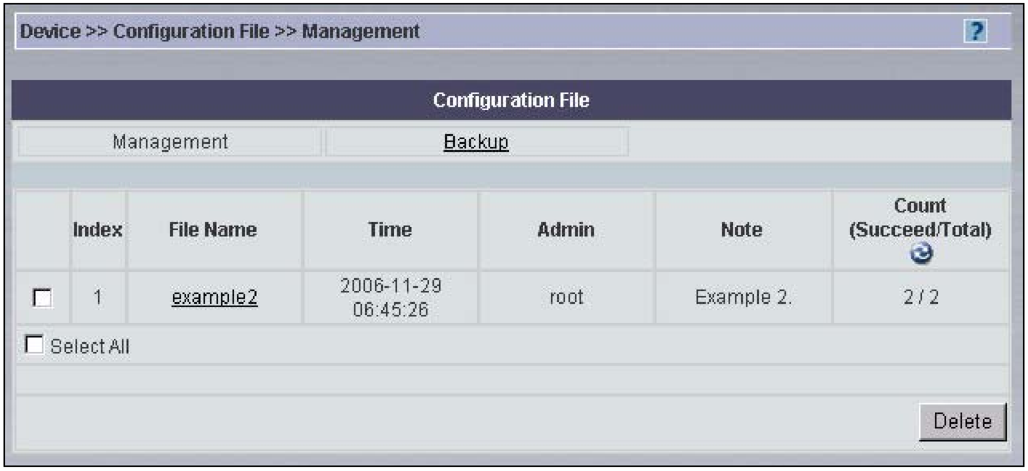
**Table 15** Device > Configuration File > Management (Device)

| TYPE | DESCRIPTION |
|---|---|
| Index | This displays a number assigned to the file |
| File Name | This displays the name of the configuration file. |
| Device Name | This displays the name of the device that was backed up. |
| Model Name | This displays the type of the device that was backed up. |
| Firmware Version | This displays the firmware version of the device when the configuration file was backed up. |
| Note | This displays a description that was entered at the time of file backup. |
| Time | This field displays the date of backup of the configuration file. |
| Administrator | This field displays the administrator who performed the backup of the configuration file. |
| Delete | Select the check box next to a configuration file and click **Delete** to remove a selected configuration file from the Vantage CNM server. |

## 3.8.3 Management (Folder)

Use this screen to manage or restore configuration files uploaded to Vantage CNM for multiple devices in the selected folder. You cannot use this screen to manage or restore configuration files uploaded to Vantage CNM for a specific device (in other words, using Figure 34 on page 72), even if that device is in the folder. To open this screen, select the folder, and click **Device** > **Configuration File** > **Management**.

**Figure 36** Device > Configuration File > Management (Folder)



|  | Index | File Name | Time | Admin | Note | Count (Succeed/Total) |
|---|---|---|---|---|---|---|
| □ | 1 | example2 | 2006-11-29 06:45:26 | root | Example 2. | 2 / 2 |

□ Select All

The following table describes the fields in this screen.

**Table 16** Device > Configuration File > Management (Folder)

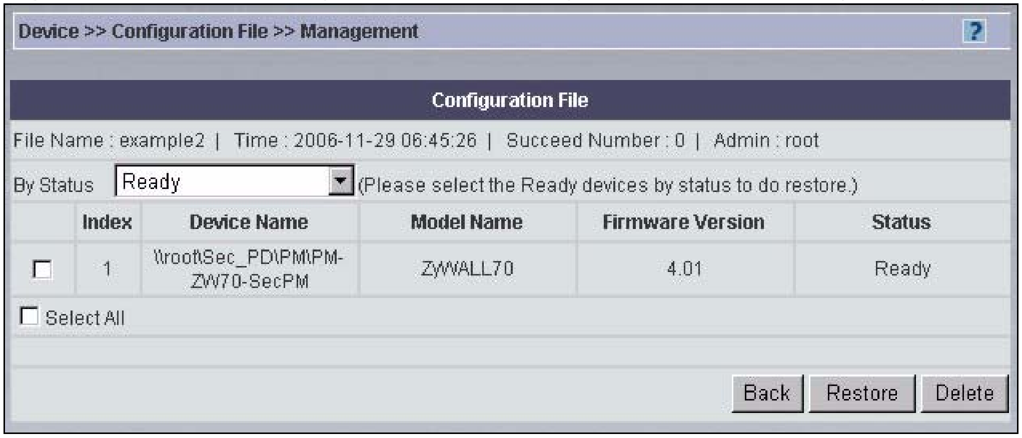
| TYPE | DESCRIPTION |
|---|---|
| Index | This displays a number assigned to the set of configuration files. |
| File Name | This displays the name of the set of configuration files. Click the file name to edit or restore the configuration files for one or more devices in the folder. |
| Time | This field displays the date of backup of the configuration files. |
| Admin | This field displays the administrator who performed the backup of the configuration files. |
| Note | This displays a description that was entered at the time of file backup. |
| Count | This field tracks the progress while Vantage CNM backs up configuration files for one or more devices. It displays the number of devices whose backups are complete and the total number of devices that are supposed to be backed up. |
| Select All | Select this to select all sets of configuration files. |
| Delete | Select the check box next to one or more sets of configuration files and click **Delete** to remove the selected set(s) from the Vantage CNM server. |

## 3.8.4 Edit/Restore Configuration Files (Folder)

Use this screen to restore configuration files for one or more devices in the selected set of configuration files. To open this screen, select a folder, click **Device** > **Configuration File** > **Management**, and then click the set of configuration files.

You have to select **Ready** in the **By Status** field before you can restore any configuration files.

**Figure 37** Device > Configuration File > Management > Edit/Restore (Folder)



Device >> Configuration File >> Management

Configuration File

File Name : example2 | Time : 2006-11-29 06:45:26 | Succeed Number : 0 | Admin : root

By Status: Ready (Please select the Ready devices by status to do restore.)

| | Index | Device Name | Model Name | Firmware Version | Status |
|---|---|---|---|---|---|
| □ | 1 | \\root\Sec_PD\PM\PM-ZW70-SecPM | ZyWALL70 | 4.01 | Ready |

□ Select All

The following table describes the fields in this screen.

**Table 17** Device > Configuration File > Management > Edit/Restore (Folder)

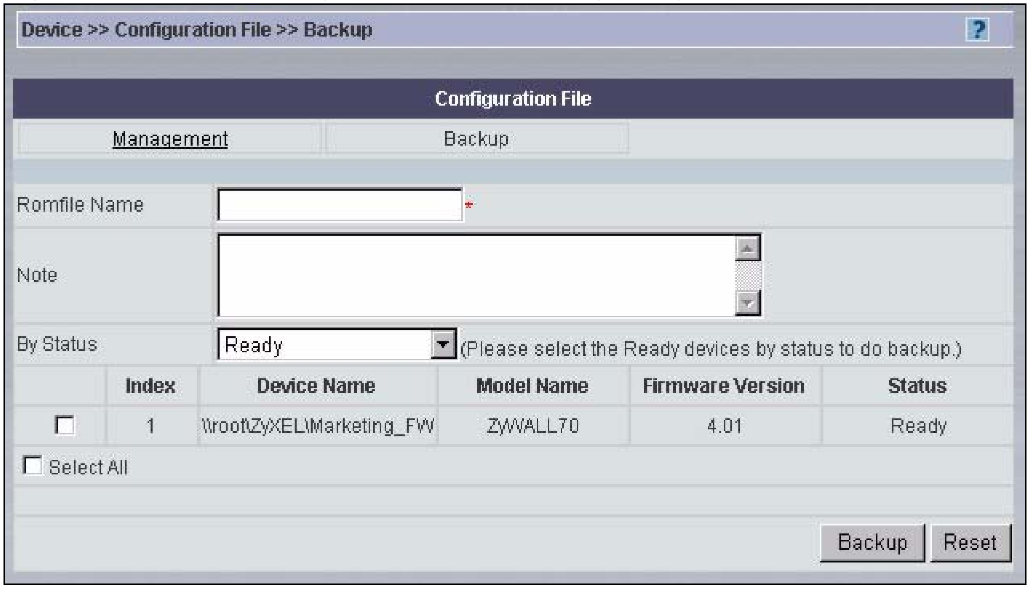
| TYPE | DESCRIPTION |
|---|---|
| File Name | This displays the name of the set of configuration files. |
| Time | This field displays the date of backup of the configuration files. |
| Succeed Number | This field displays the number of devices whose backups are complete. |
| Admin | This field displays the administrator who performed the backup of the configuration files. |
| By Status | Select **Ready**. You can only restore the configuration file of a device that is **Ready**. If a device does not appear in the list, select a different status to find out why the device is not available for restoring configuration files right now. |
| Index | This field displays the device list number. |
| Device Name | This displays the name of the device that was backed up. |
| Model Name | This displays the type of the device that was backed up. |
| Firmware Version | This displays the firmware version of the device when the configuration file was backed up. |
| Status | This displays the current status of the device. You can only restore the configuration file of a device that is **Ready**. |
| Select All | Select this to select all the devices. |
| Back | Click this to return to the previous screen. |
| Restore | Select the check box next to one or more configuration files and click this to restore the selected configuration files to the devices. |
| Delete | Select the check box next to one or more configuration files and click this to remove the selected configuration files from the set. |

## 3.8.5 Backup (Folder)

Use this screen to back up configuration files for one or more devices in the specified folder. The configuration files must be stored in the Vantage CNM server. Use Figure 34 on page 72 to restore the configuration files to a specific device in the folder. To open this screen, select a folder, and then click **Device** > **Configuration File** > **Backup**.

You have to select **Ready** in the **By Status** field before you can back up any configuration files.

**Figure 38** Device > Configuration File > Backup (Folder)



| | | | | | |
|---|---|---|---|---|---|
| Romfile Name | * | | | | |
| Note | | | | | |
| By Status | Ready (Please select the Ready devices by status to do backup.) | | | | |
| | Index | Device Name | Model Name | Firmware Version | Status |
| ☐ | 1 | \\root\ZyXEL\Marketing_FW | ZyWALL70 | 4.01 | Ready |

☐ Select All

The following table describes the fields in this screen.

**Table 18** Device > Configuration File > Backup (Folder)

| TYPE | DESCRIPTION |
|---|---|
| Romfile Name | Enter the name of the set of configuration files. The name must be 1-20 characters long, and you cannot use spaces or the \ / : * ? < > \| “ characters.<br>This name is also used in the name of each configuration file in the set, if you look at the configuration files for a specific device in the folder. Vantage CNM automatically appends a string of numbers followed by “.rom” to this name. |
| Note | Type a description of the file backup. This description is displayed in the **Device > Configuration > Management** screen for each device (see Figure 35 on page 73) and for the folder (see Figure 36 on page 74). |
| By Status | Select **Ready**. You can only back up the configuration file of a device that is **Ready**. If a device does not appear in the list, select a different status to find out why the device is not available for backup right now. |
| Index | This field displays the device list number. |
| Device Name | This displays the name of the device that was backed up. |
| Model Name | This displays the type of the device that was backed up. |

**Table 18** Device > Configuration File > Backup (Folder) (continued)

| TYPE | DESCRIPTION |
|---|---|
| Firmware Version | This displays the firmware version of the device when the configuration file was backed up. |
| Status | This displays the current status of the device. You can only back up the configuration file of a device that is **Ready**. |
| Select All | Select this to select all the devices. |
| Backup | Select the check box next to one or more devices and click this to back up the configuration files for the selected devices. |
| Reset | Click this to return the screen to its default values. |

## 3.9 Signature Profile

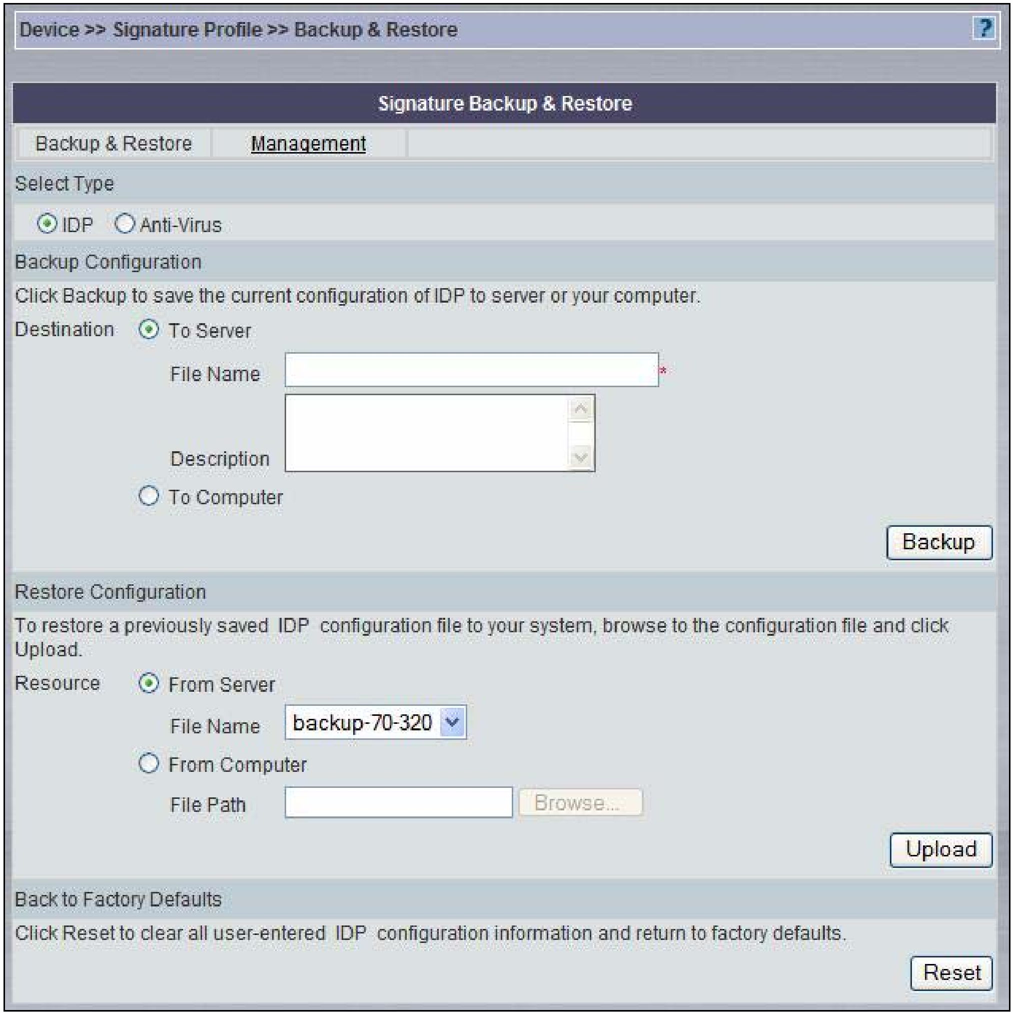
Use this menu item to manage, back up and restore the configuration and signatures for services such as IDP and anti-virus. The menu item displays different screens depending on whether you selected a device or a folder before you clicked this menu item.

### 3.9.1 Backup & Restore (Device)

Use this screen to back up and restore the configuration and signatures for a specific device. The configuration may be stored in the Vantage CNM server or on the computer from which you access Vantage CNM. You can also use this screen to reset the service configuration to its factory default settings. To open this screen, select a device, and then click **Device > Signature Profile > Backup & Restore**.

You cannot use this screen if the device's Turbo Card is not installed.

**Figure 39** Device > Signature Profile > Backup & Restore (Device)



Device >> Signature Profile >> Backup & Restore

Signature Backup & Restore

Backup & Restore | Management

Select Type

● IDP ○ Anti-Virus

Backup Configuration

Click Backup to save the current configuration of IDP to server or your computer.

Destination ● To Server

File Name *

Description

○ To Computer

Backup

Restore Configuration

To restore a previously saved IDP configuration file to your system, browse to the configuration file and click Upload.

Resource ● From Server

File Name backup-70-320

○ From Computer

File Path Browse...

Upload

Back to Factory Defaults

Click Reset to clear all user-entered IDP configuration information and return to factory defaults.

Reset

The following table describes the fields in this screen.

**Table 19** Device > Signature Profile > Backup & Restore (Device)

| TYPE | DESCRIPTION |
|---|---|
| Select Type | Select the service whose configuration and signatures you want to back up, restore, or reset. |
| Backup Configuration | |
| To Server | Select the radio button to save the configuration file and signatures on the Vantage CNM server. |
| File Name | Type in the location and name of the configuration file and signatures you want to create. |
| Description | Type a description of the file backup. |
| To Computer | Select the radio button to save the configuration file and signatures to your computer. If you select this and click **Backup**, you will be prompted where to save the file on your computer. |
| Backup | Click this to save the specified configuration file and signatures. |
| Restore Configuration | |

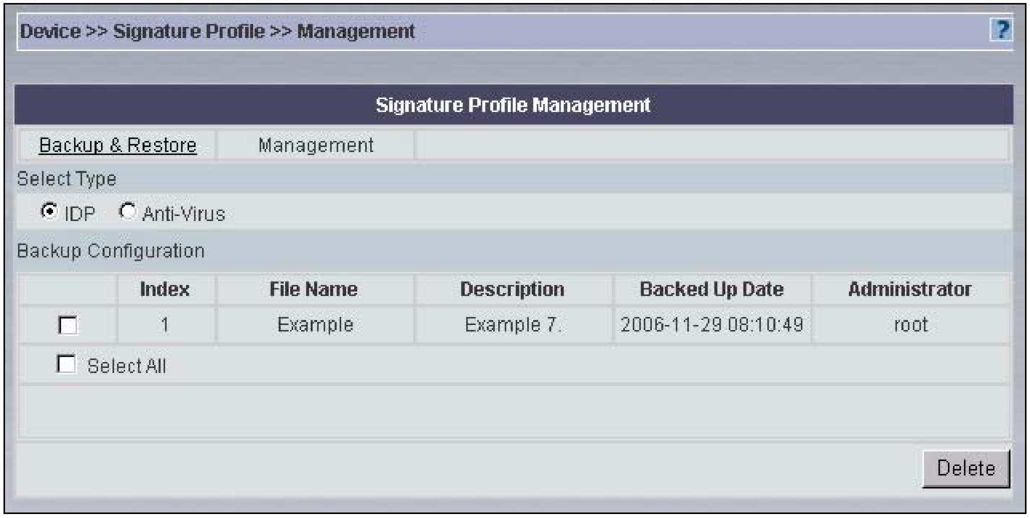
**Table 19** Device > Signature Profile > Backup & Restore (Device) (continued)

| TYPE | DESCRIPTION |
|---|---|
| From Server | Select this radio button to upload a configuration file and signatures from the Vantage CNM server. |
| File Name | Select the configuration file and signatures you want to upload to the selected device. |
| From Computer | Select this radio button to upload a configuration file and signatures from your computer. |
| File Path and Name | Type in the name and location of the file you want to upload, or click **Browse...** to find it. |
| Upload | Click **Upload** to begin the upload process. |
| Back to Factory Defaults | |
| Reset | Click this to reset the configuration for the selected service to its factory defaults. This erases any changes, including custom signatures. |

## 3.9.2 Management (Device)

Use this screen to manage sets of configuration files and signatures uploaded to Vantage CNM for the selected device. To open this screen, select the device, and click **Device** > **Signature Profile** > **Management**.

**Figure 40** Device > Signature Profile > Management (Device)



Device >> Signature Profile >> Management

Signature Profile Management

Backup & Restore | Management

Select Type

● IDP ○ Anti-Virus

Backup Configuration

| | Index | File Name | Description | Backed Up Date | Administrator |
|---|---|---|---|---|---|
| □ | 1 | Example | Example 7. | 2006-11-29 08:10:49 | root |

□ Select All

Delete

The following table describes the fields in this screen

**Table 20** Device > Signature Profile > Management (Device)

| TYPE | DESCRIPTION |
|---|---|
| Select Type | Select the service whose configuration and signatures you want to manage. |
| Backup Configuration | |
| Index | This displays the index number associated with the configuration files and signatures. |
| File Name | This displays the name associated with the configuration file and signatures. |
| Description | This displays a description that was entered at the time of backup. |

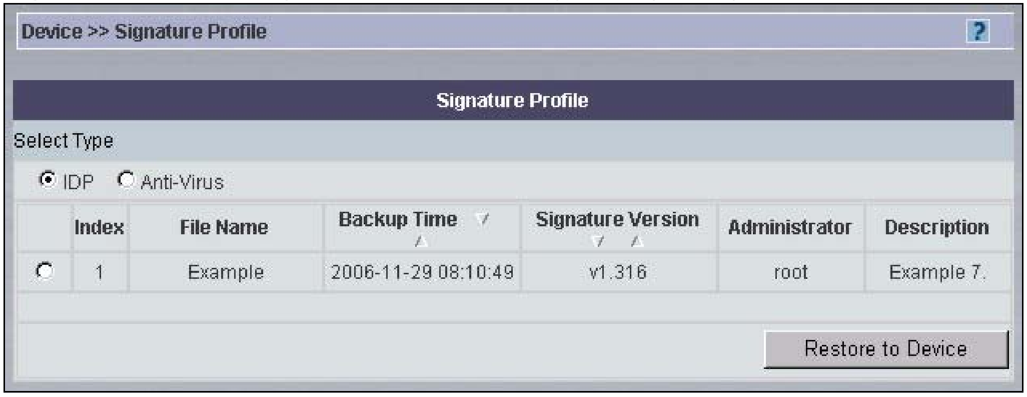
**Table 20** Device > Signature Profile > Management (Device) (continued)

| TYPE | DESCRIPTION |
|---|---|
| Backed Up Date | This field displays the date of backup. |
| Administrator | This field displays the administrator who performed the backup. |
| Select All | Select this to select all sets of configuration files and signatures. |
| Delete | Select the check box next to one or more sets of configuration files and signatures and click **Delete** to remove the selected set(s) from the Vantage CNM server. |

## 3.9.3 Management (Folder)

Use this screen to restore sets of configuration files and signatures uploaded to Vantage CNM to one or more devices in the selected folder. You can track the status and look at the results of this operation in the Group Operation Report. See Section 28.6 on page 327. To open this screen, select the folder, and click **Device > Signature Profile > Management**.

**Figure 41** Device > Signature Profile > Management (Folder)



Select Type

● IDP ○ Anti-Virus

| | Index | File Name | Backup Time | Signature Version | Administrator | Description |
|---|---|---|---|---|---|---|
| ○ | 1 | Example | 2006-11-29 08:10:49 | v1.316 | root | Example 7. |

The following table describes the fields in this screen

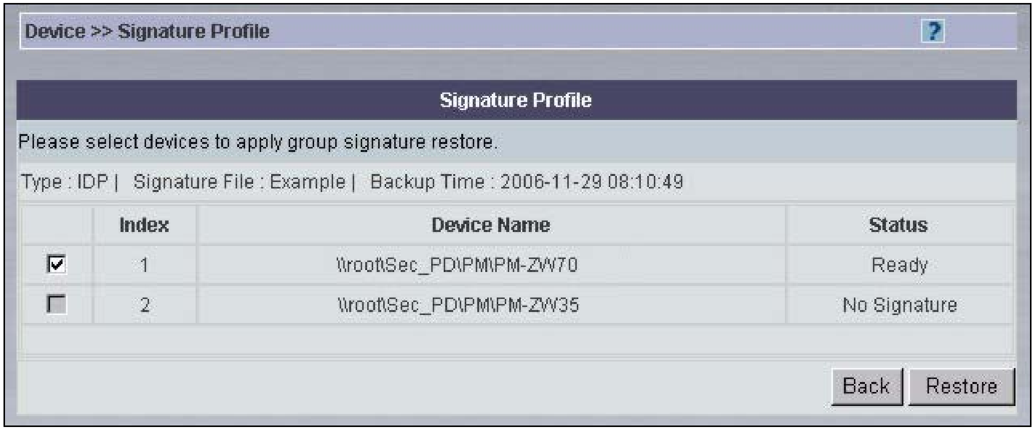
**Table 21** Device > Signature Profile > Management (Folder)

| TYPE | DESCRIPTION |
|---|---|
| Select Type | Select the service whose configuration and signatures you want to restore. |
| Index | This displays an index number associated with the configuration file and signatures. |
| File Name | This displays the name associated with the configuration file and signatures. |
| Backup Time | This field displays the date of backup of the configuration file and signatures. |
| Signature Version | This field displays the version of the signatures at the time the backup was created. |
| Administrator | This field displays the administrator who performed the backup of the configuration file. |
| Description | This displays a description that was entered at the time of file backup. |
| Restore to Device | Select the radio button of the configuration file and signatures you want to restore and click this to restore them to one or more devices in the selected folder. |

### 3.9.4 Restore (Folder)

Use this screen to restore sets of configuration files and signatures uploaded to Vantage CNM to one or more devices in the selected folder. You can track the status and look at the results of this operation in the Group Operation Report. See Section 28.6 on page 327. To open this screen, select the folder, click **Device** > **Signature Profile** > **Management**, select the configuration file and signatures you want to restore, and then click **Restore to Device**.

**Figure 42** Device > Signature Profile > Management > Restore to Device (Folder)



Please select devices to apply group signature restore.

Type : IDP | Signature File : Example | Backup Time : 2006-11-29 08:10:49

| | Index | Device Name | Status |
|---|---|---|---|
| ☑ | 1 | \\root\Sec_PD\PM\PM-ZW70 | Ready |
| □ | 2 | \\root\Sec_PD\PM\PM-ZW35 | No Signature |

The following table describes the fields in this screen

**Table 22** Device > Signature Profile > Management > Restore to Device (Folder)

| TYPE | DESCRIPTION |
|---|---|
| Type | This field displays the service whose configuration and signatures you want to restore. |
| Signature File | This field displays the name associated with the configuration file and signatures. |
| Backup Time | This field displays the date of backup of the configuration file and signatures. |
| Index | This field displays the index number associated with each device. |
| Device Name | This field displays the name of each device that is on in the folder. |
| Status | This field displays the status of the device with respect to the subscription service. |
| Back | Click this to return to the previous screen. |
| Restore | Select the check box next to one or more devices and click this to restore the specified configuration file and signatures to them. |

# PART III
# Configuration

The examples in this section use one of the most comprehensive examples of each screen, not every variation for each device type and firmware version. If you are unable to find a specific screen or field in this User's Guide, please see the User's Guide for the device for more information.

Configuration > X Auth  (259)

Configuration > DNS  (263)

Configuration > Remote MGMT  (271)

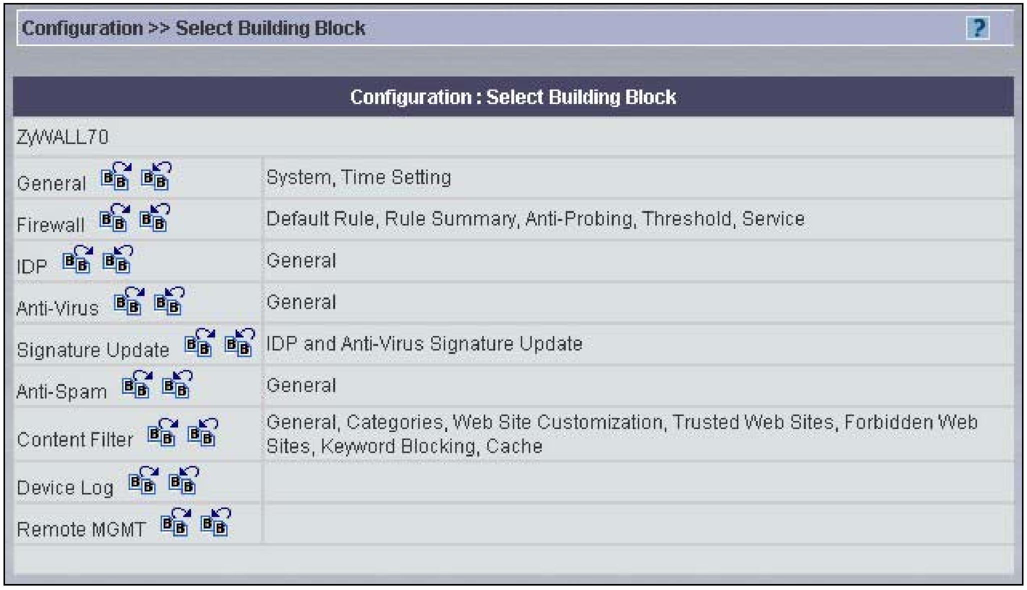
# 4

# Configuration > Select Building Block

## 4.1 Select Building Block

Use this menu item to load building blocks to the selected device or to create building blocks from the current configuration of the selected device. See Chapter 24 on page 277 for more information about building blocks. To open this menu item, select the device, and click **Configuration** > **Select Building Block**.

**Figure 43** Configuration > Select Building Block



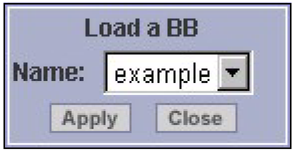
Configuration >> Select Building Block

| Configuration : Select Building Block | |
|---|---|
| ZyWALL70 | |
| General | System, Time Setting |
| Firewall | Default Rule, Rule Summary, Anti-Probing, Threshold, Service |
| IDP | General |
| Anti-Virus | General |
| Signature Update | IDP and Anti-Virus Signature Update |
| Anti-Spam | General |
| Content Filter | General, Categories, Web Site Customization, Trusted Web Sites, Forbidden Web Sites, Keyword Blocking, Cache |
| Device Log | |
| Remote MGMT | |

This screen displays the type of the selected device, each type of building block, and a summary of the information in each type of building block.

Click the **Load a BB** icon to load a building block to the selected device. The following pop-up screen appears.

**Figure 44** Configuration > Select Building Block > Load a BB



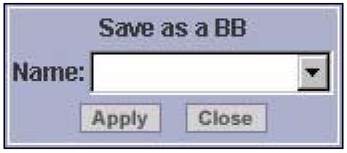
Load a BB

Name: example

Select the building block you want to load to the selected device, and click **Apply**.

Click the **Save as a BB** icon to save the current configuration of the selected device as a building block. The following pop-up screen appears.

**Figure 45** Configuration > Select Building Block > Save as a BB



Enter the name of the new building block, and click **Apply**. The name must be 1-32 alphanumeric characters or underscores (_). It cannot include spaces. The name is case-sensitive.

# 5

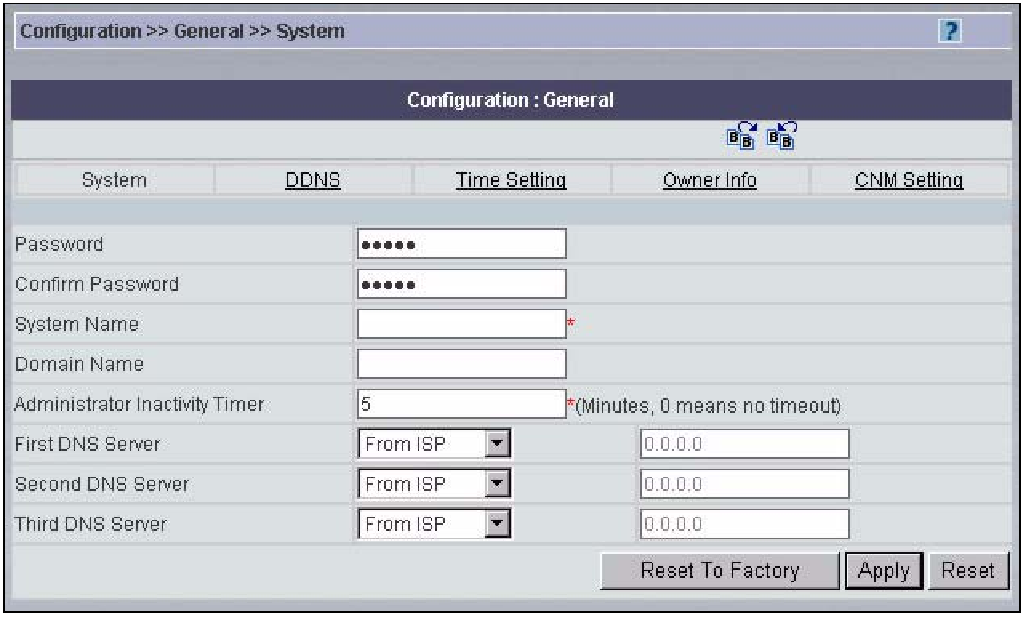
# Configuration > General

This section shows you how to configure the **General** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 5.1 System

Use this screen to set the password, system name, domain name, idle timeout, and DNS servers for the device. To open this screen, click **Configuration** > **General** > **System**.

**Figure 46** Configuration > General > System



Configuration >> General >> System

Configuration : General

| System | DDNS | Time Setting | Owner Info | CNM Setting |
|---|---|---|---|---|

| | | |
|---|---|---|
| Password | ●●●●● | |
| Confirm Password | ●●●●● | |
| System Name | * | |
| Domain Name | | |
| Administrator Inactivity Timer | 5 *(Minutes, 0 means no timeout) | |
| First DNS Server | From ISP | 0.0.0.0 |
| Second DNS Server | From ISP | 0.0.0.0 |
| Third DNS Server | From ISP | 0.0.0.0 |

The following table describes the fields in this screen.

**Table 23** Configuration > General > System

| FIELD | DESCRIPTION |
|---|---|
| Password | Enter the password used to access the device. |
| Confirm Password | Re-enter the password used to access the device. |
| User Password | Enter the user password used to access the device. |
| Confirm User Password | Re-enter the user password used to access the device. |

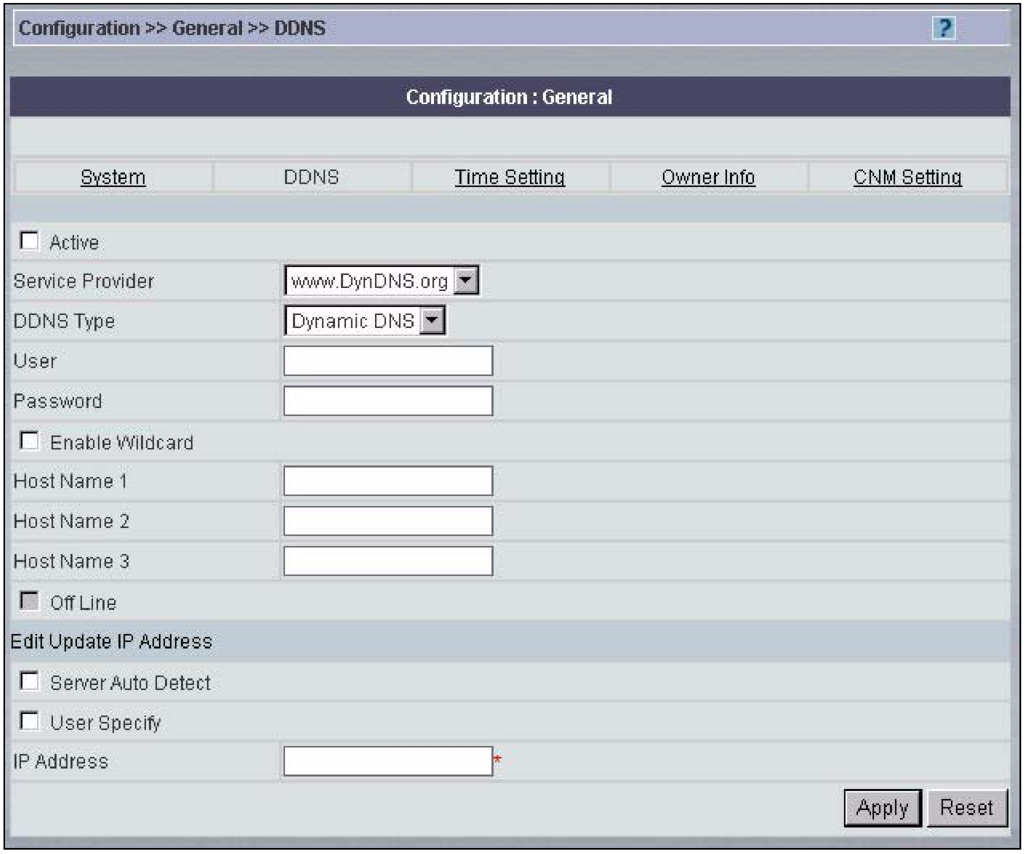
**Table 23** Configuration > General > System (continued)

| FIELD | DESCRIPTION |
|---|---|
| System Name | Enter a unique name here for the device for identification purposes. The device name cannot exceed 31 characters. |
| Domain Name | The Domain Name entry is what is propagated to the DHCP clients on the LAN side of the target device. If you leave this blank, the domain name obtained by the device via DHCP from the ISP is used. |
| Administrator Inactivity Timer | Set how long a management session can remain idle before it expires. After it expires, you have to log back into the device. |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. These DNS servers refer to the device system DNS server. The device uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the timeserver.<br>Select **From ISP** if the ISP dynamically assigns the device DNS server information. The text box to the right then displays the (read-only) DNS server IP address that the ISP assigns.<br>Select **User-Defined** if you want to assign the DNS server IP address yourself. Enter the DNS server's IP address in the field to the right.<br>Select **None** if you do not want to configure device system DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN and DDNS. |
| Reset to Factory | Click this button to upload the factory-default configuration file of the device. This resets every setting, not just the system settings in this screen, to its default value. |
| Apply | Click this to save your changes to the device. |
| Reset | Click this to begin configuring the screen afresh. |

## 5.2 DDNS

Use this screen to configure your Dynamic DNS (DDNS) on the device. To open this screen, click **Configuration** > **General** > **DDNS**.

**Figure 47** Configuration > General > DDNS



Service Provider: www.DynDNS.org

DDNS Type: Dynamic DNS

The following table describes the fields in this screen.

**Table 24** Configuration > General > DDNS

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to enable dynamic DNS. |
| Service Provider | Select the name of your Dynamic DNS service provider. |
| DDNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider. |
| User | Enter the user name for your Dynamic DNS account. |
| Password | Enter the password assigned to you. |
| Enable Wildcard | Select this to enable DYNDNS Wildcard. |
| Host Names 1~3 | Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (","). |
| Off Line | This option is available when **CustomDNS** is selected in the **DDNS Type field**. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| Edit Update IP Address: | |
| Server Auto Detect | Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option. |
| User Specify | Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address. |
| IP Address | Enter the IP address if you select the **User Specify** option. |

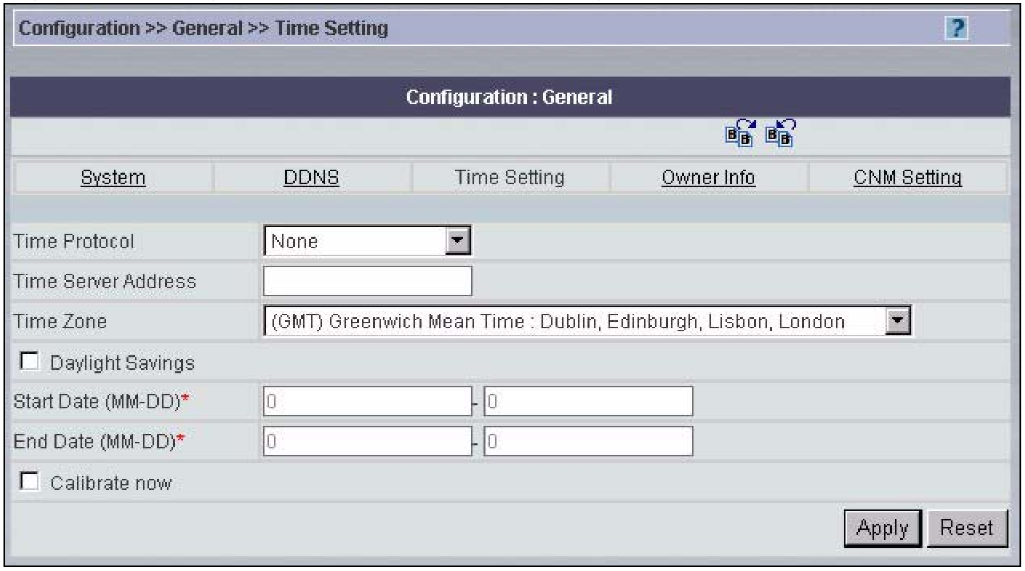
**Table 24** Configuration > General > DDNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| E-Mail (Prestige Only) | Type the e-mail address that you provided to your Dynamic DNS service provider. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.3 Time Setting

Use this screen to configure the time settings on the device. To open this screen, click **Configuration** > **General** > **Time Setting**.

**Figure 48** Configuration > General > Time Setting



Configuration >> General >> Time Setting

Configuration : General

| | |
|---|---|
| Time Protocol | None |
| Time Server Address | |
| Time Zone | (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London |
| □ Daylight Savings | |
| Start Date (MM-DD)* | 0 - 0 |
| End Date (MM-DD)* | 0 - 0 |
| □ Calibrate now | |

The following table describes the fields in this screen.

**Table 25** Configuration > General > Time Setting

| LABEL | DESCRIPTION |
|---|---|
| Time Protocol<br>(or Use Time Server when Bootup) | Select the time service protocol that your timeserver sends when you turn on the device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.<br>The main difference between them is the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC 1305),** is similar to Time (RFC 868).<br>Select **None** to enter the time and date manually. |
| Time Server Address | Enter the IP address or domain name of your timeserver. Check with your ISP/ network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw). |
| Time Zone | Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |

**Table 25** Configuration > General > Time Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Daylight Savings | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.<br>Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field.<br>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date | Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field.<br>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Calibrate now (Prestige only) | Select the check box to have your device use the specified timeserver to set its internal system clock. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

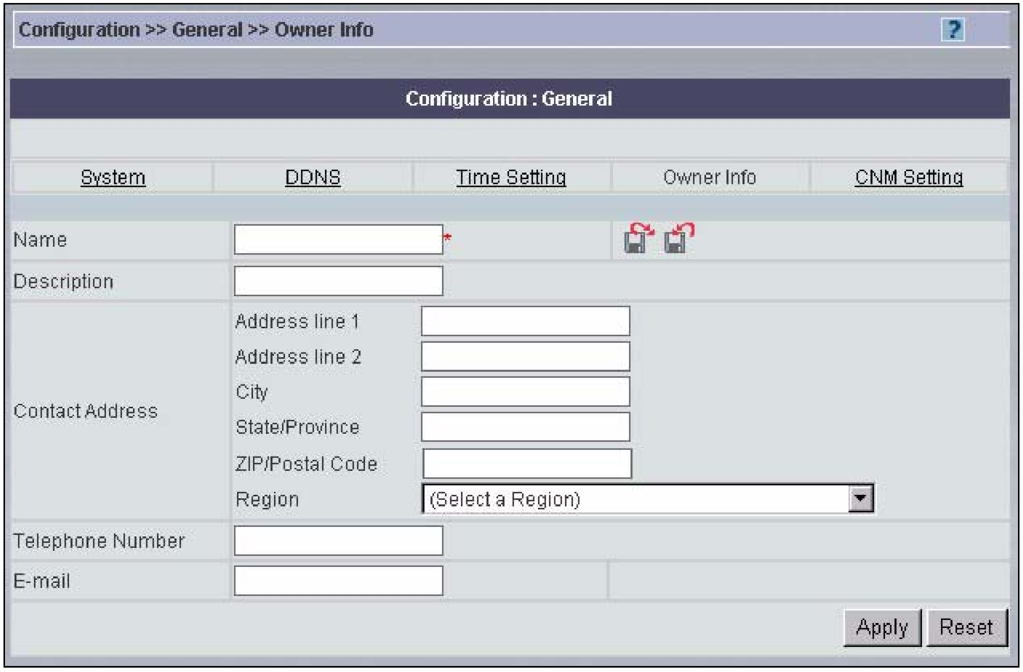
## 5.4 Owner Info

Use this screen to identify the owner of the device. The contact information is used when Vantage CNM sends notifications to the device owner, in addition to being available to other administrators. This information is stored in Vantage CNM, not on the device.

You can specify the information manually, or you can copy an entry from the **System > Address Book** screen (Section 26.5 on page 298). You can also use the information in this screen to create an entry in the **System > Address Book** screen.

To open this screen, click **Configuration > General > Owner Info**.

**Figure 49** Configuration > General > Owner Info



Configuration >> General >> Owner Info

Configuration : General

Name *

Description

Contact Address: Address line 1, Address line 2, City, State/Province, ZIP/Postal Code, Region (Select a Region)

Telephone Number

E-mail

The following table describes the fields in this screen.

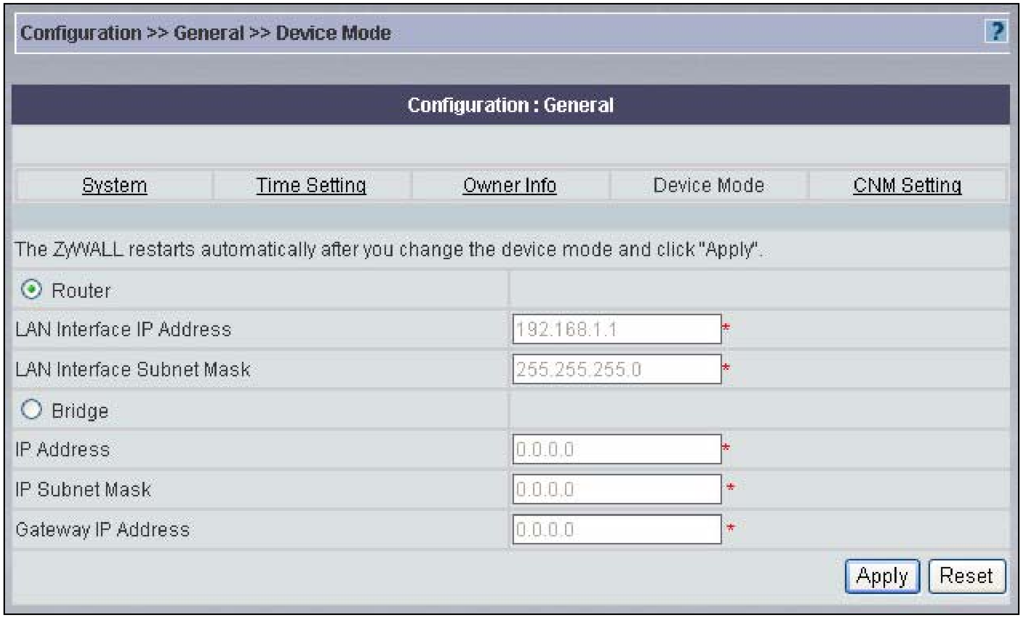
**Table 26** Configuration > General > Owner Info

| TYPE | DESCRIPTION |
|---|---|
| Name | Type the full name of the owner of this device. You must enter 1-30 printable ASCII characters, and spaces are allowed. |
| Description | Type some extra information about this customer. You can use up to 80 printable ASCII characters, and spaces are allowed. |
| Contact Address | Type the complete customer mailing address here. |
| Address line 1, 2 | Type the customer's building number, street and city zone (if applicable) here. |
| City | Type the full city or town name. |
| State/Province | Type the state or province. |
| ZIP/Postal Code | Type the zip or postal code here. |
| Region | Select the country or region from the list. |
| Telephone Number | Type the customer's telephone number including country code and area code here. |
| E-mail | Type the customer's e-mail address here. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.5 Device Mode

Use this screen to configure the device mode and basic settings for the device mode on the device. To open this screen, click **Configuration > General > Device Mode**.

**Figure 50** Configuration > General > Device Mode



Configuration >> General >> Device Mode

Configuration : General

The ZyWALL restarts automatically after you change the device mode and click "Apply".

● Router

LAN Interface IP Address: 192.168.1.1 *

LAN Interface Subnet Mask: 255.255.255.0 *

○ Bridge

IP Address: 0.0.0.0 *

IP Subnet Mask: 0.0.0.0 *

Gateway IP Address: 0.0.0.0 *

The following table describes the fields in this screen.

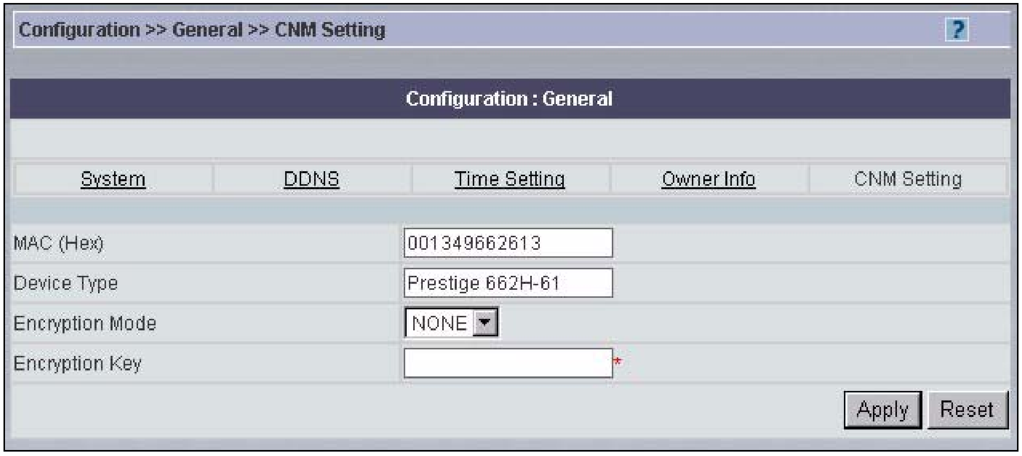
**Table 27** Configuration > General > Device Mode

| FIELD | DESCRIPTION |
|---|---|
| Router | Select this radio button, then click **Apply** to set the device to router mode. |
| LAN Interface IP Address | This field displays the IP address of the LAN port. |
| LAN Interface Subnet Mask | This field displays the subnet mask of the LAN port. |
| Bridge | Select this radio button and configure the following fields, then click **Apply** to set the device to bridge mode. |
| IP Address | Enter the IP address of your device in dotted decimal notation. |
| IP Subnet Mask | Enter the IP subnet mask of the device. |
| Gateway IP Address | Enter the gateway IP address. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 5.6 CNM Setting

Use this screen to configure the Vantage CNM settings on the device. To open this screen, click **Configuration > General > CNM Setting**.

**Figure 51** Configuration > General > CNM Setting



Configuration >> General >> CNM Setting

Configuration : General

| | |
|---|---|
| MAC (Hex) | 001349662613 |
| Device Type | Prestige 662H-61 |
| Encryption Mode | NONE |
| Encryption Key | * |

The following table describes the fields in this screen.

**Table 28** Configuration > General > CNM Setting

| FIELD | DESCRIPTION |
|---|---|
| MAC (Hex) | This field displays the LAN MAC address of the device. Vantage CNM uses the MAC address to identify the device. This is entered when you manually register the device. |
| Device Type | This field displays the device type selected in the object tree. |
| Encryption Mode | You may choose to encrypt traffic between the device and the Vantage CNM server here. Choose from **None** (no encryption), **DES** or **3DES**. The device must be set to the same encryption mode (and have the same encryption key) as the Vantage CNM server.<br>You do not need to add NAT or firewall rules when you encrypt this traffic.<br>To set the encryption mode on the device, do the following:<br>Go to CI mode (SMT 24.8 for devices with SMT menus)<br>Type '`CNM encrymode X`' where:<br>Value of X Encryption Mode<br>0 None<br>1 DES<br>2 3DES |
| Encryption Key | Type an eight-character alphanumeric (“0” to “9”, “a” to “z”) for **DES** encryption and a 24-character alphanumeric (“0” to “9”, “a” to “z”) for **3DES** encryption. To set the encryption key on the device, type '`CNM encrykey xxxxxxxxx`' where ‘`xxxxxxxxx’` is the hexadecimal secret key number you used in the Vantage CNM server. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 6

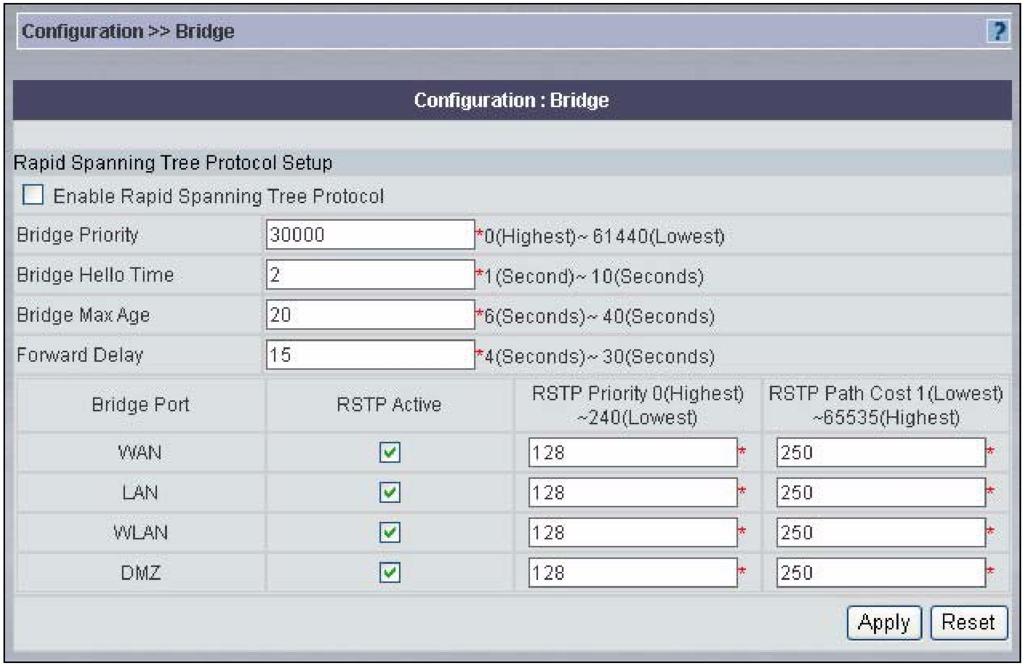
# Configuration > Bridge

The device must be in bridge mode to use this menu item.

## 6.1 Bridge

Use this screen to configure Rapid Spanning Tree Protocol (RSTP) on the device. You must be in bridge mode to use this screen. To open this screen, select the device, and click **Configuration** > **Bridge**.

**Figure 52** Configuration > Bridge



Configuration >> Bridge

Configuration : Bridge

Rapid Spanning Tree Protocol Setup

☐ Enable Rapid Spanning Tree Protocol

| | | |
|---|---|---|
| Bridge Priority | 30000 | *0(Highest)~ 61440(Lowest) |
| Bridge Hello Time | 2 | *1(Second)~ 10(Seconds) |
| Bridge Max Age | 20 | *6(Seconds)~ 40(Seconds) |
| Forward Delay | 15 | *4(Seconds)~ 30(Seconds) |

| Bridge Port | RSTP Active | RSTP Priority 0(Highest) ~240(Lowest) | RSTP Path Cost 1(Lowest) ~65535(Highest) |
|---|---|---|---|
| WAN | ☑ | 128 * | 250 * |
| LAN | ☑ | 128 * | 250 * |
| WLAN | ☑ | 128 * | 250 * |
| DMZ | ☑ | 128 * | 250 * |

The following table describes the fields in this screen.

**Table 29** Configuration > Bridge

| FIELD | DESCRIPTION |
|---|---|
| Enable Rapid Spanning Tree Protocol | Select this to activate RSTP on the device. |
| Bridge Priority | Enter a number between 0 and 61440 as bridge priority of the device.<br>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the root. If multiple devices have the lowest priority, the device with the lowest MAC address becomes the root.<br>The lower the numeric value you assign, the higher the priority for this bridge.<br>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forward Delay. |
| Bridge Hello Time | Enter the interval (between 1 and 10) in seconds that the root bridge waits before sending a hello packet. |
| Bridge Max Age | Enter the interval (between 6 and 40) in seconds that a bridge waits to get a Hello BPDU from the root bridge. |
| Forward Delay | Enter the length of time (between 4 and 30) in seconds that a bridge remains in the listening and learning port states. |
| Bridge Port | This field displays each port on the device. |
| RSTP Active | Select the check box to enable RSTP on the corresponding port. |
| RSTP Priority | Enter a number between 0 and 240 as RSTP priority for the corresponding port. Zero is the highest. |
| RSTP Path Cost | Enter a number between 1 and 65535 as RSTP path cost for the corresponding port. 65535 is the highest. |
| Apply | Click this to save your changes to the device. |
| Reset | Click this to begin configuring the screen afresh. |

# 7

# Configuration > LAN/WLAN/DMZ

This section shows you how to configure the **LAN**, **WLAN**, or **DMZ** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 7.1 LAN

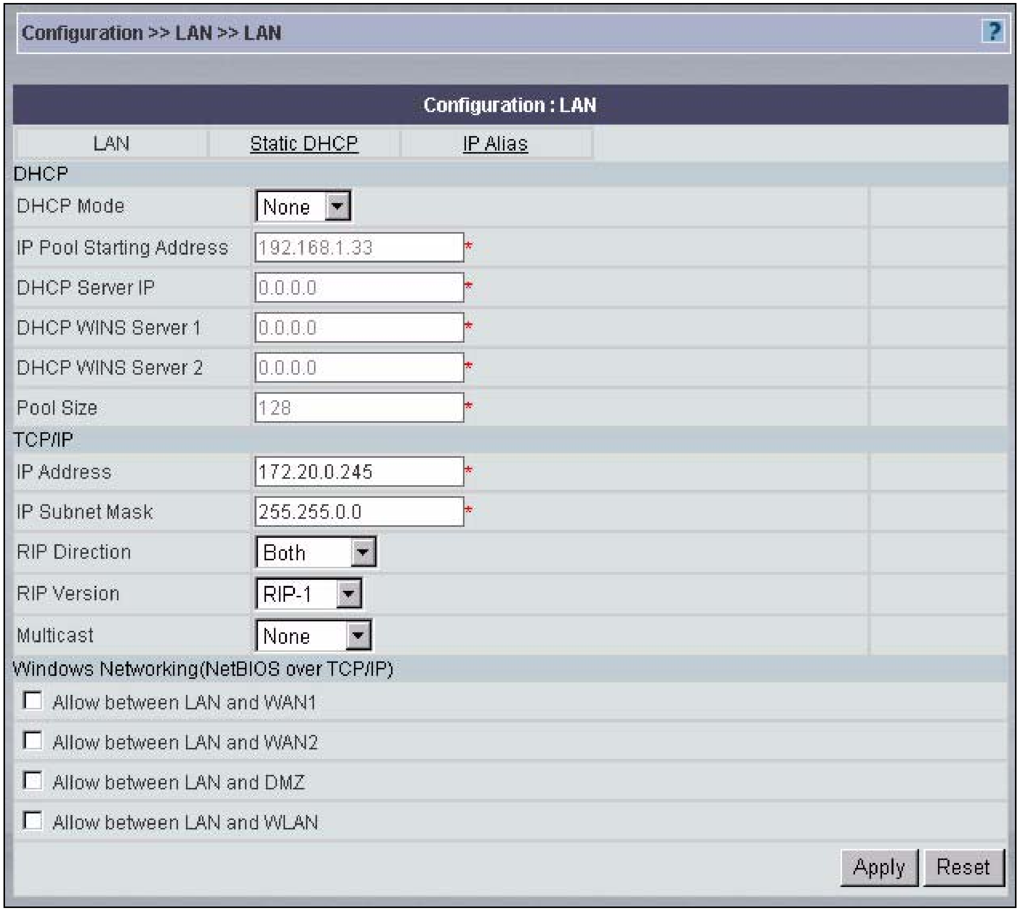
This screen is explained separately for ZyWALL and Prestige devices.

### 7.1.1 LAN (ZyWALL)

This section refers only to the LAN screen, but the information is applicable for the LAN, WLAN, and DMZ screens.

Use this screen to configure the DHCP settings, TCP/IP settings, and NetBIOS settings for the LAN on a ZyWALL. To open this screen, click **Configuration** > **LAN** > **LAN**.

**Figure 53** Configuration > LAN > LAN (ZyWALL)



Configuration >> LAN >> LAN

Configuration : LAN

DHCP

| | |
|---|---|
| DHCP Mode | None |
| IP Pool Starting Address | 192.168.1.33 * |
| DHCP Server IP | 0.0.0.0 * |
| DHCP WINS Server 1 | 0.0.0.0 * |
| DHCP WINS Server 2 | 0.0.0.0 * |
| Pool Size | 128 * |

TCP/IP

| | |
|---|---|
| IP Address | 172.20.0.245 * |
| IP Subnet Mask | 255.255.0.0 * |
| RIP Direction | Both |
| RIP Version | RIP-1 |
| Multicast | None |

Windows Networking(NetBIOS over TCP/IP)

□ Allow between LAN and WAN1

□ Allow between LAN and WAN2

□ Allow between LAN and DMZ

□ Allow between LAN and WLAN

The following table describes the fields in this screen.

**Table 30** Configuration > LAN > LAN (ZyWALL)

| LABEL | DESCRIPTION |
|---|---|
| DHCP Mode | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the device provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the device forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server IP** field.<br>Select **None** to stop the device from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| DHCP Server IP | Type the IP address of the DHCP server to which you want the device to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Pool Size | This field specifies the size, or count of the IP address pool. |

**Table 30** Configuration > LAN > LAN (ZyWALL) (continued)

| LABEL | DESCRIPTION |
|---|---|
| First DNS Server<br>Second DNS Server<br>Third DNS Server | These fields are enabled if the **DHCP Mode** is **Server**. Specify the DNS servers that are provided to DHCP clients.<br>Select **From ISP** if you want the device to use corresponding DNS server provided by the ISP.<br>Select **User-Defined** and specify the IP address if you want the device to use the specific DNS server.<br>Select **DNS Relay** if you want the device to |
| TCP/IP | |
| IP Address | Type the IP address of the device in dotted decimal notation. 192.168.1.1 is the factory default. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. The device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the device, which is 255.255.255.0. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**. |
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN. | |
| Allow between LAN and WAN1 | Select this check box to forward NetBIOS packets from the LAN to WAN port 1and from WAN port 1 to the LAN. If your firewall is enabled with the default policy set to block WAN port 1 to LAN traffic, you also need to enable the default WAN port 1 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to WAN port 1 and from WAN port 1 to the LAN. |
| Allow between LAN and WAN2 | Select this check box to forward NetBIOS packets from the LAN to WAN port 2 and from WAN port 2 to the LAN. If your firewall is enabled with the default policy set to block WAN port 2 to LAN traffic, you also need to enable the default WAN port 2 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to WAN port 2 and from WAN port 2 to the LAN. |

**Table 30** Configuration > LAN > LAN (ZyWALL) (continued)

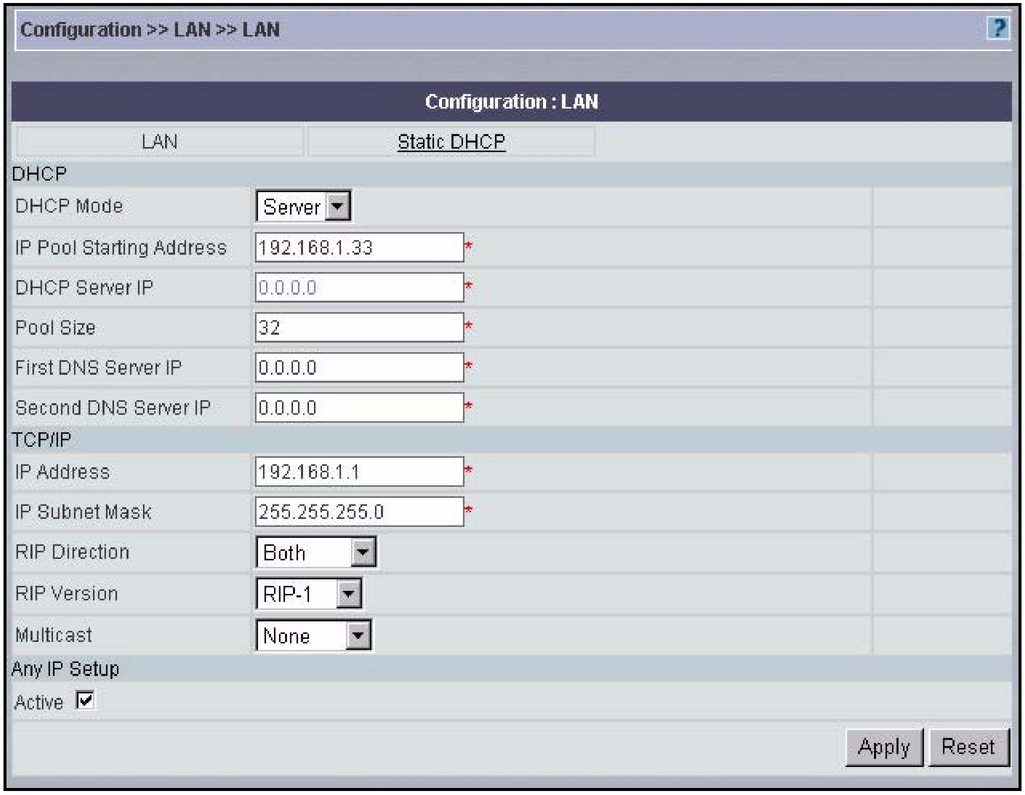
| LABEL | DESCRIPTION |
|---|---|
| Allow between LAN and DMZ | Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN. |
| Allow between LAN and WLAN | Select this check box to forward NetBIOS packets from the LAN to the WLAN and from the WLAN to the LAN.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.1.2 LAN (Prestige)

This section refers only to the LAN screen, but the information is applicable for the LAN, WLAN, and DMZ screens.

Use this screen to configure the DHCP settings, TCP/IP settings, and Any IP settings for the LAN port on a device. To open this screen, click **Configuration** > **LAN** > **LAN**.

**Figure 54** Configuration > LAN > LAN (Prestige)



Configuration >> LAN >> LAN

Configuration : LAN

LAN | Static DHCP

DHCP

| | |
|---|---|
| DHCP Mode | Server |
| IP Pool Starting Address | 192.168.1.33 * |
| DHCP Server IP | 0.0.0.0 * |
| Pool Size | 32 * |
| First DNS Server IP | 0.0.0.0 * |
| Second DNS Server IP | 0.0.0.0 * |

TCP/IP

| | |
|---|---|
| IP Address | 192.168.1.1 * |
| IP Subnet Mask | 255.255.255.0 * |
| RIP Direction | Both |
| RIP Version | RIP-1 |
| Multicast | None |

Any IP Setup

Active ☑

The following table describes the fields in this screen.

**Table 31** Configuration > LAN > LAN (Prestige)

| LABEL | DESCRIPTION |
|---|---|
| DHCP Mode | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server.<br>Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.<br>When configured as a **Server**, the device provides TCP/IP configuration for the clients. When set as a **Server**, fill in the rest of the DHCP setup fields.<br>Select **Relay** to have the device act as a DNS proxy. The device tells the DHCP clients on the LAN that the device itself is the DNS server. When a computer on the LAN sends a DNS query to the device, the device forwards the query to the device's system DNS server and relays the response back to the computer. You can select **Relay** and enter an IP Pool Starting Address. The **First DNS Server IP** and **Second DNS Server IP** will appear as read only fields. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| DHCP Server IP | If **Relay** is selected in the DHCP field above, then type the IP address of the actual, remote DHCP server here. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| First DNS Server IP<br>Second DNS Server IP | The device passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Type your First DNS Server IP and Second DNS Server IP addresses in these fields. |
| TCP/IP | |
| IP Address | Type the IP address of the device in dotted decimal notation. |

**Table 31** Configuration > LAN > LAN (Prestige) (continued)

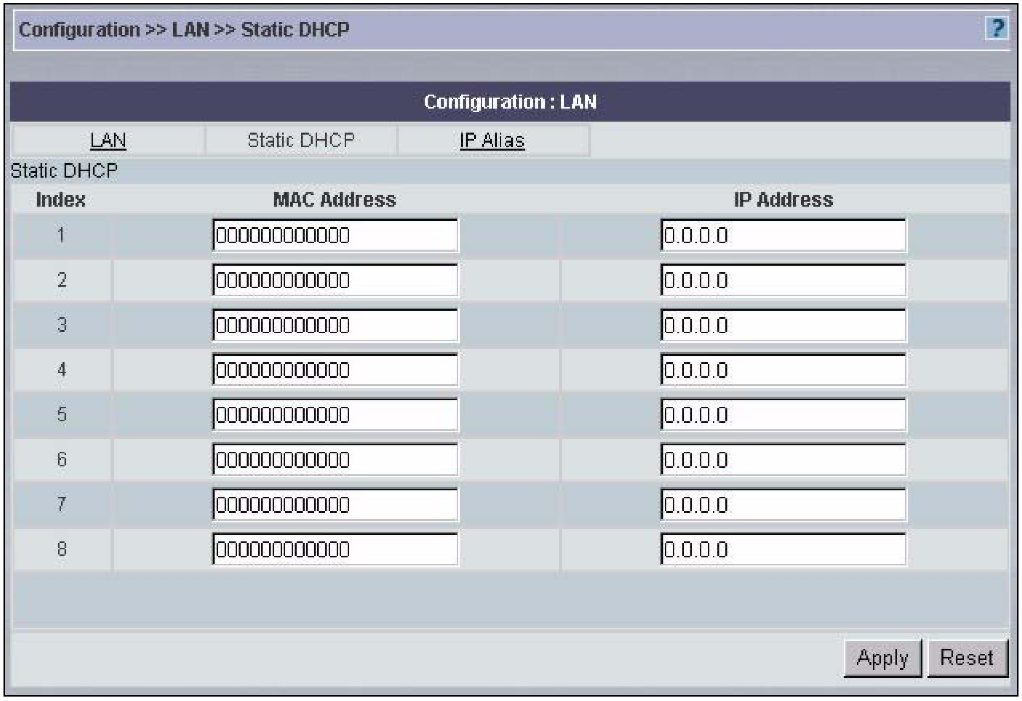
| LABEL | DESCRIPTION |
|---|---|
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Unless you are implementing subnetting, use the "natural" subnet mask, which is usually 255.255.255.0. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**. |
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interpretability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| Any IP Setup | |
| Active | Select this option to activate the Any-IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the device are not in the same subnet.<br>When you disable the Any-IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the device's LAN IP address can connect to the device or access the Internet through the device. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.2 Static DHCP

This section refers only to the LAN screen, but the information is applicable for the LAN, WLAN, and DMZ screens.

Use this screen to assign IP addresses to specific individual computers on the LAN based on their MAC addresses. To open this screen, click **Configuration > LAN > Static DHCP**.

**Figure 55** Configuration > LAN > Static DHCP



Configuration >> LAN >> Static DHCP

Configuration : LAN

Static DHCP

| Index | MAC Address | IP Address |
|---|---|---|
| 1 | 000000000000 | 0.0.0.0 |
| 2 | 000000000000 | 0.0.0.0 |
| 3 | 000000000000 | 0.0.0.0 |
| 4 | 000000000000 | 0.0.0.0 |
| 5 | 000000000000 | 0.0.0.0 |
| 6 | 000000000000 | 0.0.0.0 |
| 7 | 000000000000 | 0.0.0.0 |
| 8 | 000000000000 | 0.0.0.0 |

The following table describes the fields in this screen.

**Table 32** Configuration > LAN > Static DHCP

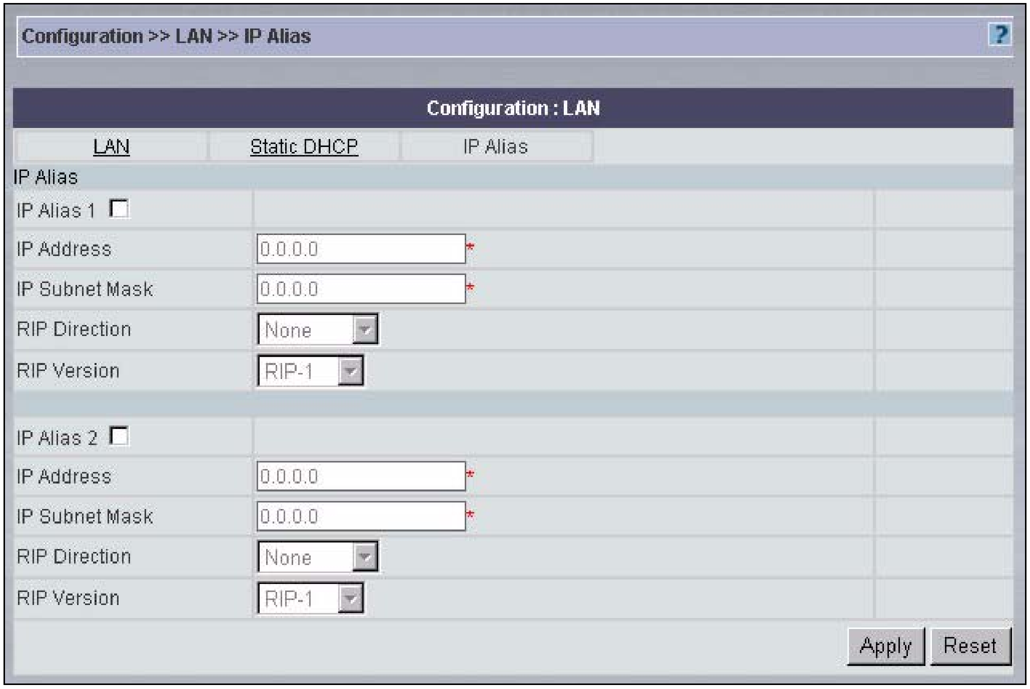
| LABEL | DESCRIPTION |
|---|---|
| Index | This is the index number of the Static IP table entry (row). |
| MAC Address | This is the MAC address of a computer on the device’s LAN. |
| IP Address | This is the IP address to be assigned to the device with the MAC address above. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.3 IP Alias

This section refers only to the LAN screen, but the information is applicable for the LAN, WLAN, and DMZ screens.

Use this screen to configure logical interfaces (subnets) via its single physical Ethernet interface with the device itself being the gateway for each network. You can also configure firewall rules to control access between the logical networks. To open this screen, click **Configuration > LAN > IP Alias**.

**Figure 56** Configuration > LAN > IP Alias



Configuration >> LAN >> IP Alias

Configuration : LAN

LAN | Static DHCP | IP Alias

IP Alias

| | |
|---|---|
| IP Alias 1 □ | |
| IP Address | 0.0.0.0 * |
| IP Subnet Mask | 0.0.0.0 * |
| RIP Direction | None |
| RIP Version | RIP-1 |
| IP Alias 2 □ | |
| IP Address | 0.0.0.0 * |
| IP Subnet Mask | 0.0.0.0 * |
| RIP Direction | None |
| RIP Version | RIP-1 |

The following table describes the fields in this screen

**Table 33** Configuration > LAN > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| IP Alias 1,2 | Select the check box to configure another network for the device. |
| IP Address | Enter the IP address of the device in dotted decimal notation. |
| IP Subnet Mask | The device automatically calculates the subnet mask based how many aliases you select. See also the appendices for more information on IP subnetting. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 8

# Configuration > Wireless Card

This section shows you how to configure the **Wireless Card** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

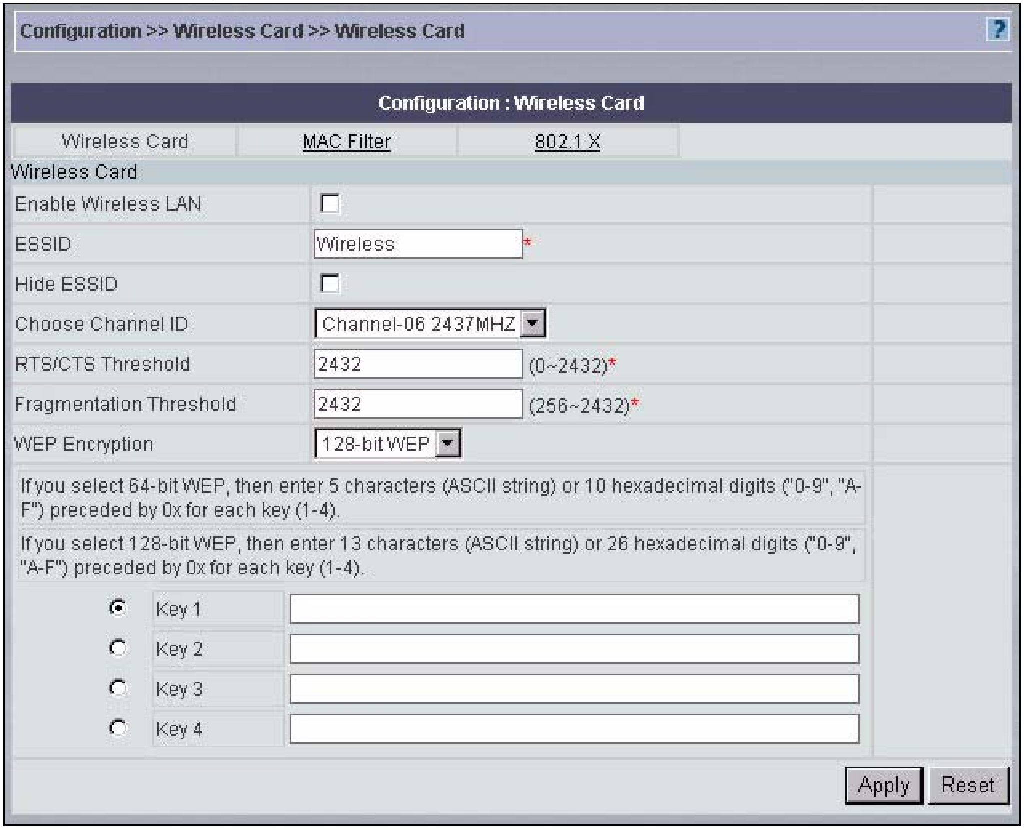
## 8.1 Wireless

This screen depends on the device type and firmware version.

### 8.1.1 Basic Wireless Settings and WEP Encryption

Use this screen to configure basic wireless settings and WEP encryption. To open this screen, click **Configuration > Wireless Card > Wireless Card**.

**Figure 57** Configuration > Wireless Card > Wireless Card (Basic Settings and WEP)



Configuration >> Wireless Card >> Wireless Card

Configuration : Wireless Card

Wireless Card

| | |
|---|---|
| Enable Wireless LAN | □ |
| ESSID | Wireless * |
| Hide ESSID | □ |
| Choose Channel ID | Channel-06 2437MHZ |
| RTS/CTS Threshold | 2432 (0~2432)* |
| Fragmentation Threshold | 2432 (256~2432)* |
| WEP Encryption | 128-bit WEP |

If you select 64-bit WEP, then enter 5 characters (ASCII string) or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4).

If you select 128-bit WEP, then enter 13 characters (ASCII string) or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4).

| | | |
|---|---|---|
| ● | Key 1 | |
| ○ | Key 2 | |
| ○ | Key 3 | |
| ○ | Key 4 | |

The following table describes the fields in this screen.

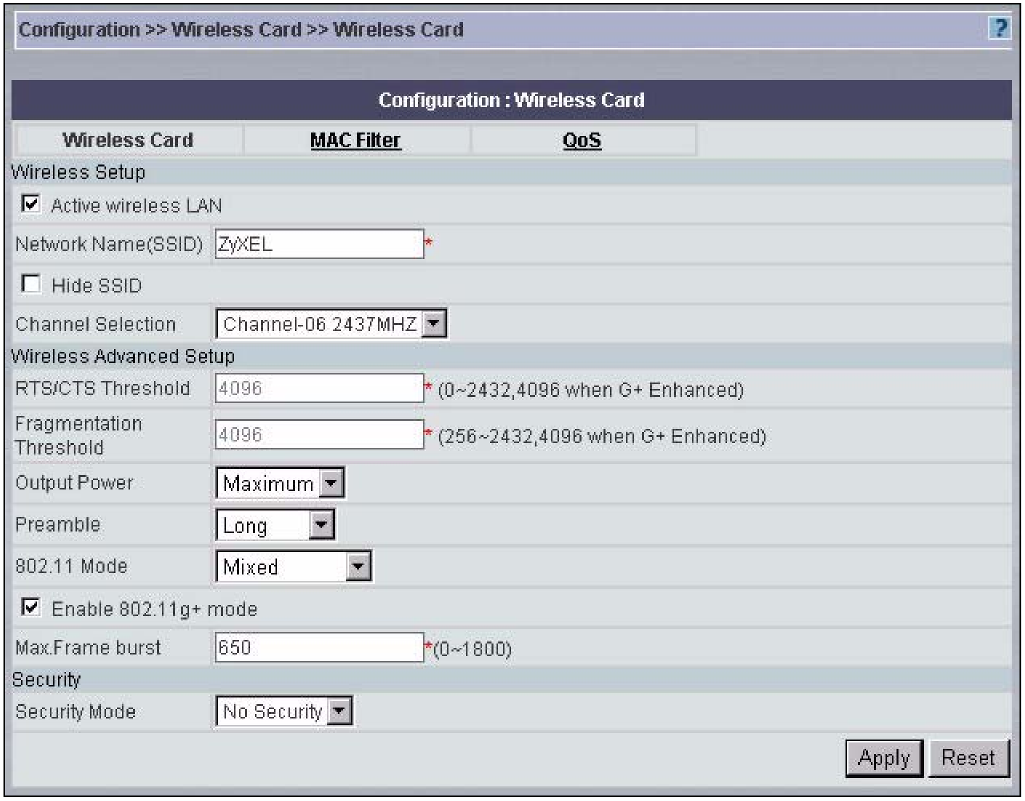
**Table 34** Configuration > Wireless Card > Wireless Card (Basic Settings and WEP)

| LABEL | DESCRIPTION |
|---|---|
| Enable Wireless LAN | You should configure some wireless security when you enable the wireless LAN. Select the check box to enable the wireless LAN. |
| ESSID | The ESSID (Extended Service Set IDentification) is a unique name to identify the device in the wireless LAN. Wireless stations associating to the device must have the same ESSID.<br>Enter a descriptive name of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive). |
| Hide ESSID | Select **Yes** to hide the ESSID in so a station cannot obtain the ESSID through AP scanning.<br>Select **No** to make the ESSID visible so a station can obtain the ESSID through AP scanning. |
| Choose Channel ID | The radio frequency used by IEEE 802.11a, b or g wireless devices is called a channel. Select a channel from the drop-down list box. |
| RTS/CTS Threshold | The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS.<br>Select the check box to change the default value and enter a new value between 0 and 2432. |
| Fragmentation Threshold | This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.<br>Select the check box to change the default value and enter a value between 256 and 2432. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select Disable to allow wireless clients to communicate with the access points without any data encryption.<br>Select **64-bit WEP**, **128-bit WEP**, or **256-bit WEP** (options vary) to enable data encryption. Select **None** to disable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **256-bit WEP** in the **WEP Encryption** field, then enter 29 characters (ASCII string) or 58 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.1.2 Advanced Wireless Settings and Wireless Security

Use this screen to configure wireless settings and wireless security. To open this screen, click **Configuration > Wireless Card > Wireless Card**.

**Figure 58** Configuration > Wireless Card > Wireless Card (Advanced Settings and Security)


Configuration >> Wireless Card >> Wireless Card
?
Configuration : Wireless Card
Wireless Card
MAC Filter
QoS
Apply
Reset

Wireless Setup

☑ Active wireless LAN

Network Name(SSID) ZyXEL *

☐ Hide SSID

Channel Selection Channel-06 2437MHZ

Wireless Advanced Setup

RTS/CTS Threshold 4096 * (0~2432,4096 when G+ Enhanced)

Fragmentation Threshold 4096 * (256~2432,4096 when G+ Enhanced)

Output Power Maximum

Preamble Long

802.11 Mode Mixed

☑ Enable 802.11g+ mode

Max.Frame burst 650 *(0~1800)

Security

Security Mode No Security

The following table describes the fields in this screen.

**Table 35** Configuration > Wireless Card > Wireless Card (Advanced Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| Wireless Setup | |
| Active Wireless LAN | You should configure some wireless security when you enable the wireless LAN. Select the check box to enable the wireless LAN. |
| Network Name(SSID) | The SSID (Service Set IDentification) is a unique name to identify the device in the wireless LAN. Wireless stations associating to the device must have the same SSID.<br>Enter a descriptive name of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive). |
| Hide SSID | Select **Yes** to hide the SSID so a station cannot obtain the SSID through AP scanning.<br>Select **No** to make the SSID visible so a station can obtain the SSID through AP scanning. |
| Channel Selection | The radio frequency used by IEEE 802.11a, b or g wireless devices is called a channel. Select a channel from the drop-down list box. |
| Wireless Advanced Setup | |

**Table 35** Configuration > Wireless Card > Wireless Card (Advanced Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| RTS/CTS Threshold | This field is enabled when **Enable 802.11g+ mode** is not selected.<br>In a wireless network which covers a large area, wireless clients are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.<br>By setting this value lower than the default value, the wireless clients must sometimes get permission to send information to the AP. The lower the value, the more often the wireless clients must get permission.<br>If this value is greater than the fragmentation threshold value (see below), then wireless clients never have to get permission to send information to the AP. |
| Fragmentation Threshold | This field is enabled when **Enable 802.11g+ mode** is not selected.<br>A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy. |
| Output Power | Specify how much output power the device should use to send wireless traffic. |
| Preamble | Select the preamble the device should use.<br>A preamble affects the timing in your wireless network. There are two preamble modes: long and short. Most wireless clients can detect the AP's preamble automatically. However, if a wireless client tries to use a different preamble mode than the AP does, it cannot communicate with the AP. |
| 802.11 Mode | Specify whether the wireless network uses **802.11b only**, **802.11g only**, or both 802.11b and 802.11g (**Mixed**). |
| Enable 802.11g+ mode | Select this to activate 802.11g+ mode, which may provide increased throughput and range. The wireless clients have to support this feature, and this feature might interfere with other wireless networks. |
| Max. Frame burst | Set this to any non-zero value to improve the performance of pure IEEE 802.11g and mixed IEEE 802.11b/g networks. In pure IEEE 802.11g networks, set this to the maximum value. In mixed networks, the higher the value, the higher the priority of IEEE 802.11g traffic. |
| Security | This section depends on the type of **Security** selected. |
| Security | Select one of the security settings.<br>Select **No Security** to allow wireless stations to communicate with the access points without any data encryption. Otherwise, select the security you need and see the following sections for more information. |
|  | These fields are displayed if the **Security** is **Static WEP**. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select Disable to allow wireless clients to communicate with the access points without any data encryption.<br>Select **64-bit WEP**, **128-bit WEP**, or **256-bit WEP** (options vary) to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **256-bit WEP** in the **WEP Encryption** field, then enter 29 characters (ASCII string) or 58 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers. |

**Table 35** Configuration > Wireless Card > Wireless Card (Advanced Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| | These fields are displayed if the **Security** is **WPA-PSK** or **WPA2-PSK**. |
| WPA Compatible | This field is only displayed if the **Security** is **WPA2-PSK**. Select this if you want the device to support WPA-PSK and WPA2-PSK. Otherwise, the device only supports WPA2-PSK. |
| Pre-Shared Key | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Group Key Update Timer | This is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. |
| | These fields are displayed if the **Security** is **WPA** or **WPA2**. |
| WPA Compatible | This field is only displayed if the **Security** is **WPA2**. Select this if you want the device to support WPA and WPA2. Otherwise, the device only supports WPA2. |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>The reauthentication timer on the RADIUS server has priority. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| WPA Group Key Update Timer | This is the rate at which the RADIUS server sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. |
| Authentication Server | |
| IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port Number | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the device.<br>The key is not sent over the network. This key must be the same on the external authentication server and device. |

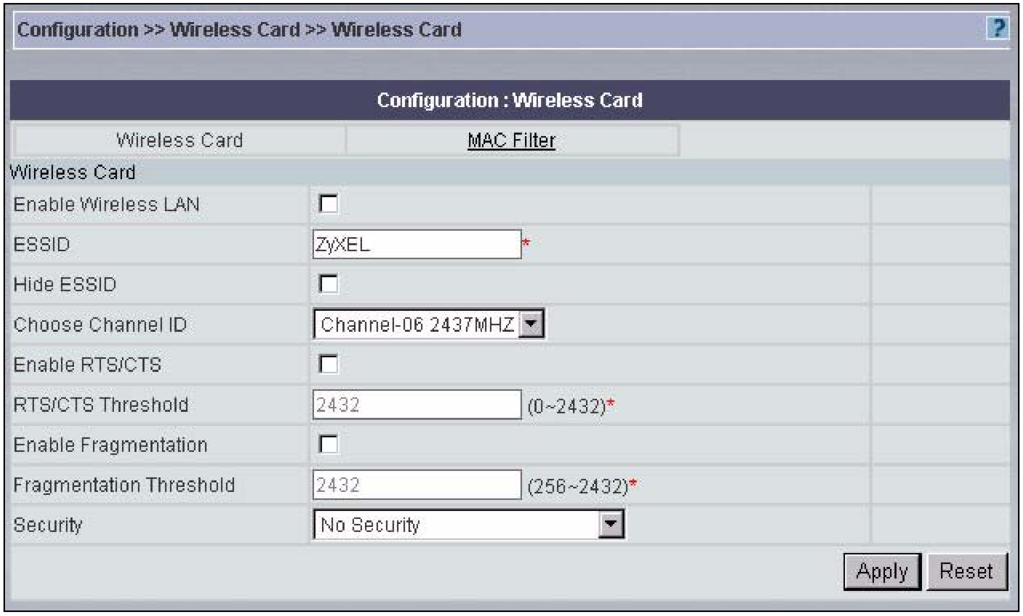
**Table 35** Configuration > Wireless Card > Wireless Card (Advanced Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| Accounting Server | |
| IP Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port Number | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the device.<br>The key is not sent over the network. This key must be the same on the external accounting server and device. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.1.3 Basic Wireless Settings and Wireless Security

Use this screen to configure basic wireless settings and wireless security. To open this screen, click **Configuration** > **Wireless Card** > **Wireless Card**.

**Figure 59** Configuration > Wireless Card > Wireless Card (Basic Settings and Security)



Configuration >> Wireless Card >> Wireless Card

Configuration : Wireless Card

Wireless Card

| | |
|---|---|
| Enable Wireless LAN | □ |
| ESSID | ZyXEL * |
| Hide ESSID | □ |
| Choose Channel ID | Channel-06 2437MHZ |
| Enable RTS/CTS | □ |
| RTS/CTS Threshold | 2432 (0~2432)* |
| Enable Fragmentation | □ |
| Fragmentation Threshold | 2432 (256~2432)* |
| Security | No Security |

The following table describes the fields in this screen.

**Table 36** Configuration > Wireless Card > Wireless Card (Basic Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| Enable Wireless LAN | You should configure some wireless security when you enable the wireless LAN. Select the check box to enable the wireless LAN. |
| ESSID | The ESSID (Extended Service Set IDentification) is a unique name to identify the device in the wireless LAN. Wireless stations associating to the device must have the same ESSID.<br>Enter a descriptive name of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive). |

**Table 36** Configuration > Wireless Card > Wireless Card (Basic Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| Hide ESSID | Select **Yes** to hide the ESSID in so a station cannot obtain the ESSID through AP scanning.<br>Select **No** to make the ESSID visible so a station can obtain the ESSID through AP scanning. |
| Choose Channel ID | The radio frequency used by IEEE 802.11a, b or g wireless devices is called a channel. Select a channel from the drop-down list box. |
| Enable RTS/ CTS | Select the check box to change the default value and enter a new value between **0** and **2432** in the next field. |
| RTS/CTS Threshold | The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS.<br>Select the check box to change the default value and enter a new value between 0 and 2432. |
| Enable Fragmentation | Select the check box to change the default value and enter a value between 256 and 2432 in the next field. |
| Fragmentation Threshold | This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.<br>Select the check box to change the default value and enter a value between 256 and 2432. |
| Security | This section depends on the type of **Security** selected. |
| Security | Select one of the security settings.<br>Select **No Security** to allow wireless stations to communicate with the access points without any data encryption. Otherwise, select the security you need and see the following sections for more information.<br>Select **No Access 802.1x + No WEP** to block wireless stations from accessing the device and to not use any data encryption. |
|  | These fields are displayed if the **Security** is **Static WEP** or **No Access 802.1x + Static WEP**. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select Disable to allow wireless clients to communicate with the access points without any data encryption.<br>Select **64-bit WEP**, **128-bit WEP**, or **256-bit WEP** (options vary) to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **256-bit WEP** in the **WEP Encryption** field, then enter 29 characters (ASCII string) or 58 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers. |
|  | These fields are displayed if the **Security** is **WPA-PSK**. |
| Pre-Shared Key | Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |

**Table 36** Configuration > Wireless Card > Wireless Card (Basic Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Group Key Update Timer | This is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. |
| | These fields are displayed if the **Security** is **WPA**. |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>The reauthentication timer on the RADIUS server has priority. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Authentication Databases | Click this to edit the settings for the local user database or RADIUS server. |
| WPA Group Key Update Timer | This is the rate at which the RADIUS server sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. |
| | These fields are displayed if the **Security** is **802.1x + Dynamic WEP**. |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>The reauthentication timer on the RADIUS server has priority. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Authentication Databases | Click this to edit the settings for the local user database or RADIUS server. |

**Table 36** Configuration > Wireless Card > Wireless Card (Basic Settings and Security)

| LABEL | DESCRIPTION |
|---|---|
| Dynamic WEP Key Exchange | Select **64-bit WEP**, **128-bit WEP**, or **256-bit WEP** (options vary) to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates. |
| | These fields are displayed if the **Security** is **802.1x + Static WEP**. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select Disable to allow wireless clients to communicate with the access points without any data encryption.<br>Select **64-bit WEP**, **128-bit WEP**, or **256-bit WEP** (options vary) to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **256-bit WEP** in the **WEP Encryption** field, then enter 29 characters (ASCII string) or 58 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers. |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>The reauthentication timer on the RADIUS server has priority. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Authentication Databases | Click this to edit the settings for the local user database or RADIUS server. |
| | These fields are displayed if the **Security** is **802.1x + No WEP**. |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>The reauthentication timer on the RADIUS server has priority. |
| Idle Timeout | The device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |

**Table 36** Configuration > Wireless Card > Wireless Card (Basic Settings and Security)

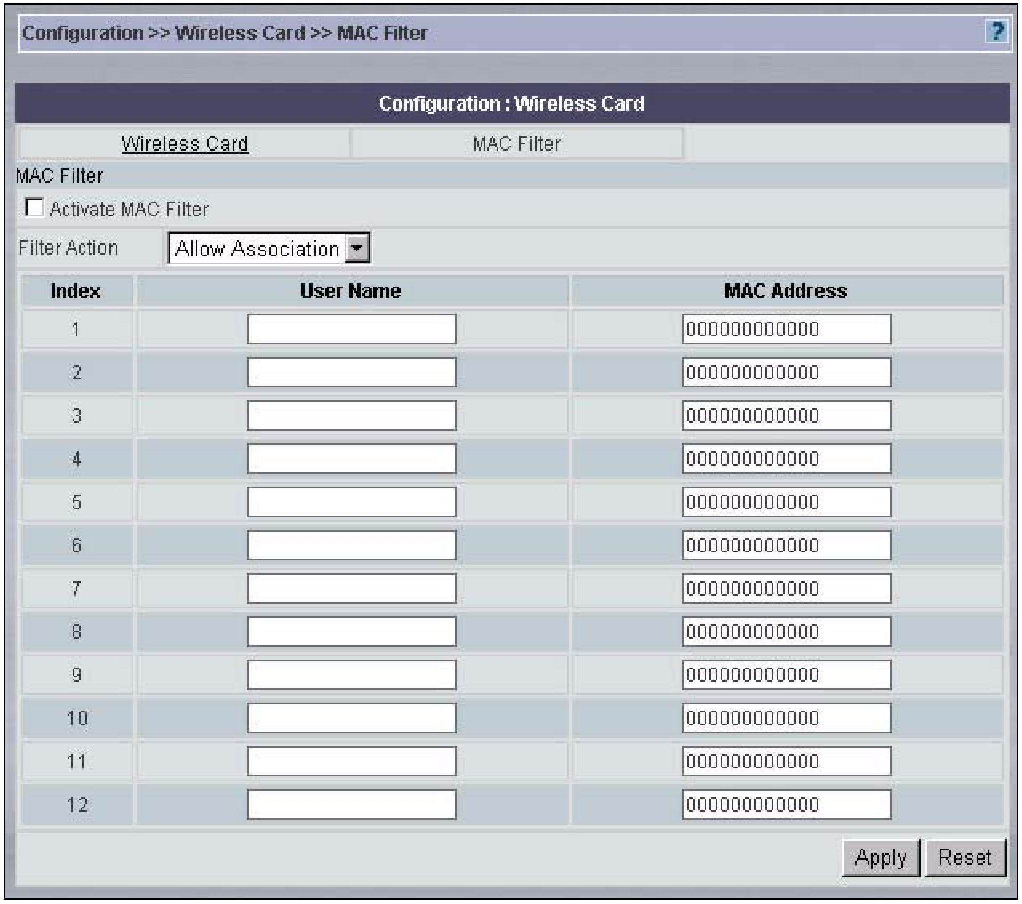
| LABEL | DESCRIPTION |
|---|---|
| Authentication Databases | Click this to edit the settings for the local user database or RADIUS server. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.2 MAC Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen. To change your device's MAC filter settings, select a device and then click **Configuration > Wireless Card** > **MAC Filter**. The screen appears as shown.

✍ Be careful not to list your computer's MAC address and set the **Action** field to **Deny Association** when managing the device via a wireless connection. This would lock you out.

**Figure 60** Configuration > Wireless Card > MAC Filter



Configuration >> Wireless Card >> MAC Filter
?
Configuration : Wireless Card
Wireless Card
MAC Filter
Apply
Reset

MAC Filter

□ Activate MAC Filter

Filter Action: Allow Association

| Index | User Name | MAC Address |
|---|---|---|
| 1 | | 000000000000 |
| 2 | | 000000000000 |
| 3 | | 000000000000 |
| 4 | | 000000000000 |
| 5 | | 000000000000 |
| 6 | | 000000000000 |
| 7 | | 000000000000 |
| 8 | | 000000000000 |
| 9 | | 000000000000 |
| 10 | | 000000000000 |
| 11 | | 000000000000 |
| 12 | | 000000000000 |

The following table describes the fields in this screen.

**Table 37** Configuration > Wireless Card > MAC Filter

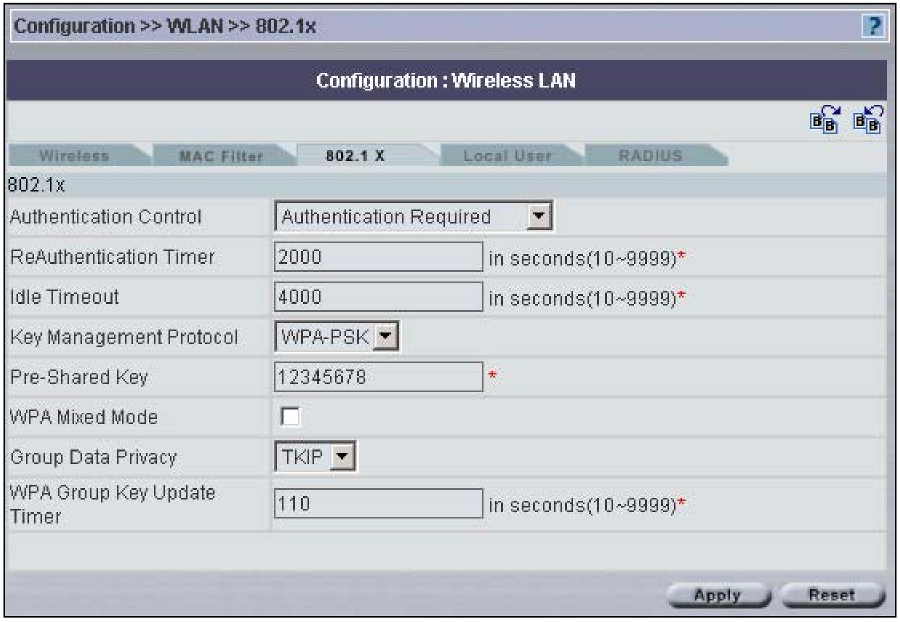
| LABEL | DESCRIPTION |
|---|---|
| Activate MAC Filter | Select this to enable MAC address filtering. |
| Filter Action | Define the filter action for the list of MAC addresses in the **MAC Address** table.<br>Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the device. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the device. |
| Index | This is the index number of the MAC address. |
| User Name | Enter a descriptive name for the MAC address. |
| MAC Address | Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc of the wireless stations that are allowed or denied access to the device in these address fields. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.3 802.1x

Use this screen to set up IEEE 802.1x, WPA, or WPA-PSK security on the device. To open this screen, click **Configuration** > **Wireless Card** > **802.1x**.

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the device for authentication.

**Figure 61** Configuration > Wireless Card > 802.1x



802.1x

| | | |
|---|---|---|
| Authentication Control | Authentication Required | |
| ReAuthentication Timer | 2000 | in seconds(10~9999)* |
| Idle Timeout | 4000 | in seconds(10~9999)* |
| Key Management Protocol | WPA-PSK | |
| Pre-Shared Key | 12345678 | * |
| WPA Mixed Mode | □ | |
| Group Data Privacy | TKIP | |
| WPA Group Key Update Timer | 110 | in seconds(10~9999)* |

The following table describes the labels in this screen.

**Table 38** Configuration > Wireless Card > 802.1x

| LABEL | DESCRIPTION |
|---|---|
| Authentication Control | To control wireless station access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**.<br>The following fields are only available when you select **Authentication Required**. |
| ReAuthentication Timer (in Seconds) | Specify how often wireless stations have to resend usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field.<br>Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes).<br>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |

**Table 38** Configuration > Wireless Card > 802.1x (continued)

| LABEL | DESCRIPTION |
|---|---|
| Idle Timeout<br>(in Seconds) | The device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again.<br>This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour). |
| Key Management Protocol | Choose the type of security you want to use. You can choose **802.1x**, **WPA**, or **WPA-PSK**. |
| | The following fields are available if the **Key Management Protocol** is **802.1x**. |
| Dynamic WEP Key Exchange | This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used.<br>Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.<br>Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to enable data encryption.<br>Up to 32 stations can access the device when you configure dynamic WEP key exchange.<br>This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**. |
| Authentication Databases | The authentication database contains wireless station login information. The local user database is the built-in database on the device. The RADIUS is an external server. Use this drop-down list box to select which database the device should use (first) to authenticate a wireless station.<br>Before you specify the priority, make sure you have set up the corresponding database correctly first.<br>Select **Local User Database Only** to have the device just check the built-in user database on the device for a wireless station's username and password.<br>Select **RADIUS Only** to have the device just check the user database on the specified RADIUS server for a wireless station's username and password.<br>Select **Local first, then RADIUS** to have the device first check the user database on the device for a wireless station's username and password. If the user name is not found, the device then checks the user database on the specified RADIUS server.<br>Select **RADIUS first, then Local** to have the device first check the user database on the specified RADIUS server for a wireless station's username and password. If the device cannot reach the RADIUS server, the device then checks the local user database on the device. When the user name is not found or password does not match in the RADIUS server, the device will not check the local user database and the authentication fails. |
| | The following fields are available if the **Key Management Protocol** is **WPA**. |
| WPA Mixed Mode | The device can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same WiFi network.<br>Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the **Group Data Privacy** field. |

**Table 38** Configuration > Wireless Card > 802.1x (continued)

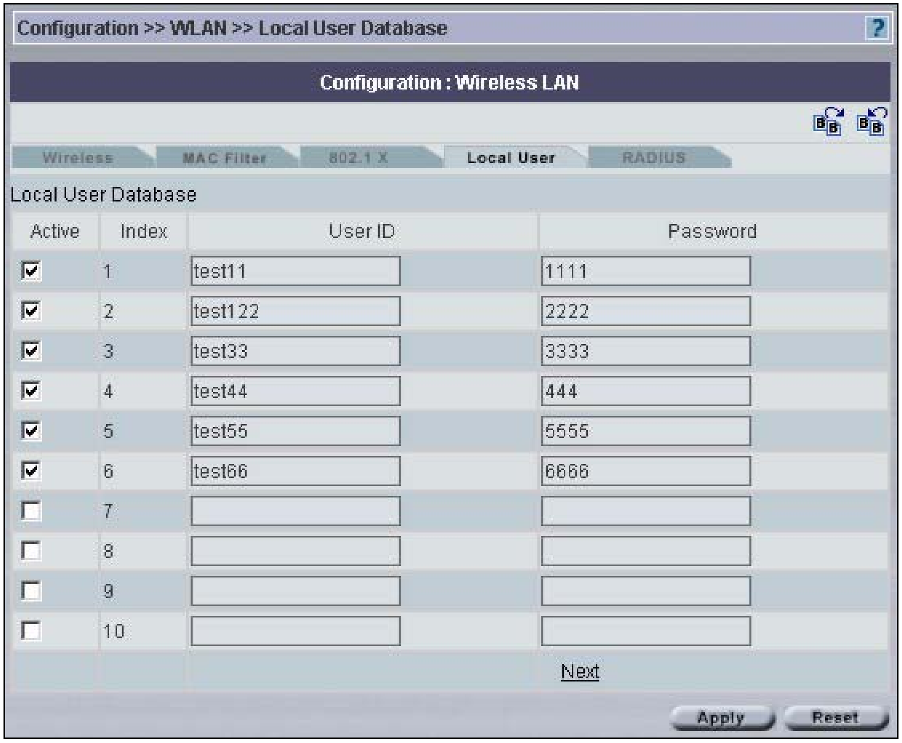
| LABEL | DESCRIPTION |
|---|---|
| Group Data Privacy | **Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**.<br>All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected. |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The device default is 1800 seconds (30 minutes). |
| Authentication Databases | When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database Only** with **802.1x Key Management Protocol**. |
| | The following fields are available if the **Key Management Protocol** is **WPA-PSK**. |
| Pre-Shared Key | The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials.<br>Type a pre-shared key from 8 to 63 printable characters (including spaces; alphabetic characters are case-sensitive). |
| WPA Mixed Mode | The device can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same WiFi network.<br>Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the **Group Data Privacy** field. |
| Group Data Privacy | **Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**.<br>All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected. |
| WPA Group Key Update Timer | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The device default is 1800 seconds (30 minutes). |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.4 Local User

By storing user profiles locally, your device is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

Select a device and then click **Configuration > Wireless Card** > **Local User**. The screen appears as shown next.

**Figure 62** Configuration > Wireless Card > Local User



Configuration >> WLAN >> Local User Database

Configuration : Wireless LAN

Local User Database

| Active | Index | User ID | Password |
|---|---|---|---|
| ☑ | 1 | test11 | 1111 |
| ☑ | 2 | test122 | 2222 |
| ☑ | 3 | test33 | 3333 |
| ☑ | 4 | test44 | 444 |
| ☑ | 5 | test55 | 5555 |
| ☑ | 6 | test66 | 6666 |
| ☐ | 7 | | |
| ☐ | 8 | | |
| ☐ | 9 | | |
| ☐ | 10 | | |

The following table describes the labels in this screen.

**Table 39** Configuration > Wireless Card > Local User

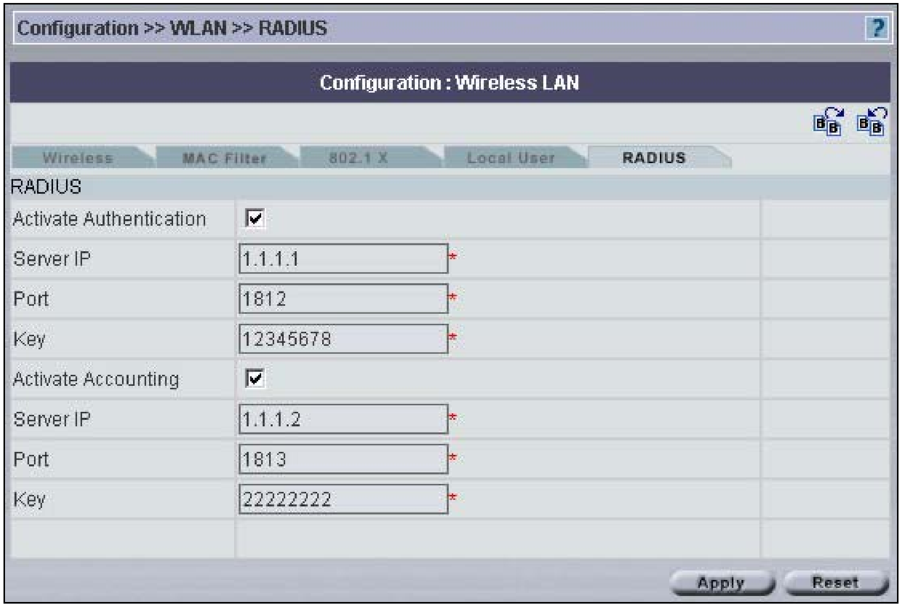
| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to enable the user profile. |
| Index | This is the local user index number. |
| User ID | Enter the user name of the user profile. |
| Password | Enter a password up to 31 characters long for this user profile. |
| Next | Select Next to view the next page of **Local User Database** entries. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.5 RADIUS

Use this screen if you want to use an external server to perform authentication.

Select a device, then click **Configuration > Wireless Card** > **RADIUS**. The screen appears as shown next.

**Figure 63** Configuration > Wireless Card > RADIUS



RADIUS

| | |
|---|---|
| Activate Authentication | ☑ |
| Server IP | 1.1.1.1 * |
| Port | 1812 * |
| Key | 12345678 * |
| Activate Accounting | ☑ |
| Server IP | 1.1.1.2 * |
| Port | 1813 * |
| Key | 22222222 * |

The following table describes the fields in this screen.

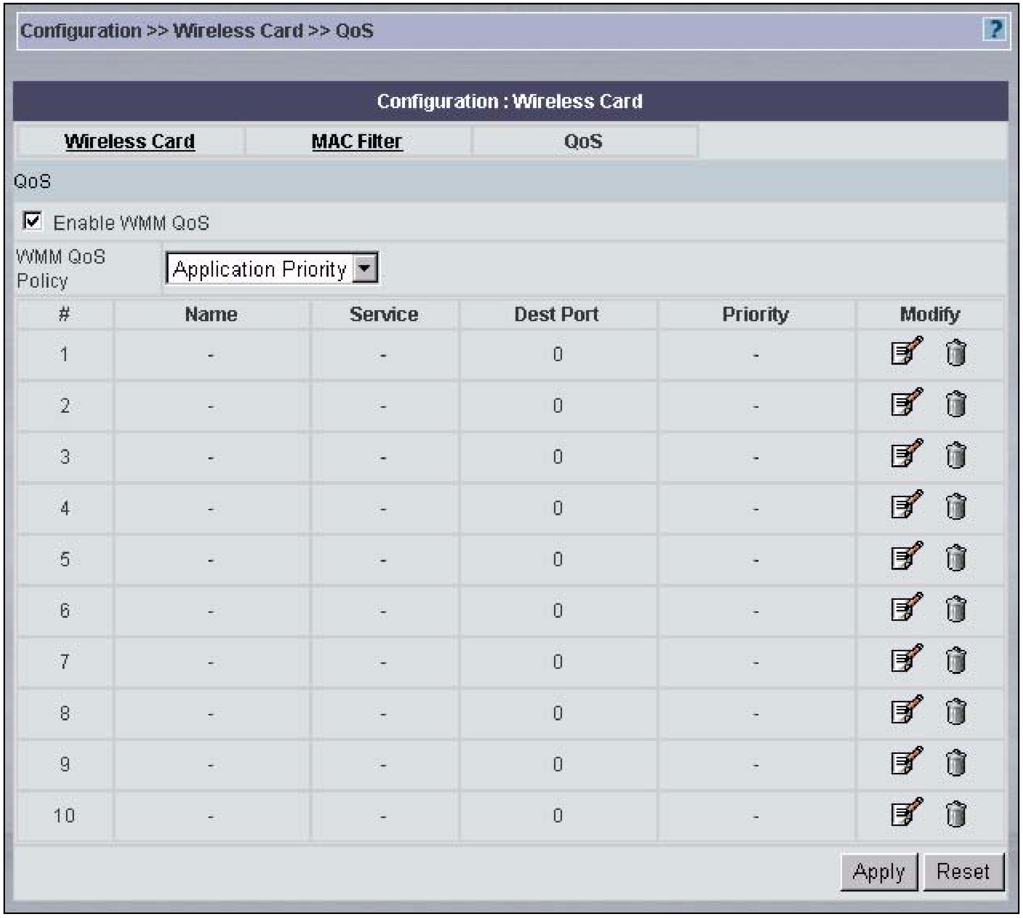
**Table 40** Configuration > Wireless Card > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Activate Authentication | Enable this feature to have the device use an external authentication server in performing user authentication.<br>Disable this feature if you will not use an external authentication server. If you disable this feature, you can still set the device to perform user authentication using the local user database. |
| Server IP | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points.<br>The key is not sent over the network. This key must be the same on the external authentication server and device. |
| Activate Accounting | Enable this feature to do user accounting through an external authentication server. |
| Server IP | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points.<br>The key is not sent over the network. This key must be the same on the external accounting server and device. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.6 QoS

Use this screen to enable and configure WiFi MultiMedia (WMM) Quality of Service (QoS) on the device. To open this screen, click **Configuration > Wireless Card > QoS**.

**Figure 64** Configuration > Wireless Card > QoS


Configuration >> Wireless Card >> QoS
?
Configuration : Wireless Card
Wireless Card
MAC Filter
QoS
QoS
Apply
Reset

☑ Enable WMM QoS

WMM QoS Policy: Application Priority

| # | Name | Service | Dest Port | Priority | Modify |
|---|---|---|---|---|---|
| 1 | - | - | 0 | - | ✎ 🗑 |
| 2 | - | - | 0 | - | ✎ 🗑 |
| 3 | - | - | 0 | - | ✎ 🗑 |
| 4 | - | - | 0 | - | ✎ 🗑 |
| 5 | - | - | 0 | - | ✎ 🗑 |
| 6 | - | - | 0 | - | ✎ 🗑 |
| 7 | - | - | 0 | - | ✎ 🗑 |
| 8 | - | - | 0 | - | ✎ 🗑 |
| 9 | - | - | 0 | - | ✎ 🗑 |
| 10 | - | - | 0 | - | ✎ 🗑 |

The following table describes the fields in this screen.

**Table 41** Configuration > Wireless Card > QoS

| LABEL | DESCRIPTION |
|---|---|
| Enable WMM QoS | Select this to enable WMM QoS on the device. |
| WMM QoS Policy | This field is enabled if **Enable WMM QoS** is selected.<br>Select **Default** to have the device automatically give a service a priority level according to the ToS value in the IP header of packets it sends.<br>Select **Application Priority** to display a list of application names, services, ports, and priorities to which you want to apply WMM QoS. |
| # | This field displays the number of an individual application entry. |
| Name | This field displays a description of an application entry. |
| Service | This field displays **FTP**, **WWW**, or **E-mail**, if the entry applies to this kind of traffic, or **User Defined** if you want to apply the entry to a different service, defined by the port number in **Dest Port**. |
| Dest Port | This field displays the destination port number used to identify traffic that follows this rule. |

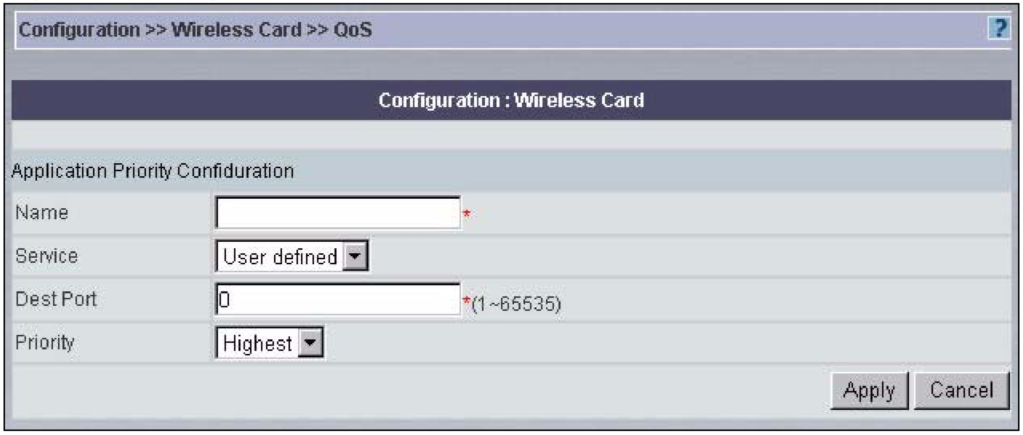
**Table 41** Configuration > Wireless Card > QoS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Priority | This field displays the WMM QoS priority assigned to traffic that follows this rule. |
| Modify | Click the **Edit** icon to edit the rule. Click the **Delete** icon to clear the rule. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.6.1 Edit QoS Rule

Use this screen to configure a WMM QoS rule. To open this screen, click **Configuration > Wireless Card > QoS > Edit**.

**Figure 65** Configuration > Wireless Card > QoS > Edit



Configuration >> Wireless Card >> QoS

Configuration : Wireless Card

Application Priority Confiduration

| | |
|---|---|
| Name | * |
| Service | User defined |
| Dest Port | 0 *(1~65535) |
| Priority | Highest |

The following table describes the fields in this screen.

**Table 42** Configuration > Wireless Card > QoS > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Type a description for this entry. |
| Service | Select **FTP**, **WWW**, or **E-mail**, if the entry applies to this kind of traffic, or **User Defined** if you want to apply the entry to a different service, defined by the port number in **Dest Port**. |
| Dest Port | This field displays the port number for the selected service, or you can type a port number for **User Defined** entries. |
| Priority | Select the ToS priority for the specified traffic.<br>**Highest**: Typically used for voice or video that is especially sensitive to jitter (variations in delay). Use this to reduce latency for improved quality.<br>**High**: Typically used for video that has some tolerance for jitter but needs to be prioritized over other data traffic.<br>**Mid**: Typically used for applications or devices that lack QoS capabilities. It is also used for traffic that is less sensitive to latency but is affected by long delays, such as web surfing.<br>**Low**: Typically used for non-critical “background” traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click this to return to the previous screen without saving any changes. |

# 9

# Configuration > WAN

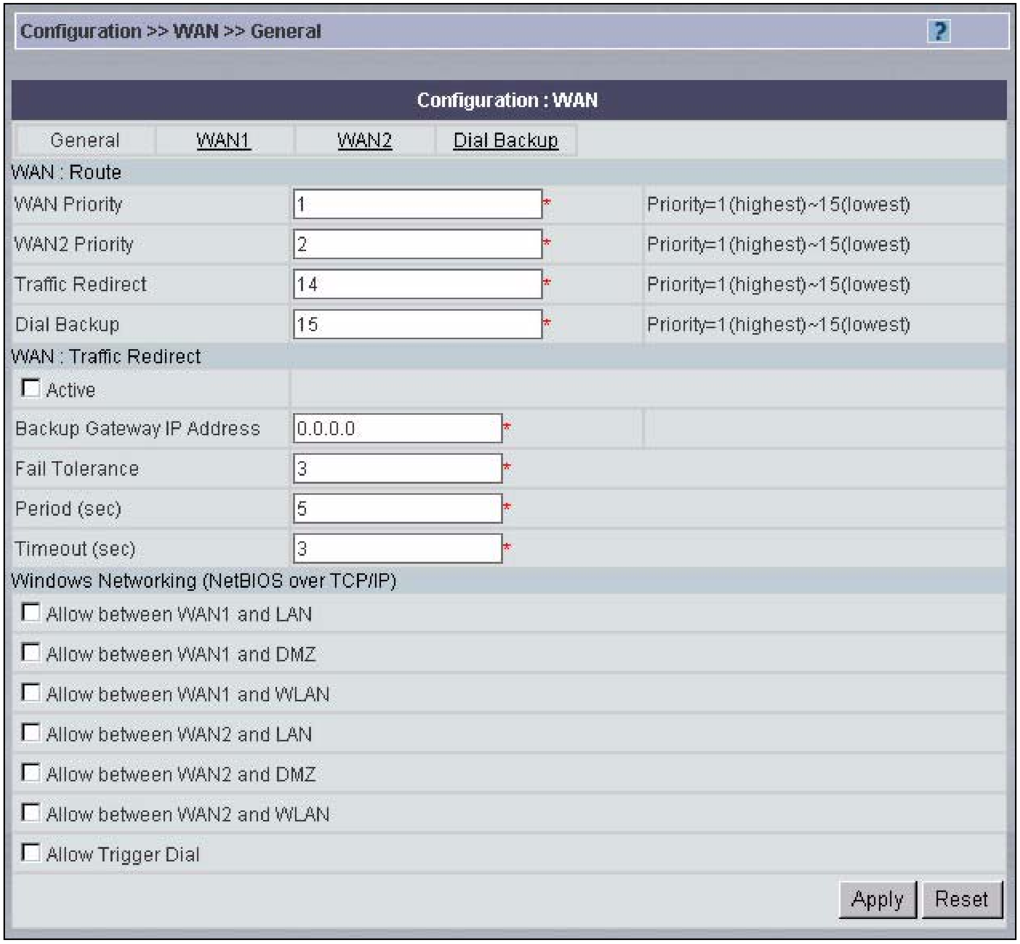
This section shows you how to configure the **WAN** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

✍ Be careful when configuring a device's WAN as an incorrect configuration could result in the device being inaccessible from Vantage CNM (or by the web configurator from the WAN) and may necessitate a site visit to correct.

## 9.1 General WAN – ZyWALL

This section gives configuration information on the fields displayed in this screen.

**Figure 66** Configuration > WAN > General – ZyWALL



Configuration >> WAN >> General

Configuration : WAN

General | WAN1 | WAN2 | Dial Backup

WAN : Route

| | | |
|---|---|---|
| WAN Priority | 1 * | Priority=1(highest)~15(lowest) |
| WAN2 Priority | 2 * | Priority=1(highest)~15(lowest) |
| Traffic Redirect | 14 * | Priority=1(highest)~15(lowest) |
| Dial Backup | 15 * | Priority=1(highest)~15(lowest) |

WAN : Traffic Redirect

□ Active

| | |
|---|---|
| Backup Gateway IP Address | 0.0.0.0 * |
| Fail Tolerance | 3 * |
| Period (sec) | 5 * |
| Timeout (sec) | 3 * |

Windows Networking (NetBIOS over TCP/IP)

□ Allow between WAN1 and LAN

□ Allow between WAN1 and DMZ

□ Allow between WAN1 and WLAN

□ Allow between WAN2 and LAN

□ Allow between WAN2 and DMZ

□ Allow between WAN2 and WLAN

□ Allow Trigger Dial

The following table describes the fields in this screen.

**Table 43** Configuration > WAN > General – ZyWALL

| LABEL | DESCRIPTION |
|---|---|
| WAN<br>WAN2<br>Traffic Redirect<br>Dial Backup | The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup** (dial backup does not apply to all device models):<br>You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15"). |
| Active | Select this check box to have the device use traffic redirect if the normal WAN connection goes down. |
| Backup Gateway IP Address | Type the IP address of your backup gateway in dotted decimal notation. The device automatically forwards traffic to this IP address if the device's Internet connection terminates. |
| Check WAN IP Address | Type the IP address the device should check to see if the gateway is still up. |
| Fail Tolerance | Type the number of times the device may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. |

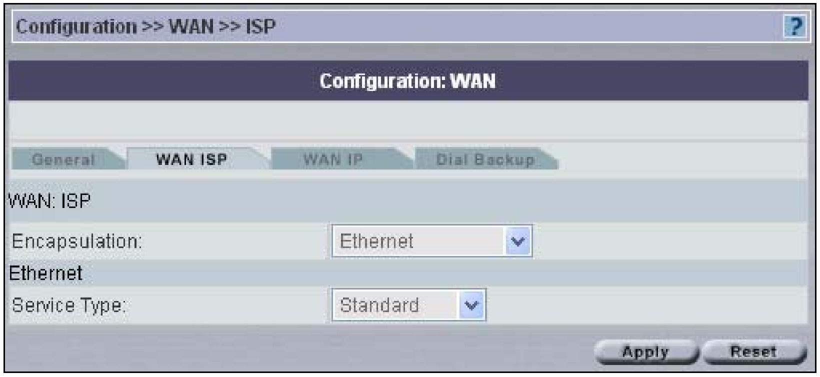
**Table 43** Configuration > WAN > General – ZyWALL (continued)

| LABEL | DESCRIPTION |
|---|---|
| Period (sec) | Type the number of seconds for the device to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic. |
| Timeout (sec) | Type the number of seconds for the device to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered "down" after the device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested. |
| Windows Networking (NetBIOS over TCP/IP): | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. |
| Allow between WAN1 and LAN | Select this check box to forward NetBIOS packets from the WAN1 port to the LAN port and from the LAN port to WAN1. If your firewall is enabled with the default policy set to block WAN port 1 to LAN traffic, you also need to enable the default WAN1 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the WAN1 port to the LAN port and from LAN port to WAN1. |
| Allow between WAN1 and DMZ | Select this check box to forward NetBIOS packets from the WAN1 port to the DMZ port and from the DMZ port to WAN1.<br>Clear this check box to block all NetBIOS packets going from the WAN1 port to the DMZ port and from DMZ port to WAN1. |
| Allow between WAN1 and WLAN | Select this check box to forward NetBIOS packets from the WAN1 port to the WLAN port and from the WLAN port to WAN1.<br>Clear this check box to block all NetBIOS packets going from the WAN1 port to the WLAN port and from WLAN port to WAN1. |
| Allow between WAN2 and LAN | Select this check box to forward NetBIOS packets from the WAN2 port to the LAN port and from the LAN port to WAN2. If your firewall is enabled with the default policy set to block WAN port 2 to LAN traffic, you also need to enable the default WAN2 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the WAN2 port to the LAN port and from LAN port to WAN2. |
| Allow between WAN2 and DMZ | Select this check box to forward NetBIOS packets from the WAN2 port to the DMZ port and from the DMZ port to WAN2.<br>Clear this check box to block all NetBIOS packets going from the WAN2 port to the DMZ port and from DMZ port to WAN2. |
| Allow between WAN1 and WLAN | Select this check box to forward NetBIOS packets from the WAN2 port to the WLAN port and from the WLAN port to WAN2.<br>Clear this check box to block all NetBIOS packets going from the WAN2 port to the WLAN port and from WLAN port to WAN2. |
| Allow Trigger Dial | Select this option to allow NetBIOS packets to initiate calls. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.2 WAN ISP – ZyWALL (one WAN port)

The screen differs by the encapsulation type chosen.

**Figure 67** Configuration > WAN > ISP (Ethernet) – ZyWALL (one WAN port)



Configuration >> WAN >> ISP

Configuration: WAN

WAN: ISP

Encapsulation: Ethernet

Ethernet

Service Type: Standard

## 9.2.1 Ethernet Encapsulation

The following table describes the labels in the **Ethernet** encapsulation screen.

**Table 44** Configuration > WAN > ISP (Ethernet) – ZyWALL (one WAN port)

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation | You must choose the Ethernet option when the WAN port is used as a regular Ethernet. |
| Service Type | Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**.<br>The following fields do not appear with the **Standard** service type. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.2.2 PPPoE Encapsulation

The device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

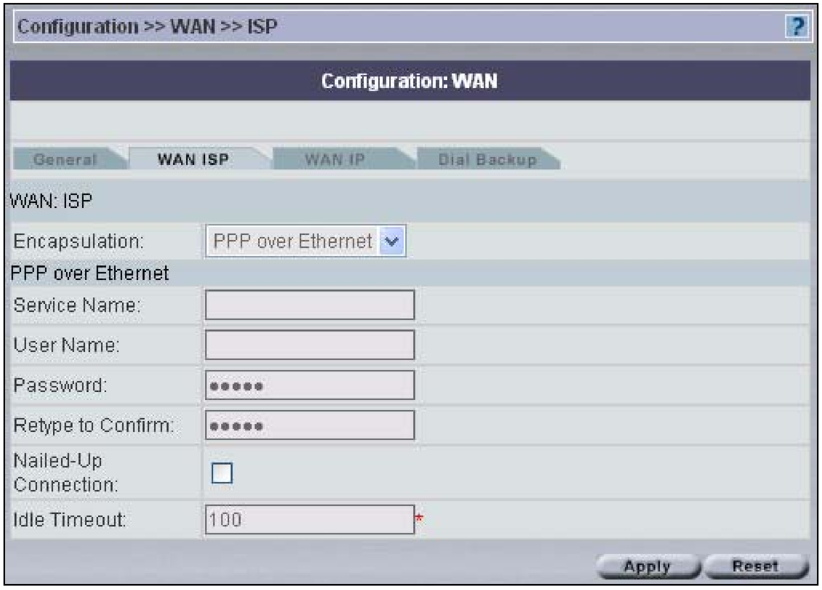
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

**Figure 68** Configuration > WAN > ISP (PPPoE) – ZyWALL (one WAN port)



Configuration >> WAN >> ISP

Configuration: WAN

WAN: ISP

Encapsulation: PPP over Ethernet

PPP over Ethernet

Service Name:

User Name:

Password: ●●●●●

Retype to Confirm: ●●●●●

Nailed-Up Connection: □

Idle Timeout: 100 *

The following table describes the labels in the **PPPoE** screen.

**Table 45** Configuration > WAN > ISP (PPPoE) – ZyWALL (one WAN port)

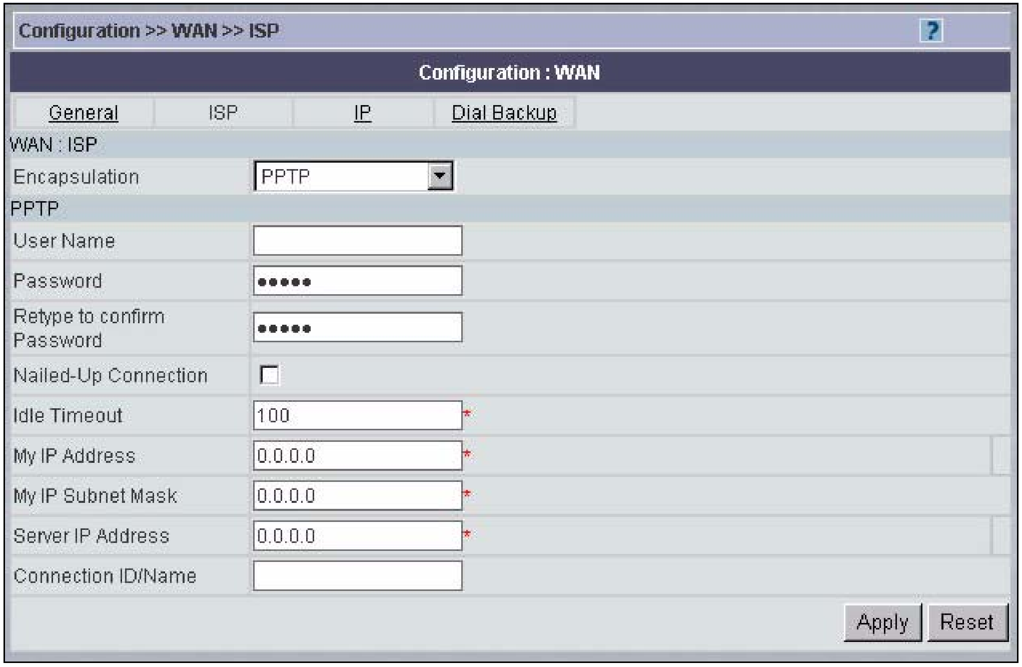
| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (for example, xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access. |
| Service Name | Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the User Name above. |
| Retype to Confirm | Type your password again to make sure that you have entered it correctly. |
| Nailed-Up Connection | Select **Nailed-Up Connection** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.2.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

**Figure 69** Configuration > WAN > ISP (PPTP) – ZyWALL (one WAN port)



WAN : ISP

| | |
|---|---|
| Encapsulation | PPTP |
| PPTP | |
| User Name | |
| Password | ••••• |
| Retype to confirm Password | ••••• |
| Nailed-Up Connection | □ |
| Idle Timeout | 100 * |
| My IP Address | 0.0.0.0 * |
| My IP Subnet Mask | 0.0.0.0 * |
| Server IP Address | 0.0.0.0 * |
| Connection ID/Name | |

The following table describes the labels in the **PPTP** screen.

**Table 46** Configuration > WAN > ISP (PPTP) – ZyWALL (one WAN port)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The device supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection. |
| PPTP Configuration | |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the User Name above. |
| Retype to confirm Password | Type your password again to make sure that you have entered it correctly. |
| Nailed-up Connection | Select **Nailed-Up Connection** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the device automatically disconnects from the PPTP server. |
| My IP Address | Type the (static) IP address assigned to you by your ISP. |
| My IP Subnet Mask | The device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the device. |
| Server IP Address | Type the IP address of the PPTP server. |

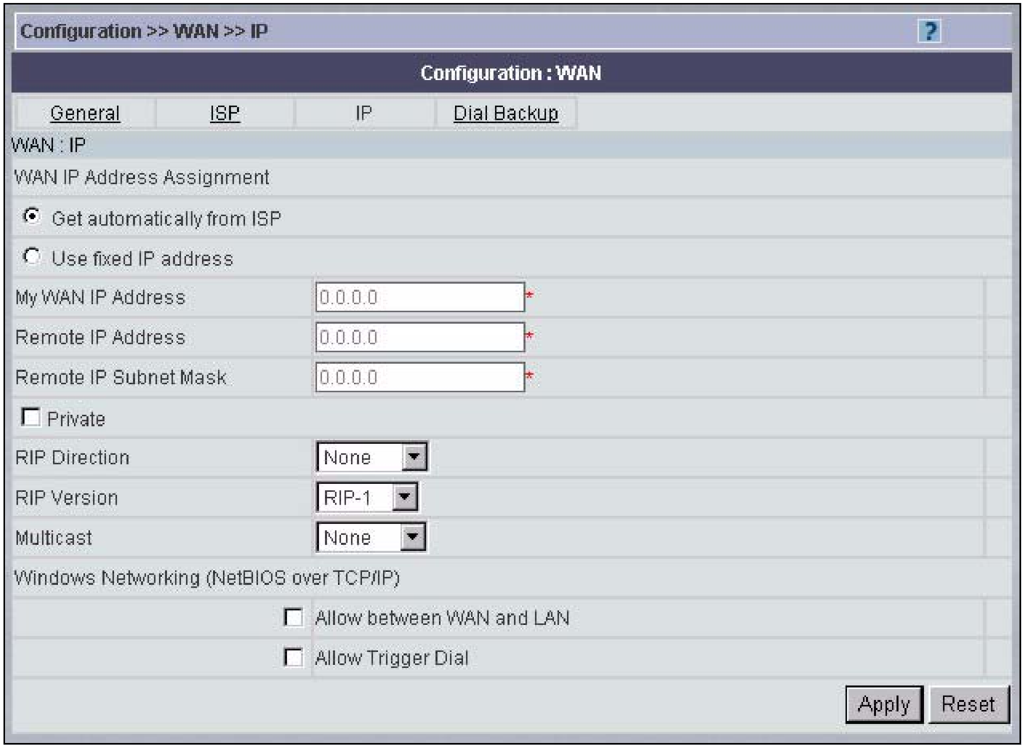
**Table 46** Configuration > WAN > ISP (PPTP) – ZyWALL (one WAN port) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Connection ID/Name | Type your identification name for the PPTP server. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.3 WAN IP – ZyWALL (one WAN port)

Use this screen to configure the WAN port's IP address. This screen depends on the type of encapsulation. To open this screen, click **Configuration** > **WAN** > **IP**.

**Figure 70** Configuration > WAN > IP – ZyWALL (one WAN port)



WAN : IP

WAN IP Address Assignment

● Get automatically from ISP

○ Use fixed IP address

| | |
|---|---|
| My WAN IP Address | 0.0.0.0 * |
| Remote IP Address | 0.0.0.0 * |
| Remote IP Subnet Mask | 0.0.0.0 * |

☐ Private

| | |
|---|---|
| RIP Direction | None |
| RIP Version | RIP-1 |
| Multicast | None |

Windows Networking (NetBIOS over TCP/IP)

☐ Allow between WAN and LAN

☐ Allow Trigger Dial

The following table describes the fields in this screen.

**Table 47** Configuration > WAN > IP – ZyWALL (one WAN port)

| LABEL | DESCRIPTION |
|---|---|
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use fixed IP address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address.** |
| My WAN IP Subnet Mask (Ethernet encapsulation) | Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |

**Table 47** Configuration > WAN > IP – ZyWALL (one WAN port) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Remote IP Address<br>Gateway IP Address | Enter the gateway or remote IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Remote IP Subnet Mask (PPPoE and PPTP encapsulation) | Enter the gateway's subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Private | This parameter determines if the device will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the device will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the device will incorporate RIP information that it receives.<br>When set to **None**, the device will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Multicast | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. | |
| Allow between WAN and LAN | Select this option to forward NetBIOS packets between the WAN port and the LAN port. |
| Allow Trigger Dial | Select this option to allow NetBIOS packets to initiate calls. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

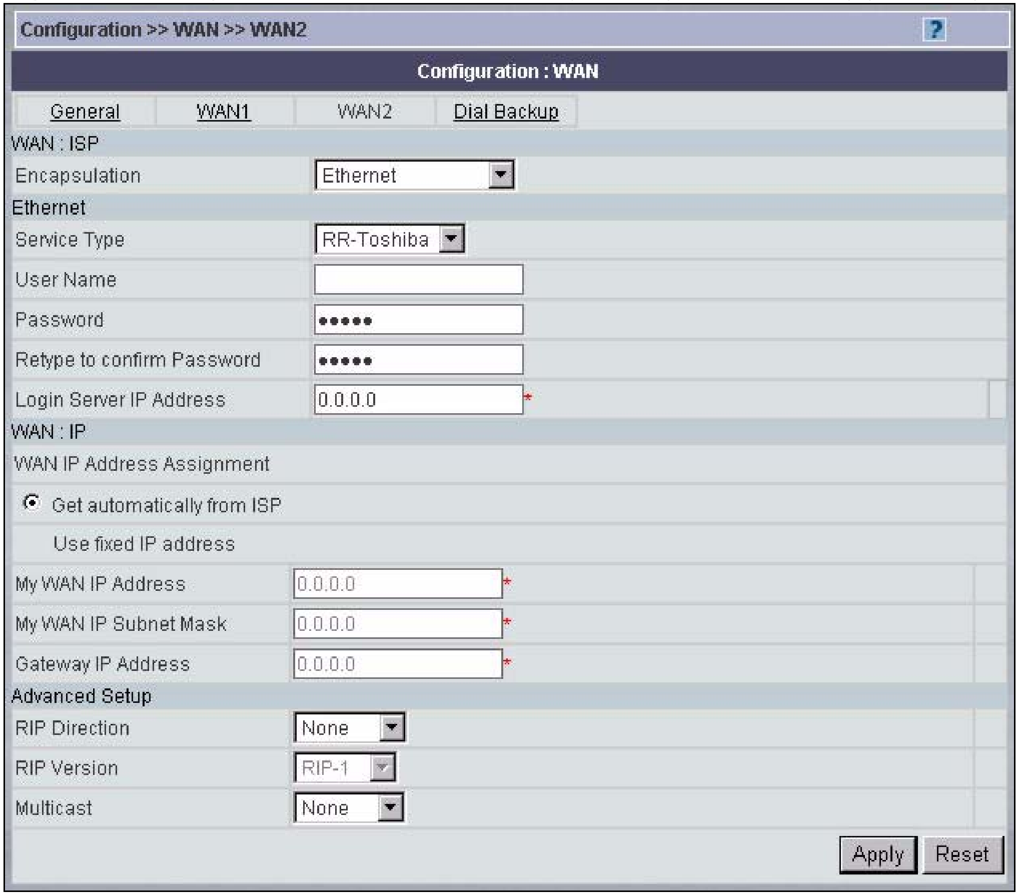
## 9.4 WAN1 and WAN2 (two WAN ports)

The ZyWALL 4.00 screens are organized differently than the previous versions because it has two WAN ports. Use the **WAN1** and **WAN2** tabs to configure the **WAN1** and **WAN2** ports. These tabs are similar and vary by encapsulation type.

### 9.4.1 Ethernet Encapsulation

Use this screen to configure an Ethernet connection on one of the device's WAN ports. To open this screen, click **Configuration** > **WAN** > **WAN1/2**.

**Figure 71** Configuration > WAN > WAN1/2 – ZyWALL (two WAN ports) (Ethernet)



Configuration >> WAN >> WAN2

Configuration : WAN

WAN : ISP

Encapsulation: Ethernet

Ethernet

Service Type: RR-Toshiba

User Name:

Password: ●●●●●

Retype to confirm Password: ●●●●●

Login Server IP Address: 0.0.0.0 *

WAN : IP

WAN IP Address Assignment

● Get automatically from ISP

Use fixed IP address

My WAN IP Address: 0.0.0.0 *

My WAN IP Subnet Mask: 0.0.0.0 *

Gateway IP Address: 0.0.0.0 *

Advanced Setup

RIP Direction: None

RIP Version: RIP-1

Multicast: None

The following table describes the labels in this screen.

**Table 48** Configuration > WAN > WAN1/2 – ZyWALL (two WAN ports) (Ethernet)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | You must choose the Ethernet option when the WAN port is used as a regular Ethernet. |

**Table 48** Configuration > WAN > WAN1/2 – ZyWALL (two WAN ports) (Ethernet) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service Type | Choose from **Standard**, **RR-Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**.<br>The following fields do not appear with the **Standard** service type. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to confirm Password | Type your password again to make sure that you have entered is correctly. |
| Login Server IP Address | Type the authentication server IP address here if your ISP gave you one.<br>This field is not available for Telia Login. |
| Telia Login Server (Telia Login only) | Type the domain name of the Telia login server, for example login1.telia.com. |
| Relogin Every(mins) (Telia Login only) | The Telia server logs the Vantage CNM out if the Vantage CNM does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the Vantage CNM to wait between logins. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use fixed IP address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| My WAN IP Subnet Mask | Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Gateway IP Address | Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Advanced Setup | |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the Vantage CNM will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the Vantage CNM will incorporate RIP information that it receives.<br>When set to **None**, the Vantage CNM will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |

**Table 48** Configuration > WAN > WAN1/2 – ZyWALL (two WAN ports) (Ethernet) (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Vantage CNM sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Apply | Click **Apply** to save your changes back to the Vantage CNM. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.4.2 PPPoE Encapsulation

PPPoE (Point-to-Point Protocol over Ethernet) is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

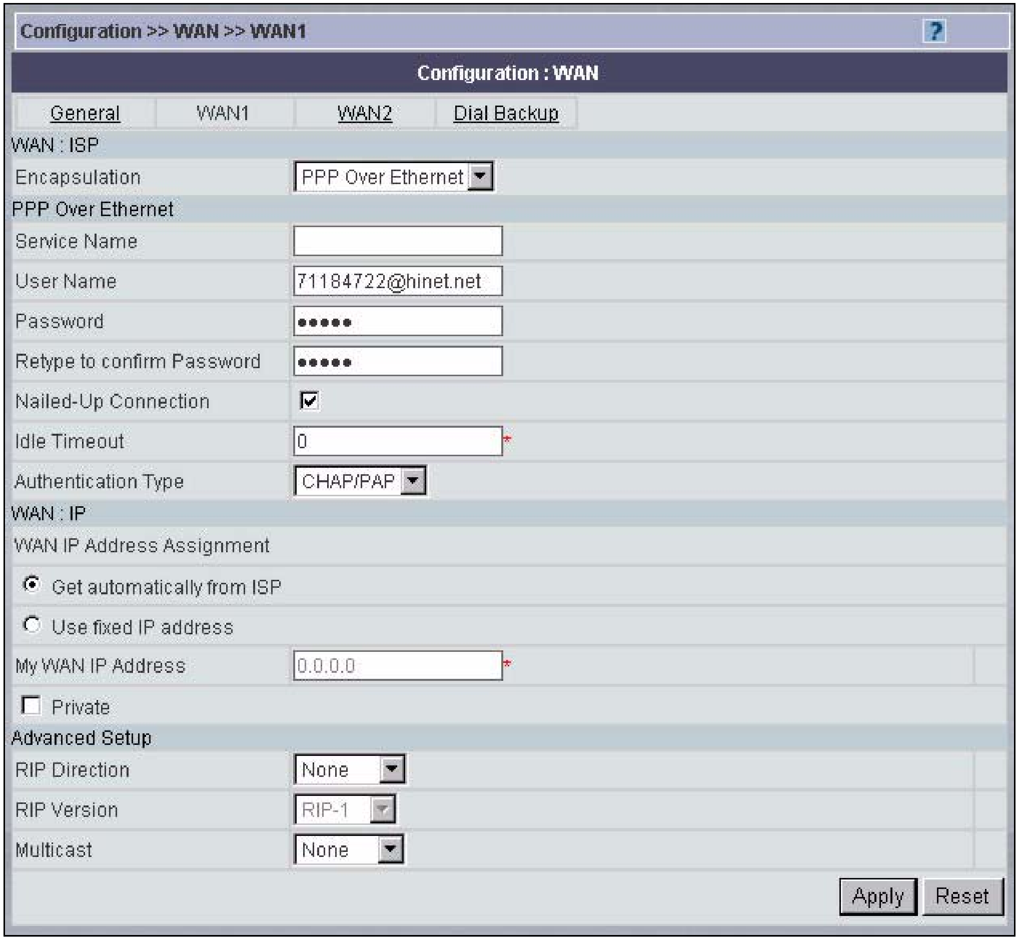
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the device does that part of the task. Furthermore, with NAT, all of the LANs’ computers will have access.

**Figure 72** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPPoE)



Configuration >> WAN >> WAN1

Configuration : WAN

WAN : ISP

| | |
|---|---|
| Encapsulation | PPP Over Ethernet |

PPP Over Ethernet

| | |
|---|---|
| Service Name | |
| User Name | 71184722@hinet.net |
| Password | ●●●●● |
| Retype to confirm Password | ●●●●● |
| Nailed-Up Connection | ☑ |
| Idle Timeout | 0 * |
| Authentication Type | CHAP/PAP |

WAN : IP

WAN IP Address Assignment

● Get automatically from ISP

○ Use fixed IP address

| | |
|---|---|
| My WAN IP Address | 0.0.0.0 * |

□ Private

Advanced Setup

| | |
|---|---|
| RIP Direction | None |
| RIP Version | RIP-1 |
| Multicast | None |

The following table describes the labels in this screen.

**Table 49** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPPoE)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (for example, DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access. |
| Service Name | Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to confirm Password | Type your password again to make sure that you have entered is correctly. |

**Table 49** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPPoE) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Nailed-Up Connection | Select this if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the device automatically disconnects from the PPPoE server. |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your Vantage CNM accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your Vantage CNM accepts CHAP only.<br>**PAP** - Your Vantage CNM accepts PAP only. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address.** |
| Private | This parameter determines if the device will include this route to a remote node in its RIP broadcasts.<br>Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts. |
| Advanced Setup | |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the Vantage CNM will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the Vantage CNM will incorporate RIP information that it receives.<br>When set to **None**, the Vantage CNM will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Vantage CNM sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Multicast | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |

**Table 49** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPPoE) (continued)

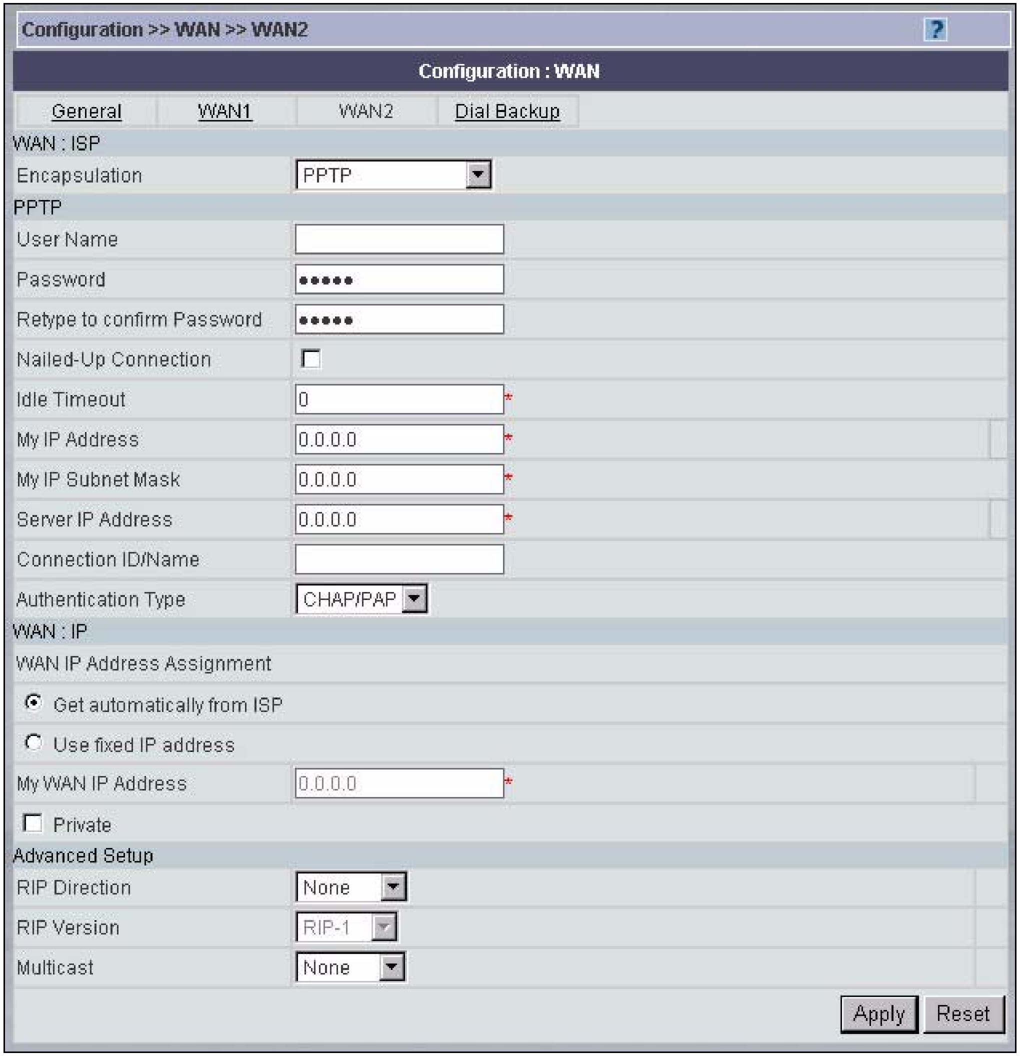
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the Vantage CNM. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.4.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

**Figure 73** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPTP)



Configuration >> WAN >> WAN2

Configuration : WAN

WAN : ISP

| | |
|---|---|
| Encapsulation | PPTP |

PPTP

| | |
|---|---|
| User Name | |
| Password | ••••• |
| Retype to confirm Password | ••••• |
| Nailed-Up Connection | □ |
| Idle Timeout | 0 * |
| My IP Address | 0.0.0.0 * |
| My IP Subnet Mask | 0.0.0.0 * |
| Server IP Address | 0.0.0.0 * |
| Connection ID/Name | |
| Authentication Type | CHAP/PAP |

WAN : IP

WAN IP Address Assignment

● Get automatically from ISP

○ Use fixed IP address

| | |
|---|---|
| My WAN IP Address | 0.0.0.0 * |

□ Private

Advanced Setup

| | |
|---|---|
| RIP Direction | None |
| RIP Version | RIP-1 |
| Multicast | None |

The following table describes the labels in this screen.

**Table 50** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPTP)

| LABEL | DESCRIPTION |
|---|---|
| WAN: ISP | |
| Encapsulation | Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The device supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection. |
| PPTP | |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to confirm Password | Type your password again to make sure that you have entered is correctly. |
| Nailed-up Connection | Select this if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the device automatically disconnects from the PPTP server. |
| My IP Address | Type the (static) IP address assigned to you by your ISP. |
| My IP Subnet Mask | Type the subnet mask assigned to you by your ISP. |
| Server IP Address | Type the IP address of the PPTP server. |
| Connection ID/ Name | Type your identification name for the PPTP server. |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your device accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your device accepts CHAP only.<br>**PAP** - Your device accepts PAP only. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use fixed IP address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| Private | This parameter determines if the device will include this route to a remote node in its RIP broadcasts.<br>Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts. |
| Advanced Setup | |

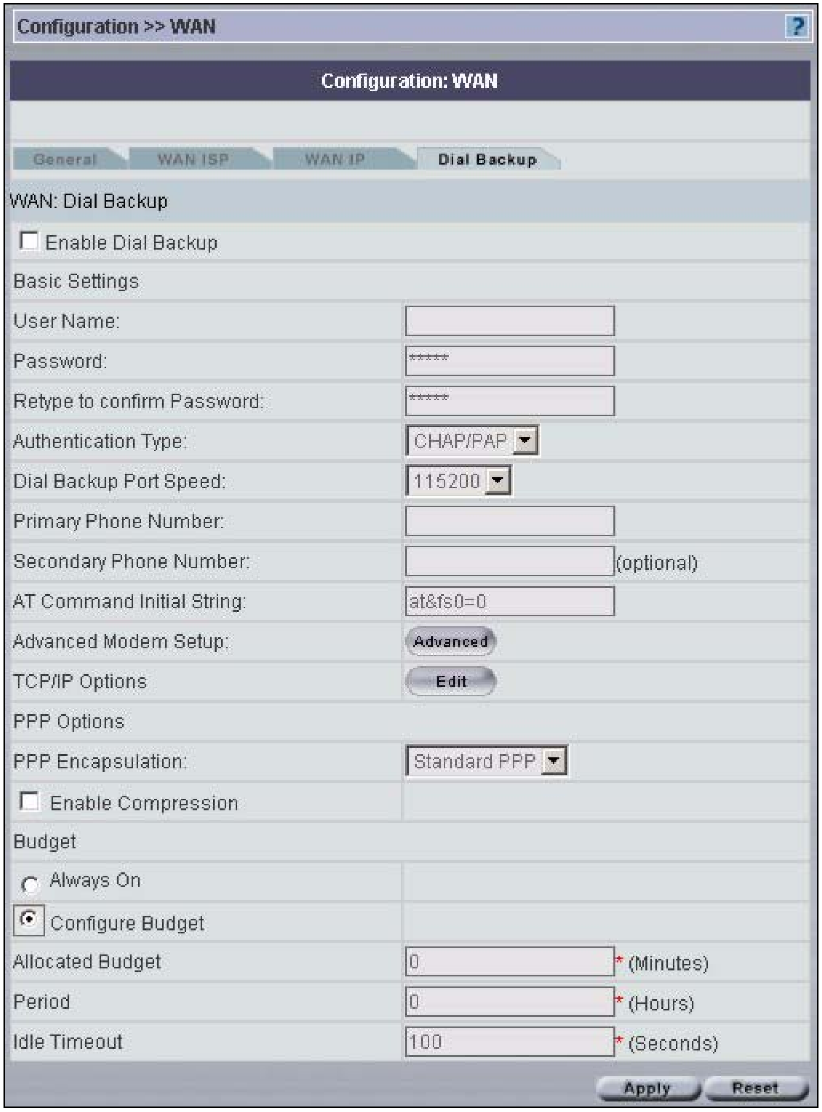
**Table 50** Configuration > WAN > WAN1 – ZyWALL (two WAN ports) (PPTP) (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the device will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the device will incorporate RIP information that it receives.<br>When set to **None**, the device will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Multicast | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Apply | Click **Apply** to save your changes back to the Vantage CNM. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.5 Dial Backup – ZyWALL

Vantage CNM can communicate with the device using Dial Backup if the main WAN connection goes down. Use this screen to configure Dial Backup on the device.

**Figure 74** Configuration > WAN > Dial Backup – ZyWALL



Configuration: WAN

WAN: Dial Backup

☐ Enable Dial Backup

Basic Settings

| | |
|---|---|
| User Name: | |
| Password: | ***** |
| Retype to confirm Password: | ***** |
| Authentication Type: | CHAP/PAP |
| Dial Backup Port Speed: | 115200 |
| Primary Phone Number: | |
| Secondary Phone Number: | (optional) |
| AT Command Initial String: | at&fs0=0 |
| Advanced Modem Setup: | Advanced |
| TCP/IP Options | Edit |

PPP Options

| | |
|---|---|
| PPP Encapsulation: | Standard PPP |
| ☐ Enable Compression | |

Budget

○ Always On

● Configure Budget

| | |
|---|---|
| Allocated Budget | 0 * (Minutes) |
| Period | 0 * (Hours) |
| Idle Timeout | 100 * (Seconds) |

The following table describes the labels in this screen.

**Table 51** Configuration > WAN > Dial Backup – ZyWALL

| LABEL | DESCRIPTION |
|---|---|
| Enable Dial Backup | Select this check box to turn on dial backup. |
| Basic Settings | |
| User Name | Type the user name assigned by your ISP. |
| Password | Type the password assigned by your ISP. |
| Retype to confirm Password | Type your password again to make sure that you have entered it correctly. |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - The device accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - The device accepts CHAP only.<br>**PAP** - The device accept PAP only. |

**Table 51** Configuration > WAN > Dial Backup – ZyWALL (continued)

| LABEL | DESCRIPTION |
|---|---|
| Dial Backup Port Speed | Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps. |
| Primary/ Secondary Phone Number | Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, the device dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| AT Command Initial String | Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands. |
| Advanced Modem Setup | Click **Advanced** to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup. |
| TCP/IP Options | Click **Edit** to display the **Dial Backup TCP/IP Options** screen. |
| PPP Options | |
| PPP Encapsulation | Select **CISCO PPP** from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**. |
| Enable Compression | Select this check box to turn on stac compression. |
| Budget | |
| Always On | Select this check box to have the dial backup connection on all of the time. |
| Configure Budget | Select this check box to have the dial backup connection on during the time that you select. |
| Allocated Budget | Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. |
| Period | Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). |
| Idle Timeout | Type the number of seconds of idle time (when there is no traffic from the device to the remote node) for the device to wait before it automatically disconnects the dial backup connection. This option applies only when the device initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**). |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.5.1 Advanced Modem Setup – ZyWALL

### 9.5.1.1 AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both Dial and Init strings.

#### 9.5.1.1.1 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the device uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

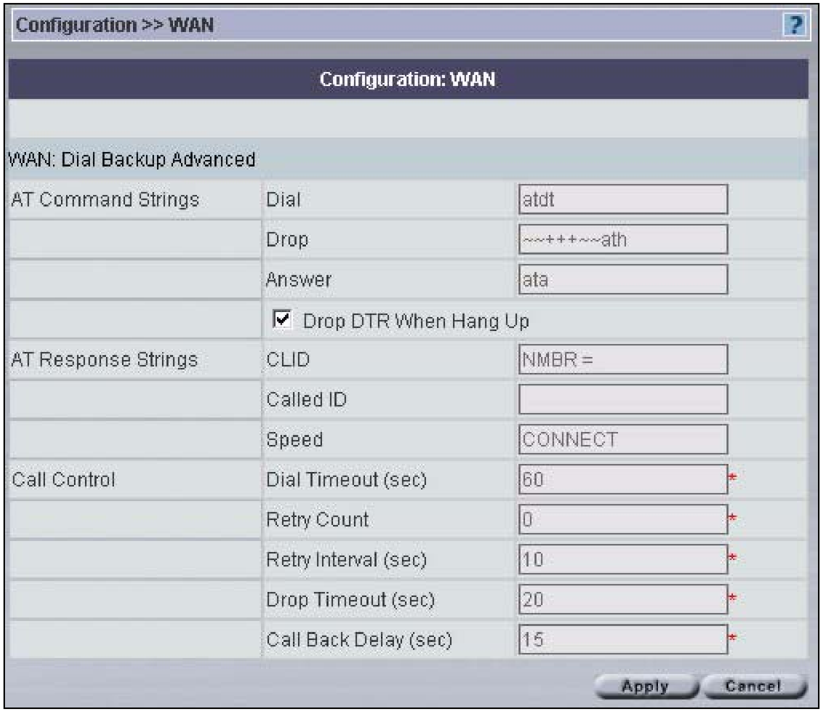
#### 9.5.1.1.2 Response Strings

The response strings tell the device the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

Click the **Advanced** button in the **Advanced Modem Setup** in the **Dial Backup** screen to display the **Dial Backup Advanced** screen shown next.

Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

**Figure 75** Configuration > WAN > Dial Backup > Advanced – ZyWALL



Configuration >> WAN

Configuration: WAN

WAN: Dial Backup Advanced

| | | |
|---|---|---|
| AT Command Strings | Dial | atdt |
| | Drop | ~~+++~~ath |
| | Answer | ata |
| | ☑ Drop DTR When Hang Up | |
| AT Response Strings | CLID | NMBR = |
| | Called ID | |
| | Speed | CONNECT |
| Call Control | Dial Timeout (sec) | 60 * |
| | Retry Count | 0 * |
| | Retry Interval (sec) | 10 * |
| | Drop Timeout (sec) | 20 * |
| | Call Back Delay (sec) | 15 * |

The following table describes the labels in this screen.

**Table 52** Configuration > WAN > Dial Backup > Advanced – ZyWALL

| LABEL | DESCRIPTION | EXAMPLE |
|---|---|---|
| AT Command Strings | | |
| Dial | Type the AT Command string to make a call. | atdt |

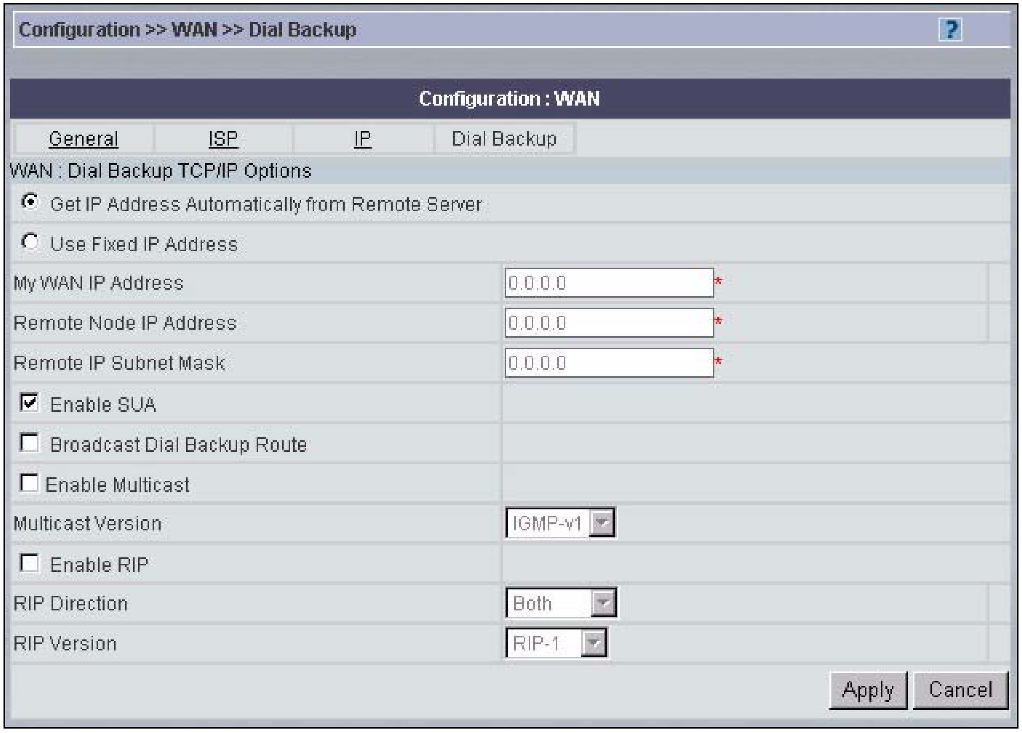
**Table 52** Configuration > WAN > Dial Backup > Advanced – ZyWALL (continued)

| LABEL | DESCRIPTION | EXAMPLE |
|---|---|---|
| Drop | Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time. | ~~+++~~ath |
| Answer | Type the AT Command string to answer a call. | ata |
| Drop DTR When Hang Up | Select this check box to have the device drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out. | |
| AT Response Strings | | |
| CLID | Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the device capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. | NMBR |
| Called ID | Type the keyword preceding the dialed number. | |
| Speed | Type the keyword preceding the connection speed. | CONNECT |
| Call Control | | |
| Dial Timeout (sec) | Type a number of seconds for the device to try to set up an outgoing call before timing out (stopping). | 60 |
| Retry Count | Type a number of times for the device to retry a busy or no-answer phone number before blacklisting the number. | 0 |
| Retry Interval (sec) | Type a number of seconds for the device to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. | 10 |
| Drop Timeout (sec) | Type the number of seconds for the device to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. | 20 |
| Call Back Delay (sec) | Type a number of seconds for the device to wait between dropping a callback request call and dialing the corresponding callback call. | 15 |
| Apply | Click **Apply** to save your changes back to the device. | |
| Cancel | Click **Cancel** to begin configuring this screen afresh. | |

## 9.5.2 Edit Dial Backup – ZyWALL

Click **Edit** in the **TCP/IP** field in the screen shown in Figure 74 on page 139 to display the next screen.

**Figure 76** Configuration > WAN > Dial Backup > Edit – ZyWALL



Configuration >> WAN >> Dial Backup

Configuration : WAN

WAN : Dial Backup TCP/IP Options

● Get IP Address Automatically from Remote Server

○ Use Fixed IP Address

| | |
|---|---|
| My WAN IP Address | 0.0.0.0 * |
| Remote Node IP Address | 0.0.0.0 * |
| Remote IP Subnet Mask | 0.0.0.0 * |
| ☑ Enable SUA | |
| □ Broadcast Dial Backup Route | |
| □ Enable Multicast | |
| Multicast Version | IGMP-v1 |
| □ Enable RIP | |
| RIP Direction | Both |
| RIP Version | RIP-1 |

The following table describes the fields in this screen.

**Table 53** Configuration > WAN > Dial Backup > Edit – ZyWALL

| LABEL | DESCRIPTION |
|---|---|
| Get IP Address Automatically from Remote Server | Type the login name assigned by your ISP for this remote node. |
| Use Fixed IP Address | Select this check box if your ISP assigned you a fixed IP address, and then enter the IP address in the following field. |
| My WAN IP Address | Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local device, not the remote router. |
| Remote Node IP Address | Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static). |
| Remote IP Subnet Mask | Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static). |
| Enable SUA | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.<br>**SUA** (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the device will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information).<br>Select the check box to enable SUA. Clear the check box to disable SUA so the device does not perform any NAT mapping for the dial backup connection. |

**Table 53** Configuration > WAN > Dial Backup > Edit – ZyWALL (continued)

| LABEL | DESCRIPTION |
|---|---|
| Broadcast Dial Backup Route | Select this check box to forward the backup route broadcasts to the WAN. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*. |
| Enable RIP | Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

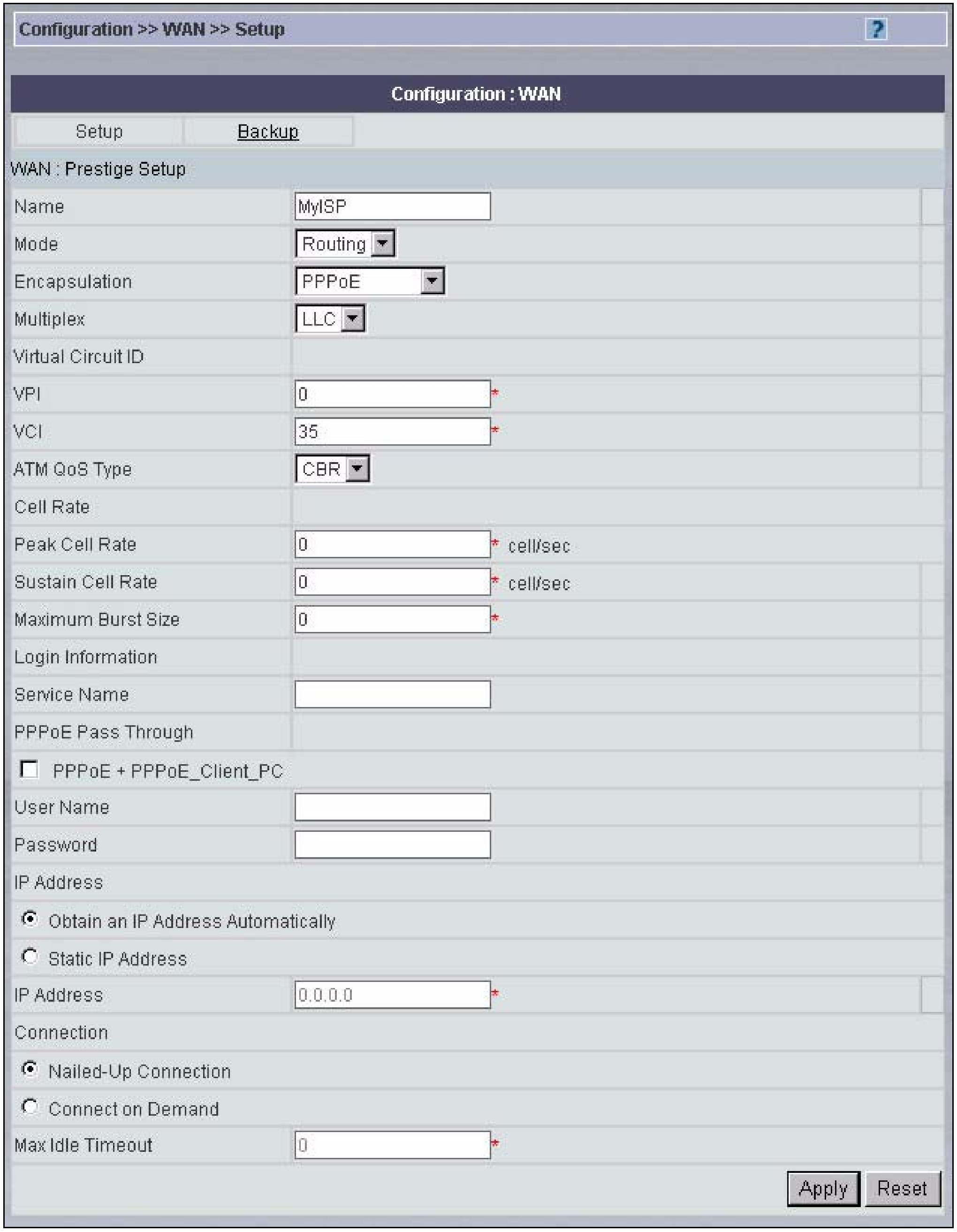
# 9.6 General WAN – Prestige

This section gives background and configuration information on the fields displayed in this screen.

## 9.6.1 Prestige WAN Setup

The fields in this screen vary depending on the mode and encapsulation. Select a device in the object tree and then select **Configuration > WAN**.

**Figure 77** Configuration > WAN > Setup – Prestige



Configuration >> WAN >> Setup

Configuration : WAN

Setup | Backup

WAN : Prestige Setup

| | |
|---|---|
| Name | MyISP |
| Mode | Routing |
| Encapsulation | PPPoE |
| Multiplex | LLC |
| Virtual Circuit ID | |
| VPI | 0 * |
| VCI | 35 * |
| ATM QoS Type | CBR |
| Cell Rate | |
| Peak Cell Rate | 0 * cell/sec |
| Sustain Cell Rate | 0 * cell/sec |
| Maximum Burst Size | 0 * |
| Login Information | |
| Service Name | |
| PPPoE Pass Through | |
| □ PPPoE + PPPoE_Client_PC | |
| User Name | |
| Password | |
| IP Address | |
| ● Obtain an IP Address Automatically | |
| ○ Static IP Address | |
| IP Address | 0.0.0.0 * |
| Connection | |
| ● Nailed-Up Connection | |
| ○ Connect on Demand | |
| Max Idle Timeout | 0 * |

The following table describes the fields in this screen.

**Table 54** Configuration > WAN > Setup – Prestige

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter the name of your Internet Service Provider, for example, MyISP. This information is for identification purposes only. |
| Mode | Select **Routing** from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**. |

**Table 54** Configuration > WAN > Setup – Prestige (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation | Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field.<br>If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**.<br>If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**. |
| Multiplex | Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. |
| Virtual Circuit ID | VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information. |
| VPI | The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. |
| VCI | The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you. |
| ATM QoS Type | Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications. |
| Cell Rate | Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections. |
| Peak Cell Rate | Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. |
| Sustain Cell Rate | The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. |
| Maximum Burst Size | Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. |
| Login Information | (PPPoA and PPPoE encapsulation only) |
| Service Name | This field is only available when **PPPoE** encapsulation is selected. Type the **PPPoE** service name provided to you. **PPPoE** uses a service name to identify and reach the **PPPoE** server. |
| PPPoE + PPPoE_Client_PC(PPPoE encapsulation only) | This field is only available when **PPPoE** encapsulation is selected.<br>Select the check box to enable PPPoE pass through. In addition to the device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. |
| User Name | Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given. |
| Password | Enter the password associated with the user name above. |

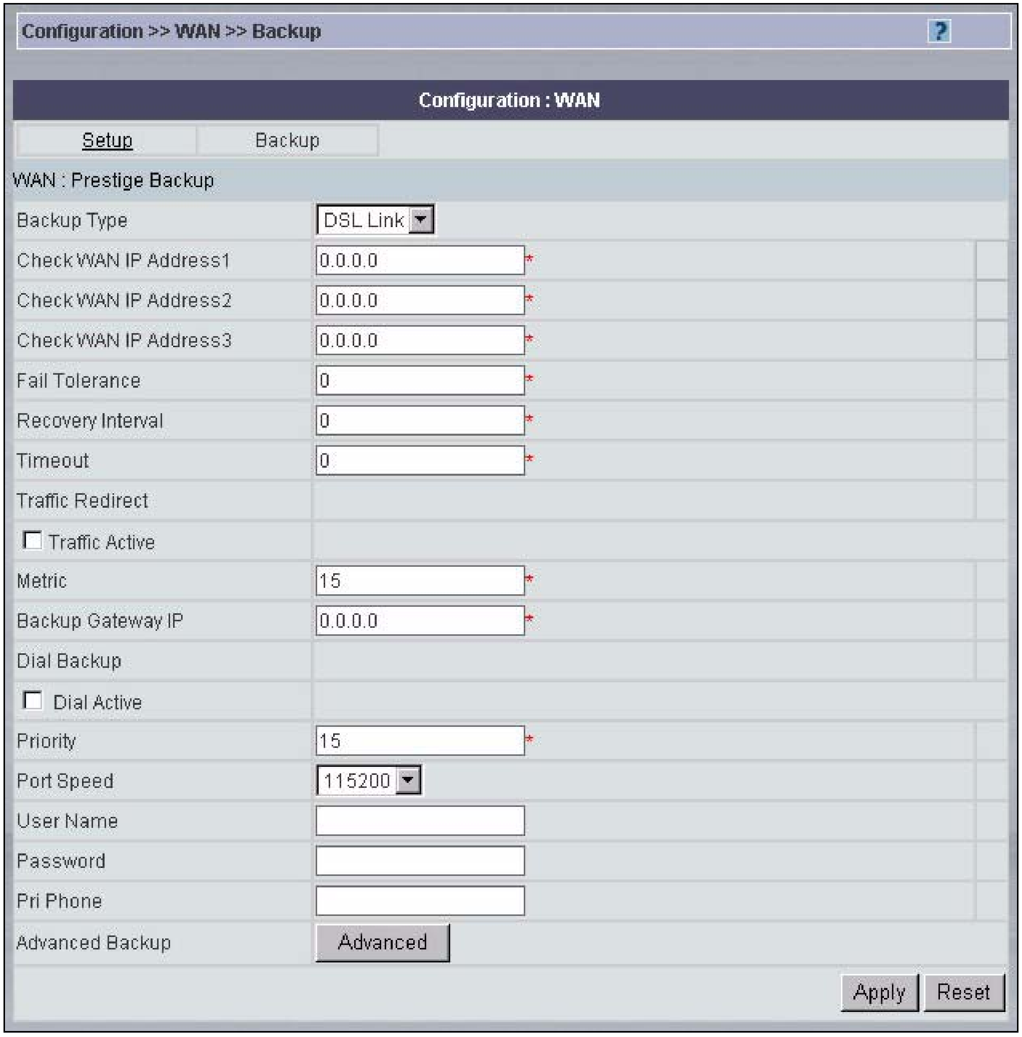
**Table 54** Configuration > WAN > Setup – Prestige (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This option is available if you select **Routing** in the **Mode** field.<br>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.<br>Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below. |
| Connection<br>(PPPoA and PPPoE encapsulation only) | The schedule rule(s) in SMT menu 26 have priority over your **Connection** settings. |
| Nailed-Up Connection | Select **Nailed-Up Connection** when you want your connection up all the time. The device will try to bring up the connection automatically if it is disconnected. |
| Connect on Demand | Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field. |
| Max Idle Timeout | Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout. |
| Zero Configuration | Select this if you want the device to automatically try to configure the Internet connection. See the device's User's Guide for more information. |
| Subnet Mask (ENET ENCAP only) | Enter the subnet mask provided by your ISP. |
| ENET ENCAP Gateway (ENET ENCAP only) | Enter the IP address of the gateway provided by your ISP. |
| Apply | Click **Apply** to save the changes. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.6.2 WAN Backup - Prestige

To change your device's WAN backup settings, click **WAN** > **Backup**. The screen appears as shown.

**Figure 78** Configuration > WAN > Backup – Prestige



WAN : Prestige Backup

| | |
|---|---|
| Backup Type | DSL Link |
| Check WAN IP Address1 | 0.0.0.0 * |
| Check WAN IP Address2 | 0.0.0.0 * |
| Check WAN IP Address3 | 0.0.0.0 * |
| Fail Tolerance | 0 * |
| Recovery Interval | 0 * |
| Timeout | 0 * |
| Traffic Redirect | |
| □ Traffic Active | |
| Metric | 15 * |
| Backup Gateway IP | 0.0.0.0 * |
| Dial Backup | |
| □ Dial Active | |
| Priority | 15 * |
| Port Speed | 115200 |
| User Name | |
| Password | |
| Pri Phone | |
| Advanced Backup | Advanced |

The following table describes the fields in this screen.

**Table 55** Configuration > WAN > Backup – Prestige

| LABEL | DESCRIPTION |
|---|---|
| Backup Type | Select the method that the device uses to check the DSL connection.<br>Select **DSL Link** to have the device check if the connection to the DSLAM is up. Select **ICMP** to have the device periodically ping the IP addresses configured in the **Check WAN IP Address** type fields. |
| Check WAN IP Address1-3 | Configure this field to test your device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).<br>If you activate either traffic redirect or dial backup, you must configure at least one IP address here.<br>When using a WAN backup connection, the device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response. |
| Fail Tolerance | Type the number of times (2 recommended) that your device may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection). |

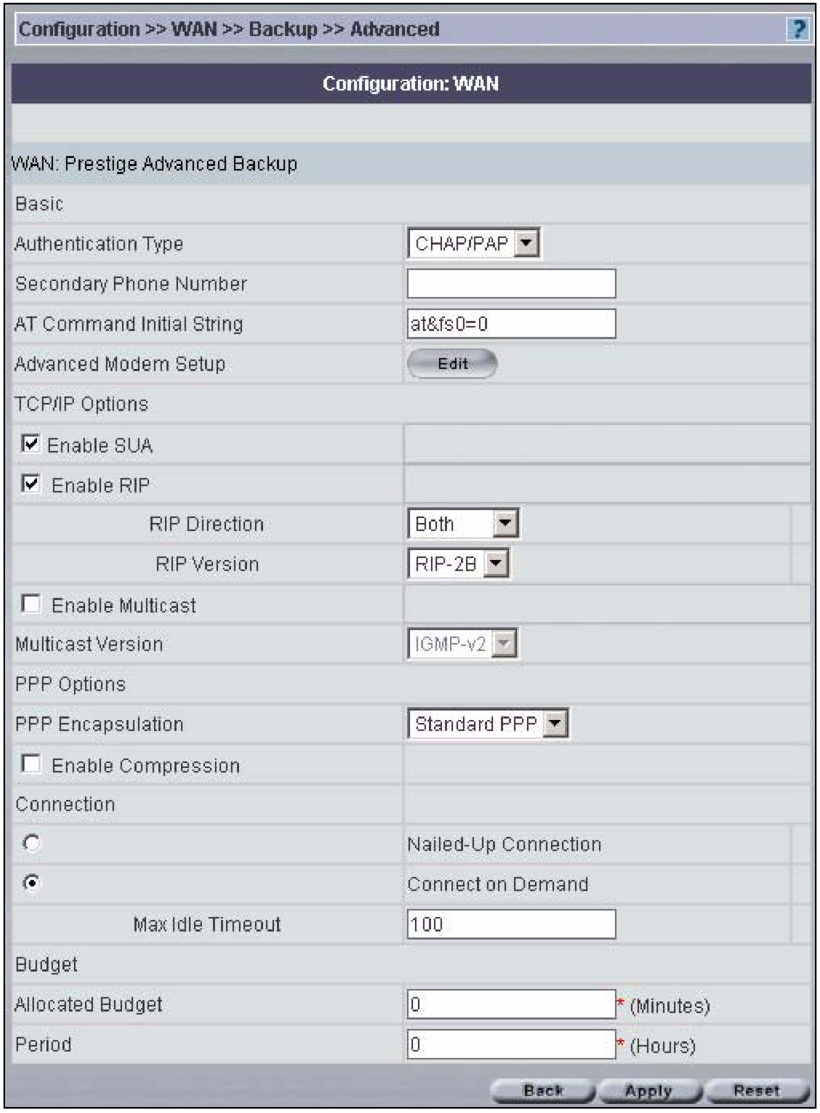
**Table 55** Configuration > WAN > Backup – Prestige (continued)

| LABEL | DESCRIPTION |
|---|---|
| Recovery Interval | When the device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection.<br>Type the number of seconds (30 recommended) for the device to wait between checks. Allow more time if your destination IP address handles lots of traffic. |
| Timeout | Type the number of seconds (3 recommended) for your device to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested. |
| Traffic Redirect | |
| Active | Select this check box to have the device use traffic redirect if the normal WAN connection goes down.<br>If you activate traffic redirect, you must configure at least one Check WAN IP Address. |
| Metric | This field sets this route's priority among the routes the device uses.<br>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost". |
| Backup Gateway IP | Type the IP address of your backup gateway in dotted decimal notation. The device automatically forwards traffic to this IP address if the device's Internet connection terminates. |
| Dial Backup | |
| Dial Active | Select this check box to turn on dial backup.<br>If you activate dial backup, you must configure at least one Check WAN IP Address. |
| Priority | This field sets this route's priority among the three routes the device uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority.<br>If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**. |
| Port Speed | Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps. |
| User Name | Type the login name assigned by your ISP. |
| Password | Type the password assigned by your ISP. |
| Pri Phone | Type the first (primary) phone number from the ISP for this remote node. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| Advanced Backup | Click this button to display the **Advanced Backup** screen and edit more details of your WAN backup setup. |
| Apply | Click **Apply** to save the changes. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

### 9.6.3 Advanced WAN Backup – Prestige

Use this screen to edit your device's advanced WAN backup settings. To open this screen, click **WAN** > **WAN Backup** and the **Advanced Backup** button.

**Figure 79** Configuration > WAN Backup > Advanced – Prestige



Configuration >> WAN >> Backup >> Advanced

Configuration: WAN

WAN: Prestige Advanced Backup

| | |
|---|---|
| Basic | |
| Authentication Type | CHAP/PAP |
| Secondary Phone Number | |
| AT Command Initial String | at&fs0=0 |
| Advanced Modem Setup | Edit |
| TCP/IP Options | |
| ☑ Enable SUA | |
| ☑ Enable RIP | |
| RIP Direction | Both |
| RIP Version | RIP-2B |
| □ Enable Multicast | |
| Multicast Version | IGMP-v2 |
| PPP Options | |
| PPP Encapsulation | Standard PPP |
| □ Enable Compression | |
| Connection | |
| ○ | Nailed-Up Connection |
| ● | Connect on Demand |
| Max Idle Timeout | 100 |
| Budget | |
| Allocated Budget | 0 * (Minutes) |
| Period | 0 * (Hours) |

The following table describes the fields in this screen.

**Table 56** Configuration > WAN Backup > Advanced – Prestige

| LABEL | DESCRIPTION |
|---|---|
| Basic | |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your device accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your device accepts CHAP only.<br>**PAP** - Your device accept PAP only. |

**Table 56** Configuration > WAN Backup > Advanced – Prestige (continued)

| LABEL | DESCRIPTION |
|---|---|
| Primary/ Secondary Phone Number | Type the first (primary) phone number from the ISP for this remote node. If the primary phone number is busy or does not answer, your device dials the secondary phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| AT Command Initial String | Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your dial backup port for specific AT commands. |
| Advanced Modem Setup | Click the **Edit** button to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup. |
| TCP/IP Options | |
| Enable SUA | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.<br>SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the device will use Address Mapping Set 255 in the SMT. |
| Enable RIP | Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the device will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the device will incorporate RIP information that it receives. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the device sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*. |
| PPP Options | |
| PPP Encapsulation **Standard PPP**. | Select **CISCO PPP** from the drop-down list box if your backup WAN device uses **Cisco PPP** encapsulation; otherwise select |
| Enable Compression | Select this check box to enable stac compression. |
| Connection | |

**Table 56** Configuration > WAN Backup > Advanced – Prestige (continued)

| LABEL | DESCRIPTION |
|---|---|
| Nailed-Up Connection | Select **Nailed-Up Connection** when you want your connection up all the time. The device will try to bring up the connection automatically if it is disconnected. |
| Connect on Demand | Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field. |
| Max Idle Timeout | Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout. |
| Budget | The configuration in the **Budget** fields has priority over your **Connection** settings. |
| Allocated Budget | Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. If you set the **Allocated Budget** to 0, you will not be able to use the dial backup connection. |
| Period | Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). If you set the **Period** to 0, there is no budget control and the device uses the **Connection** settings. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save the changes. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.6.4 Advanced Modem Setup – Prestige

Click **Edit** in the **Advanced Modem Setup** field. See the section on ZyWALL advanced modem setup on page 140 for configuration of this screen.

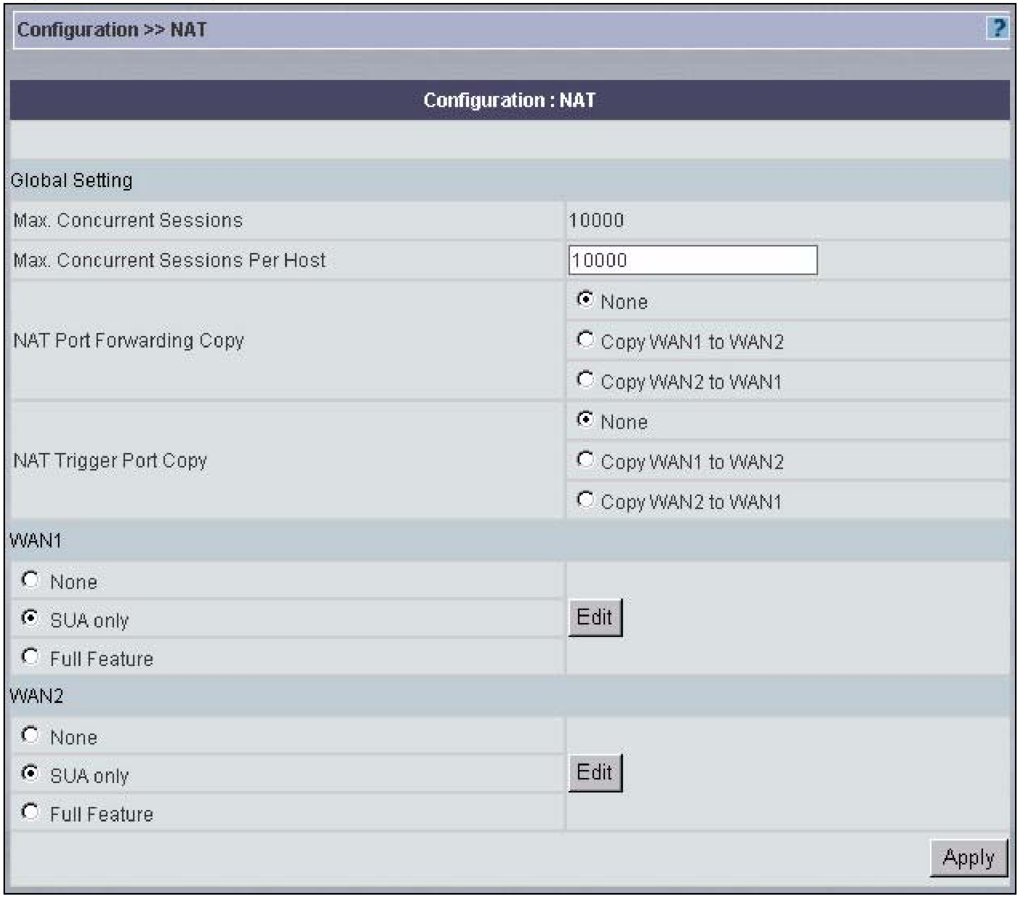
# Configuration > NAT

This section shows you how to configure the **NAT** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 10.1 NAT

Use this screen to specify what type of NAT the device should use and to configure any global NAT settings. To open this screen, click **Configuration** > **NAT**.

**Figure 80** Configuration > NAT



| | |
|---|---|
| Global Setting | |
| Max. Concurrent Sessions | 10000 |
| Max. Concurrent Sessions Per Host | 10000 |
| NAT Port Forwarding Copy | ● None<br>○ Copy WAN1 to WAN2<br>○ Copy WAN2 to WAN1 |
| NAT Trigger Port Copy | ● None<br>○ Copy WAN1 to WAN2<br>○ Copy WAN2 to WAN1 |
| WAN1 | |
| ○ None<br>● SUA only<br>○ Full Feature | Edit |
| WAN2 | |
| ○ None<br>● SUA only<br>○ Full Feature | Edit |
| | Apply |

The following table describes the fields in this screen.

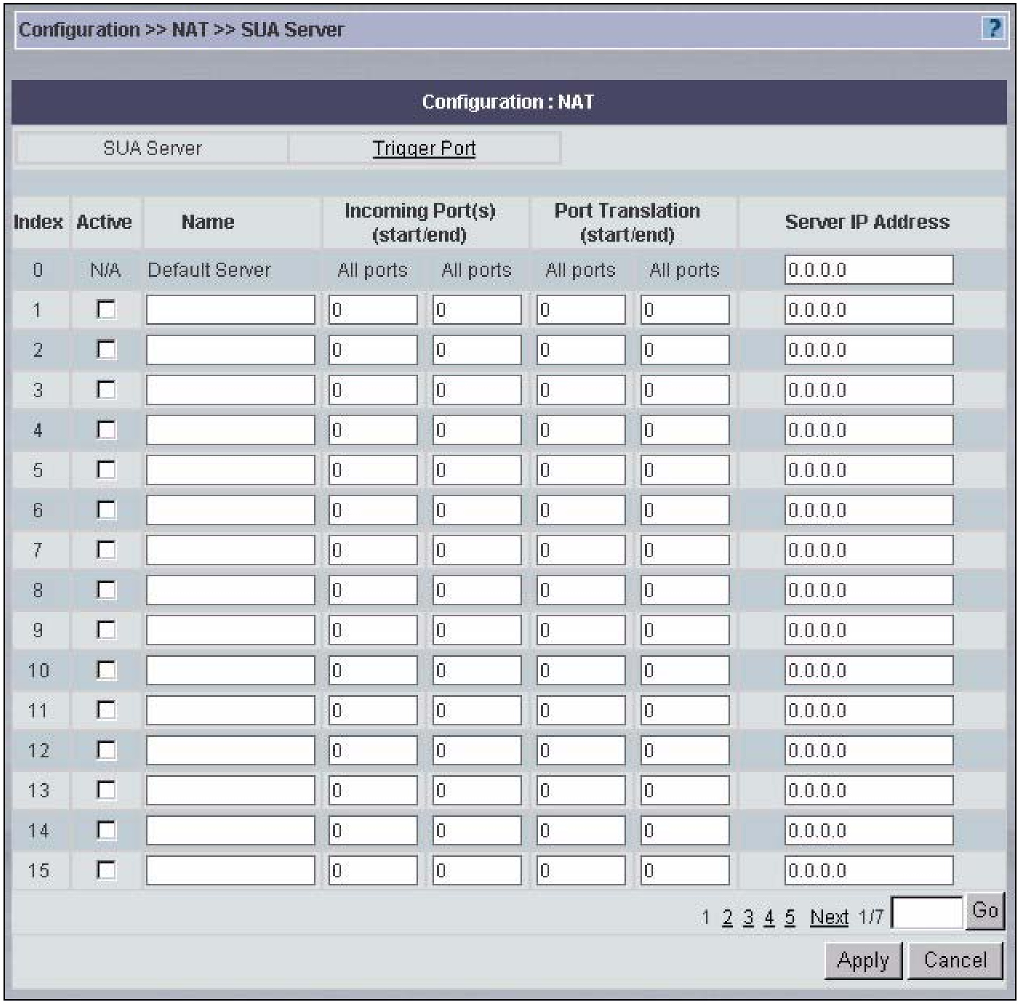
**Table 57** Configuration > NAT

| LABEL | DESCRIPTION |
|---|---|
| Global Setting | |
| Max. Concurrent Sessions | This read-only field displays the highest number of NAT sessions that the device will permit at one time. |
| Max. Concurrent Sessions Per Host | Use this field to set the highest number of NAT sessions that the device will permit a host to have at one time. |
| NAT Port Forwarding Copy | Click **Copy WAN1 to WAN 2** (or **Copy WAN2 to WAN 1**) to duplicate this WAN port's NAT port forwarding rules on the other WAN port.<br>Note: Using the copy button overwrites the other WAN port's existing rules.<br>The copy button is best suited for initial NAT configuration where you have configured NAT port forwarding rules for one port and want to use similar rules for the other WAN port. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN port to the other. |
| NAT Trigger Port Copy | Click **Copy WAN1 to WAN 2** (or **Copy WAN2 to WAN 1**) to duplicate this WAN port's NAT trigger port rules on the other WAN port.<br>Note: Using the copy button overwrites the other WAN port's existing rules.<br>The copy button is best suited for initial NAT configuration where you have configured NAT trigger port rules for one port and want to use similar rules for the other WAN port. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN port to the other. |
| | Use this section to select what kind of NAT the device should use. In some cases, the device might be able to use different kinds of NAT on different ports. |
| None | Select **None** to disable NAT on the device. |
| SUA Only | Select **SUA Only** to apply many-to-one mapping only (sufficient if the device has only one public IP address). |
| Full Feature | Select **Full Feature** to avail of multiple mapping types. |
| Edit | Click **Edit** to advance to the selected feature. |
| Apply | Click **Apply** to begin configuring this screen afresh. |

## 10.2 SUA Server

Use this screen to configure port forwarding on the device. To open this screen, click **Configuration > NAT**, select **SUA Only** or **Full Feature**, click **Edit**, and select **SUA Server**.

**Figure 81** Configuration > NAT > SUA Server



| Index | Active | Name | Incoming Port(s) (start/end) | | Port Translation (start/end) | | Server IP Address |
|---|---|---|---|---|---|---|---|
| 0 | N/A | Default Server | All ports | All ports | All ports | All ports | 0.0.0.0 |
| 1 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 2 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 3 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 4 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 5 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 6 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 7 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 8 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 9 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 10 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 11 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 12 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 13 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 14 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |
| 15 | □ | | 0 | 0 | 0 | 0 | 0.0.0.0 |

The following table describes the labels in this screen.

**Table 58** Configuration > NAT > SUA Server

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the number of an individual SUA server entry. You may select a rule to edit or delete it. |
| Active | Select this check box to enable the SUA server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry. |
| Name | Type a name to identify this port-forwarding rule. To delete a SUA server entry, erase the name, and click **Apply**. |
| Default Server<br>All Ports | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen or remote management will be discarded. |
| Incoming Port(s) | Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field. |

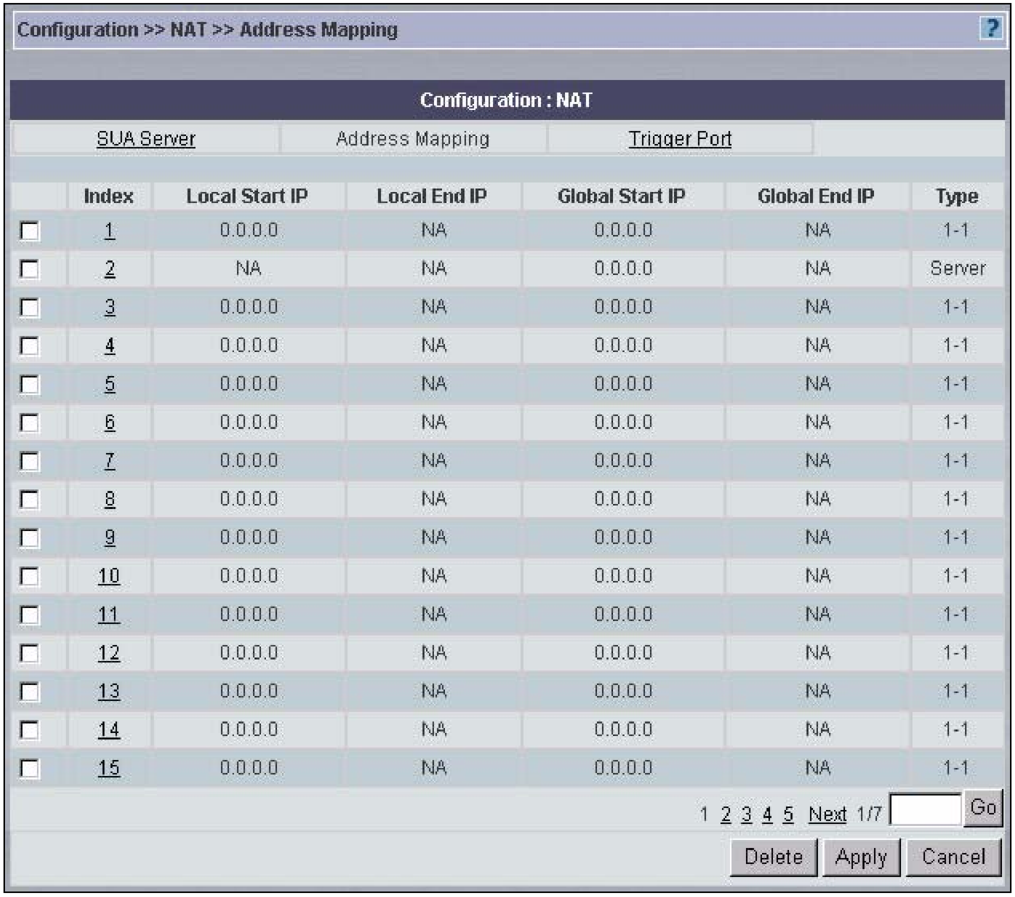
**Table 58** Configuration > NAT > SUA Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Translation | Enter the port number here to which you want the device to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the device automatically calculates the last port of the translated port range. |
| Server IP Address | Type the IP address of the inside server. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click **Cancel** to return to the previous screen. |

## 10.3 Address Mapping

Use this screen to configure various types of network address translation (NAT) on the device. To open this screen, click **Configuration** > **NAT**, select **Full Feature**, click **Edit**, and select **Address Mapping**.

**Figure 82** Configuration > NAT > Address Mapping



| | Index | Local Start IP | Local End IP | Global Start IP | Global End IP | Type |
|---|---|---|---|---|---|---|
| □ | 1 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 2 | NA | NA | 0.0.0.0 | NA | Server |
| □ | 3 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 4 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 5 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 6 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 7 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 8 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 9 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 10 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 11 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 12 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 13 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 14 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |
| □ | 15 | 0.0.0.0 | NA | 0.0.0.0 | NA | 1-1 |

The following table describes the labels in this screen.

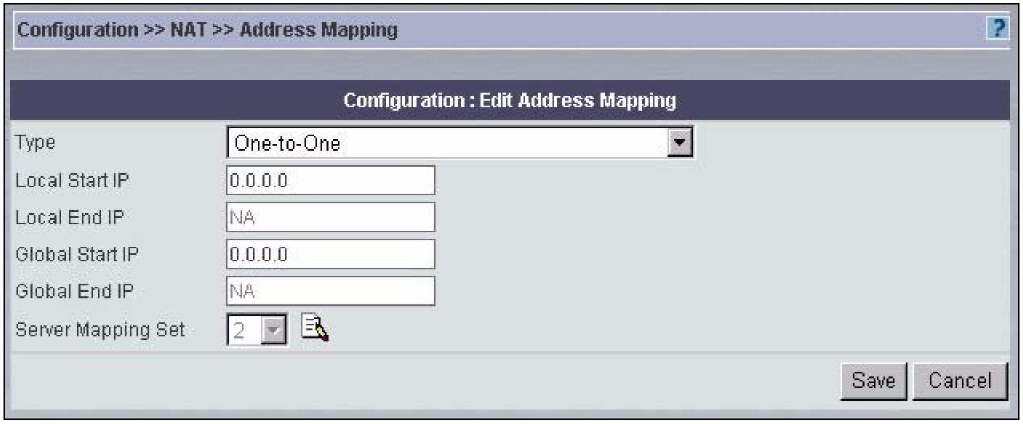
**Table 59** Configuration > NAT > Address Mapping

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the number of an individual entry. You may select a rule to edit by going to the **Edit Address Mapping** screen for that rule. |
| Local Start IP | This refers to the Inside Local Address (ILA), which is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types. |
| Global End IP | This is the ending Inside Global Address (IGA), which is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |
| Type | 1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.<br>2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (in other words, PAT, or port address translation), ZyXEL's Single User Account feature that previous routers supported only.<br>3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One** mode maps each local IP address to unique global IP addresses.<br>5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Delete | Select the radio button next to a rule and click **Delete** to delete the address-mapping rule. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click **Cancel** to close this screen without applying any changes. |

## 10.3.1 Edit Address Mapping Rule

Use this screen to edit an address mapping rule on the device. To open this screen, click **Configuration** > **NAT**, select **Full Feature**, click **Edit**, select **Address Mapping**, and click the **Index** field for the rule.

**Figure 83** Configuration > NAT > Address Mapping > Edit



Configuration >> NAT >> Address Mapping

Configuration : Edit Address Mapping

| | |
|---|---|
| Type | One-to-One |
| Local Start IP | 0.0.0.0 |
| Local End IP | NA |
| Global Start IP | 0.0.0.0 |
| Global End IP | NA |
| Server Mapping Set | 2 |

The following table describes the labels in this screen.

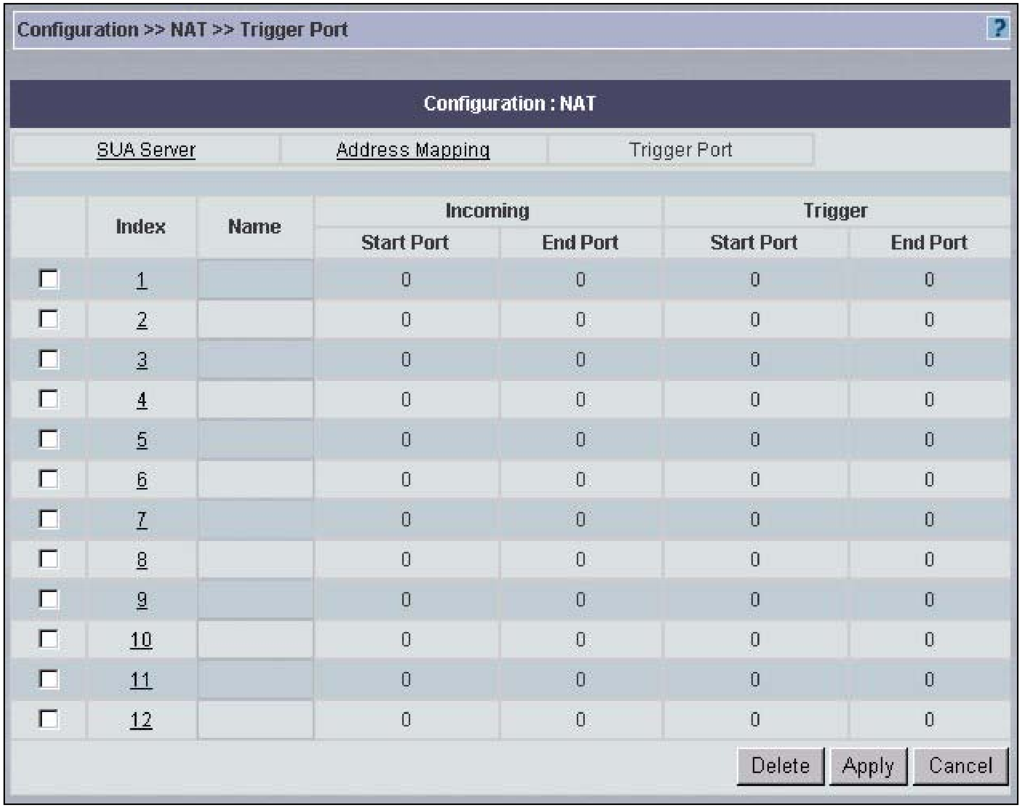
**Table 60** Configuration > NAT > Address Mapping > Edit

| LABEL | DESCRIPTION |
|---|---|
| Type | When you select **Type** you can choose a server mapping set. Choose the port mapping type from one of the following.<br>1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.<br>2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (in other words, PAT, or port address translation), ZyXEL's Single User Account feature.<br>3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses.<br>5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address.<br>This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |
| Server Mapping Set | This field is only available in the device and when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server set from the **NAT > Address Mapping** screen.<br>Click the link to go to the **NAT > SUA Server** screen to edit a server set that you have selected in the **Server Mapping Set** field. |
| Save | Click **Save** to save your changes back to the device. |
| Cancel | Click **Cancel** to return to the previous screen. |

## 10.4 Trigger Port

Use this screen to configure trigger port forwarding on the device. To open this screen, click **Configuration > NAT**, select **SUA Only** or **Full Feature**, click **Edit**, and select **Trigger Port**.

**Figure 84** Configuration > NAT > Trigger Port



| | Index | Name | Incoming | | Trigger | |
|---|---|---|---|---|---|---|
| | | | Start Port | End Port | Start Port | End Port |
| □ | 1 | | 0 | 0 | 0 | 0 |
| □ | 2 | | 0 | 0 | 0 | 0 |
| □ | 3 | | 0 | 0 | 0 | 0 |
| □ | 4 | | 0 | 0 | 0 | 0 |
| □ | 5 | | 0 | 0 | 0 | 0 |
| □ | 6 | | 0 | 0 | 0 | 0 |
| □ | 7 | | 0 | 0 | 0 | 0 |
| □ | 8 | | 0 | 0 | 0 | 0 |
| □ | 9 | | 0 | 0 | 0 | 0 |
| □ | 10 | | 0 | 0 | 0 | 0 |
| □ | 11 | | 0 | 0 | 0 | 0 |
| □ | 12 | | 0 | 0 | 0 | 0 |

The following table describes the labels in this screen.

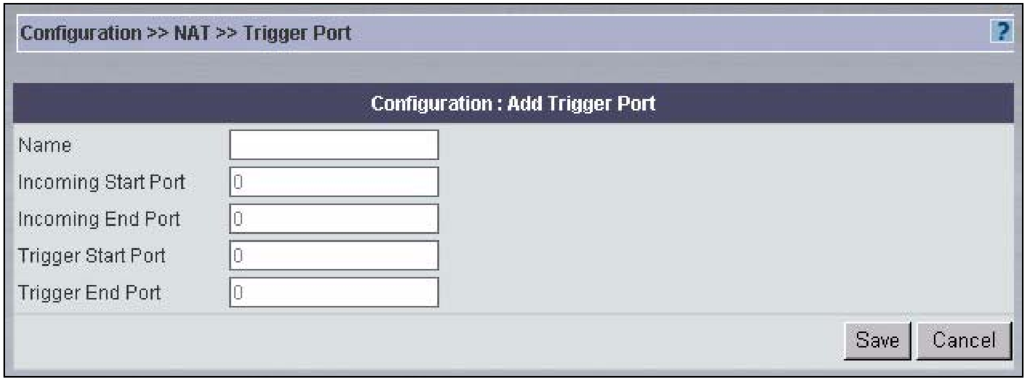
**Table 61** Configuration > NAT > Trigger Port

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the number of an individual entry. You may select a rule to edit. |
| Name | This field displays a unique name (up to 15 characters) for identification purposes. |
| Incoming | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Start Port | This field displays a port number or the starting port number in a range of port numbers. |
| End Port | This field displays a port number or the ending port number in a range of port numbers. |
| Trigger | The trigger port is a port (or a range of ports) that causes (or triggers) the device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Start Port | This field displays a port number or the starting port number in a range of port numbers. |
| End Port | This field displays a port number or the ending port number in a range of port numbers. |
| Delete | Select a rule and then click **Delete** to erase it. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | This field displays a port number or the ending port number in a range of port numbers. |

### 10.4.1 Edit Trigger Port Rule

Use this screen to edit a trigger port forwarding rule on the device. To open this screen, click **Configuration** > **NAT**, select **SUA Only** or **Full Feature**, click **Edit**, select **Trigger Port**, and click the **Index** field for the rule.

**Figure 85** Configuration > NAT > Trigger Port > Edit



Configuration >> NAT >> Trigger Port

Configuration : Add Trigger Port

| | |
|---|---|
| Name | |
| Incoming Start Port | 0 |
| Incoming End Port | 0 |
| Trigger Start Port | 0 |
| Trigger End Port | 0 |

The following table describes the labels in this screen.

**Table 62** Configuration > NAT > Trigger Port > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces. |
| | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Incoming Start Port | Type a port number or the starting port number in a range of port numbers. |
| Incoming End Port | Type a port number or the ending port number in a range of port numbers. |
| | The trigger port is a port (or a range of ports) that causes (or triggers) the device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Trigger Start Port | Type a port number or the starting port number in a range of port numbers. |
| Trigger End Port | Type a port number or the ending port number in a range of port numbers. |
| Save | Click **Save** to save your changes back to the device. |
| Cancel | Click **Cancel** to return to the previous screen. |

# 11

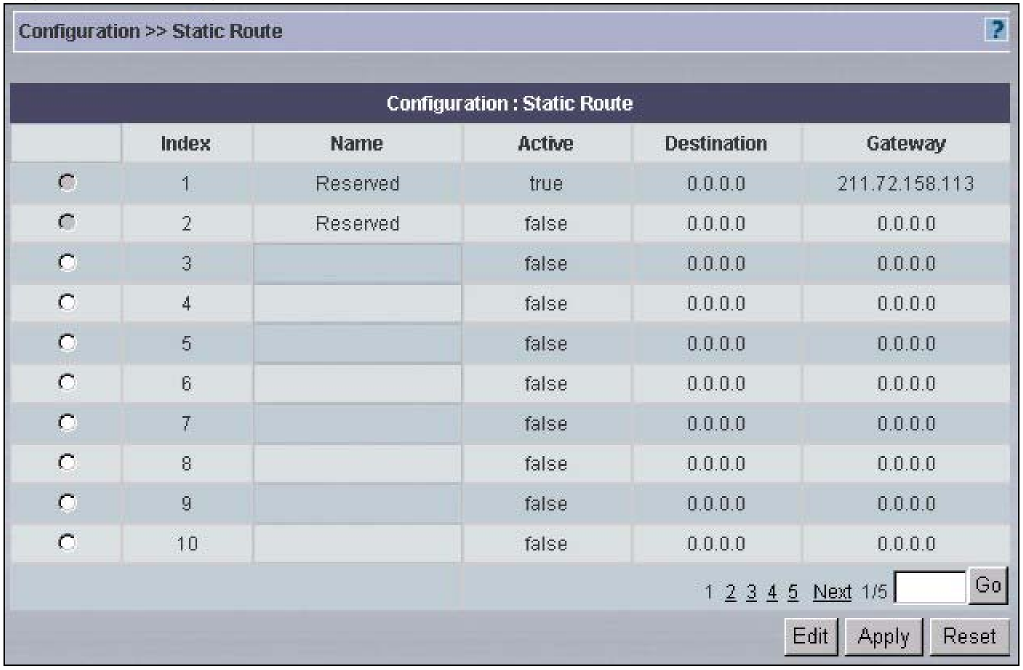
# Configuration > Static Route

This section shows you how to configure the **Static Route** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 11.1 Static Route

Use this screen to tell the device about networks that are not directly connected to the device. To open this screen, click **Configuration** > **Static Route**.

**Figure 86** Configuration > Static Route



Configuration >> Static Route

Configuration : Static Route

| | Index | Name | Active | Destination | Gateway |
|---|---|---|---|---|---|
| ○ | 1 | Reserved | true | 0.0.0.0 | 211.72.158.113 |
| ○ | 2 | Reserved | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 3 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 4 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 5 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 6 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 7 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 8 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 9 | | false | 0.0.0.0 | 0.0.0.0 |
| ○ | 10 | | false | 0.0.0.0 | 0.0.0.0 |

The following table describes the labels in this screen.

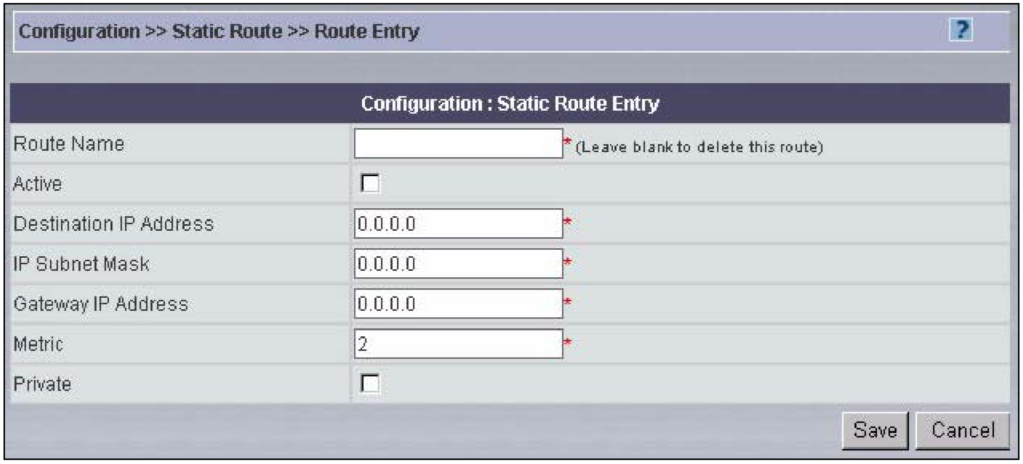
**Table 63** Configuration > Static Route

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the number of an individual entry. You may select a rule to edit or delete it. |
| Name | This is the name that describes or identifies this route. To delete a static route, erase the name and then click apply. |
| Active | This field shows whether this static route is active or not. |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Gateway | This is the IP address of the gateway. The gateway is an immediate neighbor of the device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as the device; over the WAN, the gateway must be the IP address of one of the remote nodes. |
| Edit | Click a static route index number and then click **Edit** to set up a static route on the device. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.1.1 Edit Static Route

Use this screen to edit a static route in the device. To open this screen, click **Configuration** > **Static Route**, select a static route, and click **Edit**.

**Figure 87** Configuration > Static Route > Edit



Configuration >> Static Route >> Route Entry

Configuration : Static Route Entry

| | |
|---|---|
| Route Name | * (Leave blank to delete this route) |
| Active | □ |
| Destination IP Address | 0.0.0.0 * |
| IP Subnet Mask | 0.0.0.0 * |
| Gateway IP Address | 0.0.0.0 * |
| Metric | 2 * |
| Private | □ |

The following table describes the labels in this screen.

**Table 64** Configuration > Static Route > Edit

| LABEL | DESCRIPTION |
|---|---|
| Route Name | Enter the name of the IP static route. Leave this field blank to delete this static route. |
| Active | This check box allows you to activate/deactivate this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |

**Table 64** Configuration > Static Route > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway IP Address | Enter the IP address of the gateway. The gateway is an immediate neighbor of the device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as the device; over the WAN, the gateway must be the IP address of one of the Remote Nodes. |
| Metric | Metric represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number. |
| Private | This parameter determines if the device will include this route to a remote node in its RIP broadcasts.<br>Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts. |
| Save | Click **Save** to save your changes back to the device. |
| Cancel | Click **Cancel** to return to the previous screen. |

# 12

# Configuration > VPN

This section shows you how to configure the **VPN** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

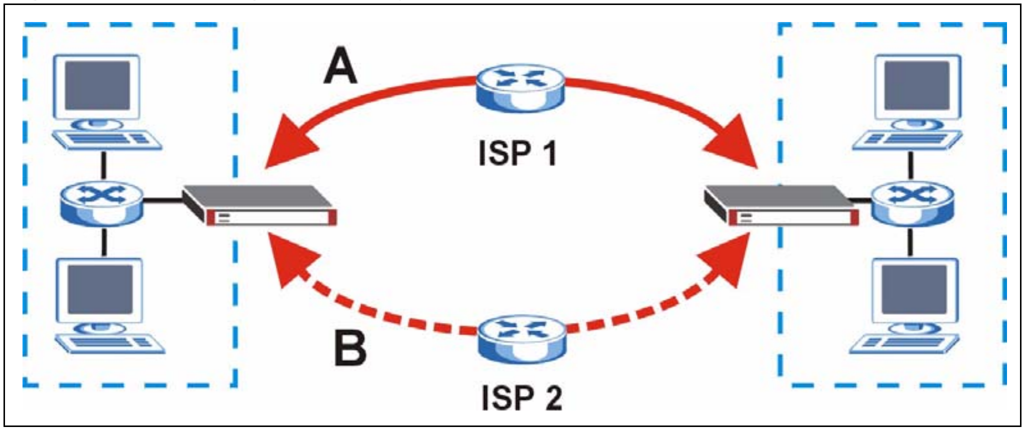
There are two sets of **VPN** screens, VPN version 1.0 and VPN version 1.1. The version depends on the device's type and firmware version.

## 12.1 IPSec High Availability

IPSec high availability (also known as VPN high availability) allows you to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down.

In the following figure, if the primary VPN tunnel (A) goes down, the device uses the redundant VPN tunnel (B).

**Figure 88** IPSec High Availability



When setting up a IPSec high availability VPN tunnel, the remote IPSec router:

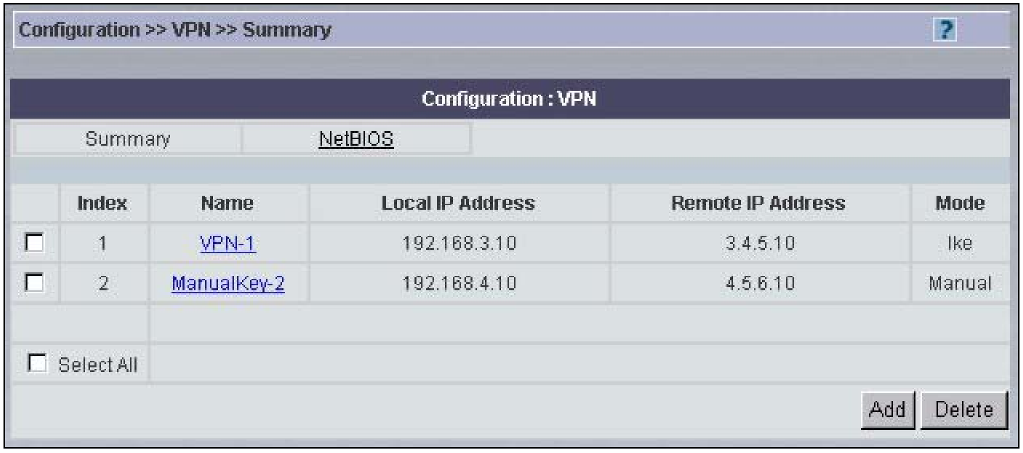
- Must have multiple WAN connections
- Only needs the configure one corresponding IPSec rule
- Should only have IPSec high availability settings in its corresponding IPSec rule if your device has multiple WAN connections
- Should ideally identify itself by a domain name or dynamic domain name (it must otherwise have My Address set to 0.0.0.0)
- Should use a WAN connectivity check to this device's WAN IP address

If the remote IPSec router is not a device, you may also want to avoid setting the IPSec rule to nailed up.

## 12.2 VPN Tunnel Summary (VPN version 1.0)

Select a device and then click **Configuration** > **VPN**.

**Figure 89** Configuration > VPN > Summary



| | Index | Name | Local IP Address | Remote IP Address | Mode |
|---|---|---|---|---|---|
| □ | 1 | VPN-1 | 192.168.3.10 | 3.4.5.10 | Ike |
| □ | 2 | ManualKey-2 | 192.168.4.10 | 4.5.6.10 | Manual |

□ Select All

The following table describes the labels in this screen.

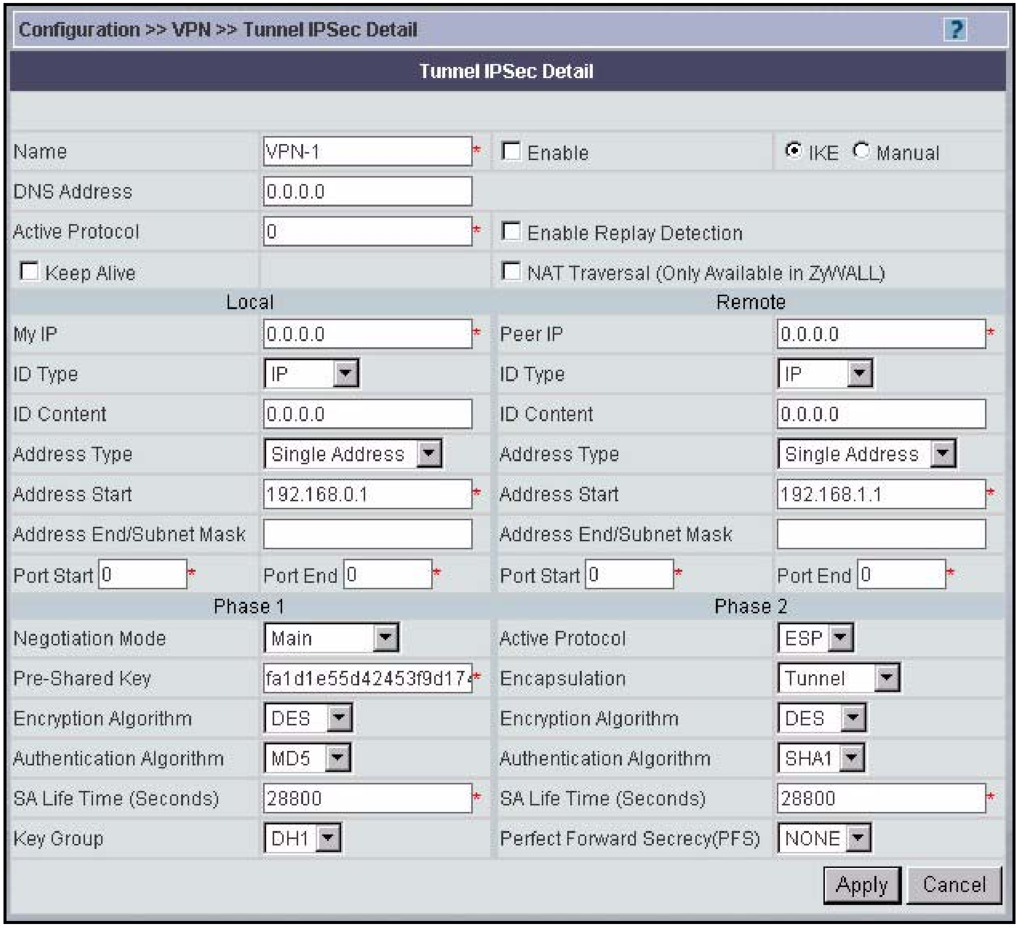
**Table 65** Configuration > VPN > Summary

| LABEL | Description |
|---|---|
| Index | This is the VPN policy index number. |
| Name | This field displays the identification name for this VPN policy. |
| Local IP Address | This field displays the IP address(es) of the network behind the device. |
| Remote IP Address | This field displays the IP address(es) of the network behind the remote device. |
| Mode | This field displays whether this VPN tunnel uses an IKE SA (**Ike**) or manual keys (**Manual**). |
| Select All | Select this to select all VPN tunnels. |
| Add | Click **Add** to create a new VPN tunnel or to modify an existing one. |
| Delete | Select a rule and then click **Delete** to erase it. All rules can be deleted if you check the **Select All** check box and click **Delete**. |

### 12.2.1 Add a VPN Tunnel

You can create a single-ended VPN tunnel using Vantage CNM by selecting **N/A** from the **Remote Device** field. This allows you to create a VPN tunnel between a device and another IPSec router. You must make sure the remote IPSec router VPN settings correspond to the device VPN settings.

**Figure 90** Configuration > VPN > Summary > Add/Edit



Configuration >> VPN >> Tunnel IPSec Detail

Tunnel IPSec Detail

| | | | |
|---|---|---|---|
| Name | VPN-1 * | □ Enable | ● IKE ○ Manual |
| DNS Address | 0.0.0.0 | | |
| Active Protocol | 0 * | □ Enable Replay Detection | |
| □ Keep Alive | | □ NAT Traversal (Only Available in ZyWALL) | |
| Local | | Remote | |
| My IP | 0.0.0.0 * | Peer IP | 0.0.0.0 * |
| ID Type | IP | ID Type | IP |
| ID Content | 0.0.0.0 | ID Content | 0.0.0.0 |
| Address Type | Single Address | Address Type | Single Address |
| Address Start | 192.168.0.1 * | Address Start | 192.168.1.1 * |
| Address End/Subnet Mask | | Address End/Subnet Mask | |
| Port Start 0 * | Port End 0 * | Port Start 0 * | Port End 0 * |
| Phase 1 | | Phase 2 | |
| Negotiation Mode | Main | Active Protocol | ESP |
| Pre-Shared Key | fa1d1e55d42453f9d17 * | Encapsulation | Tunnel |
| Encryption Algorithm | DES | Encryption Algorithm | DES |
| Authentication Algorithm | MD5 | Authentication Algorithm | SHA1 |
| SA Life Time (Seconds) | 28800 * | SA Life Time (Seconds) | 28800 * |
| Key Group | DH1 | Perfect Forward Secrecy(PFS) | NONE |

The following table describes the labels in this screen.

**Table 66** Configuration > VPN > Summary > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | This is a VPN name for identification purposes. |
| Enable | Select this check box to make the VPN rule active. |
| IKE/Manual | Select either **IKE** or **Manual** to manage encryption keys. If you select the **IKE** method, you must configure the IKE fields. **Manual** is useful for troubleshooting if you have problems using **IKE** key management. |
| DNS Address | Type a domain name (up to 31 characters) by which to identify the local or remote IPSec router. |
| Active Protocol | Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol. |
| Enable Replay Detection | As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box. |

**Table 66** Configuration > VPN > Summary > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Keep Alive | When you initiate an IPSec tunnel with keep alive enabled, the device automatically renegotiates the tunnel when the IPSec SA lifetime period expires. In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both IPSec routers must have a compatible keep alive feature enabled in order for this feature to work.<br>If the device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the device. |
| NAT Traversal (Only Available in ZyWALL) | Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.<br>The remote IPSec router must also have NAT traversal enabled.<br>You can use NAT traversal with ESP protocol using Transport or Tunnel mode, but not with AH protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router. |
| Local/Remote | |
| My IP | This is the IP address of the local and remote computer(s) of the VPN tunnel. |
| Peer IP | Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the device automatically use the address in the **Secure Gateway** field. |
| ID Type | Select **IP** to identify this device by its IP address.<br>Select **DNS** to identify this device by a domain name.<br>Select **E-mail** to identify this device by an e-mail address.<br>You do not configure the local ID type and content when you set **Authentication Method** to **Certificate**. The device takes them from the certificate you select. |
| ID Content | When you select **IP** in the **Local ID Type** field, type the IP address of your computer. The device uses the IP address in the **My IP Address** field if you configure the local **Content** field to **0.0.0.0** or leave it blank.<br>It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations.<br>• When there is a NAT router between the two IPSec routers.<br>• When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.<br>• With **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this device. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. |
| Address Type | This is the IP address(es) of computer(s) behind the device or the remote device.<br>The same (static) IP address is displayed twice in the **Address Start** and **Address End** fields when the **Address Type** field is configured to **Single**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Address Type** is configured to **Range**.<br>A (static) IP address and a subnet mask are displayed when the **Address** Type field is configured to Subnet.<br>These addresses cannot be automatically generated by Vantage CNM. |
| Address Start | Enter the beginning IP address of the computers behind the device. |

**Table 66** Configuration > VPN > Summary > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Address End | Enter the ending IP address of the computers behind the device. |
| Port Start | **0** is the default and signifies any port.<br>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3<br>Type a port number from 0 to 65535 for the starting port in a range. |
| Port End | Type the same port number as above to specify a single port. Type a port number greater than the start port number to specify the end port in a port range. |
| Phase 1 | There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec. |
| Negotiation Mode | Select either **Main** or **Aggressive**. Aggressive mode is quicker than Main mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication. |
| Pre-Shared key | A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called pre-shared because you have to share it with another party before you can communicate with them over a secure connection. Gateways authenticate an IKE VPN session by matching pre-shared keys. Enter from 8 up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Multiple SAs connecting through a secure gateway must have the same pre-shared key. |
| Encryption Algorithm | Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency. |
| Authentication Algorithm | The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the AH and ESP protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data. |
| SA Life Time (Seconds) | Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Key Group | Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys.<br>768-bit (Group 1 - DH1) and 1024-bit (Group 2 – DH2) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys. |
| Phase 2 | There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec. |

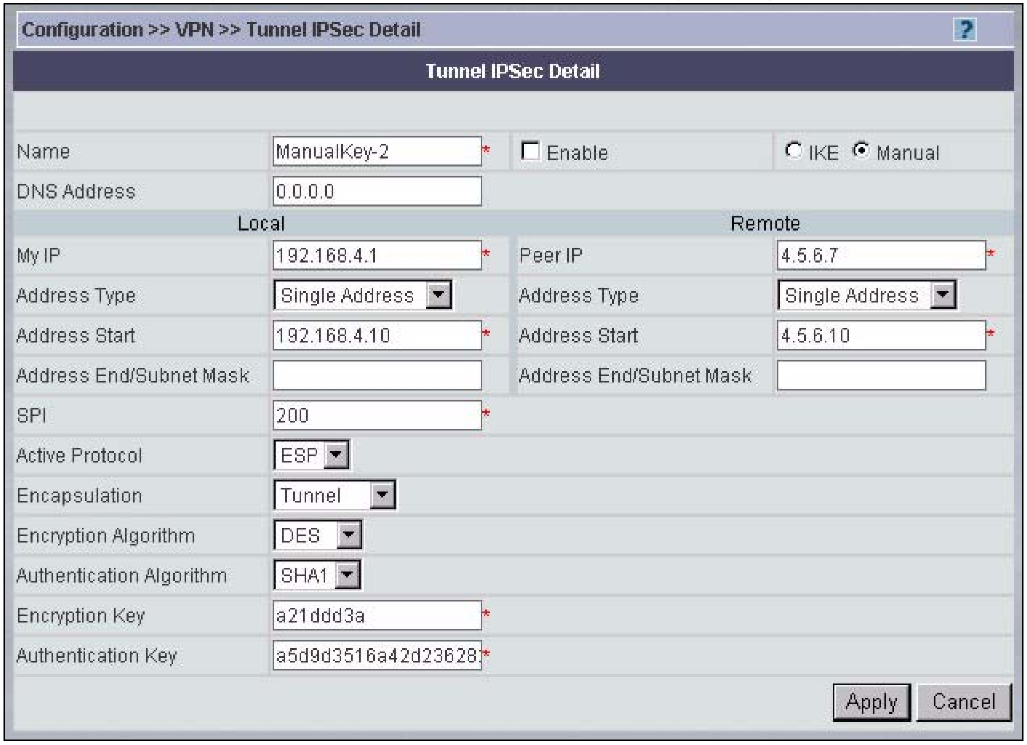
**Table 66** Configuration > VPN > Summary > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active Protocol | The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN.<br>**AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.<br>The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. |
| Encapsulation | In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With ESP, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.<br>With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. **Tunnel** mode encapsulates the entire IP packet to transmit it securely. **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation |
| Encryption Algorithm | Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency. |
| Authentication Algorithm | The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Select **MD5** for minimal security and **SHA-1** for maximum security.<br>**MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data. |
| SA Life Time (Seconds) | Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Perfect Forward Secrecy (PFS) | Choose whether to enable Perfect Forward Secrecy (**PFS**) using Diffie-Hellman public-key cryptography. Enabling **PFS** means that the key is transient. A brand new key using a new Diffie-Hellman exchange replaces the key for each new IPSec SA.<br>With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.<br>Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange). |
| Apply | Click **Apply** to apply your changes in this screen. |
| Cancel | Click **Cancel** to close this screen without applying any changes. |

## 12.2.2 Manual VPN Tunnel

Select **Manual** from Figure 90 on page 167 to proceed to the next screen.

**Figure 91** Configuration > VPN > Summary > Add/Edit (Manual)



Configuration >> VPN >> Tunnel IPSec Detail

Tunnel IPSec Detail

| | | | |
|---|---|---|---|
| Name | ManualKey-2 * | □ Enable | ○ IKE ● Manual |
| DNS Address | 0.0.0.0 | | |
| Local | | Remote | |
| My IP | 192.168.4.1 * | Peer IP | 4.5.6.7 * |
| Address Type | Single Address | Address Type | Single Address |
| Address Start | 192.168.4.10 * | Address Start | 4.5.6.10 * |
| Address End/Subnet Mask | | Address End/Subnet Mask | |
| SPI | 200 * | | |
| Active Protocol | ESP | | |
| Encapsulation | Tunnel | | |
| Encryption Algorithm | DES | | |
| Authentication Algorithm | SHA1 | | |
| Encryption Key | a21ddd3a * | | |
| Authentication Key | a5d9d3516a42d23628 * | | |

The following table describes the labels in this screen.

**Table 67** Configuration > VPN > Summary > Add/Edit (Manual)

| LABEL | DESCRIPTION |
|---|---|
| Name | Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the device drops trailing spaces. |
| Enable | Select this check box to activate this VPN policy. |
| IKE / Manual | Select **IKE** or **Manual**. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management. |
| DNS Address | Type a domain name (up to 31 characters) by which to identify the local or remote IPSec router. |
| Local / Remote | Local / Remote IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| My IP | This is the IP address of the local and remote computer(s) of the VPN tunnel. |
| Peer IP | Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the device automatically use the address in the **Secure Gateway** field. |

**Table 67** Configuration > VPN > Summary > Add/Edit (Manual) (continued)

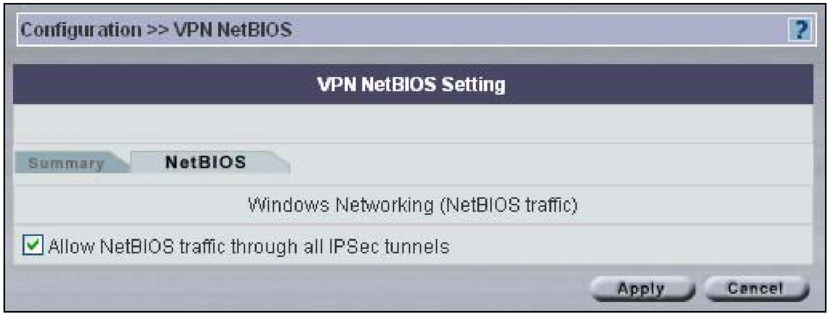
| LABEL | DESCRIPTION |
|---|---|
| Address Start | When the **Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind the device. When the **Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the LAN behind the device. When the **Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind the device. |
| Address End/Subnet Mask | When the **Address Type** field is configured to **Single**, this field is N/A. When the **Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind the device. When the **Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind the device. |
| SPI | Type a number (base 10) from 1 to 999999 for the Security Parameter Index. |
| Active Protocol | Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields.<br>Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field. |
| Encapsulation | Select **Tunnel** mode or **Transport** mode from the drop-down list box. |
| Encryption Algorithm | Select **DES**, **3DES** or **NULL** from the drop-down list box.<br>When you use **DES** or **3DES**, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the messages. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| Authentication Algorithm | When you use **SHA1** or **MD5**, both sender and receiver must know the **Authentication Key**, which can be used to generate and verify a message authentication code. Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| Encryption Key | This field only applies when you select **ESP**. With **DES**, type a unique key 8 ASCII characters long. With **3DES**, type a unique key 24 ASCII characters long. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Authentication Key | Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 12.3 NetBIOS (VPN version 1.0)

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.

Select a device, click **Configuration** > **VPN** > **NetBIOS** to bring up the next screen.

**Figure 92** Configuration > VPN > NetBIOS



Configuration >> VPN NetBIOS

VPN NetBIOS Setting

Windows Networking (NetBIOS traffic)

☑ Allow NetBIOS traffic through all IPSec tunnels

The following table describes the labels in this screen.

**Table 68** Configuration > VPN > NetBIOS

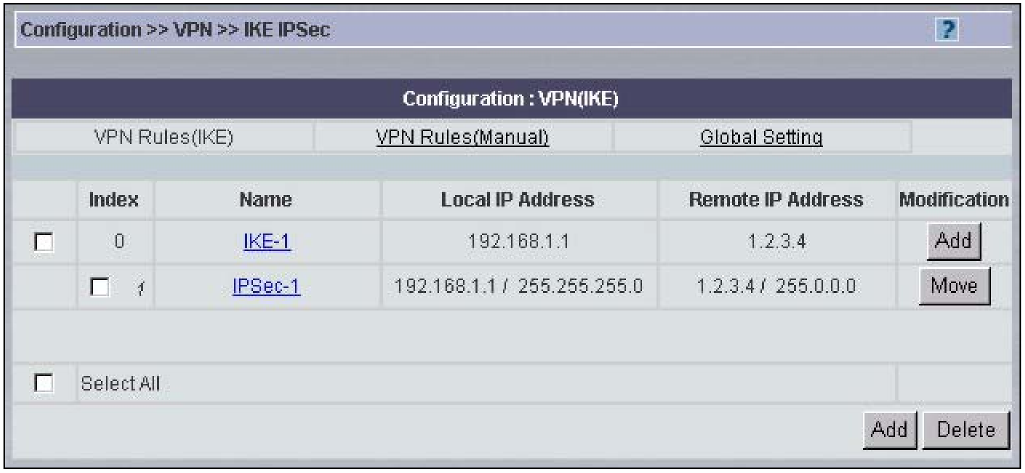
| LABEL | DESCRIPTION |
|---|---|
| Allow NetBIOS traffic through all IPSec tunnels | Select the check box to permit NetBIOS packets through the VPN connection. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 12.4 VPN Rules (IKE) (VPN version 1.1)

Select a device and then click **Configuration** > **VPN**.

This is a read-only menu of your IPSec rule (tunnel). To add an IPSec rule (or gateway policy), click the **Add** button in the **Modification** column. Edit an IPSec rule by clicking the **Name** hyperlink to configure the associated submenus.

**Figure 93** Configuration > VPN > VPN Rules (IKE)



| | Index | Name | Local IP Address | Remote IP Address | Modification |
|---|---|---|---|---|---|
| □ | 0 | IKE-1 | 192.168.1.1 | 1.2.3.4 | Add |
| | □ 1 | IPSec-1 | 192.168.1.1 / 255.255.255.0 | 1.2.3.4 / 255.0.0.0 | Move |
| □ | Select All | | | | |

The following table describes the labels in this screen.

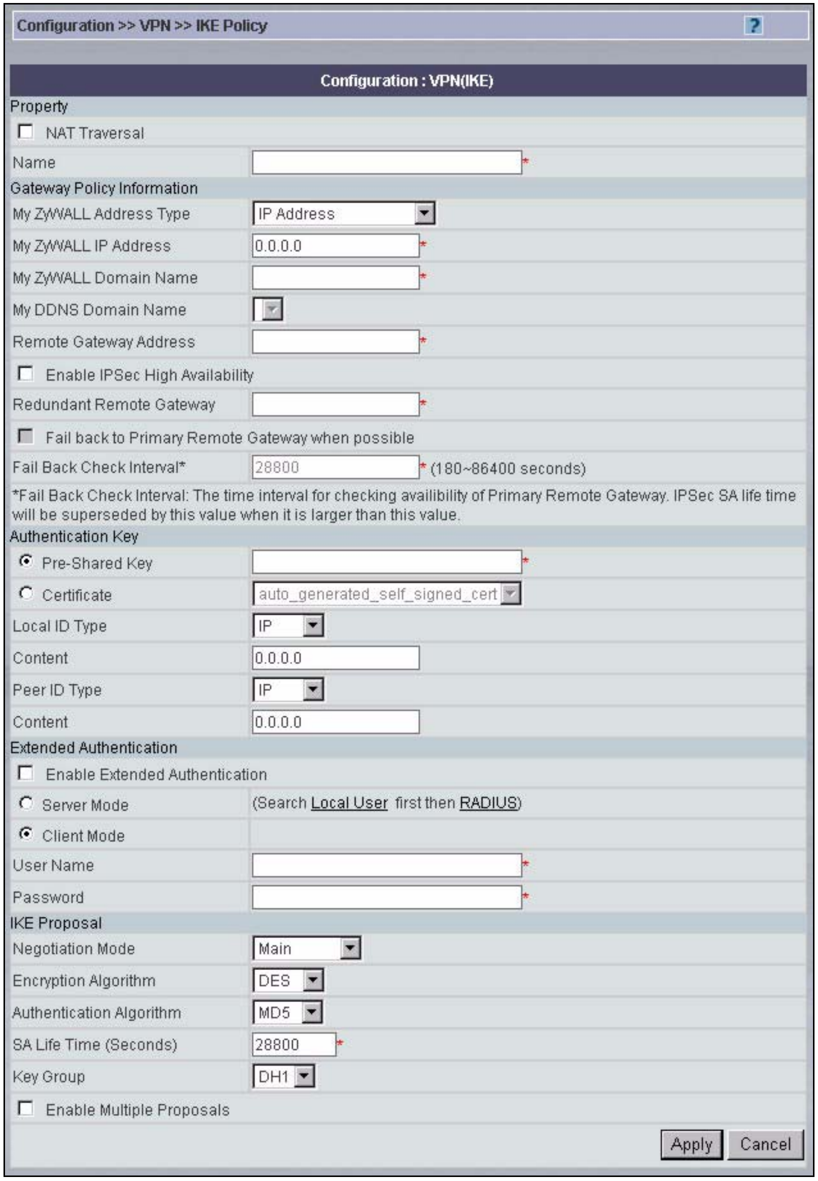
**Table 69** Configuration > VPN > VPN Rules (IKE)

| LABEL | DESCRIPTION |
|---|---|
| Index | This field displays the VPN policy index number. |
| Name | This field identifies a VPN policy gateway. Click the hyperlink to go open a screen where you can edit the gateway policy. |
| Local IP Address | This field displays one or a range of IP address(es) of the computer(s) behind the device. |
| Remote IP Address | This is the WAN IP address of the IPSec router with which you are making the VPN connection. |
| Modification | Click the **Add** button in this field to go to a screen where you can configure an IKE IPSec rule.<br>Click the **Move** button to change the order in which the IPSec rules display. |
| Select All | Select this check box to select the check boxes for all VPN rules. |
| Add | Click the **Add** button to go to a screen where you can configure a VPN gateway policy. |
| Delete | Select a check box(es) next to a rule and click **Delete** to remove a VPN rule(s). |

## 12.4.1 VPN Rules (IKE) > Gateway Policy Add

In the **VPN Rule (IKE)** screen, click the **Add** button to display the **IKE Policy** screen.

**Figure 94** Configuration > VPN > IKE Policy



Configuration >> VPN >> IKE Policy

Configuration : VPN(IKE)

Property

□ NAT Traversal

| | |
|---|---|
| Name | * |

Gateway Policy Information

| | |
|---|---|
| My ZyWALL Address Type | IP Address |
| My ZyWALL IP Address | 0.0.0.0 * |
| My ZyWALL Domain Name | * |
| My DDNS Domain Name | |
| Remote Gateway Address | * |

□ Enable IPSec High Availability

| | |
|---|---|
| Redundant Remote Gateway | * |

□ Fail back to Primary Remote Gateway when possible

| | |
|---|---|
| Fail Back Check Interval* | 28800 * (180~86400 seconds) |

*Fail Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

| | |
|---|---|
| ● Pre-Shared Key | * |
| ○ Certificate | auto_generated_self_signed_cert |
| Local ID Type | IP |
| Content | 0.0.0.0 |
| Peer ID Type | IP |
| Content | 0.0.0.0 |

Extended Authentication

□ Enable Extended Authentication

| | |
|---|---|
| ○ Server Mode | (Search Local User first then RADIUS) |
| ● Client Mode | |
| User Name | * |
| Password | * |

IKE Proposal

| | |
|---|---|
| Negotiation Mode | Main |
| Encryption Algorithm | DES |
| Authentication Algorithm | MD5 |
| SA Life Time (Seconds) | 28800 * |
| Key Group | DH1 |

□ Enable Multiple Proposals

The following table describes the labels in this screen.

**Table 70** Configuration > VPN > IKE Policy

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| NAT Traversal | Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.<br>Note: The remote IPSec router must also have NAT traversal enabled.<br>You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router. |
| Name | Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the device drops trailing spaces. |
| Gateway Policy Information | |
| My ZyWALL Address Type | This field specifies how the IP address of the device is specified.<br>**IP Address**: The device's IP address is a static IP address.<br>**Domain Name**: The device's IP address is the IP address mapped to a specified domain name.<br>**DDNS Domain Name**: The device's IP address is the IP address mapped to a specified DDNS domain name.<br>The VPN tunnel has to be rebuilt if the device's IP address changes after setup. |
| My ZyWALL IP Address | This field is enabled if **My ZyWALL Address Type** is **IP Address**.<br>Enter the device's static WAN IP address or leave the field set to 0.0.0.0. The following applies if this field is configured as **0.0.0.0**:<br>• When the WAN port operation mode is set to **Active/Passive**, the device uses the IP address (static or dynamic) of the WAN port that is in use.<br>• When the WAN port operation mode is set to **Active/Active**, the device uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the device uses the IP address of the other WAN port.<br>• If both WAN connections go down, the device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect. |
| My ZyWALL Domain Name | This field is enabled if **My ZyWALL Address Type** is **IP Address**.<br>Enter the domain name associated with the device in the VPN tunnel. |
| My DDNS Domain Name | This field is enabled if **My ZyWALL Address Type** is **IP Address**.<br>Select the DDNS domain name associated with the device in the VPN tunnel. Use the **DDNS** screens to configure these domain names. |

**Table 70** Configuration > VPN > IKE Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Remote Gateway Address | Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.<br>In order to have more than one active rule with the **Remote Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.<br>If you configure an active rule with **0.0.0.0** in the **Remote Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Remote Gateway Address** field set to **0.0.0.0**. |
| Enable IPSec High Availability | Turn on the high availability feature to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down. The remote IPSec router must have a second WAN connection in order for you to use this.<br>To use this, you must identify both the primary and the redundant remote IPSec routers by WAN IP address or domain name (you cannot set either to **0.0.0.0**). |
| Redundant Remote Gateway | Type the WAN IP address or the domain name (up to 31 characters) of the backup IPSec router to use when the device cannot not connect to the primary remote gateway. |
| Fail back to Primary Remote Gateway when possible | Select this to have the device change back to using the primary remote gateway if the connection becomes available again. |
| Fail Back Check Interval* | Set how often the device should check the connection to the primary remote gateway while connected to the redundant remote gateway.<br>Each gateway policy uses one or more network policies. If the fall back check interval is shorter than a network policy's SA life time, the fall back check interval is used as the check interval and network policy SA life time. If the fall back check interval is longer than a network policy's SA life time, the SA lifetime is used as the check interval and network policy SA life time. |
| Authentication Key | |
| Pre-Shared Key | Select the **Pre-Shared Key** radio button and type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.<br>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends. |
| Certificate | Select the **Certificate** radio button to identify the device by a certificate.<br>Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen where you can view the device's list of certificates. |
| Local ID Type | Select **IP** to identify this device by its IP address.<br>Select **DNS** to identify this device by a domain name.<br>Select **E-mail** to identify this device by an e-mail address.<br>You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The device takes them from the certificate you select. |

**Table 70** Configuration > VPN > IKE Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Content | When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The device automatically uses the IP address in the **My ZyWALL** field (refer to the **My ZyWALL** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.<br>It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations.<br>• When there is a NAT router between the two IPSec routers.<br>• When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.<br>When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this device in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. |
| Peer ID Type | Select from the following when you set **Authentication Key** to **Pre-shared Key**.<br>• Select **IP** to identify the remote IPSec router by its IP address.<br>• Select **DNS** to identify the remote IPSec router by a domain name.<br>• Select **E-mail** to identify the remote IPSec router by an e-mail address.<br>Select from the following when you set **Authentication Key** to **Certificate**.<br>• Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection.<br>• Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection.<br>• Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection.<br>• Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection.<br>• Select **Any** to have the device not check the remote IPSec router's ID. |

**Table 70** Configuration > VPN > IKE Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Content | The configuration of the peer content depends on the peer ID type.<br>Do the following when you set **Authentication Key** to **Pre-shared Key**.<br>• For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the device will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description).<br>• For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.<br>It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations:<br>• When there is a NAT router between the two IPSec routers.<br>• When you want the device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.<br>Do the following when you set **Authentication Key** to **Certificate**.<br>• For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the device will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description).<br>• For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection.<br>• For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces.<br>• For **Any**, the peer **Content** field is not available.<br>• Regardless of how you configure the **ID Type** and **Content** fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules. |
| Extended Authentication | |
| Enable Extended Authentication | Select this check box to activate extended authentication. |
| Server Mode | Select **Server Mode** to have this device authenticate extended authentication clients that request this VPN connection.<br>You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server.<br>Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of user names and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the device to check an external RADIUS server.<br>During authentication, if the device (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server. |
| Client Mode | Select **Client Mode** to have your device use a username and password when initiating this VPN connection to the extended authentication server device. Only a VPN extended authentication client can initiate this VPN connection. |
| User Name | Enter a user name for your device to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode. |
| Password | Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. |

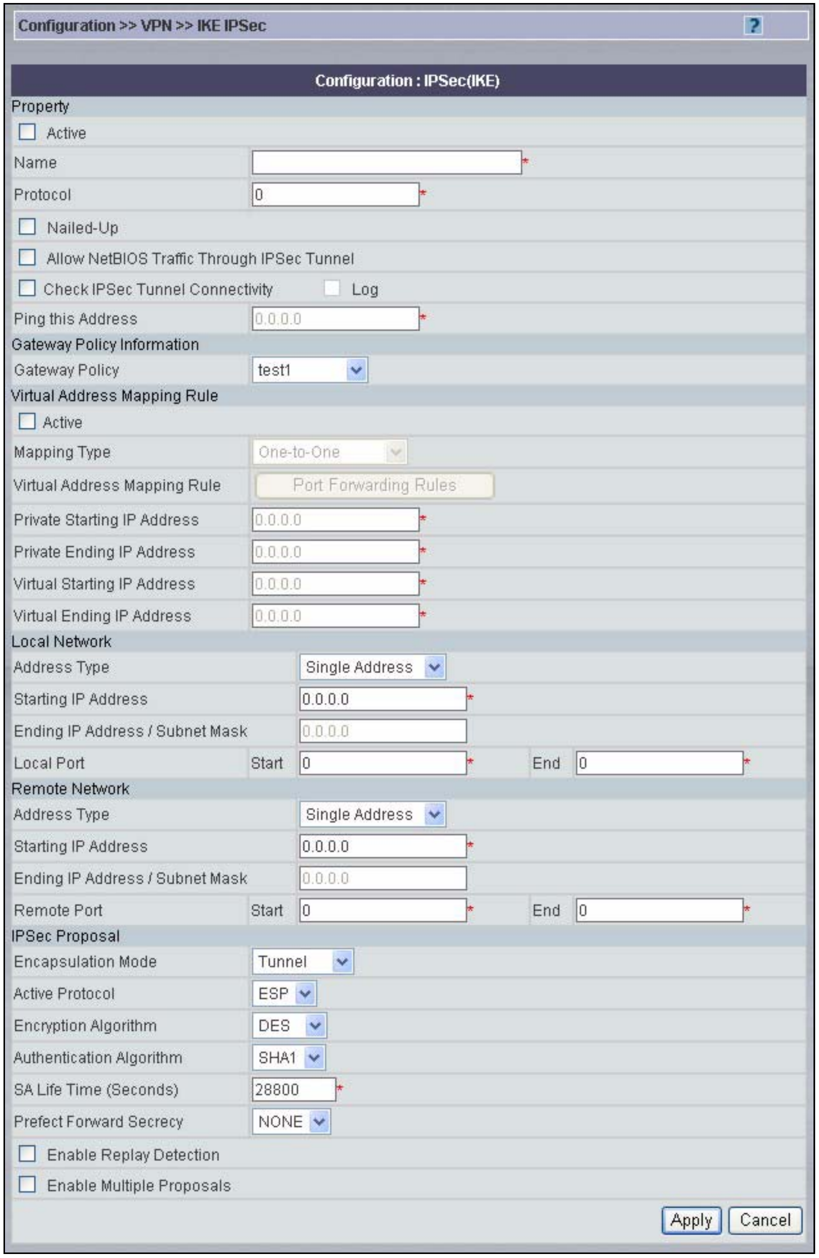
**Table 70** Configuration > VPN > IKE Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| IKE Proposal | |
| Negotiation Mode | Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | Select **DES**, **3DES** or **AES** from the drop-down list box.<br>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**. |
| Authentication Algorithm | Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days).<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Key Group | You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. |
| Enable Multiple Proposals | Select this check box to allow the device to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA.<br>When you enable multiple proposals, the device allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule.<br>Clear this check box to have the device use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 12.4.2 VPN Rules (IKE) > Network Policy Edit

In the **VPN Rule (IKE)** screen, click the **Add** button in the **Modification** field or a **Name** hyperlink to display the **IKE IPSec** screen.

**Figure 95** Configuration > VPN > IKE IPSec



Configuration >> VPN >> IKE IPSec

Configuration : IPSec(IKE)

Property

□ Active

Name: *

Protocol: 0 *

□ Nailed-Up

□ Allow NetBIOS Traffic Through IPSec Tunnel

□ Check IPSec Tunnel Connectivity □ Log

Ping this Address: 0.0.0.0 *

Gateway Policy Information

Gateway Policy: test1

Virtual Address Mapping Rule

□ Active

Mapping Type: One-to-One

Virtual Address Mapping Rule: Port Forwarding Rules

Private Starting IP Address: 0.0.0.0 *

Private Ending IP Address: 0.0.0.0 *

Virtual Starting IP Address: 0.0.0.0 *

Virtual Ending IP Address: 0.0.0.0 *

Local Network

Address Type: Single Address

Starting IP Address: 0.0.0.0 *

Ending IP Address / Subnet Mask: 0.0.0.0

Local Port: Start 0 * End 0 *

Remote Network

Address Type: Single Address

Starting IP Address: 0.0.0.0 *

Ending IP Address / Subnet Mask: 0.0.0.0

Remote Port: Start 0 * End 0 *

IPSec Proposal

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800 *

Prefect Forward Secrecy: NONE

□ Enable Replay Detection

□ Enable Multiple Proposals

The following table describes the labels in this screen.

**Table 71** Configuration > VPN > IKE IPSec

| LABEL | DESCRIPTION |
|---|---|
| Active | If the **Active** check box is selected, packets for the tunnel trigger the device to build the tunnel.<br>Clear the **Active** check box to turn the network policy off. The device does not apply the policy. Packets for the tunnel do not trigger the tunnel.<br>If you clear the **Active** check box while the tunnel is up (and click **Apply**), you turn off the network policy and the tunnel goes down. |
| Name | Type a name to identify this VPN network policy. You may use any character, including spaces, but the device drops trailing spaces. |

**Table 71** Configuration > VPN > IKE IPSec (continued)

| LABEL | DESCRIPTION |
|---|---|
| Protocol | Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol. |
| Nailed-Up | Select this check box to turn on the nailed up feature for this SA.<br>Turn on nailed up to have the device automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The device also reinitiates the SA when it restarts.<br>The device also rebuilds the tunnel if it was disconnected due to the output or input idle timer. |
| Allow NetBIOS Traffic Through IPSec Tunnel | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.<br>Select this check box to send NetBIOS packets through the VPN connection. |
| Check IPSec Tunnel Connectivity | Select the check box and configure an IP address in the **Ping this Address** field to have the device periodically test the VPN tunnel to the remote IPSec router.<br>The device pings the IP address every minute. The device starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires, the device disconnects the VPN tunnel. |
| Log | Select this check box to set the device to create logs when it cannot ping the remote device. |
| Ping this Address | If you select **Check IPSec Tunnel Connectivity**, enter the IP address of a computer at the remote IPSec network. The computer's IP address must be in this IP policy's remote range (see the **Remote Network** fields). |
| Gateway Policy Information | |
| Gateway Policy | Select the gateway policy with which you want to use the VPN policy. |
| Virtual Address Mapping Rule | Virtual address mapping over VPN is available with the routing and zero configuration modes. |
| Active | Enable this feature to have the device use virtual (translated) IP addresses for the local network for the VPN connection. You do not configure the **Local Network** fields when you enable virtual address mapping.<br>Virtual address mapping allows local and remote networks to have overlapping IP addresses. Virtual address mapping (NAT over IPSec) translates the source IP addresses of computers on your local network to other (virtual) IP addresses before sending the packets to the remote IPSec router. This translation hides the source IP addresses of computers in the local network. |
| Mapping Type | Select **One-to-One** to translate a single (static) IP address on your LAN to a single virtual IP address.<br>Select **Many-to-One** to translate a range of (static) IP addresses on your LAN to a single virtual IP address. Many-to-one rules are for traffic going out from your LAN, through the VPN tunnel, to the remote network. Use port forwarding rules to allow incoming traffic from the remote network.<br>Select **Many One-to-One** to translate a range of (static) IP addresses on your LAN to a range of virtual IP addresses. |
| Virtual Address Mapping Rule | If you are configuring a **Many-to-One** rule, click this button to go to a screen where you can configure port forwarding for your VPN tunnels. The VPN network policy port forwarding rules let the device forward traffic coming in through the VPN tunnel to the appropriate IP address. |

**Table 71** Configuration > VPN > IKE IPSec (continued)

| LABEL | DESCRIPTION |
|---|---|
| Private Starting IP Address | Specify the IP addresses of the devices behind the device that can use the VPN tunnel.<br>When you select **One-to-One** in the **Type** field, enter the (static) IP address of a computer on the LAN behind your device.<br>When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the beginning (static) IP address in a range of computers on the LAN behind your device. |
| Private Ending IP Address | When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the ending (static) IP address in a range of computers on the LAN behind your device. |
| Virtual Starting IP Address | Enter the (static) IP addresses that represent the translated private IP addresses. These must correspond to the remote IPSec router's configured remote IP addresses.<br>When you select **One-to-One** or **Many-to-One** in the **Type** field, enter an IP address as the translated IP address. Many-to-one rules are only for traffic going to the remote network. Use port forwarding rules to allow incoming traffic from the remote network.<br>When you select **Many One-to-One** in the **Type** field, enter the beginning IP address of a range of translated IP addresses. |
| Virtual Ending IP Address | When you select **Many One-to-One** in the **Type** field, enter the ending (static) IP address of a range of translated IP addresses.<br>The size of the private address range must be equal to the size of the translated virtual address range. |
| Local Network | Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your device. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your device. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your device. |
| Ending IP Address/ Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your device. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your device. |
| Local Port | 0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| Remote Network | Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |

**Table 71** Configuration > VPN > IKE IPSec (continued)

| LABEL | DESCRIPTION |
|---|---|
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/ Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router. |
| Remote Port | 0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| IPSec Proposal | |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode. |
| Active Protocol | Select the security protocols used for an SA.<br>Both **AH** and **ESP** increase the device's processing requirements and communications latency (delay). |
| Encryption Algorithm | When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| SA Life Time (Seconds) | Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Perfect Forward Secret (PFS) | Perfect Forward Secret (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure.<br>Select **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower). |
| Enable Replay Detection | As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box. |

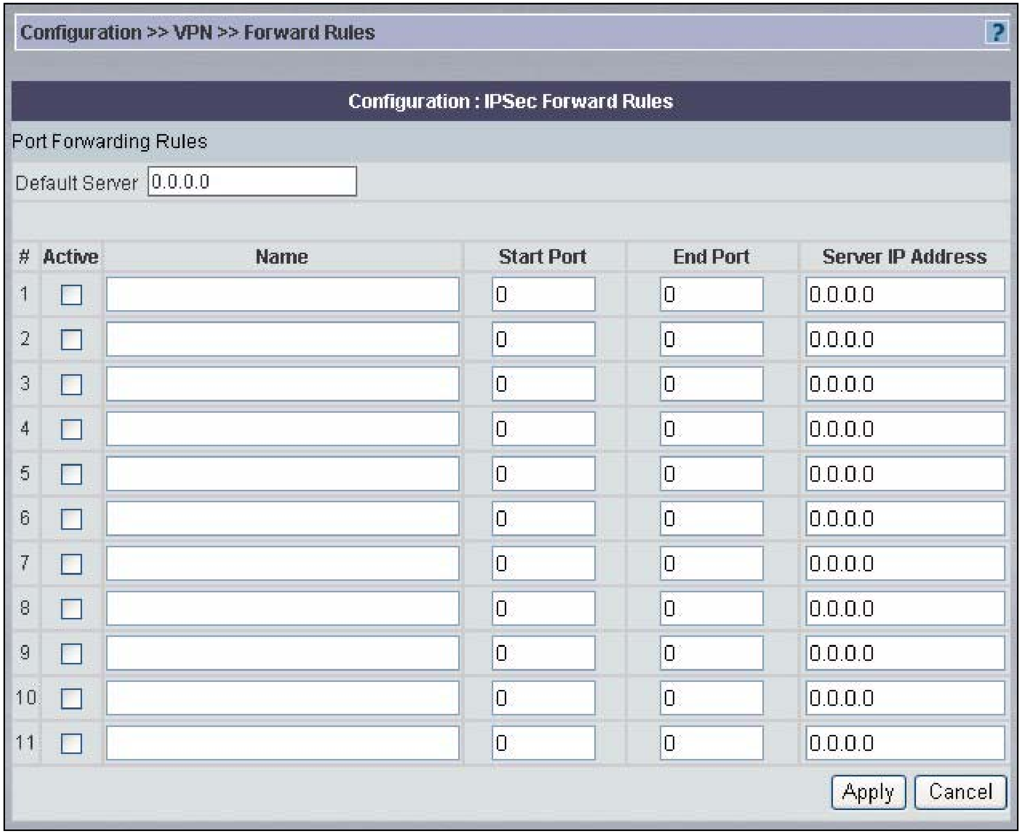
**Table 71** Configuration > VPN > IKE IPSec (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Multiple Proposals | Select this check box to allow the device to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA.<br>When you enable multiple proposals, the device allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule.<br>Clear this check box to have the device use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

## 12.4.3 Edit Port Forwarding in VPN

In the **VPN Rule (IPSec)** screen, click the **Port Forwarding** button in the **Virtual Address Mapping Rule** section.

**Figure 96** Configuration > VPN > IKE IPSec > Port Forwarding Rules



Configuration >> VPN >> Forward Rules

Configuration : IPSec Forward Rules

Port Forwarding Rules

Default Server 0.0.0.0

| # | Active | Name | Start Port | End Port | Server IP Address |
|---|---|---|---|---|---|
| 1 | □ | | 0 | 0 | 0.0.0.0 |
| 2 | □ | | 0 | 0 | 0.0.0.0 |
| 3 | □ | | 0 | 0 | 0.0.0.0 |
| 4 | □ | | 0 | 0 | 0.0.0.0 |
| 5 | □ | | 0 | 0 | 0.0.0.0 |
| 6 | □ | | 0 | 0 | 0.0.0.0 |
| 7 | □ | | 0 | 0 | 0.0.0.0 |
| 8 | □ | | 0 | 0 | 0.0.0.0 |
| 9 | □ | | 0 | 0 | 0.0.0.0 |
| 10 | □ | | 0 | 0 | 0.0.0.0 |
| 11 | □ | | 0 | 0 | 0.0.0.0 |

The following table describes the labels in this screen.

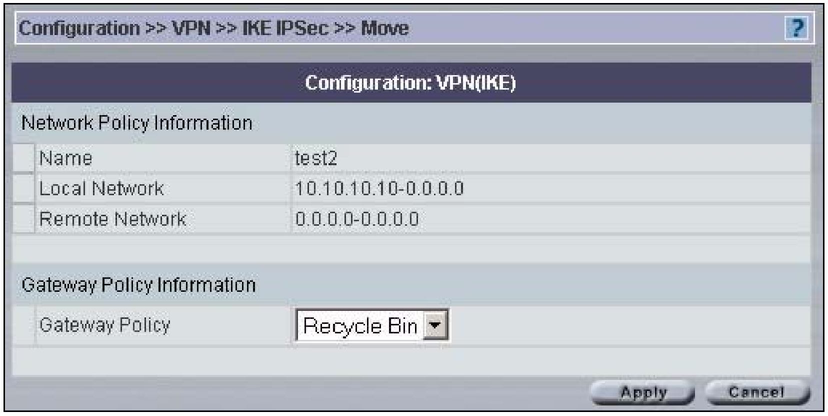
**Table 72** Configuration > VPN > IKE IPSec > Port Forwarding Rules

| LABEL | DESCRIPTION |
|---|---|
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, all packets received for ports not specified in this screen are discarded. |
| # | Number of an individual port forwarding server entry. |
| Active | Select this check box to activate the port forwarding server entry. |
| Name | Enter a descriptive name for identifying purposes. |
| Start Port | Type a port number in this field.<br>To forward only one port, type the port number again in the **End Port** field.<br>To forward a series of ports, type the start port number here and the end port number in the **End Port** field. |
| End Port | Type a port number in this field.<br>To forward only one port, type the port number in the **Start Port** field above and then type it again in this field.<br>To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above. |
| Server IP Address | Type your server IP address in this field. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main IPSec VPN screen. |

## 12.4.4 VPN Rules (IKE) > Network Policy Move

Click the **Move** button icon in the VPN Rules (IKE) screen to display the screen shown next. Use this screen to associate a network policy to a gateway policy.

**Figure 97** Configuration > VPN > IKE IPSec > Move



Configuration >> VPN >> IKE IPSec >> Move

Configuration: VPN(IKE)

Network Policy Information

| | |
|---|---|
| Name | test2 |
| Local Network | 10.10.10.10-0.0.0.0 |
| Remote Network | 0.0.0.0-0.0.0.0 |

Gateway Policy Information

| | |
|---|---|
| Gateway Policy | Recycle Bin |

The following table describes the labels in this screen.

**Table 73** Configuration > VPN > IKE IPSec > Move

| LABEL | DESCRIPTION |
|---|---|
| Network Policy Information | The following fields display the general network settings of this VPN policy. |
| Name | This field displays the policy name. |

**Table 73** Configuration > VPN > IKE IPSec > Move (continued)

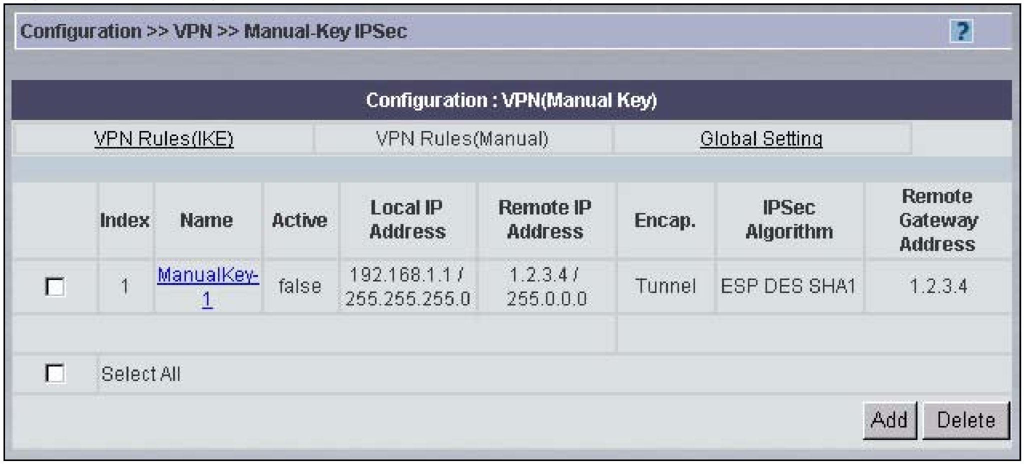
| LABEL | DESCRIPTION |
|---|---|
| Local Network | This field displays one or a range of IP address(es) of the computer(s) behind the device. |
| Remote Network | This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router. |
| Gateway Policy Information | |
| Gateway Policy | Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy.<br>If you do not want to associate a network policy to any gateway policy, select **Recycle Bin** from the drop-down list box. The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in the **VPN Rules (IKE)** screen. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

## 12.5 VPN Rules (Manual) (VPN version 1.1)

Select a device, click **Configuration > VPN** > **VPN Rules(manual)** tab to open the VPN Rules screen. This is a read-only menu of your IPSec rules (tunnels). Edit an IPSec rule by clicking the edit icon to configure the associated submenus.

You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

**Figure 98** Configuration > VPN > Manual-Key IPSec



Configuration >> VPN >> Manual-Key IPSec

Configuration : VPN(Manual Key)

| | Index | Name | Active | Local IP Address | Remote IP Address | Encap. | IPSec Algorithm | Remote Gateway Address |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | ManualKey-1 | false | 192.168.1.1 / 255.255.255.0 | 1.2.3.4 / 255.0.0.0 | Tunnel | ESP DES SHA1 | 1.2.3.4 |
| □ | Select All | | | | | | | |

The following table describes the labels in this screen.

**Table 74** Configuration > VPN > Manual-Key IPSec

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the VPN policy index number. |
| Name | This field displays the identification name for this VPN policy. Click the hyperlink to edit the VPN policy. |

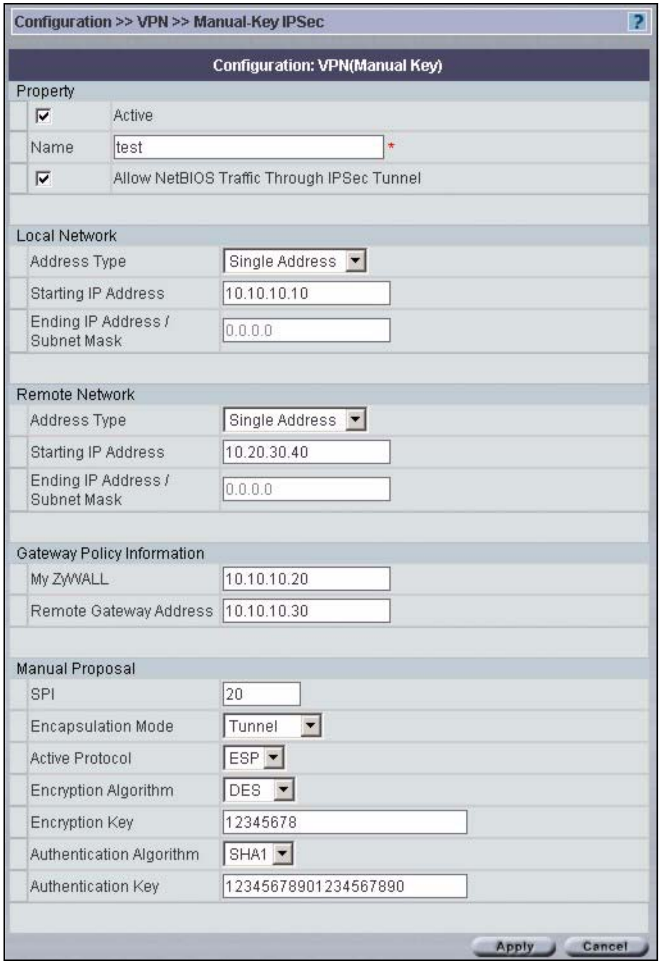
**Table 74** Configuration > VPN > Manual-Key IPSec (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active | This field displays whether the VPN policy is active or not. A **true** signifies that this VPN policy is active; **false** signifies that this VPN policy is not active. |
| Local IP Address | This is the IP address(es) of computer(s) on your local network behind your device.<br>The same (static) IP address is displayed twice when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**. |
| Remote IP Address | This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router.<br>This field displays **N/A** when the **Remote Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.<br>The same (static) IP address is displayed twice when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**. |
| Encap. | This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection). |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both **AH** and **ESP** increase device processing requirements and communications latency (delay). |
| Remote Gateway Address | This is the static WAN IP address or domain name of the remote IPSec router. |
| Add | Click **Add** to add a new VPN policy. |
| Delete | Select a policy and click **Delete** to remove the VPN policy. A window displays asking you to confirm that you want to delete the VPN rule. When a VPN policy is deleted, subsequent policies move up in the page list. |

### 12.5.1 VPN Rules (Manual) > Edit

Manual key management is useful if you have problems with IKE key management. Click a **Name** hyperlink in the **VPN Rules (Manual)** screen to edit VPN rules.

**Figure 99** Configuration > VPN > Manual-Key IPSec > Edit



Configuration >> VPN >> Manual-Key IPSec

Configuration: VPN(Manual Key)

Property

☑ Active

Name: test *

☑ Allow NetBIOS Traffic Through IPSec Tunnel

Local Network

Address Type: Single Address

Starting IP Address: 10.10.10.10

Ending IP Address / Subnet Mask: 0.0.0.0

Remote Network

Address Type: Single Address

Starting IP Address: 10.20.30.40

Ending IP Address / Subnet Mask: 0.0.0.0

Gateway Policy Information

My ZyWALL: 10.10.10.20

Remote Gateway Address: 10.10.10.30

Manual Proposal

SPI: 20

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Encryption Key: 12345678

Authentication Algorithm: SHA1

Authentication Key: 12345678901234567890

The following table describes the labels in this screen.

**Table 75** Configuration > VPN > Manual-Key IPSec > Edit

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| Active | Select this check box to activate this VPN policy. |
| Name | Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the device drops trailing spaces. |
| Allow NetBIOS Traffic Through IPSec Tunnel | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.<br>Select this check box to send NetBIOS packets through the VPN connection. |
| Local Network | Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |

**Table 75** Configuration > VPN > Manual-Key IPSec > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your device. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your device. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your device. |
| Ending IP Address/Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your device. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your device. |
| Remote Network | Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router. |
| Gateway Policy Information | |
| My ZyWALL | Enter the WAN IP address or domain name of your device or leave the field set to **0.0.0.0**. The VPN tunnel has to be rebuilt if the **My ZyWALL** IP address changes after setup.<br>The following applies if the **My ZyWALL** field is configured as **0.0.0.0**:<br>• When the WAN port operation mode is set to Active/Passive, the device uses the IP address (static or dynamic) of the WAN port that is in use.<br>• When the WAN port operation mode is set to Active/Active, the device uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the device uses the IP address of the other WAN port.<br>• If both WAN connections go down, the device uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect. |
| Remote Gateway Addr | Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. |

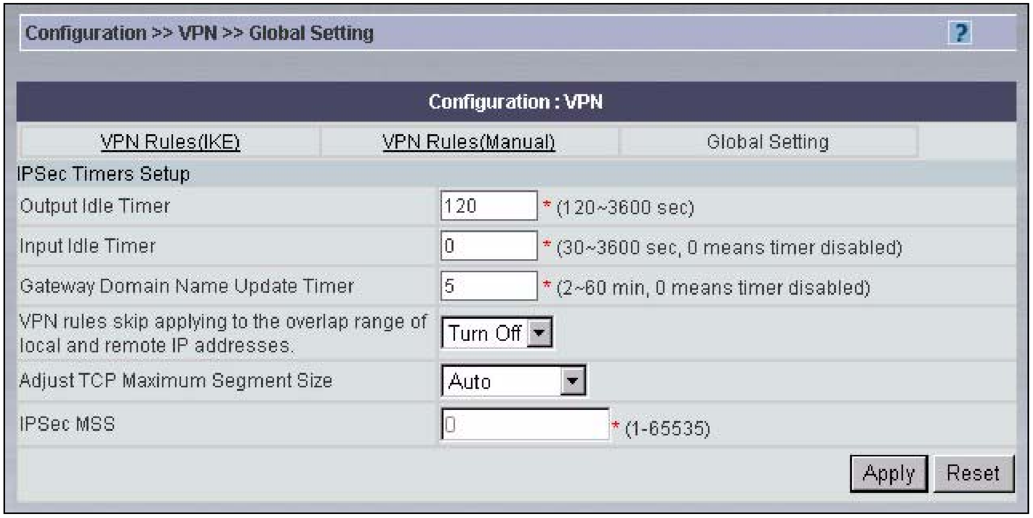
**Table 75** Configuration > VPN > Manual-Key IPSec > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Manual Proposal | |
| SPI | Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9". |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode from the drop-down list box. |
| Active Protocol | Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).<br>Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described next). |
| Encryption Algorithm | Select **DES**, **3DES** or **NULL** from the drop-down list box.<br>When **DES** is used for data communications, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| Authentication Algorithm | Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| Encryption Key | This field is applicable when you select **ESP** in the **Active Protocol** field above.<br>With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Authentication Key | Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Apply | Click **Apply** to save your changes back to the device. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 12.6 VPN Global Setting (VPN version 1.1)

Select a device, click **Configuration > VPN** > **Global Setting** tab to open the screen shown next. Use this screen to change your device's global settings.

**Figure 100** Configuration > VPN > Global Setting



IPSec Timers Setup

| | |
|---|---|
| Output Idle Timer | 120 * (120~3600 sec) |
| Input Idle Timer | 0 * (30~3600 sec, 0 means timer disabled) |
| Gateway Domain Name Update Timer | 5 * (2~60 min, 0 means timer disabled) |
| VPN rules skip applying to the overlap range of local and remote IP addresses. | Turn Off |
| Adjust TCP Maximum Segment Size | Auto |
| IPSec MSS | 0 * (1-65535) |

The following table describes the labels in this screen.

**Table 76** Configuration > VPN > Global Setting

| LABEL | DESCRIPTION |
|---|---|
| Output Idle Timer | When traffic is sent to a remote IPSec router from which no reply is received after the specified time period, the device checks the VPN connectivity. If the remote IPSec router does not reply, the device automatically disconnects the VPN tunnel.<br>Enter the time period (between 30 and 3600 seconds) to wait before the device checks all of the VPN connections to remote IPSec routers.<br>Enter **0** to disable this feature. |
| Input Idle Timer | When no traffic is received from a remote IPSec router after the specified time period, the device checks the VPN connectivity. If the remote IPSec router does not reply, the device automatically disconnects the VPN tunnel.<br>Enter the time period (between 30 and 3600 seconds) to wait before the device checks all of the VPN connections to remote IPSec routers.<br>Enter **0** to disable this feature. |
| Gateway Domain Name Update Timer | This field is applicable when you enter a domain name to identify the device and/or the remote secure gateway.<br>Enter the time period (between 2 and 60 minutes) to wait before the device updates the domain name and IP address mapping through a DNS server. The device rebuilds the VPN tunnel if it finds that the domain name is now using a different IP address (any users of the VPN tunnel will be temporarily disconnected).<br>Enter **0** to disable this feature. |
| VPN rules skip applying to the overlap range of local and remote IP addresses | When you configure a VPN rule, the device checks to make sure that the IP addresses in the local and remote networks do not overlap. Select **Turn Off** box to disable the check if you need to configure a VPN policy with overlapping local and remote IP addresses.<br>Note: If a VPN policy's local and remote IP addresses overlap, you may not be able to access the device on your LAN because the device automatically triggers a VPN tunnel to the remote device with the same IP address. |

**Table 76** Configuration > VPN > Global Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Adjust TCP Maximum Segment Size | The TCP packets are larger after the device encrypts them for VPN. The device fragments packets that are larger than a connection's MTU (Maximum Transmit Unit).<br>In most cases you should leave this set to **Auto**. The device automatically sets the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type.<br>Select **Off** to not adjust the MSS for the encrypted TCP packets.<br>If your network environment causes fragmentation issues that are affecting your throughput performance, you can manually set a smaller MSS for the TCP packets that are to be encrypted by VPN. Select **User Define**, and specify a size in the **IPSec MSS** field. |
| IPSec MSS | This field is enabled if **Adjust TCP Maximum Segment Size** is **User Define**.<br>Specify the Maximum Segment Size (MSS) for the TCP packets that are to be encrypted by VPN. Specify a size from 0~1460 bytes. 0 has the device use the auto setting. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 13

# Configuration > Firewall

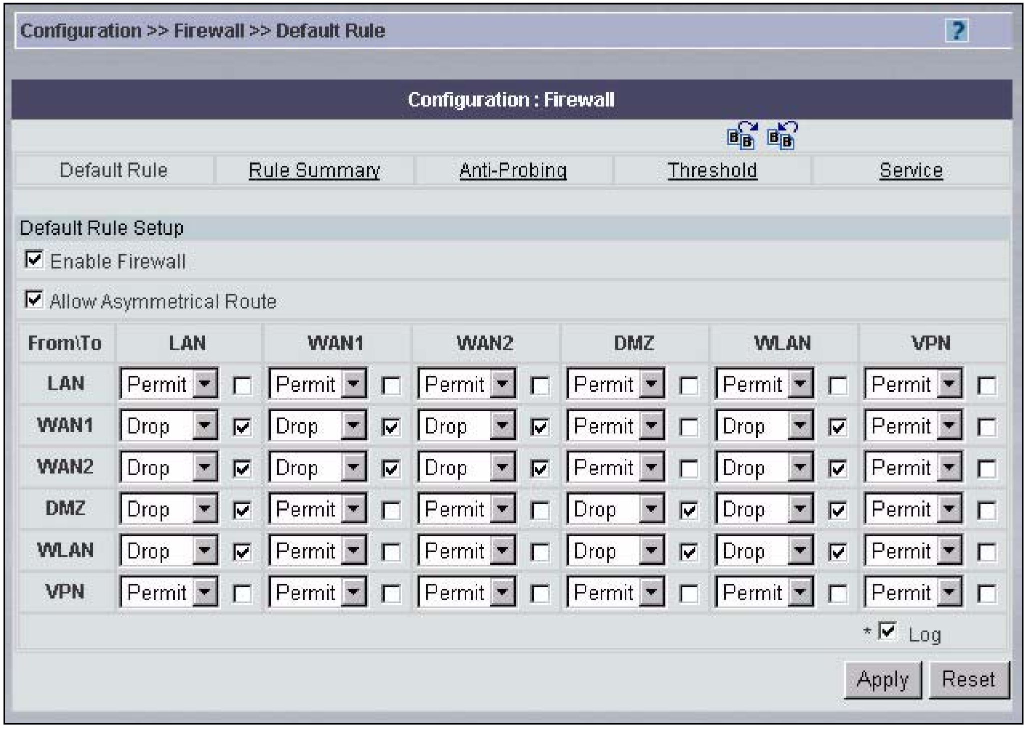
This section shows you how to configure the **Firewall** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 13.1 Default Rule

Use this screen to configure global settings for the firewall and to set the default rules for packets in each direction. You can also configure the default rules in the **Rule Summary** screen for each direction.

To open this screen, click **Configuration** > **Firewall** > **Default Rule**.

**Figure 101** Configuration > Firewall > Default Rule



Configuration >> Firewall >> Default Rule

Configuration : Firewall

Default Rule Setup

☑ Enable Firewall

☑ Allow Asymmetrical Route

| From\To | LAN | | WAN1 | | WAN2 | | DMZ | | WLAN | | VPN | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| LAN | Permit | □ | Permit | □ | Permit | □ | Permit | □ | Permit | □ | Permit | □ |
| WAN1 | Drop | ☑ | Drop | ☑ | Drop | ☑ | Permit | □ | Drop | ☑ | Permit | □ |
| WAN2 | Drop | ☑ | Drop | ☑ | Drop | ☑ | Permit | □ | Drop | ☑ | Permit | □ |
| DMZ | Drop | ☑ | Permit | □ | Permit | □ | Drop | ☑ | Drop | ☑ | Permit | □ |
| WLAN | Drop | ☑ | Permit | □ | Permit | □ | Drop | ☑ | Drop | ☑ | Permit | □ |
| VPN | Permit | □ | Permit | □ | Permit | □ | Permit | □ | Permit | □ | Permit | □ |

* ☑ Log

The following table describes the labels in this screen.

**Table 77** Configuration > Firewall > Default Rule

| LABEL | DESCRIPTION |
|---|---|
| Default Rule Setup | |
| Enable Firewall | Select this check box to activate the firewall. The device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Allow Asymmetrical Route | Select this check box to have the device firewall ignore the use of triangle route topology on the network. See the device's User's Guide for more on triangle route topology. |
| Attack Detected Alert | Select this check box to have the device generate an alert when a DoS attack (as defined in the **Configuration > Firewall > Threshold** screen in Section 13.4 on page 202) is detected. |
| From, To | Set the firewall's default actions based on the direction of travel of packets. Here are some example descriptions of the directions of travel.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the device or the device itself. The device does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the device through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The device applies the firewall to the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The device applies the firewall to the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the device. This is the case when the device is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the device. The device applies the firewall to the traffic after decrypting it.<br>Note: The VPN connection directions apply to the traffic going to or from the device's VPN tunnels. They do not apply to other VPN traffic for which the device is not one of the gateways (VPN pass-through traffic).<br>Here are the default actions from which you can select.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>The firewall rules for the WAN port with a higher route priority also apply to the dial backup connection. |
| Log | Select the check box next to a direction of packet travel to create a log when the above action is taken for packets that are traveling in that direction and do not match any of your customized rules. |

**Table 77** Configuration > Firewall > Default Rule (continued)

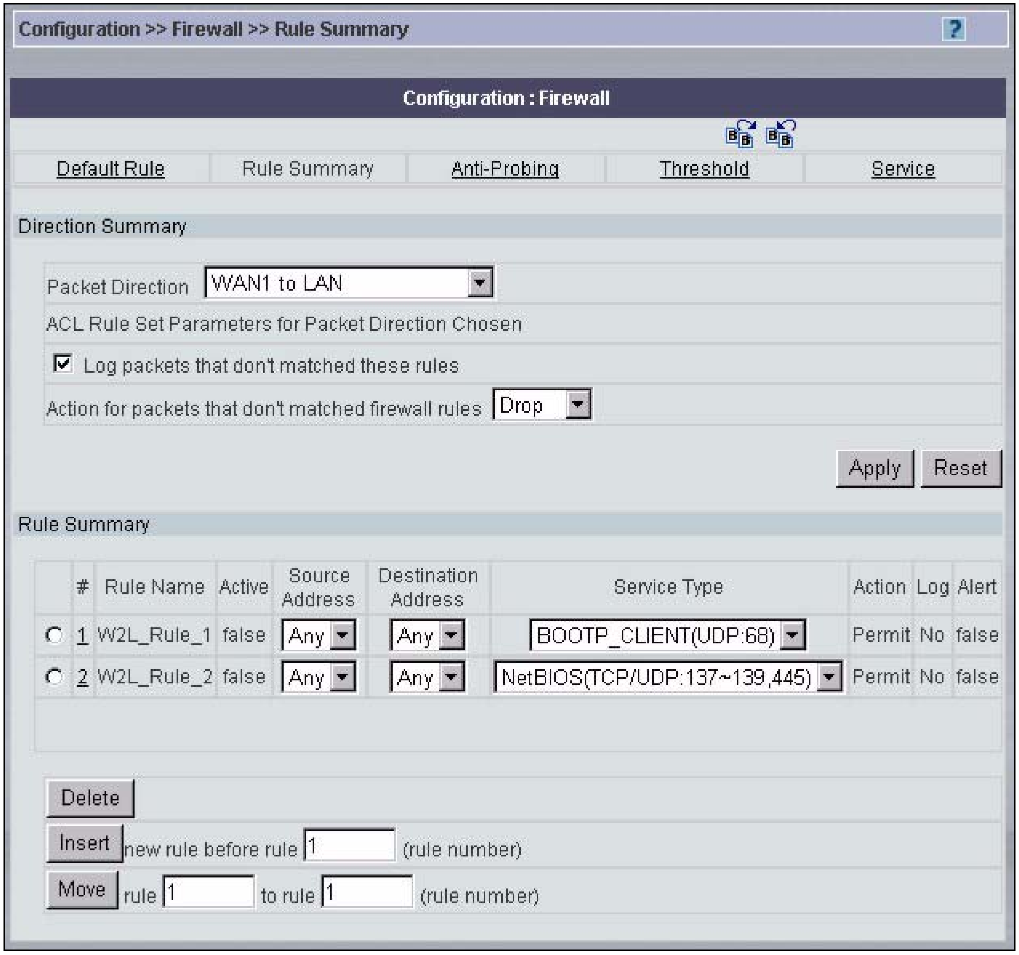
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click this to reset this screen to its last saved values. |

## 13.2 Rule Summary

Use the **Insert** button to add a new rule before an existing rule. Use **Move** to put an existing rule in a different place.

Select a device and then click **Configuration** > **Firewall** > **Rule Summary**.

**Figure 102** Configuration > Firewall > Rule Summary



Configuration >> Firewall >> Rule Summary

Configuration : Firewall

Default Rule | Rule Summary | Anti-Probing | Threshold | Service

Direction Summary

Packet Direction: WAN1 to LAN

ACL Rule Set Parameters for Packet Direction Chosen

☑ Log packets that don't matched these rules

Action for packets that don't matched firewall rules: Drop

Apply | Reset

Rule Summary

| | # | Rule Name | Active | Source Address | Destination Address | Service Type | Action | Log | Alert |
|---|---|---|---|---|---|---|---|---|---|
| ○ | 1 | W2L_Rule_1 | false | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | false |
| ○ | 2 | W2L_Rule_2 | false | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | false |

Delete

Insert new rule before rule 1 (rule number)

Move rule 1 to rule 1 (rule number)

The following table describes the labels in this screen.

**Table 78** Configuration > Firewall > Rule Summary

| LABEL | DESCRIPTION |
|---|---|
| Direction Summary | Firewall rules are grouped based on the direction of travel of packets to which they apply. Select a direction from the drop-down list box. |
| Packet Direction | Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules. |

**Table 78** Configuration > Firewall > Rule Summary (continued)

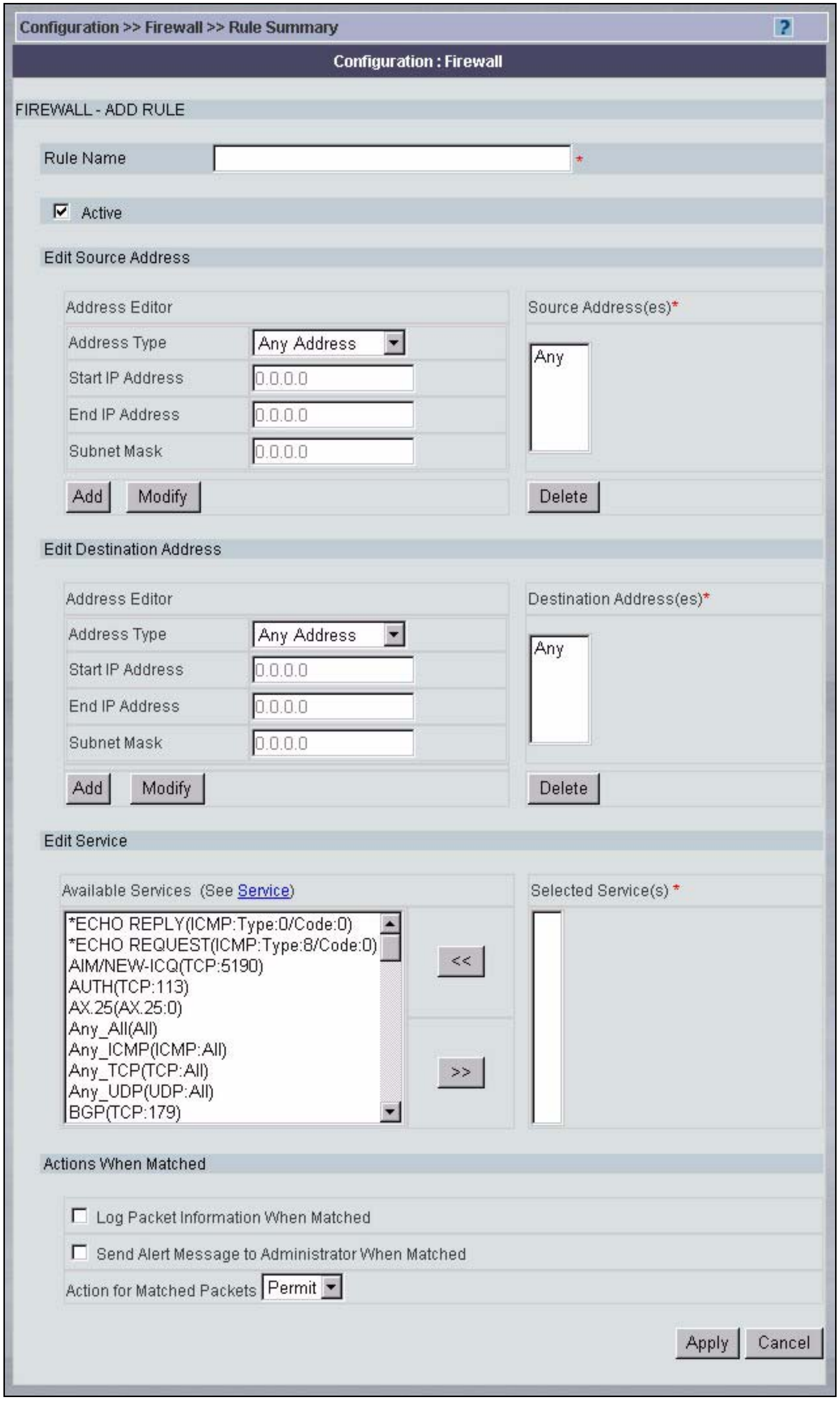
| LABEL | DESCRIPTION |
|---|---|
| Log packets that don't match these rules. | Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below. |
| Action for packets that don't match firewall rules | Select what action the device should take for packets that don't match any of the firewall rules you configured.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click this to reset this screen to its last saved values. |
| | The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above. Select an ACL hyperlink to edit that ACL rule. |
| # | This is your firewall rule number. Select a rule hyperlink to edit that rule. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules. |
| Rule Name | This is the name of the firewall rule. |
| Active | This field displays whether a firewall is turned on (**true**) or not (**false**). |
| Source Address | This field lists the source IP address of the incoming packet. |
| Destination Address | This field lists the destination IP address of the outgoing packet. |
| Service Type | This field displays the services to which this firewall rule applies. See Figure 103 on page 199 for more information. |
| Action | This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**). |
| Log | This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**). |
| Alert | This field tells you whether this rule generates an alert (**true**) or not (**false**) when the rule is matched. |
| Delete | Select a rule index and then click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action. |
| Insert | Type the index number for where you want to put a rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.<br>Click **Insert** to display this screen and refer to the following table for information on the fields. |
| Move | Select a rule's Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. |
| Add | Click **Add** to create a new firewall rule. |
| Apply | Click **Apply** to save your changes back to the device. |

## 13.2.1 Add/Edit

Each device has a different number of rules and custom ports; see the device User Guide for more details.

In Figure 102 on page 197, select an existing rule to edit it or click **Insert** to create a new firewall rule.

**Figure 103** Configuration > Firewall > Rule Summary > Edit



Configuration >> Firewall >> Rule Summary

Configuration : Firewall

FIREWALL - ADD RULE

Rule Name *

☑ Active

Edit Source Address

Address Editor

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Source Address(es)*: Any

Edit Destination Address

Address Editor

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Destination Address(es)*: Any

Edit Service

Available Services (See Service)

```
*ECHO REPLY(ICMP:Type:0/Code:0)
*ECHO REQUEST(ICMP:Type:8/Code:0)
AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
AX.25(AX.25:0)
Any_All(All)
Any_ICMP(ICMP:All)
Any_TCP(TCP:All)
Any_UDP(UDP:All)
BGP(TCP:179)
```

Selected Service(s) *

Actions When Matched

☐ Log Packet Information When Matched

☐ Send Alert Message to Administrator When Matched

Action for Matched Packets: Permit

The following table describes the labels in this screen.

**Table 79** Configuration > Firewall > Rule Summary > Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed. |
| Active | Select this to turn this rule on. Clear this to turn this rule off. |
| Edit Source/ Destination Address | |
| Address Type | Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add | Click **Add** to add a new address to the **Source** or **Destination Address(es)** box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Modify | To edit an existing source or destination address, select it from the box and click **Modify**. |
| Delete | Highlight an existing source or destination address from the **Source** or **Destination Address(es)** box above and click **Delete** to remove it. |
| Edit Service | |
| Available/ Selected Services | Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Service(s)** box on the right. To remove a service, highlight it in the **Selected Service(s)** box on the right, then click **<<**.<br>Next to the name of a service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type). For example, look at the DNS entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the **Service** link to go to the **Service screen where you can** configure custom service ports. See the device User’s Guide for a list of commonly used services and port numbers.<br>You can use the [CTRL] key and select multiple services at once. |
| Actions When Matched | |
| Log Packet Information When Matched | This field determines if a log for packets that match the rule is created (**Yes**) or not (**No**). Go to the **Log Settings** page and select the **Access Control** logs category to have the device record these logs. |
| Send Alert Message to Administrator When Matched | Select the check box to have the device generate an alert when the rule is matched. |

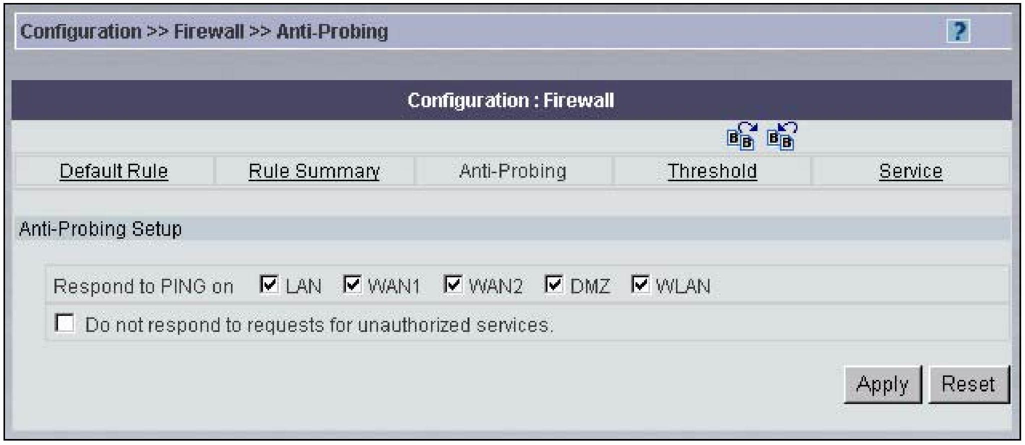
**Table 79** Configuration > Firewall > Rule Summary > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action for Matched Packets | Use the drop-down list box to select what the firewall is to do with packets that match this rule.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN.<br>Note: You may also need to configure the remote management settings if you want to allow a WAN computer to manage the device or restrict management from the LAN. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 13.3 Anti-Probing

Click **Configuration** > **Firewall** > **Anti-Probing** to open the following screen. Configure this screen to help keep the device hidden from probing attempts. You can specify which of the device's interfaces will respond to Ping requests and whether or not the device is to respond to probing for unused ports.

**Figure 104** Configuration > Firewall > Anti-Probing



Anti-Probing Setup

Respond to PING on ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN

□ Do not respond to requests for unauthorized services.

The following table describes the labels in this screen.

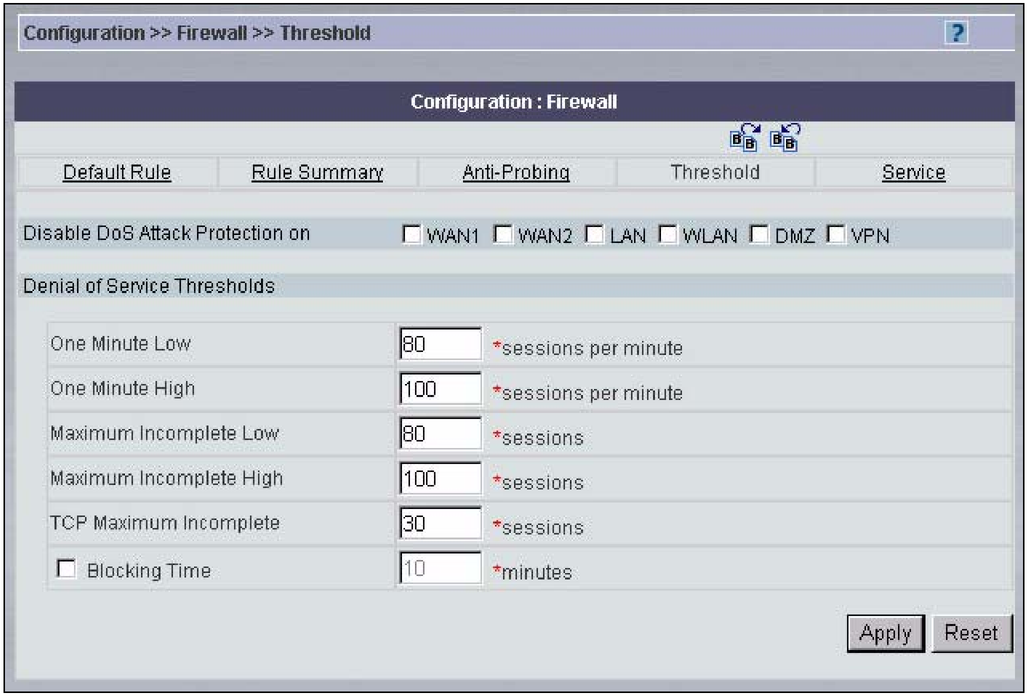
**Table 80** Configuration > Firewall > Anti-Probing

| LABEL | DESCRIPTION |
|---|---|
| Respond to PING on | Select the interfaces on which you want the device to reply to incoming Ping requests. |
| Do not respond to requests for unauthorized services. | Select this option to prevent hackers from finding the device by probing for unused ports. If you select this option, the device will not respond to port request(s) for unused ports, thus leaving the unused ports and the device unseen. If this option is not selected, the device will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports.<br>Note that the probing packets must first traverse the device's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the device reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 13.4 Threshold

Click **Configuration > Firewall > Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

**Figure 105** Configuration > Firewall > Threshold



Disable DoS Attack Protection on □ WAN1 □ WAN2 □ LAN □ WLAN □ DMZ □ VPN

Denial of Service Thresholds

| | | |
|---|---|---|
| One Minute Low | 80 | *sessions per minute |
| One Minute High | 100 | *sessions per minute |
| Maximum Incomplete Low | 80 | *sessions |
| Maximum Incomplete High | 100 | *sessions |
| TCP Maximum Incomplete | 30 | *sessions |
| □ Blocking Time | 10 | *minutes |

The following table describes the labels in this screen.

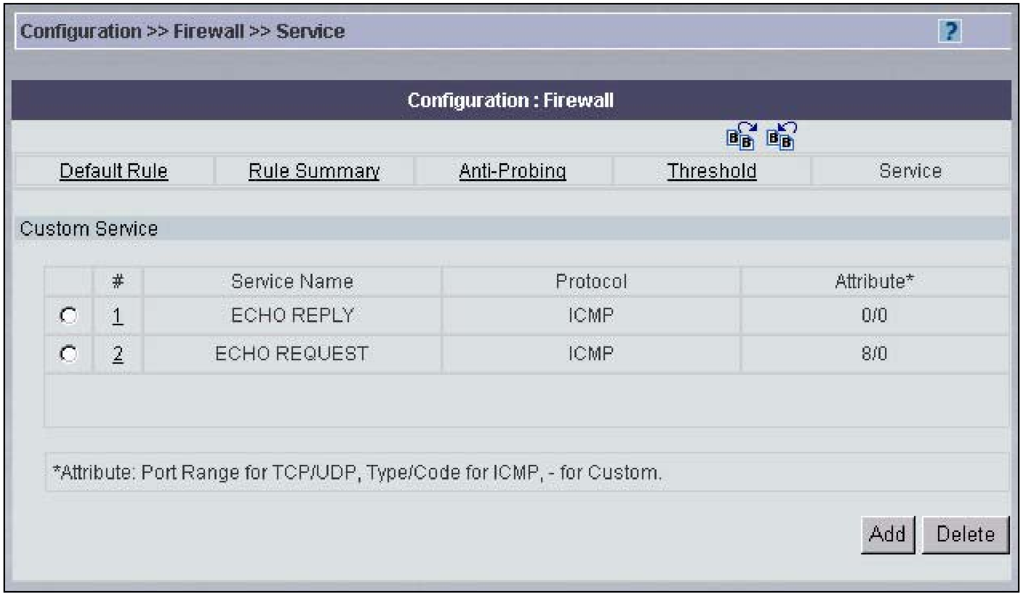
**Table 81** Configuration > Firewall > Threshold

| LABEL | DESCRIPTION |
|---|---|
| Disable DoS Attack Protection on | Select the interface(s) (or VPN tunnels) for which you want the device to not use the Denial of Service protection thresholds. This disables DoS protection on the selected interface (or all VPN tunnels).<br>You may want to disable DoS protection for an interface if the device is treating valid traffic as DoS attacks. Another option would be to raise the thresholds. |
| Denial of Service Thresholds | The device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute. |
| One Minute Low | This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number. |
| One Minute High | This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the device deletes half-open sessions as required to accommodate new connection attempts.<br>For example, if you set the one minute high to 100, the device starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low. |
| Maximum Incomplete Low | This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number. |
| Maximum Incomplete High | This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.<br>For example, if you set the maximum incomplete high to 100, the device starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low. |
| TCP Maximum Incomplete | An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.<br>Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The device sends alerts whenever the **TCP Maximum Incomplete** is exceeded. |
| Blocking Time | Select the action that the device takes when the TCP maximum incomplete threshold is reached.<br>Select the check box if you want the device to deny new connection requests for the number of minutes that you specify (between 1 and 255).<br>Clear the check box if you want the device to delete the oldest half open session when a new connection request comes. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 13.5 Service

Click **Configuration** > **Firewall** > **Service** to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the device.

**Figure 106** Configuration > Firewall > Service



|  | # | Service Name | Protocol | Attribute* |
|---|---|---|---|---|
| ○ | 1 | ECHO REPLY | ICMP | 0/0 |
| ○ | 2 | ECHO REQUEST | ICMP | 8/0 |

*Attribute: Port Range for TCP/UDP, Type/Code for ICMP, - for Custom.

The following table describes the labels in this screen.

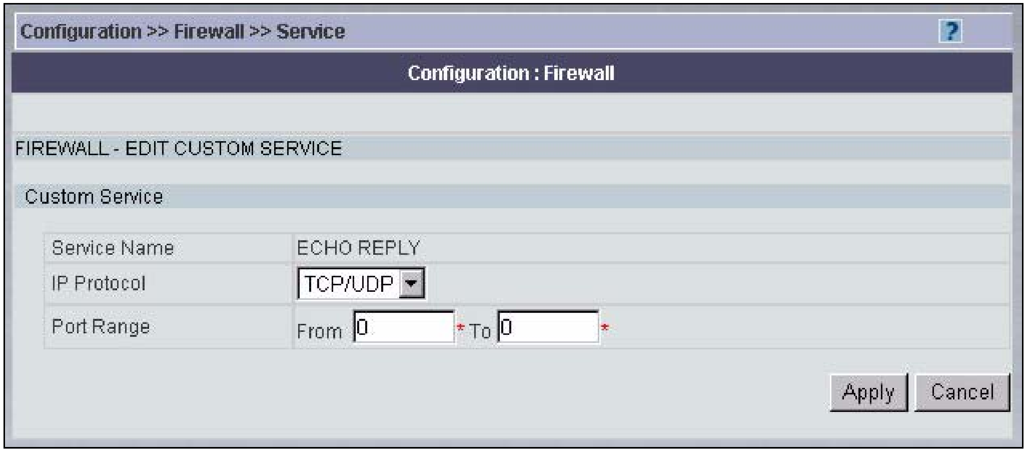
**Table 82** Configuration > Firewall > Service

| LABEL | DESCRIPTION |
|---|---|
| Custom Service | This table shows all configured custom services. |
| # | This is the index number of the custom service. Click the number to go to the screen where you can edit the service. |
| Service Name | This is the name of the service. |
| Protocol | This is the IP protocol type.<br>If you selected **Custom**, this is the IP protocol value you entered. |
| Attribute | This field displays the IP port number(s) or ICMP type and code that defines the service. |
| Add | Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services. |
| Delete | Click the delete icon to remove an existing service. |

### 13.5.1 Edit Service

Click **Configuration** > **Firewall** > **Service** and then click an existing service's index number or click **Add** to open the screen as shown next. Use this screen to configure a custom service entry not is not predefined in the device.

**Figure 107** Configuration > Firewall > Service > Add/Edit


Configuration >> Firewall >> Service
?
Configuration : Firewall
FIREWALL - EDIT CUSTOM SERVICE
Custom Service
Apply
Cancel

| | |
|---|---|
| Service Name | ECHO REPLY |
| IP Protocol | TCP/UDP |
| Port Range | From 0 * To 0 * |

The following table describes the labels in this screen.

**Table 83** Configuration > Firewall > Service > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Service Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the left parentheses “(“. Spaces are allowed. |
| IP Protocol | Choose the IP protocol (**TCP**, **UDP**, **TCP/UDP**, **ICMP** or **Custom**) that defines your customized service from the drop down list box.<br>If you select **Custom**, specify the protocol’s number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on. |
| Port Range | Enter the port number (from 1 to 255) that defines the customized service<br>To specify one port only, enter the port number in the **From** field and enter it again in the **To** field.<br>To specify a span of ports, enter the first port in the **From** field and enter the last port in the **To** field. |
| Type/Code | This field is available only when you select **ICMP** in the **IP Protocol** field.<br>The ICMP messages are identified by their types and in some cases codes.<br>Enter the type number in the **Type** field and select the **Code** radio button and enter the code number if any. |
| Custom Protocol | This field is available only when you select **Custom** in the **IP Protocol** field.<br>Specify the protocol’s number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 14

# Configuration > Port Roles

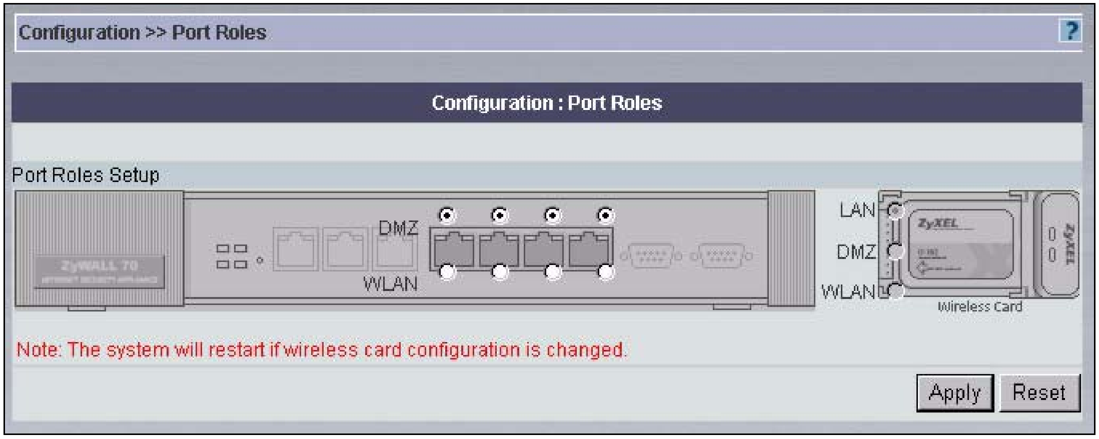
This section shows you how to configure the **Port Roles** screen. Please see the device's User's Guide for more information about this screen.

## 14.1 Port Roles

Use this screen to set ports as part of the LAN, DMZ and/or WLAN interface. When you change the role of a port, you often change its IP address on the port. Make sure you do not disconnect the device from Vantage CNM or administrators.

To change your device's port role settings, click **Configuration** > **Port Roles**. The screen appears as shown.

**Figure 108** Configuration > Port Roles



Configuration >> Port Roles

Configuration : Port Roles

Port Roles Setup

Note: The system will restart if wireless card configuration is changed.

The radio buttons correspond to Ethernet ports on the front panel of the device. The following table describes the labels in this screen.

**Table 84** Configuration > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the device's LAN IP address and MAC address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the device's DMZ IP address and MAC address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN. The port will use the device's WLAN IP address and MAC address. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 15

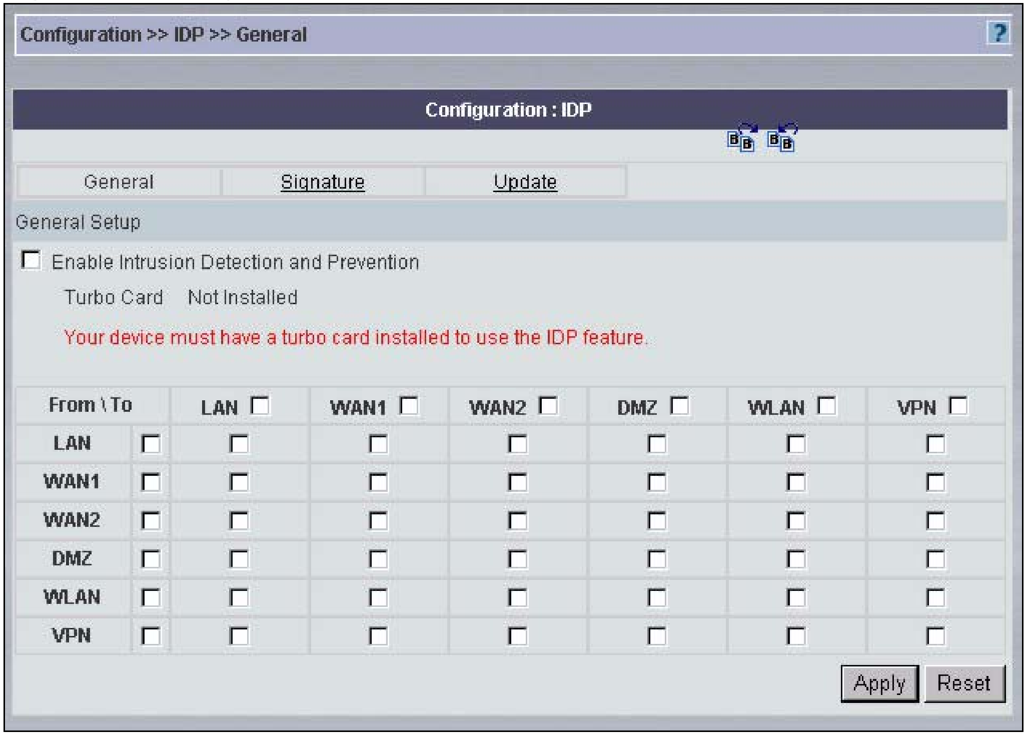
# Configuration > IDP

This section shows you how to configure the **IDP** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 15.1 General Setup

Use this screen to enable IDP on the device and choose what interface(s) you want to protect from intrusions. To open this screen, click **Configuration > IDP > General**.

**Figure 109** Configuration > IDP > General



General Setup

□ Enable Intrusion Detection and Prevention

Turbo Card Not Installed

Your device must have a turbo card installed to use the IDP feature.

| From \ To | | LAN □ | WAN1 □ | WAN2 □ | DMZ □ | WLAN □ | VPN □ |
|---|---|---|---|---|---|---|---|
| LAN | □ | □ | □ | □ | □ | □ | □ |
| WAN1 | □ | □ | □ | □ | □ | □ | □ |
| WAN2 | □ | □ | □ | □ | □ | □ | □ |
| DMZ | □ | □ | □ | □ | □ | □ | □ |
| WLAN | □ | □ | □ | □ | □ | □ | □ |
| VPN | □ | □ | □ | □ | □ | □ | □ |

The following table describes the labels in this screen.

**Table 85** Configuration > IDP > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Intrusion Detection and Protection | Select this check box to enable IDP on the device. When this check box is cleared the device is in IDP “bypass” mode and no IDP checking is done. |
| Turbo Card | This field displays whether or not a device’s Turbo Card is installed.<br>Note: You cannot configure and save the IDP or Anti-Virus screens if the device’s Turbo Card is not installed. |
| From, To | Select the check box to apply IDP to packets based on the direction of travel. Select or clear a row or column’s first check box (with the interface label) to select or clear the interface’s whole row or column.<br>For example, **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the device or the device itself. The device does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the device through a VPN tunnel and is going to the selected “to” interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the device’s LAN interface. The device checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected “from” interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The device checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the device. This is the case when the device is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the device. The device checks the traffic after decrypting it (before encrypting it again).<br>Note: The VPN connection directions apply to the traffic going to or from the device’s VPN tunnels. They do not apply to other VPN traffic for which the device is not one of the gateways (VPN pass-through traffic). |
| Apply | Click this button to save your changes back to the device. |
| Reset | Click this button to begin configuring this screen afresh. |

## 15.2 IDP Signatures

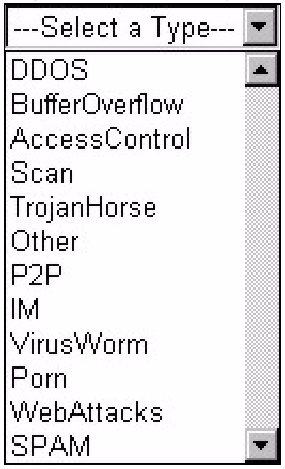
The rules that define how to identify and respond to intrusions are called “signatures”. Click **Configuration > IDP** > **Signatures** to see the device’s signatures.

### 15.2.1 Attack Types

Click **Configuration > IDP** > **Signature**. The **Attack Type** list box displays all intrusion types supported by the device. **Other** covers all intrusion types not covered by other types listed.

To see signatures for a specific intrusion type, select that type from the **Attack Type** list box.

**Figure 110** Configuration > IDP > Signature > Attack Types



The following table describes each attack type.

**Table 86** Configuration > IDP > Signature > Attack Types

| TYPE | DESCRIPTION |
|---|---|
| DDoS | The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system. |
| BufferOverflow | A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.<br>Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices. |
| AccessControl | Access control refers to procedures and controls that limit or detect access. Access control is used typically to control user access to network resources such as servers, directories, and files. |
| Scan | Scan refers to all port, IP or vulnerability scans. Hackers scan ports to find targets. They may use a TCP connect() call, SYN scanning (half-open scanning), Nmap etc. After a target has been found, a vulnerability scanner can be used to exploit exposures. |
| TrojanHorse | A Trojan horse is a harmful program that's hidden inside apparently harmless programs or data. It could be used to steal information or remotely control a device. |
| Other | This category refers to signatures for attacks that do not fall into the previously mentioned categories. |
| P2P | Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the device, P2P refers to peer-to-peer applications such as eMule, eDonkey, BitTorrent, iMesh etc. |
| IM | IM (Instant Messaging) refers to chat applications. Chat is real-time communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any member can type a message that will appear on the monitors of all the other participants. |

**Table 86** Configuration > IDP > Signature > Attack Types (continued)

| TYPE | DESCRIPTION |
|---|---|
| VirusWorm | A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources thus slowing or stopping other tasks.<br>The IDP VirusWorm category refers to network-based viruses and worms. The Anti-Virus (AV) screen refers to file-based viruses and worms. Refer to the anti-virus chapter for additional information on file-based anti-virus scanning in the device. |
| Porn | The device can block web sites if their URLs contain certain pornographic words. It cannot block web pages containing those words if the associated URL does not. |
| WebAttacks | Web attack signatures refer to attacks on web servers such as IIS (Internet Information Services). |
| SPAM | Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Refer to the anti-spam chapter for more detailed information. |

## 15.2.2 Intrusion Severity

Intrusions are assigned a severity level based on the following table. The intrusion severity level then determines the default signature action.

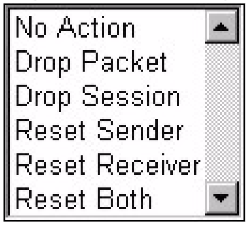
**Table 87** Configuration > IDP > Signature > Intrusion Severity

| SEVERITY | DESCRIPTION |
|---|---|
| Severe | These are intrusions that try to run arbitrary code or gain system privileges. |
| High | These are known serious vulnerabilities or intrusions that are probably not false alarms. |
| Medium | These are medium threats, access control intrusions or intrusions that could be false alarms. |
| Low | These are mild threats or intrusions that could be false alarms. |
| Very Low | These are possible intrusions caused by traffic such as Ping, trace route, ICMP queries etc. |

## 15.2.3 Signature Actions

You can enable/disable individual signatures. You can log and/or have an alert sent when traffic meets a signature criteria. You can also change the default action to be taken when a packet or stream matches a signature. The following figure and table describes these actions. Note that in addition to these actions, a log may be generated or an alert sent, if those check boxes are selected and the signature is enabled.

**Figure 111** Configuration > IDP > Signature > Actions



The following table describes signature actions.

**Table 88** Configuration > IDP > Signature > Actions

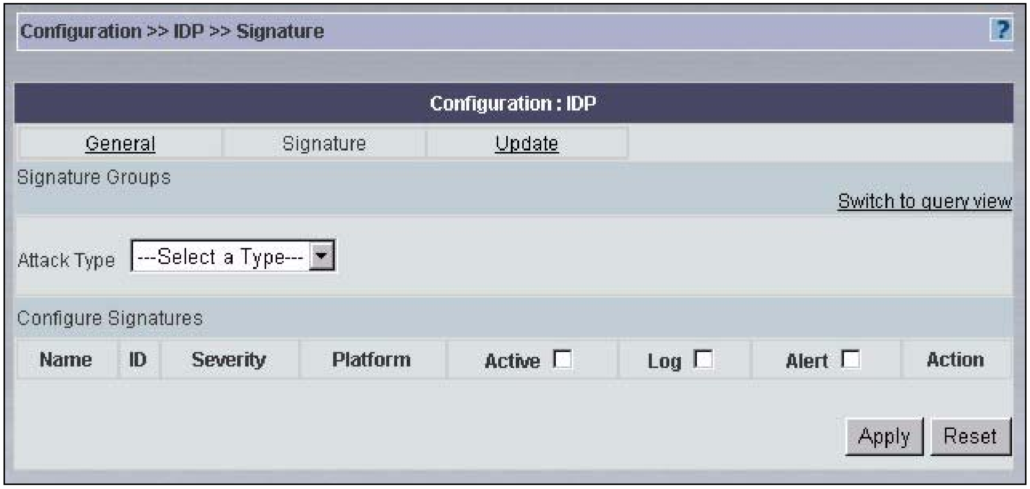
| ACTION | DESCRIPTION |
|---|---|
| No Action | The intrusion is detected but no action is taken. |
| Drop Packet | The packet is silently discarded. |
| Drop Session | When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Reset Sender | When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Reset Receiver | When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Reset Both | When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |

## 15.2.4 Configuring IDP Signatures

Use this screen to see the device's "group view" signature screen where you can view signatures by attack type. To search for signatures based on other criteria such as signature name or ID, then click the **Switch to query view** link to go to the "query view" screen.

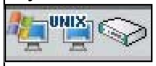
You can take actions on these signatures as described in Section 15.2.3 on page 212. To revert to the default actions or to save sets of actions, go to the **Device > Signature Profile > Backup & Restore** screen.

**Figure 112** Configuration > IDP > Signature (Group View)



The following table describes the labels in this screen.

**Table 89** Configuration > IDP > Signature (Group View)

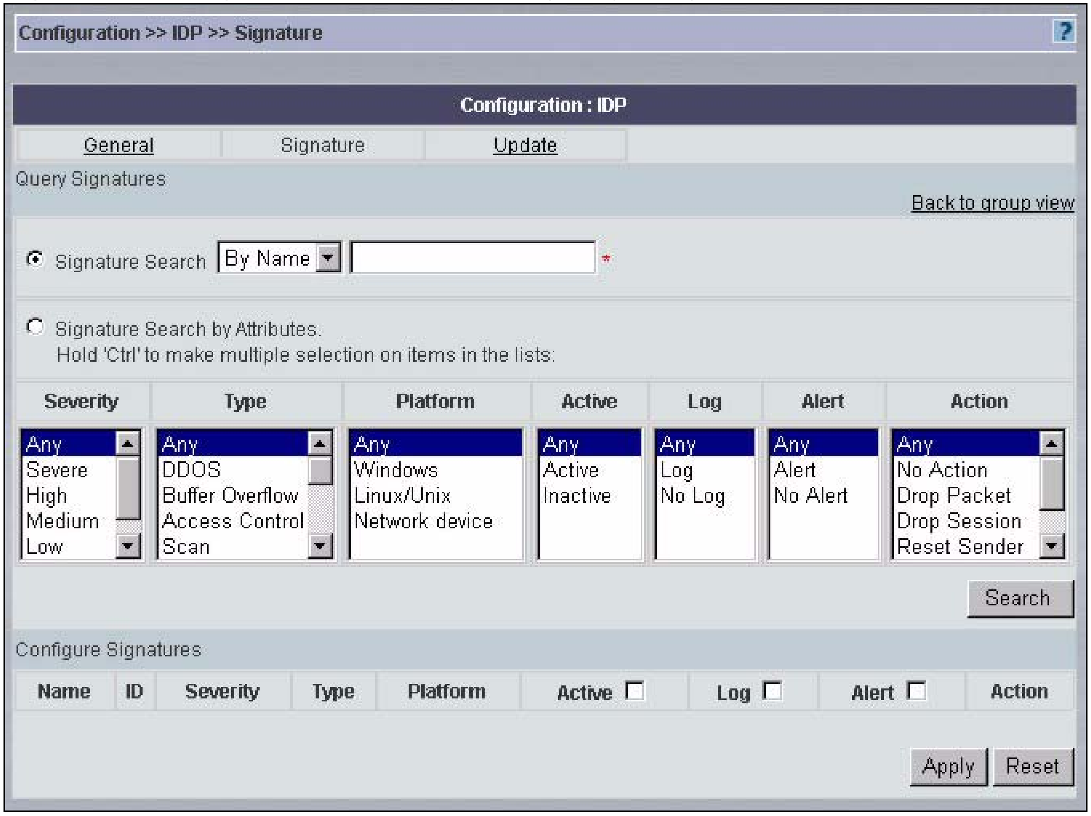
| LABEL | DESCRIPTION |
|---|---|
| Switch to query view | Click this hyperlink to go to a screen where you can search for signatures based on criteria other than attack type. |
| Attack Type | Select the type of signatures you want to view from the list box. See Section 15.2.1 on page 210 for information on types of signatures.<br>The table displays the signatures of the type that you selected. Click a column's header to sort the entries by that attribute. |
| Name | The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion. |
| ID | Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information. |
| Severity | This field displays the level of threat that the intrusion may pose. See Table 87 on page 212 for more information on intrusion severity. |
| Platform | This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device, respectively.<br> |
| Active | Select the check box in the heading row to automatically select all check boxes and enable all signatures.<br>Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Log | Select this check box to have a log generated when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Alert | You can only edit the **Alert** check box when the corresponding **Log** check box is selected.<br>Select this check box to have an e-mail sent when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Action | You can change the default signature action here. See Table 88 on page 213 for more details on actions. |
| Apply | Click this button to save your changes back to the device. |
| Reset | Click this button to begin configuring this screen afresh. |

### 15.2.5 Query View

Use this screen to see the device's "group view" signature screen, then click the **Switch to query view** link to go to this 'query view" screen.

Use this screen to search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, whether or not they are active, log options, alert options or actions.

**Figure 113** Configuration > IDP > Signature (Query View)



The following table describes the fields in this screen.

**Table 90** Configuration > IDP > Signature (Query View)

| LABEL | DESCRIPTION |
|---|---|
| Back to group view | Click this button to go to the IDP group view screen where IDP signatures are grouped by attack type. |
| Signature Search | Select this to search for a specific signature name or ID (that you already know). Then select whether to search the signatures by name or ID. Then enter the name (or part of the name) or the complete ID number of the signature(s) that you want to find.<br>Note: A partial name may be searched but a complete ID number must be entered before a match can be found. |
| Signature Search by Attributes | Select this to search for signatures that match the criteria that you specify. Then select the criteria to search for. Hold down the [Ctrl] key if you want to make multiple selections from a list of attributes. |
| Severity | Search for signatures by severity level(s) (see Table 87 on page 212). |

**Table 90** Configuration > IDP > Signature (Query View) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | Search for signatures by attack type(s) (see Table 86 on page 211). Attack types are known as policy types in the group view screen. |
| Platform | Search for signatures created to prevent intrusions targeting specific operating system(s). |
| Active | Search for enabled and/or disabled signatures here. |
| Log | Search for signatures by log option here. |
| Alert | Search for signatures by alert option here. |
| Action | Search for signatures by the response the device takes when a packet matches a signature. See Table 88 on page 213 for action details. |
| Search | Click this button to begin the search. The results display at the bottom of the screen. Results may be spread over several pages depending on how broad the search criteria selected were. The tighter the criteria selected, the fewer the signatures returned. |
| Configure Signatures | The results display in a table showing the criteria as selected in the search. Click a column's header to sort the entries by that attribute. |
| Name | The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion. |
| ID | Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information. |
| Severity | This field displays the level of threat that the intrusion may pose. See Table 87 on page 212 for more information on intrusion severity. |
| Type | This field displays the what type of signature each one is. See Section 15.2.1 on page 210 for information on types of signatures. |
| Platform | This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device, respectively.<br>UNIX |
| Active | Select the check box in the heading row to automatically select all check boxes and enable all signatures.<br>Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Log | Select this check box to have a log generated when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |

**Table 90** Configuration > IDP > Signature (Query View) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Alert | You can only edit the **Alert** check box when the corresponding **Log** check box is selected.<br>Select this check box to have an e-mail sent when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Action | You can change the default signature action here. See Table 88 on page 213 for more details on actions. |
| Apply | Click this button to save your changes back to the device. |
| Reset | Click this button to begin configuring this screen afresh. |

## 15.3 Update

The device comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

You should have already registered the device at myZyXEL.com (http://www.myzyxel.com/myzyxel/) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

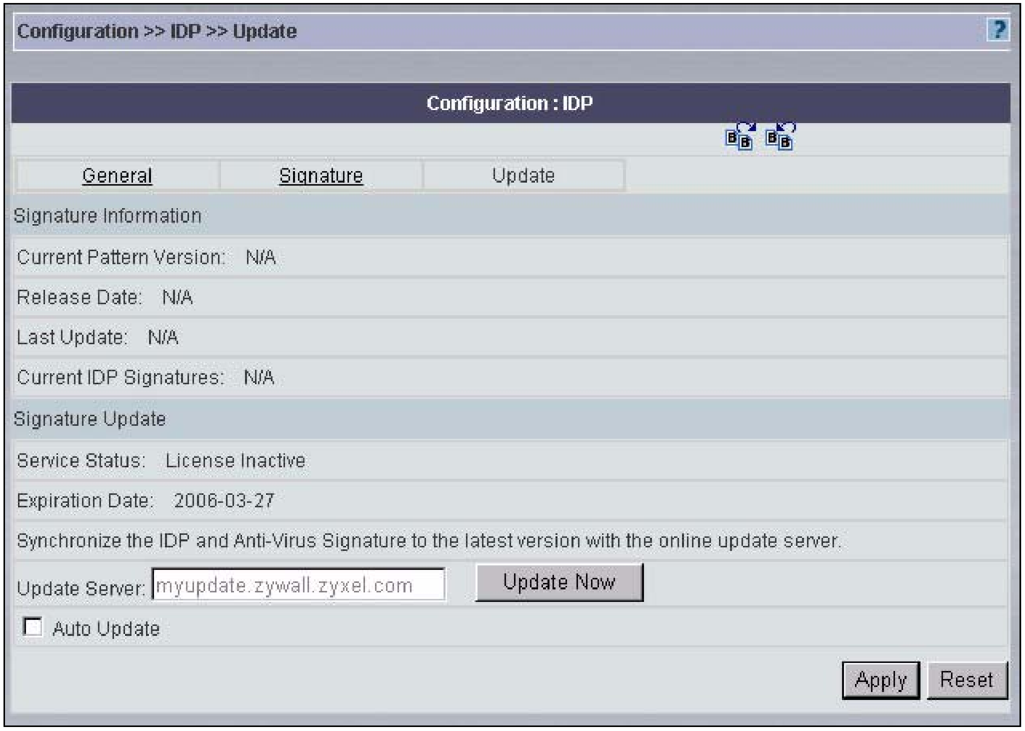
When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

File-based anti-virus signatures (see the anti-virus chapter) are included with IDP signatures. When you download new signatures using the anti-virus **Update** screen, IDP signatures are also downloaded. The version number changes both in the anti-virus **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

The device does not have to reboot when you upload new signatures.

Click **Configuration** > **IDP** > **Update**.

**Figure 114** Configuration > IDP > Update



Configuration >> IDP >> Update

Configuration : IDP

General | Signature | Update

Signature Information

Current Pattern Version: N/A

Release Date: N/A

Last Update: N/A

Current IDP Signatures: N/A

Signature Update

Service Status: License Inactive

Expiration Date: 2006-03-27

Synchronize the IDP and Anti-Virus Signature to the latest version with the online update server.

Update Server: myupdate.zywall.zyxel.com

☐ Auto Update

The following table describes the labels in this screen.

**Table 91** Configuration > IDP > Update

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | |
| Current Pattern Version | This field displays the signatures version number currently used by the device. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them.<br>This number increments as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications. |
| Release Date | This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created. |
| Last Update | This field displays the last date and time you downloaded new signatures to the device. It displays **N/A** if you have not downloaded any new signatures yet. |
| Current IDP Signatures | This field displays the number of IDP-related signatures. |
| Signature Update | |
| Service Status | This field displays **License Inactive** if you have not yet activated your trial or iCard license at myZyXEL.com.<br>It displays **License Inactive** and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired).<br>It displays **Trial Active** and an expiration date when you have activated your trial license.<br>It displays **License Active** and an expiration date when you have activated your iCard license (the expiration date is the date it will expire). |
| Update Server | This is the URL of the signature server from which you download signatures. |

**Table 91** Configuration > IDP > Update (continued)

| LABEL | DESCRIPTION |
|---|---|
| Update Now | Click this button to begin downloading signatures from the **Update Server** immediately. |
| Auto Update | Select the check box to configure a schedule for automatic signature updates. The **Hourly**, **Daily** and **Weekly** fields display when the check box is selected. The device then automatically downloads signatures from the **Update Server** regularly at the time and/or day you specify. |
| Hourly | Select this option to have the device check the update server for new signatures every hour. This may be advisable when new intrusions are currently spreading throughout the Internet. |
| Daily | Select this option to have the device check the update server for new signatures every day at the hour you select from the list box. The device uses a 24-hour clock. For example, choose 15 from the **O'clock** list box to have the device check the update server for new signatures at 3 PM every day. |
| Weekly | Select this option to have the device check the update server for new signatures once a week on the day and hour you select from the list boxes. The device uses a 24-hour clock, so for example, choose **Wednesday** and 15 from the respective list boxes to have the device check the update server for new signatures at 3PM every Wednesday. |
| Apply | Click this button to save your changes back to the device. |
| Reset | Click this button to close this screen without saving any changes. |

# 16

# Configuration > Anti-Virus

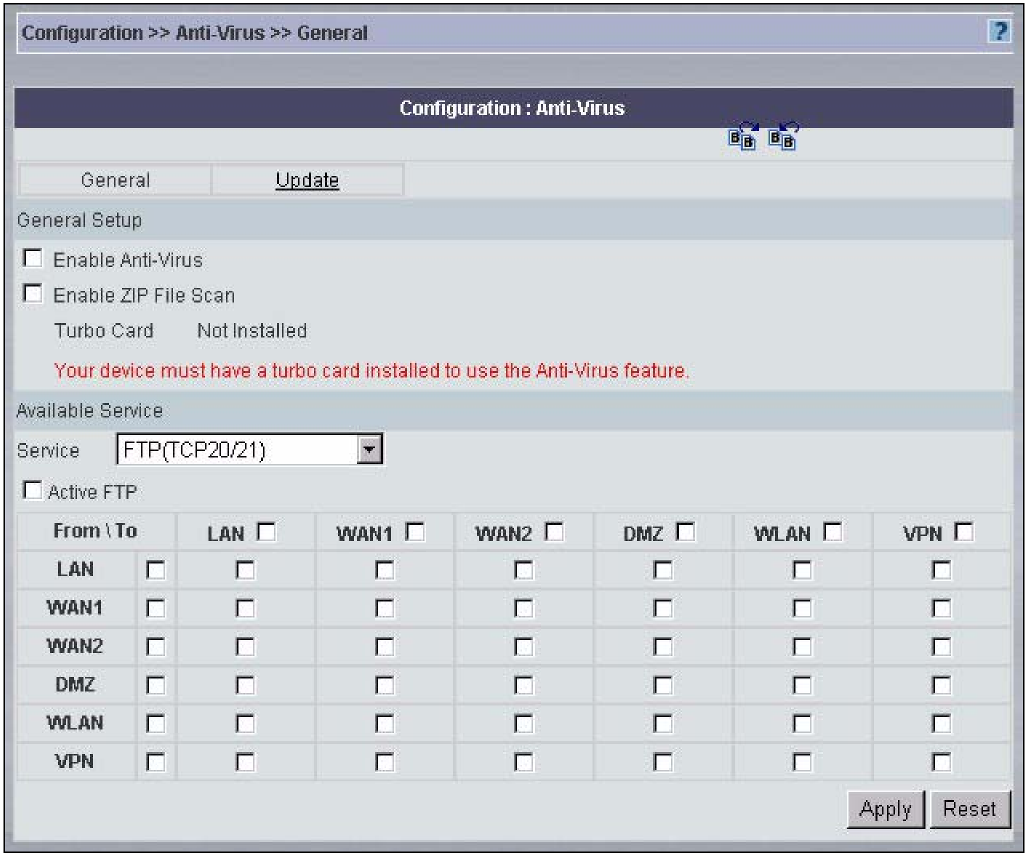
This section shows you how to configure the **Anti-Virus** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 16.1 General Anti-Virus Setup

Click **Configuration** > **Anti-Virus > General** to display the configuration screen shown next.

✍ Before you use the anti-virus feature, you must register for the service (refer to the chapter on registration for more information).

**Figure 115** Configuration > Anti-Virus > General



Configuration >> Anti-Virus >> General

Configuration : Anti-Virus

General | Update

General Setup

□ Enable Anti-Virus

□ Enable ZIP File Scan

Turbo Card Not Installed

Your device must have a turbo card installed to use the Anti-Virus feature.

Available Service

Service FTP(TCP20/21)

□ Active FTP

| From \ To | | LAN □ | WAN1 □ | WAN2 □ | DMZ □ | WLAN □ | VPN □ |
|---|---|---|---|---|---|---|---|
| LAN | □ | □ | □ | □ | □ | □ | □ |
| WAN1 | □ | □ | □ | □ | □ | □ | □ |
| WAN2 | □ | □ | □ | □ | □ | □ | □ |
| DMZ | □ | □ | □ | □ | □ | □ | □ |
| WLAN | □ | □ | □ | □ | □ | □ | □ |
| VPN | □ | □ | □ | □ | □ | □ | □ |

The following table describes the labels in this screen.

**Table 92** Configuration > Anti-Virus > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Anti-Virus | Select this check box to check traffic for viruses. The anti-virus scanner works on the following.<br>FTP traffic using TCP ports 20 and 21<br>HTTP traffic using TCP ports 80, 8080 and 3128<br>POP3 traffic using TCP port 110<br>SMTP traffic using TCP port 25 |
| Enable ZIP File Scan | Select this check box to have the device scan a ZIP file (with the “zip”, “gzip” or “gz” file extension). The device first decompresses the ZIP file and then scans the contents for viruses.<br>Note: The device decompresses a ZIP file once. The device does NOT decompress any ZIP file(s) within the ZIP file. |
| Turbo Card | This field displays whether or not a device Turbo Card is installed.<br>Note: You cannot configure and save the IDP and Anti-Virus screens if the device Turbo Card is not installed. |
| Available Service | |
| Service | This field displays the service names and standard port numbers that identify them. Select a service to display and configure anti-virus settings for it. |

**Table 92** Configuration > Anti-Virus > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active | Select **Active** to enable the anti-virus scanner for the selected service. |
| From, To | Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column.<br>For example, **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the device or the device itself. The device does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the device through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the device's LAN interface. The device checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The device checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the device. This is the case when the device is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the device. The device checks the traffic after decrypting it (before encrypting it again).<br>Note: The VPN connection directions apply to the traffic going to or from the device's VPN tunnels. They do not apply to other VPN traffic for which the device is not one of the gateways (VPN pass-through traffic). |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

## 16.2 Signature Update

The device comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

You should have already registered the device at myZyXEL.com (http://www.myzyxel.com/myzyxel/) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

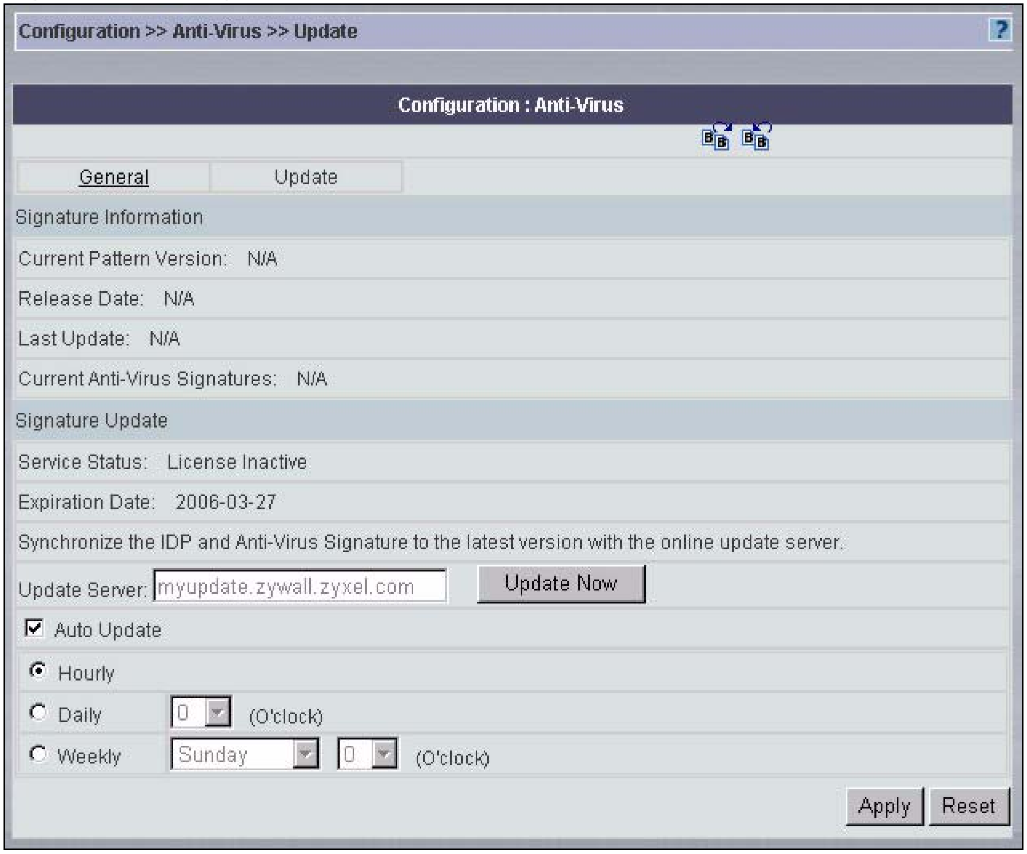
When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

IDP signatures (see the chapters on IDP) are included with file-based anti-virus signatures. When you download new signatures using the IDP **Update** screen, anti-virus signatures are also downloaded. The version number changes both in the IDP **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

The device does not have to reboot when you upload new signatures.

Click **Configuration** > **Anti-Virus** > **Update**.

**Figure 116** Configuration > Anti-Virus > Update



Configuration >> Anti-Virus >> Update

Configuration : Anti-Virus

Signature Information

Current Pattern Version: N/A

Release Date: N/A

Last Update: N/A

Current Anti-Virus Signatures: N/A

Signature Update

Service Status: License Inactive

Expiration Date: 2006-03-27

Synchronize the IDP and Anti-Virus Signature to the latest version with the online update server.

Update Server: myupdate.zywall.zyxel.com

☑ Auto Update

● Hourly

○ Daily 0 (O'clock)

○ Weekly Sunday 0 (O'clock)

The following table describes the labels in this screen.

**Table 93** Configuration > Anti-Virus > Update

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | |
| Current Pattern Version | This field displays the signatures version number currently used by the device. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them.<br>This number increments as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications. |
| Release Date | This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created. |
| Last Update | This field displays the last date and time you downloaded new signatures to the device. It displays **N/A** if you have not downloaded any new signatures yet. |
| Current Anti-Virus Signatures | This field displays the number of Anti-Virus-related signatures. |
| Signature Update | |
| Service Status<br>Expiration Date | This field displays **License Inactive** if you have not yet activated your trial or iCard license at myZyXEL.com.<br>It displays **License Inactive** and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired).<br>It displays **Trial Active** and an expiration date when you have activated your trial license.<br>It displays **License Active** and an expiration date when you have activated your iCard license (the expiration date is the date it will expire). |
| Update Server | This is the URL of the signature server from which you download signatures. |
| Update Now | Click this button to begin downloading signatures from the **Update Server** immediately. |
| Auto Update | Select the check box to configure a schedule for automatic signature updates. The **Hourly**, **Daily** and **Weekly** fields display when the check box is selected. The device then automatically downloads signatures from the **Update Server** regularly at the time and/or day you specify. |
| Hourly | Select this option to have the device check the update server for new signatures every hour. This may be advisable when new viruses are currently spreading throughout the Internet. |
| Daily | Select this option to have the device check the update server for new signatures every day at the hour you select from the list box. The device uses a 24-hour clock. For example, choose 15 from the **O'clock** list box to have the device check the update server for new signatures at 3 PM every day. |
| Weekly | Select this option to have the device check the update server for new signatures once a week on the day and hour you select from the list boxes. The device uses a 24-hour clock, so for example, choose **Wednesday** and **15** from the respective list boxes to have the device check the update server for new signatures at 3PM every Wednesday. |
| Apply | Click this button to save your changes back to the device. |
| Reset | Click this button to close this screen without saving any changes. |

# 17

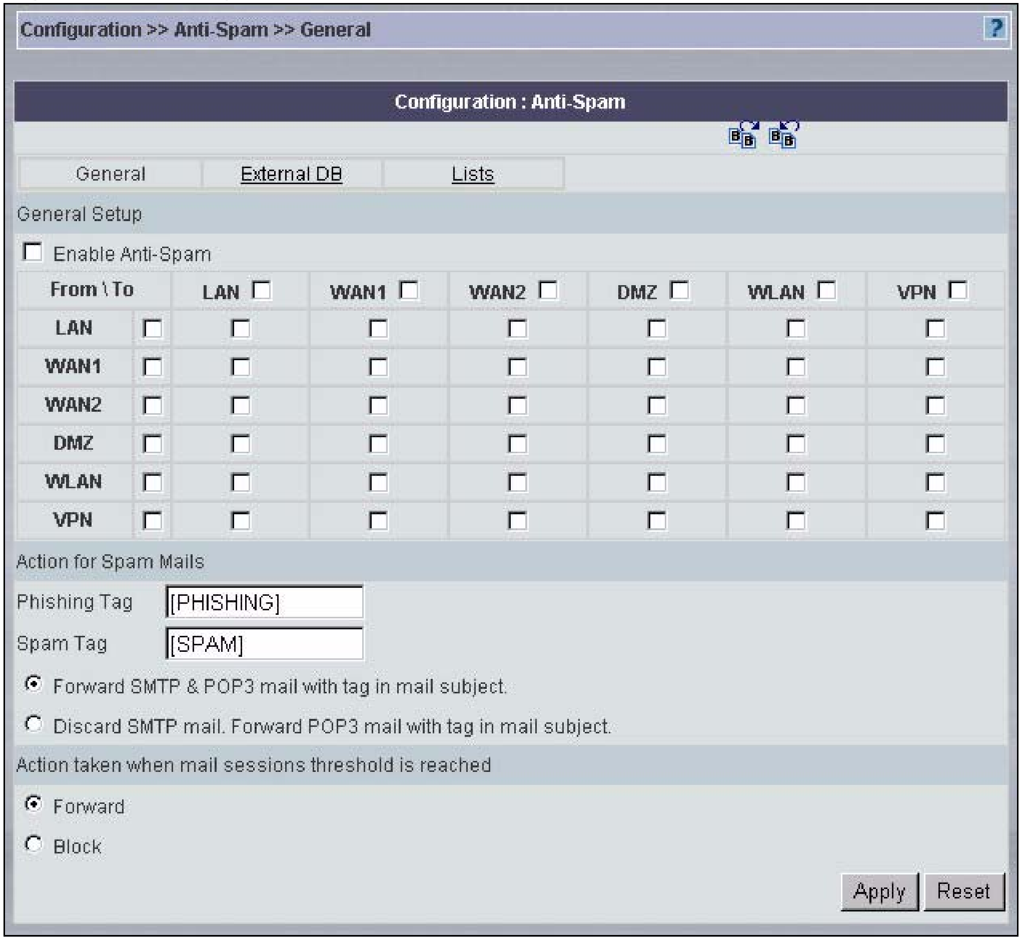
# Configuration > Anti-Spam

This section shows you how to configure the **Anti-Spam** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 17.1 Anti-Spam General Screen

Click **Configuration** > **Anti-Spam > General** to open the **Anti-Spam General** screen. Use this screen to turn the anti-spam feature on or off and set how the device treats spam.

**Figure 117** Configuration > Anti-Spam > General



Configuration >> Anti-Spam >> General

Configuration : Anti-Spam

General | External DB | Lists

General Setup

□ Enable Anti-Spam

| From \ To | | LAN □ | WAN1 □ | WAN2 □ | DMZ □ | WLAN □ | VPN □ |
|---|---|---|---|---|---|---|---|
| LAN | □ | □ | □ | □ | □ | □ | □ |
| WAN1 | □ | □ | □ | □ | □ | □ | □ |
| WAN2 | □ | □ | □ | □ | □ | □ | □ |
| DMZ | □ | □ | □ | □ | □ | □ | □ |
| WLAN | □ | □ | □ | □ | □ | □ | □ |
| VPN | □ | □ | □ | □ | □ | □ | □ |

Action for Spam Mails

Phishing Tag [PHISHING]

Spam Tag [SPAM]

● Forward SMTP & POP3 mail with tag in mail subject.

○ Discard SMTP mail. Forward POP3 mail with tag in mail subject.

Action taken when mail sessions threshold is reached

● Forward

○ Block

The following table describes the labels in this screen.

**Table 94** Configuration > Anti-Spam > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Anti-Spam | Select this check box to check traffic for spam SMTP (TCP port 25 and POP3 (TCP port 110) e-mail. |
| From, To | Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column.<br>For example, **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the device or the device itself. The device does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the device through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the device's LAN interface. The device checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The device checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the device. This is the case when the device is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the device. The device checks the traffic after decrypting it (before encrypting it again).<br>Note: The VPN connection directions apply to the traffic going to or from the device's VPN tunnels. They do not apply to other VPN traffic for which the device is not one of the gateways (VPN pass-through traffic). |
| Action for Spam Mails | Use this section to set how the device is to handle spam mail. |
| Phishing Tag | Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that the anti-spam external database classifies as phishing.<br>Note: You must register for and enable the anti-spam external database feature in order for the device to use this tag (see the chapter on registration for details). |
| Spam Tag | Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that the device classifies as spam. |
| Forward SMTP & POP3 mail with tag in mail subject | Select this radio button to have the device forward spam e-mail with the tag that you define.<br>Even if you plan to use the discard option, you may want to use this initially as a test to check how accurate your anti-spam settings are. Check the e-mail the device forwards to you to make sure that unwanted e-mail is marked as spam and legitimate e-mail is not marked as spam. |
| Discard SMTP mail. Forward POP3 mail with tag in mail subject | Select this radio button to have the device discard spam SMTP e-mail. The device will still forward spam POP3 e-mail with the tag that you define. |

**Table 94** Configuration > Anti-Spam > General (continued)

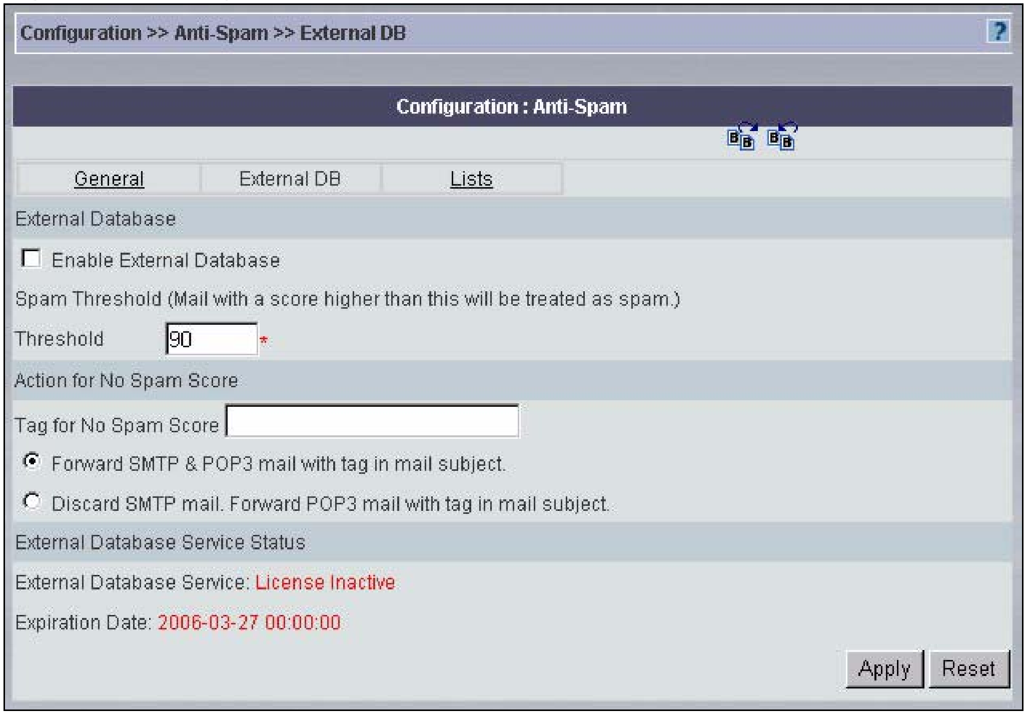
| LABEL | DESCRIPTION |
|---|---|
| Action taken when mail sessions threshold is reached | The anti-spam feature limits the number of concurrent e-mail sessions. An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the device. Use this section to configure what the device does when the number of concurrent e-mail sessions goes over the threshold (see the appendix of product specifications for the threshold).<br>Select **Forward** to have the device allow the excess e-mail sessions without any spam filtering.<br>Select **Block** to have the device drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 17.2 Anti-Spam External DB Screen

Click **Configuration** > **Anti-Spam** > **External DB** to display the **Anti-Spam External DB** screen.

Use this screen to enable or disable the use of the anti-spam external database. You can also configure the spam threshold and what to do when no valid spam score is received. You must register for this service before you can use it (see the chapter on registration for details).

**Figure 118** Configuration > Anti-Spam > External DB


Configuration >> Anti-Spam >> External DB
?
Configuration : Anti-Spam
General
External DB
Lists
Apply
Reset

External Database

☐ Enable External Database

Spam Threshold (Mail with a score higher than this will be treated as spam.)

Threshold 90 *

Action for No Spam Score

Tag for No Spam Score

● Forward SMTP & POP3 mail with tag in mail subject.

○ Discard SMTP mail. Forward POP3 mail with tag in mail subject.

External Database Service Status

External Database Service: License Inactive

Expiration Date: 2006-03-27 00:00:00

The following table describes the labels in this screen.

**Table 95** Configuration > Anti-Spam > External DB

| LABEL | DESCRIPTION |
|---|---|
| External Database | |
| Enable External Database | Enable the anti-spam external database feature to have the device calculate a digest of an e-mail and send it to an anti-spam external database.<br>The anti-spam external database sends a spam score for the e-mail back to the device. |
| Spam Threshold | The anti-spam external database checks an e-mail's digest and sends back a score that rates how likely the e-mail is to be spam. The possible range for the spam score is 0~100. The closer the score is to 100, the more likely the e-mail is to be spam.<br>Set the spam threshold (from 0 to 100) for considering an e-mail to be spam. The device classifies any e-mail with a spam score greater than or equal to the threshold as spam. It classifies any e-mail with a spam score less than the threshold as not being spam.<br>A lower threshold catches more spam e-mails, but may also classify more legitimate e-mail as spam.<br>A higher threshold lessens the chance of classifying legitimate e-mail as spam, but may allow more spam to get through. |
| Action for No Spam Score | Use this field to configure what the device does if it does not receive a valid response from the anti-spam external database.<br>If the device does not receive a response within seven seconds, it sends the e-mail digest a second time. If the device still does not receive a response after another seven seconds, it takes the action that you configure here. The device also takes this action if it receives an invalid response.<br>Here are possible reasons that would cause the device to take this action:<br>1. The device was not able to connect to the anti-spam external database.<br>2. The device connected to the anti-spam external database, but there was no HTTP response within seven seconds.<br>3. The device received an error code from the anti-spam external database.<br>4. The device received an invalid spam score (for example a number higher than 100).<br>5. The device received an unknown response to the anti-spam query. |
| Tag for No Spam Score | Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that it forwards if a valid spam score was not received within ten seconds. |
| Forward SMTP & POP3 mail with tag in mail subject | Select this radio button to have the device forward mail with the tag that you define. |
| Discard SMTP mail. Forward POP3 mail with tag in mail subject | Select this radio button to have the device discard SMTP mail. The device will still forward POP3 mail with the tag that you define. |
| External Database Service Status | This read-only field displays the status of your anti-spam external database service registration and activation.<br>**License Inactive** displays if you have not successfully registered and activated the anti-spam external database service.<br>**License Inactive** and the date your subscription expired display if your subscription to the anti-spam external database service has expired.<br>**License Active** and the subscription expiration date display if you have successfully registered the device and activated the anti-spam external database service.<br>**Trial Active** and the trial subscription expiration date display if you have successfully registered the device and activated the anti-spam external database service trial subscription. |

**Table 95** Configuration > Anti-Spam > External DB (continued)

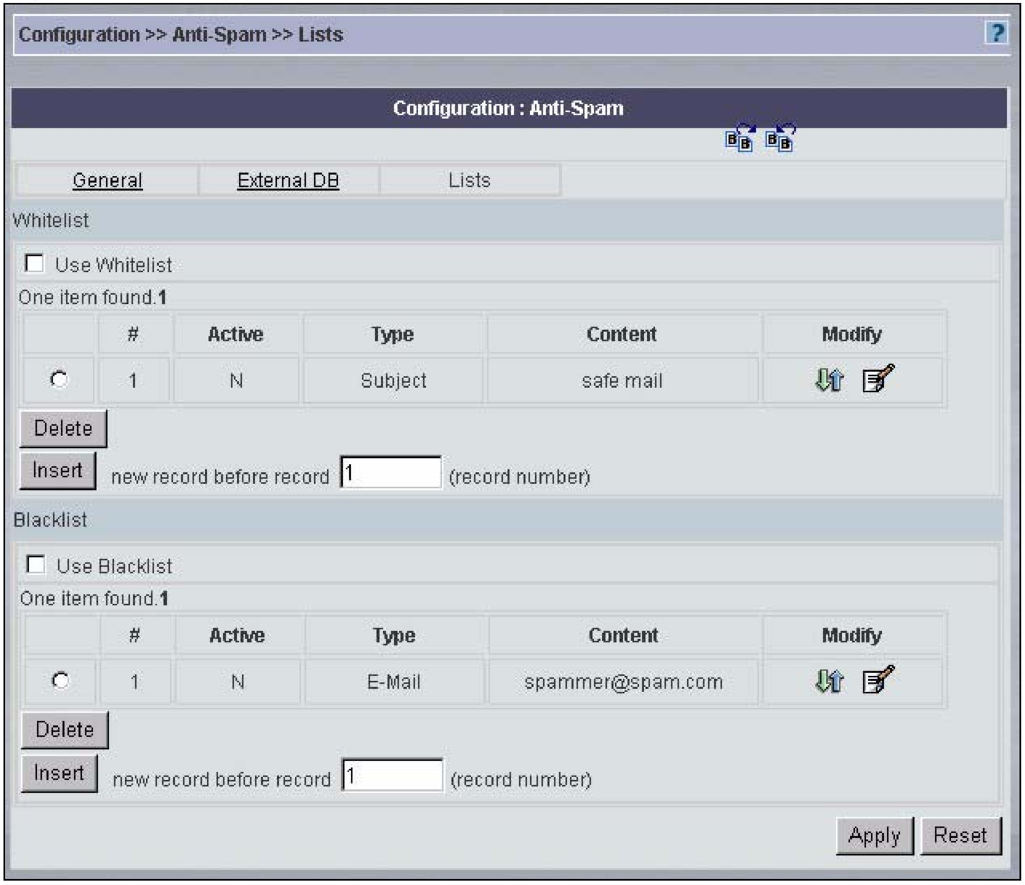
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 17.3 Anti-Spam Lists Screen

Click **Configuration** > **Anti-Spam** > **Lists** to display the **Anti-Spam Lists** screen.

Configure the whitelist to identify legitimate e-mail. Configure the blacklist to identify spam e-mail. You can create whitelist or blacklist entries based on the sender's IP address or e-mail address. You can also create entries that check for particular MIME headers, MIME header values or specific subject text.

**Figure 119** Configuration > Anti-Spam > Lists


Configuration >> Anti-Spam >> Lists
Configuration : Anti-Spam
General
External DB
Lists
Whitelist

☐ Use Whitelist

One item found.**1**

|  | # | Active | Type | Content | Modify |
|---|---|---|---|---|---|
| ○ | 1 | N | Subject | safe mail |  |

Insert new record before record 1 (record number)

☐ Use Blacklist

One item found.**1**

|  | # | Active | Type | Content | Modify |
|---|---|---|---|---|---|
| ○ | 1 | N | E-Mail | spammer@spam.com |  |

Insert new record before record 1 (record number)

The following table describes the labels in this screen.

**Table 96** Configuration > Anti-Spam > Lists

| LABEL | DESCRIPTION |
|---|---|
| Whitelist |  |
| Use Whitelist | Select this check box to have the device forward e-mail that matches a whitelist entry without doing any more anti-spam checking on that individual e-mail. |

**Table 96** Configuration > Anti-Spam > Lists (continued)

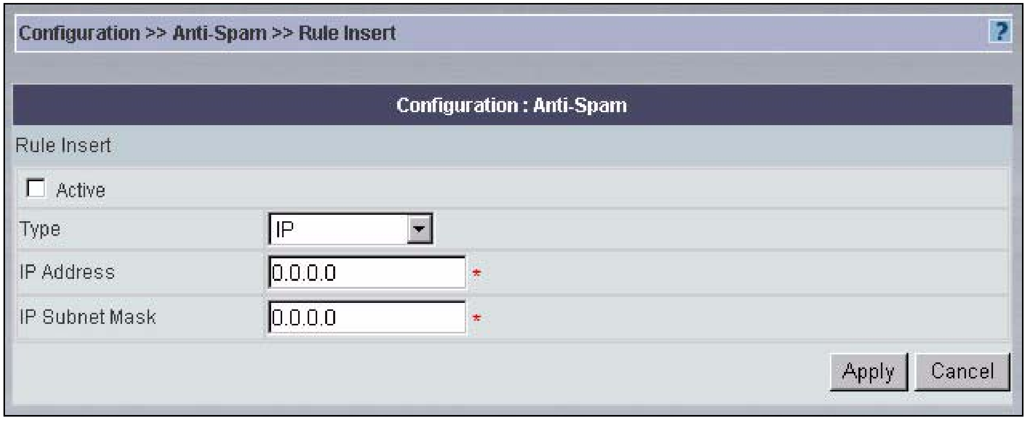
| LABEL | DESCRIPTION |
|---|---|
| # | This field shows the index number of the entry. |
| Active | This field shows whether or not an entry is turned on. |
| Type | This field displays whether the entry is based on the e-mail's source IP address, source e-mail address, an MIME header or the e-mail's subject. |
| Content | This field displays the source IP address, source e-mail address, MIME header or subject content for which the entry checks. |
| Modify | Click the **Edit** icon to change the entry. Click the **Remove** icon to delete the entry. Click the **Move** icon to change the entry's position in the list. |
| Delete | Select the radio button next to an entry, and click **Delete** to remove the entry. |
| Insert | Type the index number where you want to put an entry. For example, if you type 6, your new entry becomes number 6 and the previous entry 6 (if there is one) becomes entry 7.<br>Click **Insert** to display the screen where you edit an entry. |
| Blacklist | |
| Use Blacklist | Select this check box to have the device treat e-mail that matches a blacklist entry as spam. |
| # | This field shows the index number of the entry. |
| Active | This field shows whether or not an entry is turned on. |
| Type | This field displays whether the entry is based on the e-mail's source IP address, source e-mail address, an MIME header or the e-mail's subject. |
| Content | This field displays the source IP address, source e-mail address, MIME header or subject content for which the entry checks. |
| Modify | Click the **Edit** icon to change the entry. Click the **Remove** icon to delete the entry. Click the **Move** icon to change the entry's position in the list. |
| Delete | Select the radio button next to an entry, and click **Delete** to remove the entry. |
| Insert | Type the index number where you want to put an entry. For example, if you type 6, your new entry becomes number 6 and the previous entry 6 (if there is one) becomes entry 7.<br>Click **Insert** to display the screen where you edit an entry. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 17.3.1 Anti-Spam Lists Edit Screen

Click **Configuration** > **Anti-Spam** > **Lists** to display the **Anti-Spam Lists** screen. To create a new anti-spam whitelist or blacklist entry, type the index number where you want to put the entry and click **Insert** to display the **ANTI-SPAM Rule Edit** screen. You can also click the **Edit** icon next to an existing entry.

Use this screen to configure an anti-spam whitelist entry to identify legitimate e-mail or a blacklist entry to identify spam e-mail. You can create entries based on the sender's IP address or e-mail address. You can also create entries that check for particular MIME headers, MIME header values or specific subject text.

**Figure 120** Configuration > Anti-Spam > Lists > Add/Edit



Configuration >> Anti-Spam >> Rule Insert

Configuration : Anti-Spam

Rule Insert

| | |
|---|---|
| □ Active | |
| Type | IP |
| IP Address | 0.0.0.0 * |
| IP Subnet Mask | 0.0.0.0 * |

The following table describes the labels in this screen.

**Table 97** Configuration > Anti-Spam > Lists > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Edit | |
| Active | Turn this entry on to have the device use it as part of the whitelist or blacklist. You must also turn on the use of the corresponding list (in the **Anti-Spam Customization** screen) and the anti-spam feature (in the **Anti-Spam General** screen). |
| Type | Use this field to base the entry on the e-mail's source IP address, source e-mail address or an MIME header.<br>Select **IP** to have the device check e-mail for a specific source IP address.<br>You can create whitelist IP address entries for e-mail servers on your LAN or DMZ to speed up the device's processing of your outgoing e-mail.<br>Select **E-Mail** to have the device check e-mail for a specific source e-mail address or domain name.<br>You can create a whitelist entry for your company's domain name (or e-mail accounts) to speed up the device's processing of e-mail sent by your company's employees.<br>Select **MIME Header** to have the device check e-mail for specific MIME headers or values.<br>Configure blacklist MIME header entries to check for e-mail from bulk mail programs or that have content that are commonly used in spam. You can also configure whitelist MIME header entries to allow certain MIME headers or values that identify the e-mail as being from a trusted source.<br>Select **Subject** to have the device check e-mail for specific content in the subject line. |
| IP Address | This field displays when you select the **IP** type. Enter an IP address in dotted decimal notation. |
| IP Subnet Mask | This field displays when you select the **IP** type. Enter the subnet mask here, if applicable. |

**Table 97** Configuration > Anti-Spam > Lists > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| E-Mail Address | This field displays when you select the **E-Mail** type. Enter an e-mail address or domain name (up to 63 ASCII characters).<br>You can enter an individual e-mail address like abc@def.com.<br>If you enter a domain name, the device searches the source e-mail address string after the "@" symbol to see if it matches the domain name. For example, you configure a entry with "def.com" as the domain name. E-mails sent from def.com e-mail addresses such as "abc@def.com" match the entry. E-mails sent from mail.def.com, such as abc@mail.def.com do not match the entry since "mail.def.com" does not match "def.com".<br>You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So "mail.def.com" matches.<br>The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.<br>The device can check up to the first 63 characters of an e-mail's address. The whitelist or blacklist check fails for addresses over 63 characters. However, a whitelist or blacklist entry that uses some text followed by a wildcard only requires the device to check the number of characters before the wildcard. So the check would still work for addresses longer than 63 characters. For example, if you used "abc*", the device would only check up to the first three characters of the e-mail address. |
| Header | This field displays when you select the **MIME Header** type.<br>Type the header part of an MIME header (up to 63 ASCII characters).<br>In an MIME header, the header is the part that comes before the colon (:).<br>For example, if you want the whitelist or blacklist entry to check for the MIME header "X-MSMail-Priority: Normal", enter "X-MSMail-Priority" here as the MIME header. |
| Value | This field displays when you select the **MIME Header** type.<br>Type the value part of an MIME header (up to 63 ASCII characters).<br>In an MIME header, the part that comes after the colon is the value.<br>For example, if you want the whitelist or blacklist entry to check for the MIME header "X-MSMail-Priority: Normal", enter "Normal" here as the MIME value. |
| Subject | This field displays when you select the **Subject** type. Enter up to 63 ASCII characters of text to check for in the e-mail headers. Spaces are allowed.<br>You can use a wildcard (*). For example, if you configure "*good", any e-mail subject that ends in "good" matches. So "this is very good" and "this is not so good" both match.<br>The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.<br>The device can check up to the first 63 characters of an e-mail's subject. The whitelist or blacklist check fails for subjects over 63 characters. However, a whitelist or blacklist entry that uses some text followed by a wildcard only requires the device to check the number of characters before the wildcard. So the check would still work for subjects longer than 63 characters. For example, if you used "abc*", the device would only check up to the first three characters of the e-mail subject. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 18

# Configuration > Content Filter

This section shows you how to configure the **Content Filter** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

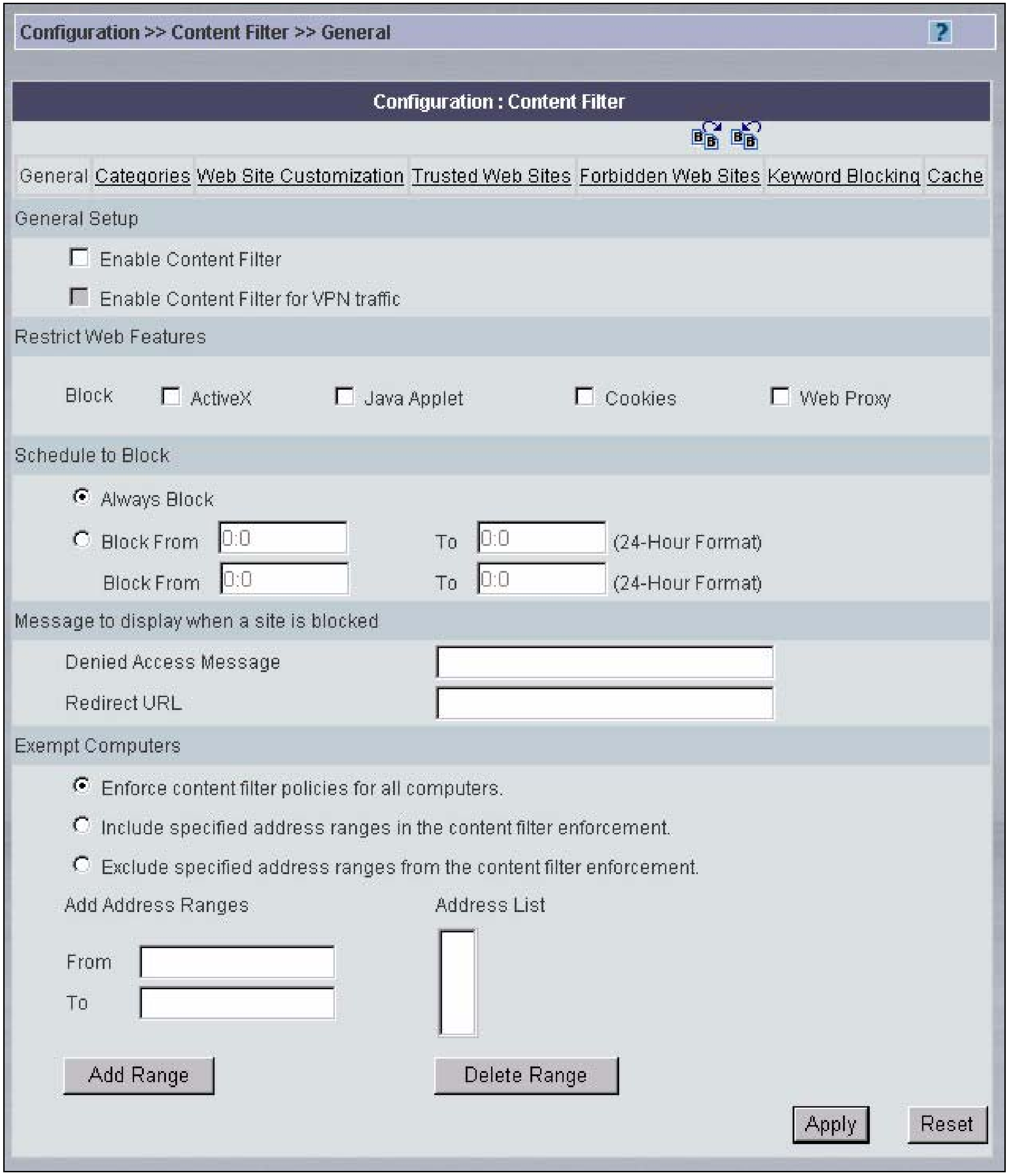
## 18.1 Content Filter General Screen

Click **Configuration** > **Content Filter > General** to open the **CONTENT FILTER General** screen.

Content filtering allows you to block certain web features, such as Cookies, and/or block access to specific websites.

Use this screen to enable content filtering, configure a schedule, and create a denial message. You can also choose specific computers to be included in or excluded from the content filtering configuration.

**Figure 121** Configuration > Content Filter > General



Configuration >> Content Filter >> General

Configuration : Content Filter

General | Categories | Web Site Customization | Trusted Web Sites | Forbidden Web Sites | Keyword Blocking | Cache

General Setup

□ Enable Content Filter

□ Enable Content Filter for VPN traffic

Restrict Web Features

Block □ ActiveX □ Java Applet □ Cookies □ Web Proxy

Schedule to Block

● Always Block

○ Block From 0:0 To 0:0 (24-Hour Format)

Block From 0:0 To 0:0 (24-Hour Format)

Message to display when a site is blocked

Denied Access Message

Redirect URL

Exempt Computers

● Enforce content filter policies for all computers.

○ Include specified address ranges in the content filter enforcement.

○ Exclude specified address ranges from the content filter enforcement.

Add Address Ranges

From

To

Address List

The following table describes the labels in this screen.

**Table 98** Configuration > Content Filter > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Content Filter | Select this check box to enable the content filter. Content filtering works on HTTP traffic that is using TCP ports 80, 119, 3128 or 8080. |

**Table 98** Configuration > Content Filter > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Content Filter for VPN traffic | Select this check box to have the content filter apply to traffic that the device sends out through a VPN tunnel or receives through a VPN tunnel. The device applies the content filter to the traffic before encrypting it or after decrypting it.<br>Note: The device can apply content filtering on the traffic going to or from the device's VPN tunnels. It does not apply to other VPN traffic for which the device is not one of the gateways (VPN pass-through traffic). |
| Restrict Web Features | Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out. |
| Block<br>ActiveX | ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. |
| Java Applet | Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds. |
| Cookies | Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID. |
| Web Proxy | A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. |
| Schedule to Block | Content filtering scheduling applies to the Filter List, Customized sites and Keywords. Restricted web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. |
| Always Block | Click this option button to have content filtering always active with Time of Day limitations not enforced. This is enabled by default. |
| Block From/To | Click this option button to have content filtering only active during the time interval specified. In the **Block From** and **To** fields, enter the time period, in 24-hour format, during which content filtering will be enforced. |
| Message to display when a site is blocked | |
| Denied Access Message | Enter a message to be displayed when a user tries to access a restricted web site. For example, "Please contact your network administrator." |
| Redirect URL | Enter the URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message.<br>Use "http://" followed by up to 120 ASCII characters. For example, http://192.168.1.17/blocked access. |
| Exempt Computers | |
| Enforce content filter policies for all computers | Select this check box to have all users on your LAN follow content filter policies. |
| Include specified address ranges in the content filter enforcement | Select this check box to have a specific range of users on your LAN follow content filter policies. |

**Table 98** Configuration > Content Filter > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Exclude specified address ranges from the content filter enforcement | Select this check box to exempt a specific range of users on your LAN from content filter policies. |
| Add Address Ranges | |
| From | Type the beginning IP address (in dotted decimal notation) of the specific range of users on your LAN. |
| To | Type the ending IP address (in dotted decimal notation) of the specific range of users on your LAN, then click **Add Range**. |
| Address List | This text field shows the address ranges that are included or excluded. |
| Add Range | Click **Add Range** after you have filled in the **From** and **To** fields above. |
| Delete Range | Click **Delete Range** after you select the range of addresses you wish to delete. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

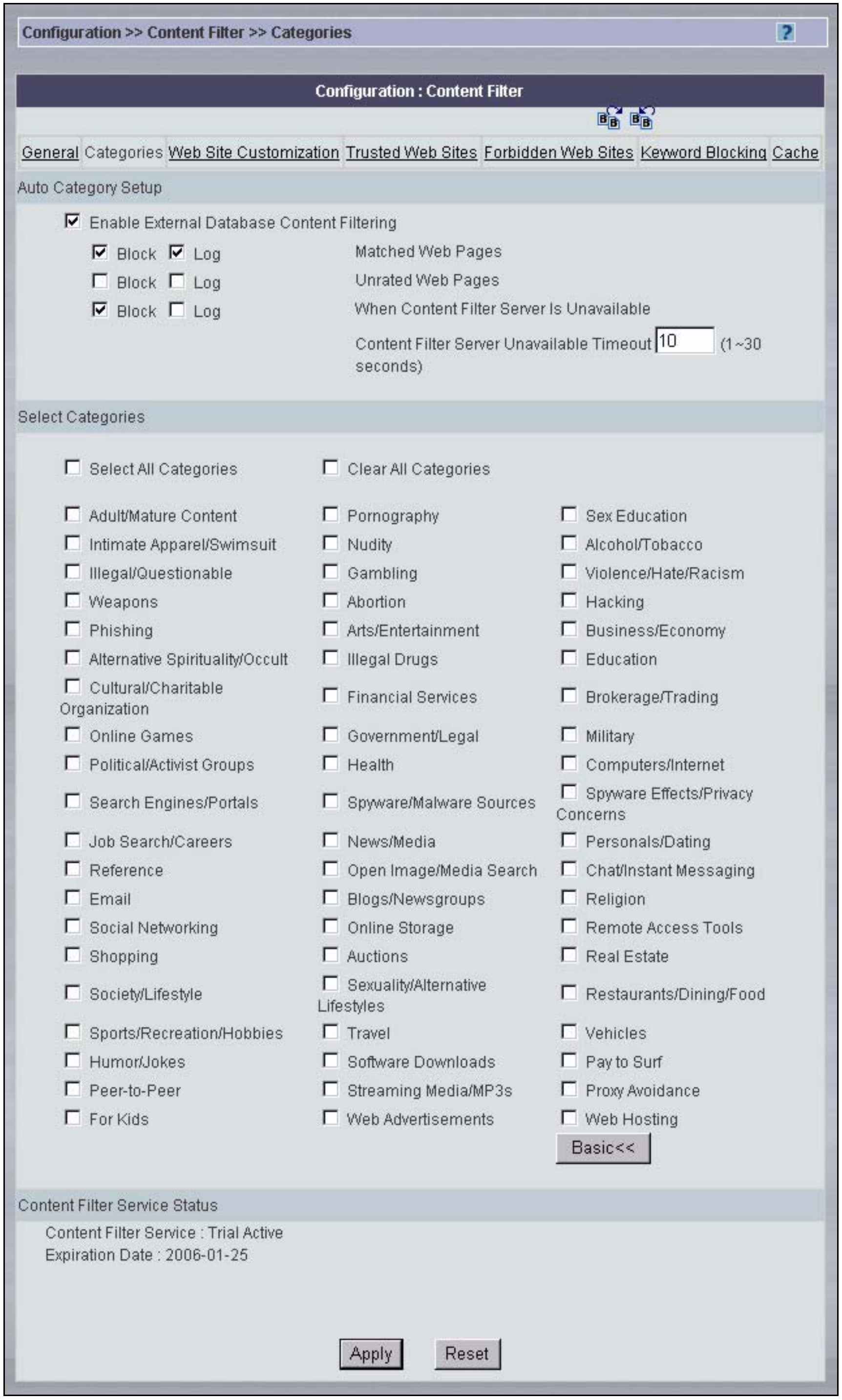
## 18.2 Content Filter Categories

Click **Configuration** >**Content Filter** > **Categories** to display the **CONTENT FILTER Categories** screen.

Use this screen to configure category-based content filtering. You can set the device to use external database content filtering and select which web site categories to block and/or log. You must register for external content filtering before you can use it. Use the **REGISTRATION** screens (see the chapter on registration) to create a myZyXEL.com account, register your device and activate the external content filtering service.

See the device User’s Guide to view content filtering reports.

**Figure 122** Configuration > Content Filter > Categories



Auto Category Setup

☑ Enable External Database Content Filtering

☑ Block ☑ Log Matched Web Pages

□ Block □ Log Unrated Web Pages

☑ Block □ Log When Content Filter Server Is Unavailable

Content Filter Server Unavailable Timeout 10 (1~30 seconds)

Select Categories

□ Select All Categories

□ Clear All Categories

□ Adult/Mature Content
□ Intimate Apparel/Swimsuit
□ Illegal/Questionable
□ Weapons
□ Phishing
□ Alternative Spirituality/Occult
□ Cultural/Charitable Organization
□ Online Games
□ Political/Activist Groups
□ Search Engines/Portals
□ Job Search/Careers
□ Reference
□ Email
□ Social Networking
□ Shopping
□ Society/Lifestyle
□ Sports/Recreation/Hobbies
□ Humor/Jokes
□ Peer-to-Peer
□ For Kids

□ Pornography
□ Nudity
□ Gambling
□ Abortion
□ Arts/Entertainment
□ Illegal Drugs
□ Financial Services
□ Government/Legal
□ Health
□ Spyware/Malware Sources
□ News/Media
□ Open Image/Media Search
□ Blogs/Newsgroups
□ Online Storage
□ Auctions
□ Sexuality/Alternative Lifestyles
□ Travel
□ Software Downloads
□ Streaming Media/MP3s
□ Web Advertisements

□ Sex Education
□ Alcohol/Tobacco
□ Violence/Hate/Racism
□ Hacking
□ Business/Economy
□ Education
□ Brokerage/Trading
□ Military
□ Computers/Internet
□ Spyware Effects/Privacy Concerns
□ Personals/Dating
□ Chat/Instant Messaging
□ Religion
□ Remote Access Tools
□ Real Estate
□ Restaurants/Dining/Food
□ Vehicles
□ Pay to Surf
□ Proxy Avoidance
□ Web Hosting

Content Filter Service Status

Content Filter Service : Trial Active
Expiration Date : 2006-01-25

The following table describes the labels in this screen.

**Table 99** Configuration > Content Filter > Categories

| LABEL | DESCRIPTION |
|---|---|
| Auto Category Setup | |
| Enable External Database Content Filtering | Enable external database content filtering to have the device check an external database to find to which category a requested web page belongs. The device then blocks or forwards access to the web page depending on the configuration of the rest of this page. |
| Matched Web Pages | Select **Block** to prevent users from accessing web pages that match the categories that you select below.<br>When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **CONTENT FILTER General** screen along with the category of the blocked web page.<br>Select **Log** to record attempts to access prohibited web pages. |
| Unrated Web Pages | Select **Block** to prevent users from accessing web pages that the external database content filtering has not categorized.<br>When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **CONTENT FILTER General** screen along with the category of the blocked web page.<br>Select **Log** to record attempts to access web pages that are not categorized. |
| When Content Filter Server Is Unavailable | Select **Block** to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:<br>There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field.<br>The device is not able to resolve the domain name of the external content filtering database.<br>There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid").<br>Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable. |
| Content Filter Server Unavailable Timeout | Specify a number of seconds (1 to 30) for the device to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the device blocks or allows access to the requested web page based on the setting in the **Block When Content Filter Server Is Unavailable** field. |
| Select Categories | |
| Select All Categories | Select this check box to restrict access to all site categories listed below. |
| Clear All Categories | Select this check box to clear the selected categories below. |
| Adult/Mature Content | Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children. |
| Pornography | Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. |

**Table 99** Configuration > Content Filter > Categories (continued)

| LABEL | DESCRIPTION |
|---|---|
| Sex Education | Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement. |
| Intimate Apparel/Swimsuit | Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered. |
| Nudity | Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals. |
| Alcohol/Tobacco | Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products. |
| Illegal/Questionable | Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers.<br>Note: This category includes sites identified as being malicious in any way (such as having viruses, spyware and etc.). |
| Gambling | Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements). |
| Violence/Hate/Racism | Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics. |
| Weapons | Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use. |
| Abortion | Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion. |
| Hacking | Pages providing information on illegal or questionable access to or the use of communications equipment/software. |
| Phishing | Selecting this category excludes pages that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (for example, credit card numbers and pin numbers). |

**Table 99** Configuration > Content Filter > Categories (continued)

| LABEL | DESCRIPTION |
|---|---|
| Arts/Entertainment | Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. |
| Business/Economy | Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services). |
| Alternative Spirituality/ Occult | Selecting this category excludes pages that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers and satanic or supernatural beings. |
| Illegal Drugs | Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia. |
| Education | Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups. |
| Cultural/Charitable Organization | Selecting this category excludes pages sponsored by cultural institutions, or those that provide information about museums, galleries, and theaters (not movie theaters). It includes groups such as 4H and the Boy Scouts of America. |
| Financial Services | Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services. |
| Brokerage/Trading | Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news. |
| Online Games | Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways. |
| Government/Legal | Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities. |
| Military | Selecting this category excludes pages that promote or provide information on military branches or armed services. |
| Political/Activist Groups | Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities. |

**Table 99** Configuration > Content Filter > Categories (continued)

| LABEL | DESCRIPTION |
|---|---|
| Health | Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition. |
| Computers/Internet | Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies. |
| Search Engines/Portals | Selecting this category excludes pages that support searching the Internet, indices, and directories. |
| Spyware/Malware Sources | Selecting this category excludes pages which distribute spyware and other malware. Spyware is defined as software which takes control of your computer, modifies computer settings, collects or reports personal information, or misrepresents itself by tricking users to install, download, or enter personal information. This includes drive-by downloads; browser hijackers; dialers; intrusive advertising; any program which modifies your homepage, bookmarks, or security settings; and keyloggers. It also includes any software which bundles spyware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as spyware if the user is reasonably notified that the software will perform these actions (in other words, it alerts that it will send personal information, be installed, or that it will log keystrokes). Note: Sites rated as spyware should have a second category assigned with them. |
| Spyware Effects/Privacy Concerns | Selecting this category excludes pages to which spyware (as defined in the Spyware/Malware Sources category) reports its findings or from which it alone downloads advertisements. Also includes sites that contain serious privacy issues, such as “phone home” sites to which software can connect and send user info; sites that make extensive use of tracking cookies without a posted privacy statement; and sites to which browser hijackers redirect users. Usually does not include sites that can be marked as Spyware/Malware. Note: Sites rated as spyware effects typically have a second category assigned with them. |
| Job Search/Careers | Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers. |
| News/Media | Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories. |
| Personals/Dating | Selecting this category excludes pages that promote interpersonal relationships. |
| Reference | Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information. |
| Open Image/Media Search | Selecting this category excludes pages with image or video search capabilities which return graphical results (for example, thumbnail pictures) that include potentially pornographic content along with non-pornographic content (as defined in the Pornography category). Sites that explicitly exclude offensive content are not included in this category. |
| Chat/Instant Messaging | Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads. |

**Table 99** Configuration > Content Filter > Categories (continued)

| LABEL | DESCRIPTION |
|---|---|
| Email | Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services. |
| Blogs/Newsgroups | Selecting this category excludes pages that offer access to Usenet news groups, blogs, or other messaging or bulletin board systems. |
| Religion | Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups). |
| Social Networking | Selecting this category excludes pages that enable people to connect with others to form an online community. Typically members describe themselves in personal web page profiles and form interactive networks, linking them with other members based on common interests or acquaintances. Instant messaging, file sharing and web logs (blogs) are common features of Social Networking sites. Note: These sites may contain offensive material in the community-created content. Sites in this category are also referred to as "virtual communities" or "online communities". This category does not include more narrowly focused sites, like those that specifically match descriptions for Personals/Dating sites or Business sites. |
| Online Storage | Selecting this category excludes pages that provide a secure, encrypted, off-site backup and restoration of personal data. These online repositories are typically used to store, organize and share videos, music, movies, photos, documents and other electronically formatted information. Sites that fit this criteria essentially act as your personal hard drive on the Internet. |
| Remote Access Tools | Selecting this category excludes pages that primarily focus on providing information about and/or methods that enables authorized access to and use of a desktop computer or private network remotely. |
| Shopping | Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons). |
| Auctions | Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements. |
| Real Estate | Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties. |
| Society/Lifestyle | Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category. |
| Sexuality/Alternative Lifestyles | Selecting this category excludes pages that provide information, promote, or cater to gay and lesbian lifestyles. This does not include pages that are sexually oriented. |
| Restaurants/Dining/Food | Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes. |
| Sports/Recreation/Hobbies | Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting. |

**Table 99** Configuration > Content Filter > Categories (continued)

| LABEL | DESCRIPTION |
|---|---|
| Travel | Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. |
| Vehicles | Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts. |
| Humor/Jokes | Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating. |
| Software Downloads | Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge. |
| Pay to Surf | Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages. |
| Peer-to-Peer | Selecting this category excludes pages that distribute software to facilitate the direct exchange of files between users, including software that enables file search and sharing across a network without dependence on a central server. |
| Streaming Media/MP3s | Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers. |
| Proxy Avoidance | Selecting this category excludes pages that provide information on how to bypass proxy server/appliance features or gain access to URLs in any way that bypasses the proxy server/appliance. This category includes any service which attempts to allow a person to bypass the Blue Coat filtering system, such as anonymous surfing services. |
| For Kids | Selecting this category excludes pages designed specifically for children. |
| Web Advertisements | Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements. |
| Web Hosting | Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services. |
| Advanced/Basic | Click **Advanced** to see an expanded list of categories, or click **Basic** to see a smaller list. |

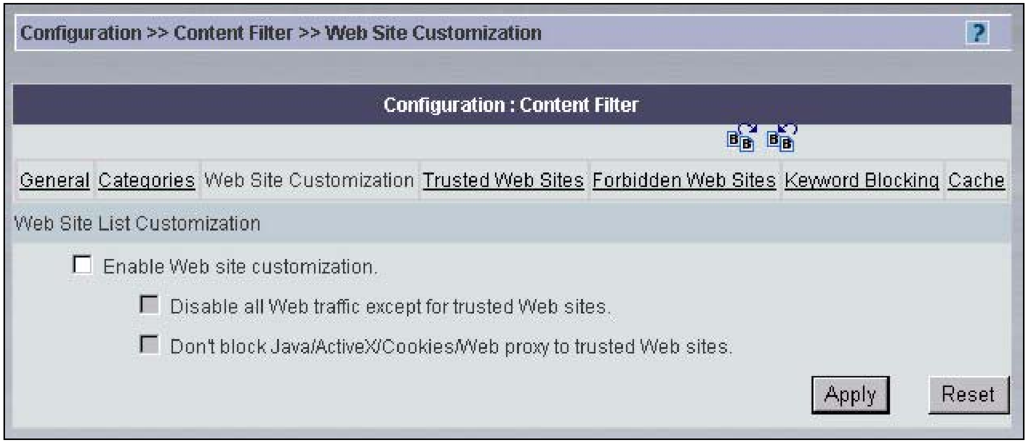
**Table 99** Configuration > Content Filter > Categories (continued)

| LABEL | DESCRIPTION |
|---|---|
| Content Filter Service Status | This read-only field displays the status of your category-based content filtering (using an external database) service subscription.<br>**License Inactive** displays if you have not registered and activated the category-based content filtering service.<br>**License Active** and the subscription expiration date display if you have registered the device and activated the category-based content filtering service.<br>**Trial Active** and the trial subscription expiration date display if you have registered the device and activated the category-based content filtering service.<br>**License Inactive** and the date your subscription expired display if your subscription to the category-based content filtering service has expired.<br>Note: After you register for content filtering, you need to wait up to five minutes for content filtering to be activated. See Section 18.1 on page 235 for how to check the content filtering activation. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 18.3 Content Filter Customization

Click **Configuration** > **Content Filter** > **Web Site Customization** to display the **CONTENT FILTER Customization** screen.

**Figure 123** Configuration > Content Filter > Web Site Customization



Configuration >> Content Filter >> Web Site Customization
?
Configuration : Content Filter
General
Categories
Web Site Customization
Trusted Web Sites
Forbidden Web Sites
Keyword Blocking
Cache
Web Site List Customization
Apply
Reset

□ Enable Web site customization.

□ Disable all Web traffic except for trusted Web sites.

□ Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites.

The following table describes the labels in this screen.

**Table 100** Configuration > Content Filter > Web Site Customization

| LABEL | DESCRIPTION |
|---|---|
| Web Site List Customization | |
| Enable Web site customization | Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names. |

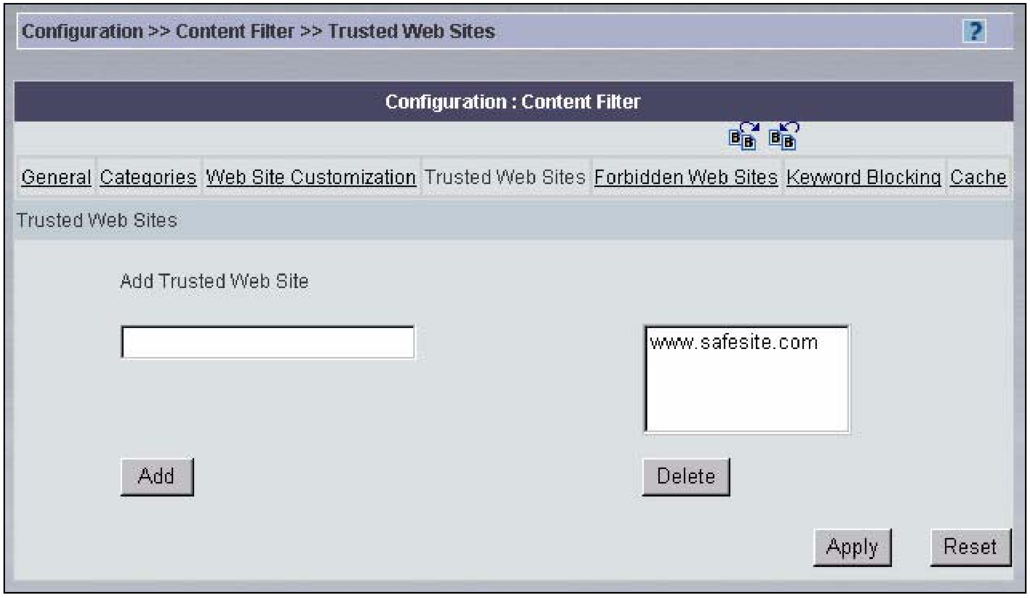
**Table 100** Configuration > Content Filter > Web Site Customization (continued)

| LABEL | DESCRIPTION |
|---|---|
| Disable all Web traffic except for trusted Web sites | When this box is selected, the device only allows Web access to sites on the **Trusted Web Site** list. If they are chosen carefully, this is the most effective way to block objectionable material. |
| Don't block Java/ActiveX/ Cookies/Web proxy to trusted Web sites | When this box is selected, the device will permit Java, ActiveX and Cookies from sites on the **Trusted Web Site** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 18.4 Content Filter Trusted Web Sites

Use this screen to create a list of good (allowed) web site addresses. Click **Configuration** > **Content Filter** > **Trusted Web Sites** to display the following screen.

**Figure 124** Configuration > Content Filter > Trusted Web Sites



The following table describes the labels in this screen.

**Table 101** Configuration > Content Filter > Trusted Web Sites

| LABEL | DESCRIPTION |
|---|---|
| Trusted Web Sites | These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries. |
| Add Trusted Web Site | Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc. |
| Trusted Web Sites | This list displays the trusted web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |

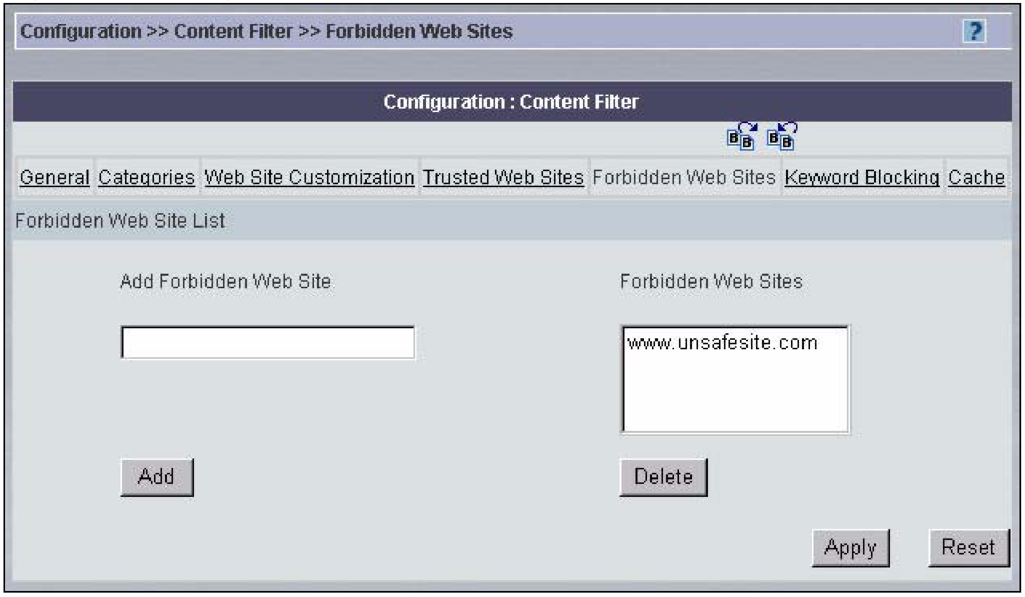
**Table 101** Configuration > Content Filter > Trusted Web Sites (continued)

| LABEL | DESCRIPTION |
|---|---|
| Delete | Select a web site name from the **Trusted Web Site List**, and then click this button to delete it from that list. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 18.5 Content Filter Forbidden Web Sites

Use this screen to create a list of bad (blocked) web site addresses. Click **Configuration** > **Content Filter** > **Forbidden Web Sites** to display the following screen.

**Figure 125** Configuration > Content Filter > Forbidden Web Sites



www.unsafesite.com

The following table describes the labels in this screen.

**Table 102** Configuration > Content Filter > Forbidden Web Sites

| LABEL | DESCRIPTION |
|---|---|
| Forbidden Web Site List | Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries. |
| Add Forbidden Web Site | Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. |
| Forbidden Web Sites | This list displays the forbidden web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Forbidden Web Site List**, and then click this button to delete it from that list. |

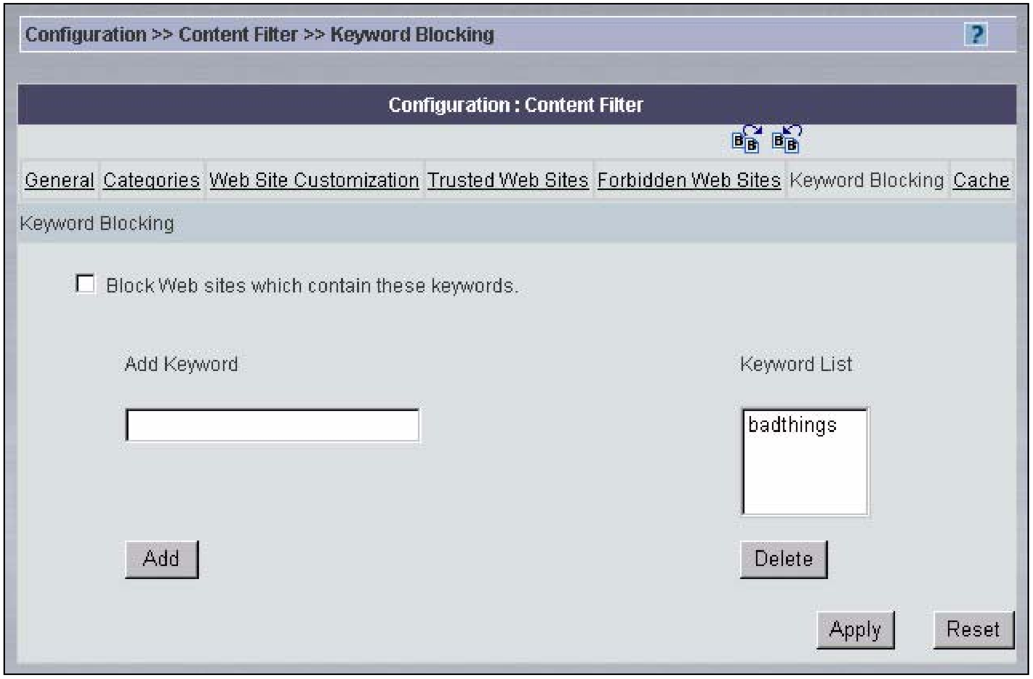
**Table 102** Configuration > Content Filter > Forbidden Web Sites (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 18.6 Content Filter Keyword Blocking

Use this screen to block web sites based on whether the web site's address contains a keyword. Click **Configuration** > **Content Filter** > **Keyword Blocking** to display the following screen.

**Figure 126** Configuration > Content Filter > Keyword Blocking


Configuration >> Content Filter >> Keyword Blocking

Configuration : Content Filter

Keyword Blocking

☐ Block Web sites which contain these keywords.

Add Keyword

Keyword List

badthings

The following table describes the labels in this screen.

**Table 103** Configuration > Content Filter > Customization

| LABEL | DESCRIPTION |
|---|---|
| Keyword Blocking | **Keyword Blocking** allows you to block websites with URLs that contain certain keywords in the domain name or IP address. See Section 18.7 on page 250 for how to set how much of the URL the device checks. |
| Block Web sites which contain these keywords. | Select this check box to enable keyword blocking. |
| Add Keyword | Enter a keyword (up to 31 printable ASCII characters) to block. You can also enter a numerical IP address. |
| Keyword List | This list displays the keywords already added. |
| Add | Click this button when you have finished adding the key words field above. |
| Delete | Select a keyword from the **Keyword List**, and then click this button to delete it from that list. |

**Table 103** Configuration > Content Filter > Customization (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 18.7 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

### 18.7.1 Domain Name or IP Address URL Checking

By default, the device checks the URL's domain name or IP address when performing keyword blocking.

This means that the device checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

### 18.7.2 Full Path URL Checking

Full path URL checking has the device check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

### 18.7.3 File Name URL Checking

Filename URL checking has the device check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

## 18.8 Content Filtering Cache

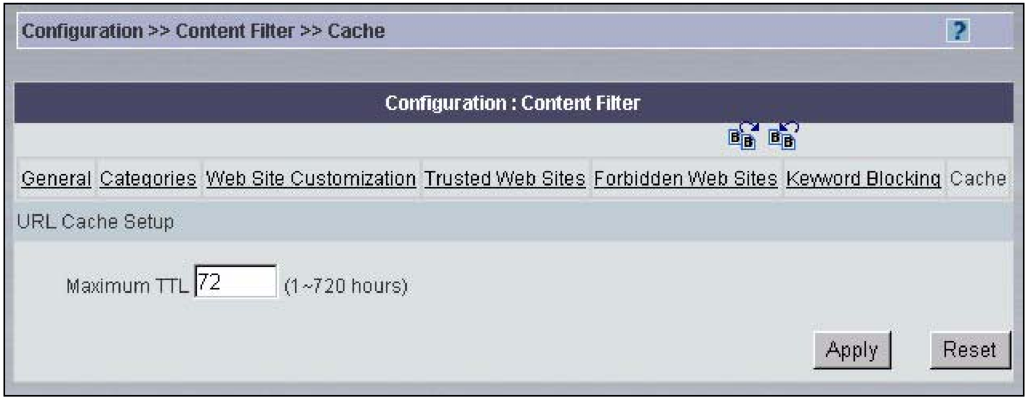
Click **Configuration > Content Filter > Cache** to display the **CONTENT FILTER Cache** screen.

Use this screen to view and configure your device's URL caching. You can also configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The device only queries the external content filtering database for sites not found in the cache.

You can remove individual entries from the cache. When you do this, the device queries the external content filtering database the next time someone tries to access that web site. This allows you to check whether a web site's category has been changed.

Please see the device's User's Guide for how to submit a web site that has been incorrectly categorized.

**Figure 127** Configuration > Content Filter > Cache



Configuration >> Content Filter >> Cache

Configuration : Content Filter

URL Cache Setup

Maximum TTL 72 (1~720 hours)

The following table describes the labels in this screen.

**Table 104** Configuration > Content Filter > Cache

| LABEL | DESCRIPTION |
|---|---|
| URL Cache Setup | |
| Maximum TTL | Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the device is to allow an entry to remain in the URL cache before discarding it. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 19

# Configuration > Device Log

This section shows you how to configure the **Device Log** screen. This screen may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 19.1 Device Log

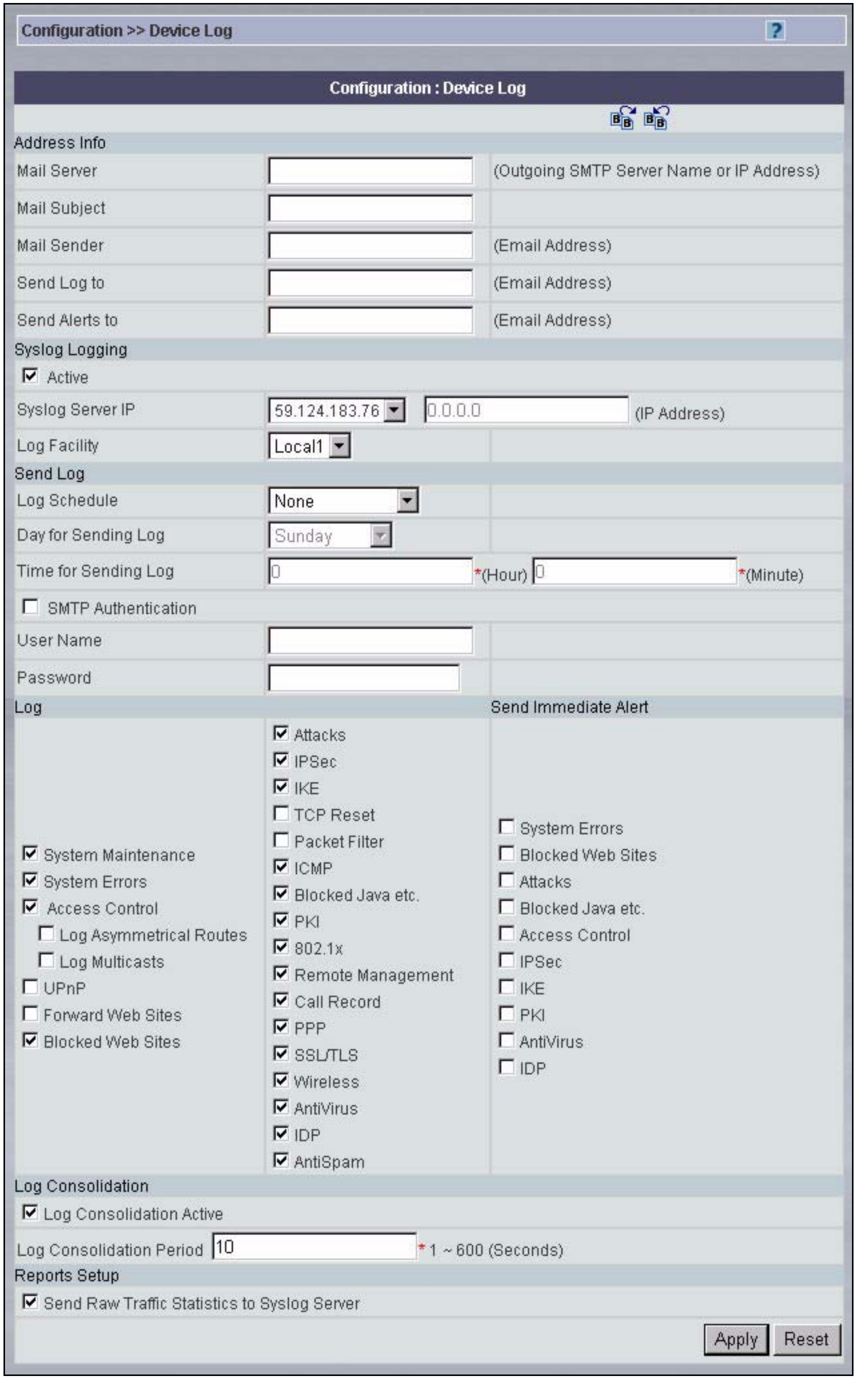
Use the **Logging Options** screen to configure to where the device is to send logs; the schedule for when the device is to send the logs and which logs and/or immediate alerts the device is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **Device** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see Log Schedule). Selecting many alert and/or log categories (especially Access Control) may result in many e-mails being sent.

To change a device's log settings, select a device, click **Configuration > Device Log**. The screen appears as shown next.

**Figure 128** Configuration > Device Log > Log Settings



Configuration >> Device Log

Configuration : Device Log

Address Info

| | | |
|---|---|---|
| Mail Server | | (Outgoing SMTP Server Name or IP Address) |
| Mail Subject | | |
| Mail Sender | | (Email Address) |
| Send Log to | | (Email Address) |
| Send Alerts to | | (Email Address) |

Syslog Logging

☑ Active

| | | |
|---|---|---|
| Syslog Server IP | 59.124.183.76 | 0.0.0.0 (IP Address) |
| Log Facility | Local1 | |

Send Log

| | | |
|---|---|---|
| Log Schedule | None | |
| Day for Sending Log | Sunday | |
| Time for Sending Log | 0 *(Hour) | 0 *(Minute) |

☐ SMTP Authentication

| | |
|---|---|
| User Name | |
| Password | |

Log

☑ System Maintenance
☑ System Errors
☑ Access Control
☐ Log Asymmetrical Routes
☐ Log Multicasts
☐ UPnP
☐ Forward Web Sites
☑ Blocked Web Sites

☑ Attacks
☑ IPSec
☑ IKE
☐ TCP Reset
☐ Packet Filter
☑ ICMP
☑ Blocked Java etc.
☑ PKI
☑ 802.1x
☑ Remote Management
☑ Call Record
☑ PPP
☑ SSL/TLS
☑ Wireless
☑ AntiVirus
☑ IDP
☑ AntiSpam

Send Immediate Alert

☐ System Errors
☐ Blocked Web Sites
☐ Attacks
☐ Blocked Java etc.
☐ Access Control
☐ IPSec
☐ IKE
☐ PKI
☐ AntiVirus
☐ IDP

Log Consolidation

☑ Log Consolidation Active

Log Consolidation Period 10 * 1 ~ 600 (Seconds)

Reports Setup

☑ Send Raw Traffic Statistics to Syslog Server

The following table describes the labels in this screen.

**Table 105** Configuration > Device Log > Log Settings

| LABEL | DESCRIPTION |
|---|---|
| Address Info | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |

**Table 105** Configuration > Device Log > Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mail Subject | Type a title that you want to be in the subject line of the log e-mail message that the device sends. |
| Mail Sender | Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the device sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Send Log To | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail. |
| Send Alerts To | Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail. |
| Syslog Logging | Syslog logging sends a log to Vantage Report or to an external syslog server used to store logs. |
| Active | Click **Active** to enable syslog logging. |
| Syslog Server IP Address | Select an instance of Vantage Report (see Section 26.8 on page 306) or select **User Define** and enter the server IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Send Log | |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>• Daily<br>• Weekly<br>• Hourly<br>• When Log is Full<br>• None.<br>If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent |
| Day for Sending Log | Use the drop down list box to select which day of the week to send the logs. |
| Time for Sending Log | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs. |
| SMTP Authentication | SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.<br>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs. |
| User Name | Enter the user name (up to 31 characters) (usually the user name of a mail account). |
| Password | Enter the password associated with the user name above. |
| Log | Select the categories of logs that you want to record. Logs include alerts. |
| Send Immediate Alert | Select the categories of alerts for which you want the device to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field. |
| Log Consolidation | |

**Table 105** Configuration > Device Log > Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| Log Consolidation Active | Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log. |
| Log Consolidation Period | Specify the time interval during which the device merges logs with identical messages into one log. |
| Reports Setup | |
| Send Raw Traffic Statistics to Syslog Server | Select the check box if you want the device to send traffic logs to Vantage Report or the specified syslog server. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 20

# Configuration > ADSL Monitor

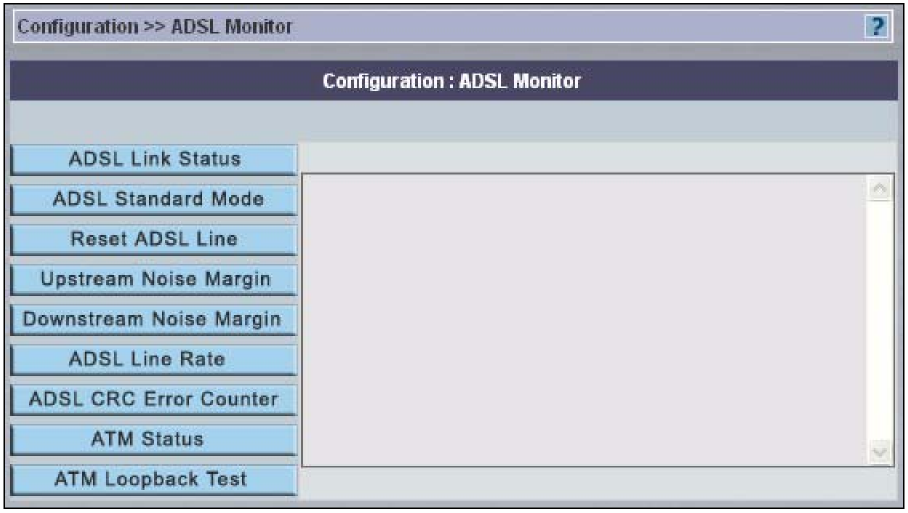
This section shows you how to configure the **ADSL Monitor** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 20.1 Configuring ADSL Monitor

Select an ADSL device and click **Configuration** > **ADSL Monitor**.

Click a label to have the information displayed in the text box.

**Figure 129** Configuration > ADSL Monitor



The following table describes the labels in this screen.

**Table 106** Configuration > ADSL Monitor

| LABEL | DESCRIPTION |
|---|---|
| ADSL Link Status | This is the status of your ADSL link. |
| ADSL Standard Mode | This refers to the operational protocol the device and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.<br>The standard the ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, noise, line quality, etc. |

**Table 106** Configuration > ADSL Monitor (continued)

| LABEL | DESCRIPTION |
|---|---|
| Reset ADSL Line | Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:<br>"Start to reset ADSL<br>Loading ADSL modem F/W...<br>Reset ADSL Line Successfully!" |
| Upstream Noise Margin | Click this button to display the upstream noise margin. |
| Downstream Noise Margin | Click this button to display the downstream noise margin. |
| ADSL Line Rate | Click this button to display the upstream and downstream rates of your ADSL link. |
| ADSL CRC Error Counter | Click this computer to have your device perform a Cyclic Redundancy Checksum. The device sends a sequence of bits to every block of data or frame. This is called a frame check sequence (FCS). The receiving computer uses a predetermined number to divide the frame. If there is a remainder, then the frame is considered corrupted and a retransmission is requested. |
| ATM Status | Click this button to view ATM status. |
| ATM Loopback Test | Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network. |

# 21

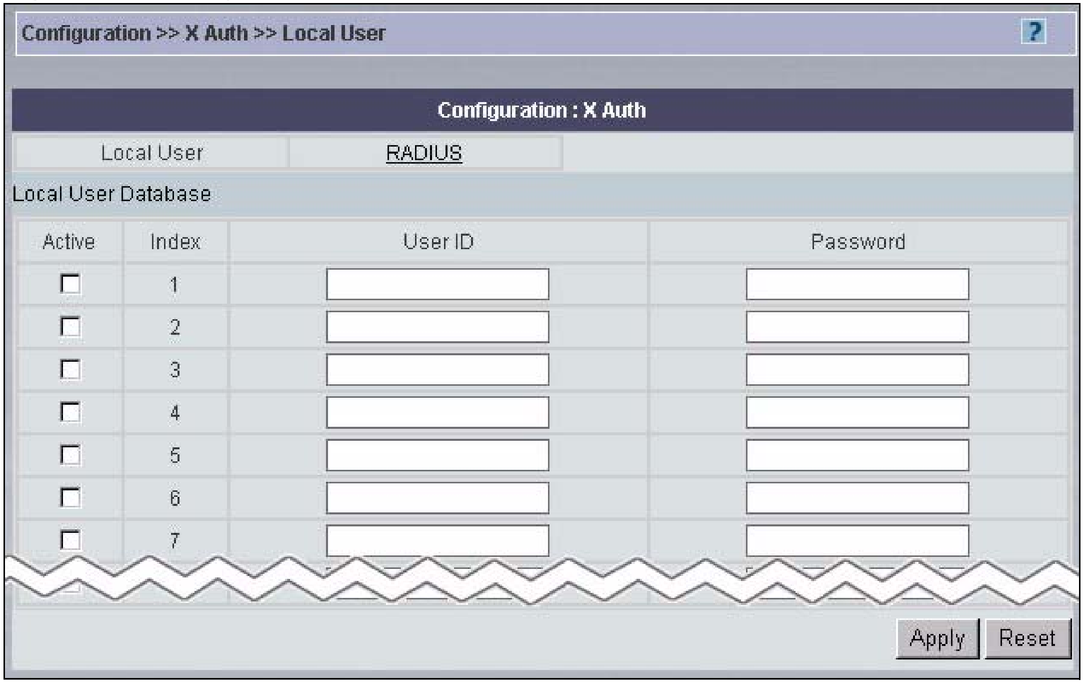
# Configuration > X Auth

This section shows you how to configure the **X Auth** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 21.1 Local User

Use this screen to change your device's local user database. To open this screen, click **Configuration** > **X Auth** > **Local User**.

**Figure 130** Configuration > X Auth > Local User



Configuration >> X Auth >> Local User

Configuration : X Auth

Local User Database

| Active | Index | User ID | Password |
|---|---|---|---|
| □ | 1 | | |
| □ | 2 | | |
| □ | 3 | | |
| □ | 4 | | |
| □ | 5 | | |
| □ | 6 | | |
| □ | 7 | | |

The following table describes the labels in this screen.

**Table 107** Configuration > X Auth > Local User

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to enable the user profile. |
| Index | This is the index number of the user profile. |
| User ID | Enter the user name of the user profile. |
| Password | Enter a password up to 31 characters long for this user profile. |

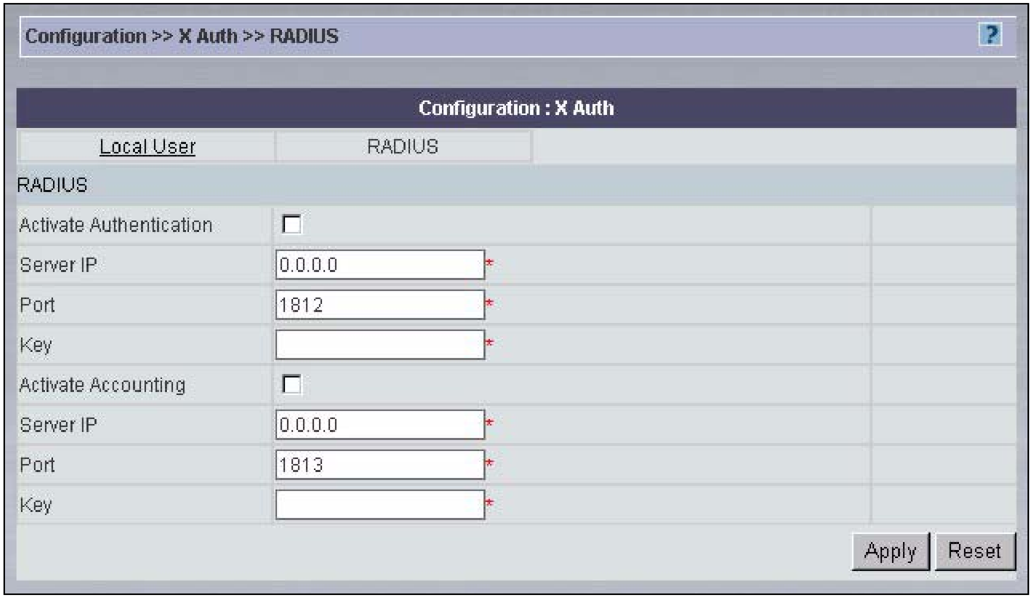
**Table 107** Configuration > X Auth > Local User (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.2 RADIUS

Use this screen to set up your device's RADIUS server settings. To open this screen, click **Configuration** > **X Auth** > **RADIUS**.

**Figure 131** Configuration > X Auth > RADIUS



Configuration >> X Auth >> RADIUS

Configuration : X Auth

Local User | RADIUS

RADIUS

| | |
|---|---|
| Activate Authentication | □ |
| Server IP | 0.0.0.0 * |
| Port | 1812 * |
| Key | * |
| Activate Accounting | □ |
| Server IP | 0.0.0.0 * |
| Port | 1813 * |
| Key | * |

The following table describes the labels in this screen.

**Table 108** Configuration > X Auth > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Activate Authentication | Select the check box to enable user authentication through an external authentication server.<br>Clear the check box to enable user authentication using the local user profile on the device. |
| Server IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the device.<br>The key is not sent over the network. This key must be the same on the external authentication server and device. |
| Activate Accounting | Select the check box to enable user accounting through an external authentication server. |

**Table 108** Configuration > X Auth > RADIUS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Server IP Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the device.<br>The key is not sent over the network. This key must be the same on the external accounting server and device. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 22

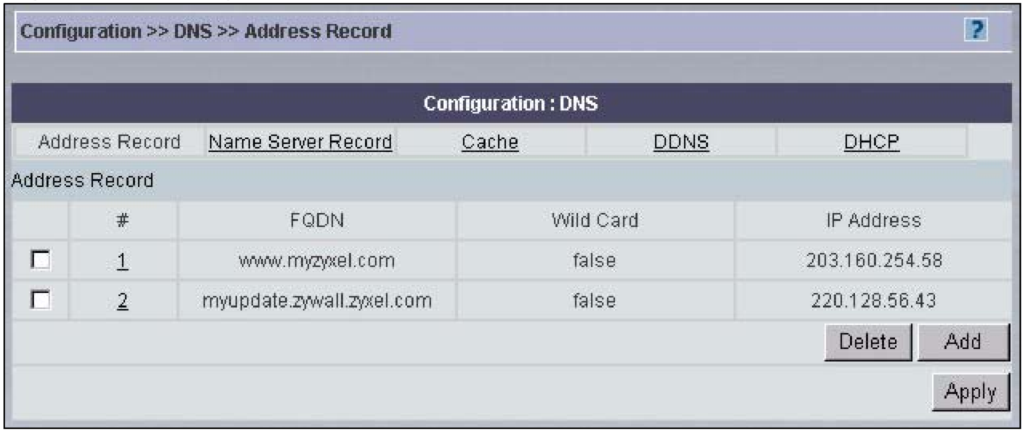
# Configuration > DNS

This section shows you how to configure the **DNS** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 22.1 Address Record

Use this screen to map a fully-qualified domain name (FQDN) to an IP address. To open this screen, click **Configuration** > **DNS** > **Address Record**.

**Figure 132** Configuration > DNS > Address Record



|  | # | FQDN | Wild Card | IP Address |
|---|---|---|---|---|
| □ | 1 | www.myzyxel.com | false | 203.160.254.58 |
| □ | 2 | myupdate.zywall.zyxel.com | false | 220.128.56.43 |

The following table describes the labels in this screen.

**Table 109** Configuration > DNS > Address Record

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the address record. Click the hyperlink to go to the screen where you can edit the record. |
| FQDN | This is a host's fully qualified domain name. |
| Wildcard | This column displays whether or not the DNS wildcard feature is enabled for this domain name. |
| IP Address | This is the IP address of a host. |
| Delete | Select an address record and then click the **Delete** button to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. |

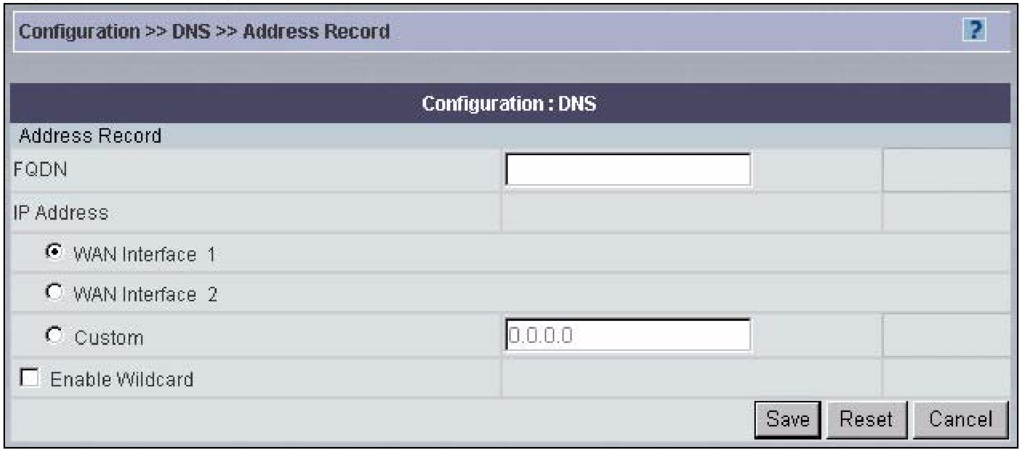
**Table 109** Configuration > DNS > Address Record (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add | Click the **Add** button to open a screen where you can add a new address record. |
| Apply | Click this to save the changes to the device. |

### 22.1.1 Add/Edit an Address Record

Use this screen to create or edit an address record.

**Figure 133** Configuration > DNS > Address Record > Add/Edit



Configuration >> DNS >> Address Record

Configuration : DNS

Address Record

FQDN

IP Address

● WAN Interface 1

○ WAN Interface 2

○ Custom 0.0.0.0

□ Enable Wildcard

The following table describes the labels in this screen.

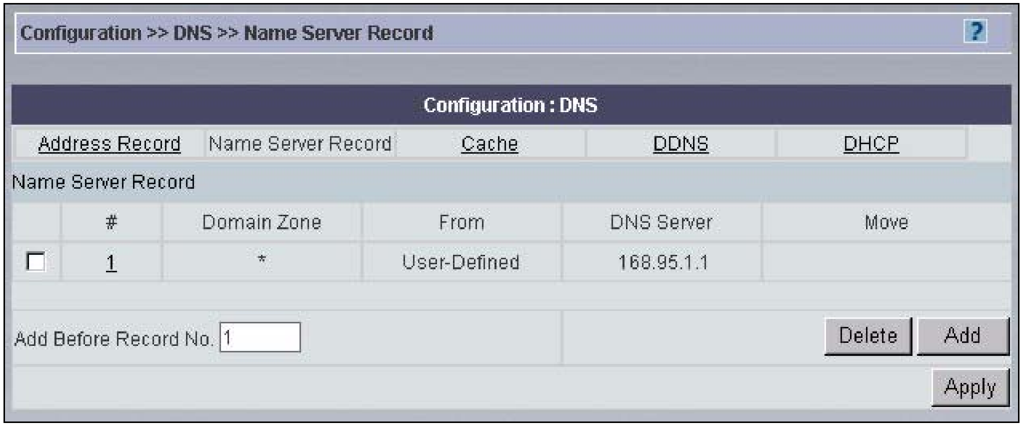
**Table 110** Configuration > DNS > Address Record > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| FQDN | Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain. |
| IP Address | If this entry is for one of the WAN ports, select the WAN port.<br>For entries that are not for one of the WAN ports, select **Custom** and enter the IP address of the host in dotted decimal notation. |
| Enable Wildcard | Select the check box to enable DNS wildcard. |
| Save | Click **Save** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 22.2 Name Server Record

Use this screen to specify the IP address of a DNS server that the device can query to resolve domain names for features like VPN, DDNS, and the time server. To open this screen, click **Configuration > DNS > Name Server Record**.

**Figure 134** Configuration > DNS > Name Server Record



Configuration >> DNS >> Name Server Record

Configuration : DNS

Name Server Record

|  | # | Domain Zone | From | DNS Server | Move |
|---|---|---|---|---|---|
| □ | 1 | * | User-Defined | 168.95.1.1 |  |

Add Before Record No. 1

The following table describes the labels in this screen.

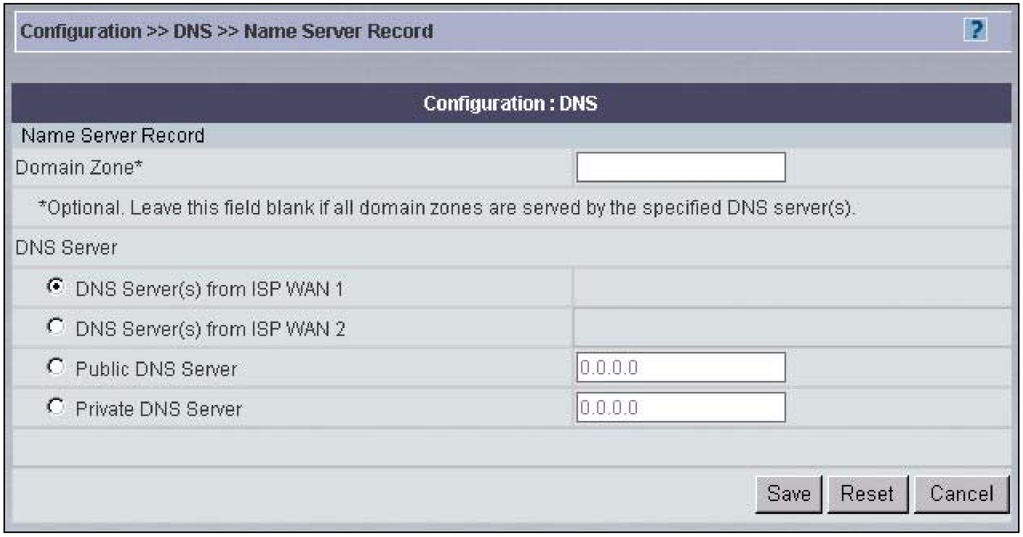
**Table 111** Configuration > DNS > Name Server Record

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the name server record. Click the hyperlink to go to the screen where you can edit the record. |
| Domain Zone | A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. |
| From | This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user. |
| DNS Server | This is the IP address of a DNS server. |
| Move | Click the icon to move the record up or down in the list. |
| Add Before Record No. | Enter the index number of the entry before which you want to insert a new entry. Click **Add** to create the entry. |
| Delete | Select a server record and then click the **Delete** button to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. |
| Add | Click the **Add** button to open a screen where you can create a new name server record. Enter the record number to which you want to insert the new server record below. |
| Apply | Click this to save the changes to the device. |

## 22.2.1 Add/Edit a Name Server Record

Use this screen to create or edit a name server record.

**Figure 135** Configuration > DNS > Name Server Record > Add/Edit



Configuration >> DNS >> Name Server Record

Configuration : DNS

Name Server Record

Domain Zone*

*Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

● DNS Server(s) from ISP WAN 1

○ DNS Server(s) from ISP WAN 2

○ Public DNS Server 0.0.0.0

○ Private DNS Server 0.0.0.0

The following table describes the labels in this screen.

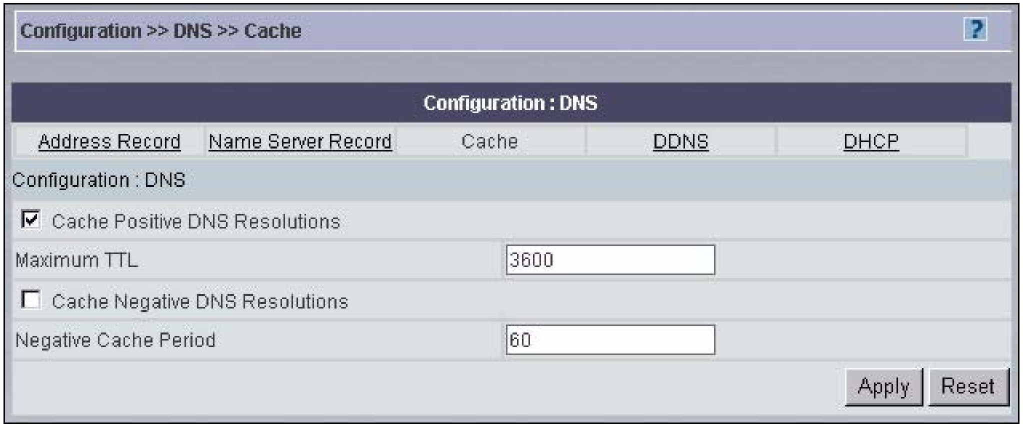
**Table 112** Configuration > DNS > Name Server Record > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Domain Zone | This field is optional.<br>A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the device receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.<br>Leave this field blank if all domain zones are served by the specified DNS server(s). |
| DNS Server | Select the **DNS Server(s) from ISP WAN 1** or **DNS Server(s) from ISP WAN 2** radio button if your ISP dynamically assigns DNS server information. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. **N/A** displays for all of the DNS server IP address fields if the device has a fixed WAN IP address.<br>Select **Public DNS Server** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.<br>**Public DNS Server** entries with the IP address set to 0.0.0.0 are not allowed.<br>Select **Private DNS Server** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right.<br>With a private DNS server, you must also configure the first DNS server entry in the **DNS LAN** screen to use **DNS Relay**.<br>You must also configure a VPN rule since the device uses a VPN tunnel when it relays DNS queries to the private DNS server. The rule must include the LAN IP address of the device as a local IP address and the IP address of the DNS server as a remote IP address.<br>**Private DNS Server** entries with the IP address set to 0.0.0.0 are not allowed. |
| Save | Click **Save** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 22.3 Cache

Use this screen to configure a device’s DNS caching. To open this screen, click **Configuration** > **DNS** > **Cache**.

**Figure 136** Configuration > DNS > Cache



Configuration : DNS

☑ Cache Positive DNS Resolutions

Maximum TTL: 3600

□ Cache Negative DNS Resolutions

Negative Cache Period: 60

The following table describes the labels in this screen.

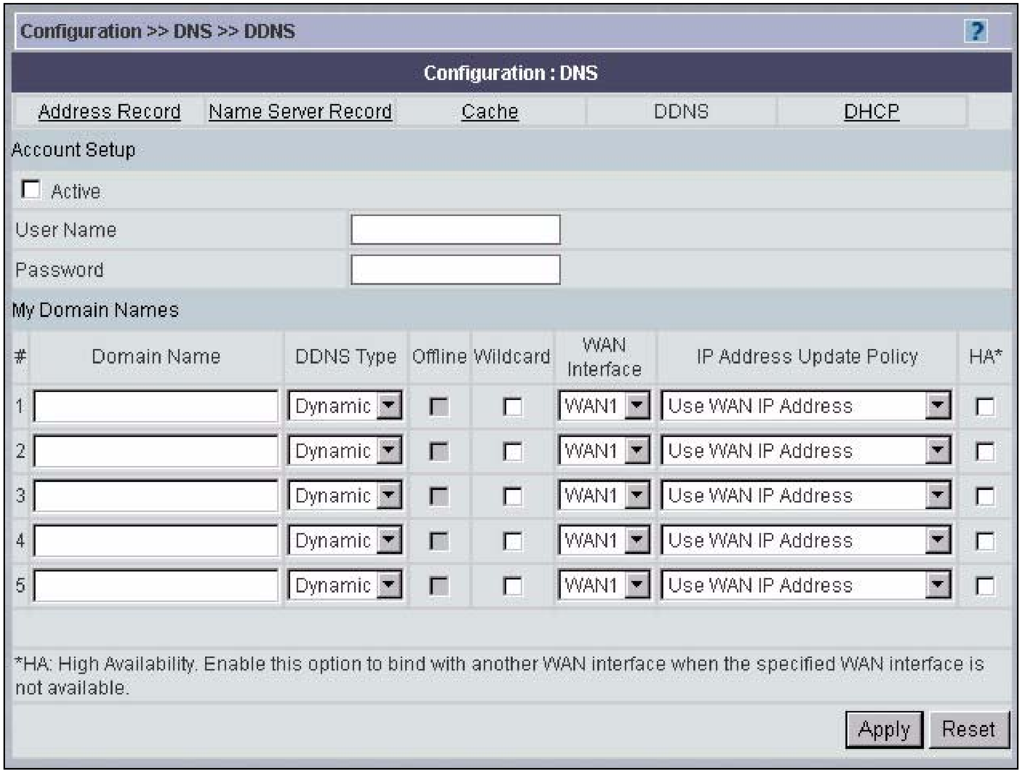
**Table 113** Configuration > DNS > Cache

| LABEL | DESCRIPTION |
|---|---|
| DNS Cache Setup | |
| Cache Positive DNS Resolutions | Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the device’s processing of commonly queried domain names and reduces the amount of traffic that the device sends out to the WAN. |
| Maximum TTL | Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the device is to allow a positive resolution entry to remain in the DNS cache before discarding it. |
| Cache Negative DNS Resolutions | Caching negative DNS resolutions helps speed up the device’s processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the device sends out to the WAN. |
| Negative Cache Period | Type the time (60 to 3600 seconds) that the device is to allow a negative resolution entry to remain in the DNS cache before discarding it. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 22.4 DDNS

Use this screen to configure your Dynamic DNS (DDNS) on the device. To open this screen, click **Configuration > DNS > DDNS**.

**Figure 137** Configuration > DNS > DDNS



Configuration >> DNS >> DDNS

Configuration : DNS

Address Record | Name Server Record | Cache | DDNS | DHCP

Account Setup

□ Active

User Name

Password

My Domain Names

| # | Domain Name | DDNS Type | Offline | Wildcard | WAN Interface | IP Address Update Policy | HA* |
|---|---|---|---|---|---|---|---|
| 1 | | Dynamic | □ | □ | WAN1 | Use WAN IP Address | □ |
| 2 | | Dynamic | □ | □ | WAN1 | Use WAN IP Address | □ |
| 3 | | Dynamic | □ | □ | WAN1 | Use WAN IP Address | □ |
| 4 | | Dynamic | □ | □ | WAN1 | Use WAN IP Address | □ |
| 5 | | Dynamic | □ | □ | WAN1 | Use WAN IP Address | □ |

*HA: High Availability. Enable this option to bind with another WAN interface when the specified WAN interface is not available.

The following table describes the labels in this screen.

**Table 114** Configuration > DNS > DDNS

| LABEL | DESCRIPTION |
|---|---|
| Account Setup | |
| Active | Select this check box to use dynamic DNS. |
| User Name | Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Password | Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed. |
| My Domain Names | |
| # | This field displays an index number for each domain name. |
| Domain Name | Enter the host names in these fields. |
| DDNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider.<br>Select **Dynamic** if you have the Dynamic DNS service.<br>Select **Static** if you have the Static DNS service.<br>Select **Custom** if you have the Custom DNS service. |
| Offline | This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| Wildcard | Select the check box to enable DYNDNS Wildcard. |
| WAN Interface | Select the WAN port to use for updating the IP address of the domain name. |

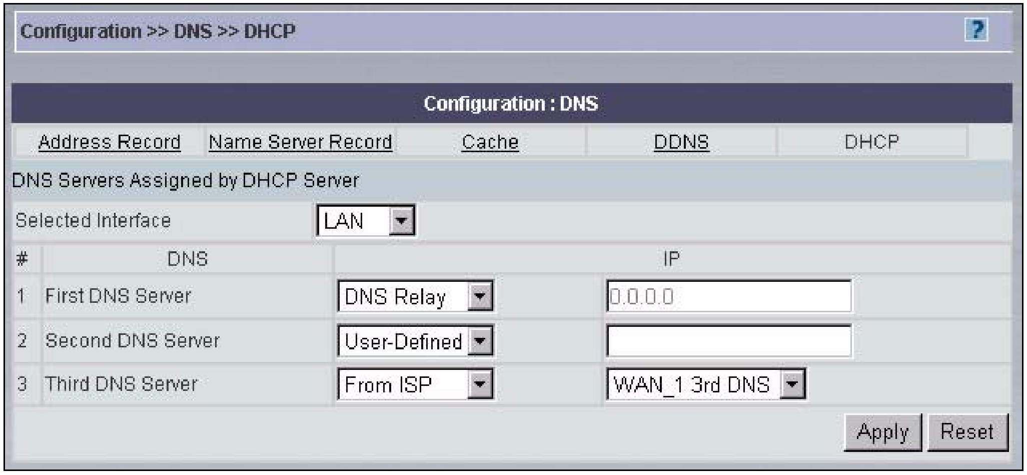
**Table 114** Configuration > DNS > DDNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Address Update Policy | Select **Use WAN IP Address** to have the device update the domain name with the WAN port's IP address.<br>Select **Use User-Defined** and enter the IP address if you have a static IP address.<br>Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.<br>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the device and the DDNS server. |
| HA | Select this check box to enable the high availability (HA) feature. High availability has the device update a domain name with another port’s IP address when the normal WAN port does not have a connection.<br>If the WAN port specified in the **WAN Interface** field does not have a connection, the device will attempt to use the IP address of another WAN port to update the domain name.<br>When the WAN ports are in the active/passive operating mode, the device will update the domain name with the IP address of whichever WAN port has a connection, regardless of the setting in the **WAN Interface** field.<br>Disable this feature and the device will only update the domain name with an IP address of the WAN port specified in the **WAN Interface** field. If that WAN port does not have a connection, the device will not update the domain name with another port’s IP address.<br>Note: If you enable high availability, DDNS can also function when the device uses the dial backup port. DDNS does not function when the device uses traffic redirect. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 22.5 DHCP

Use this screen to configure the DNS server information that the device sends to DHCP clients on the LAN, DMZ or WLAN. To open this screen, click **Configuration** > **DNS** > **DHCP**.

**Figure 138** Configuration > DNS > DHCP



Configuration >> DNS >> DHCP

Configuration : DNS

DNS Servers Assigned by DHCP Server

Selected Interface: LAN

| # | DNS | | IP |
|---|---|---|---|
| 1 | First DNS Server | DNS Relay | 0.0.0.0 |
| 2 | Second DNS Server | User-Defined | |
| 3 | Third DNS Server | From ISP | WAN_1 3rd DNS |

The following table describes the labels in this screen.

**Table 115** Configuration > DNS > DHCP

| LABEL | DESCRIPTION |
|---|---|
| DNS Servers Assigned by DHCP Server | The device passes a DNS (Domain Name System) server IP address to the DHCP clients. |
| Selected Interface | Select an interface from the drop-down list box to configure the DNS servers for the specified interface. |
| # | This is the index number of each DNS server. |
| DNS | These read-only labels represent the DNS servers. |
| IP | Select **From ISP** if your ISP dynamically assigns DNS server information (and the device's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.<br>Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.<br>Select **DNS Relay** to have the device act as a DNS proxy. The device's LAN, DMZ or WLAN IP address displays in the field to the right (read-only). The device tells the DHCP clients on the LAN, DMZ or WLAN that the device itself is the DNS server. When a computer on the LAN, DMZ or WLAN sends a DNS query to the device, the device forwards the query to the device's system DNS server (configured in the **DNS System** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you click **Apply**.<br>Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply | Click **Apply** to save your changes back to the device. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

23

# Configuration > Remote MGMT

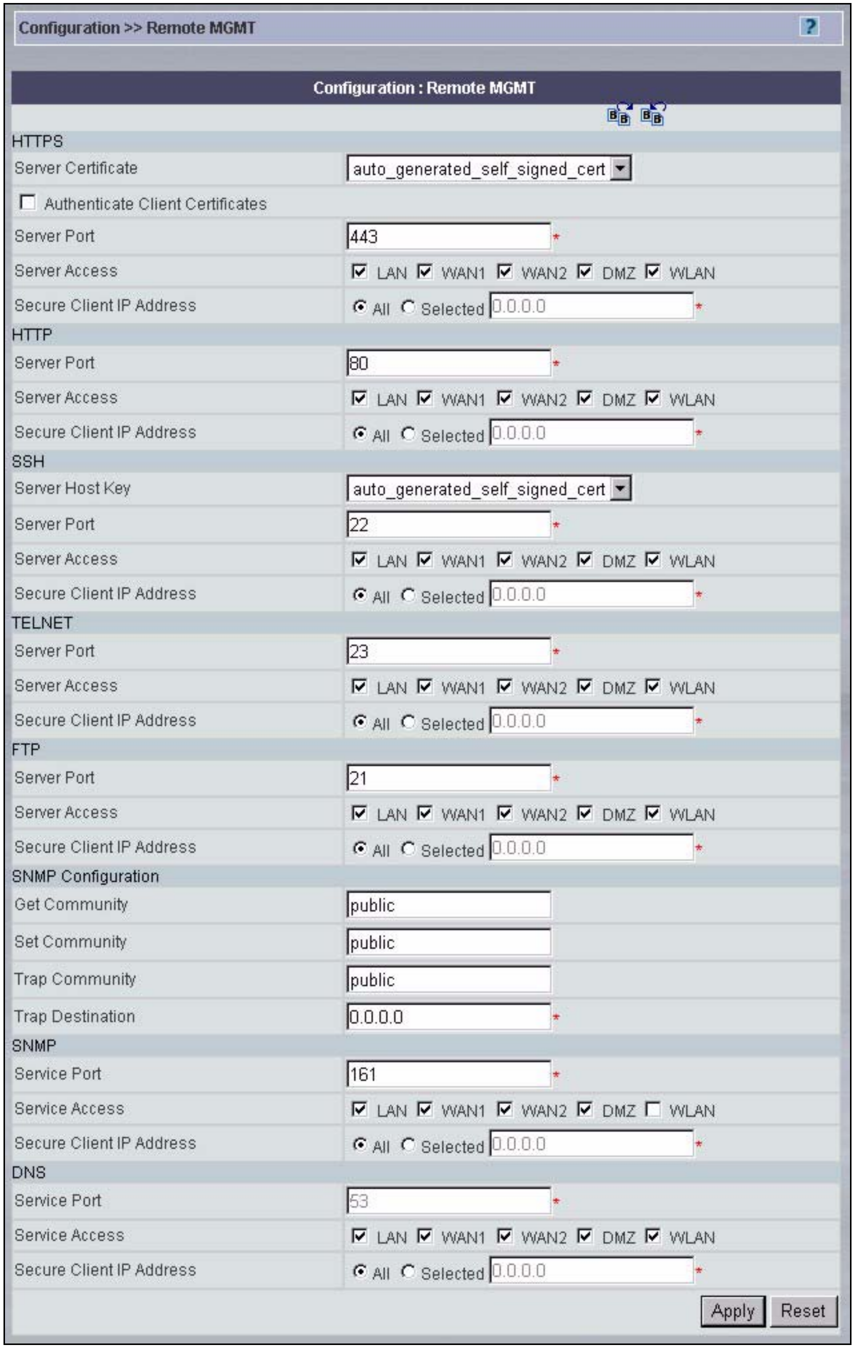
This section shows you how to configure the **Remote MGMT** screens. These screens may vary depending on which model you're configuring. Please see the device's User's Guide for more information about any of these screens or fields.

## 23.1 Remote MGMT

Use this screen to configure the device's remote management settings. To open this screen, click **Configuration** > **Remote MGMT**.

✍ It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 139** Configuration > Remote MGMT



Configuration >> Remote MGMT

Configuration : Remote MGMT

| | |
|---|---|
| HTTPS | |
| Server Certificate | auto_generated_self_signed_cert ▾ |
| □ Authenticate Client Certificates | |
| Server Port | 443 * |
| Server Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |
| HTTP | |
| Server Port | 80 * |
| Server Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |
| SSH | |
| Server Host Key | auto_generated_self_signed_cert ▾ |
| Server Port | 22 * |
| Server Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |
| TELNET | |
| Server Port | 23 * |
| Server Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |
| FTP | |
| Server Port | 21 * |
| Server Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |
| SNMP Configuration | |
| Get Community | public |
| Set Community | public |
| Trap Community | public |
| Trap Destination | 0.0.0.0 * |
| SNMP | |
| Service Port | 161 * |
| Service Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ □ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |
| DNS | |
| Service Port | 53 * |
| Service Access | ☑ LAN ☑ WAN1 ☑ WAN2 ☑ DMZ ☑ WLAN |
| Secure Client IP Address | ● All ○ Selected 0.0.0.0 * |

The following table describes the labels in this screen.

**Table 116** Configuration > Remote MGMT

| LABEL | DESCRIPTION |
|---|---|
| HTTPS | |
| Server Certificate | Select the **Server Certificate** that the device will use to identify itself. The device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the device). |

**Table 116** Configuration > Remote MGMT (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authenticate Client Certificates | Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the device by sending the device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the device. |
| Server Port | The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the device, for example 8443, then you must notify people who need to access the device web configurator to use “https:// device IP Address:**8443**” as the URL. |
| Server Access | Select the interface(s) through which a computer may access the device using this service.<br>You can allow only secure web configurator access by setting the **HTTP Server Access** field to **Disable** and setting the **HTTPS Server Access** field to an interface(s). |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the device using this service.<br>Select **All** to allow any computer to access the device using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the device using this service. |
| HTTP | |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the device using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the device using this service.<br>Select **All** to allow any computer to access the device using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the device using this service. |
| SSH | |
| Server Host Key | Select the certificate whose corresponding private key is to be used to identify the device for SSH connections. You must have certificates already configured in the **My Certificates** screen. |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the device using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the device using this service.<br>Select **All** to allow any computer to access the device using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the device using this service. |
| TELNET | |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the device using this service. |

**Table 116** Configuration > Remote MGMT (continued)

| LABEL | DESCRIPTION |
|---|---|
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the device using this service.<br>Select **All** to allow any computer to access the device using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the device using this service. |
| FTP | |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the device using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the device using this service.<br>Select **All** to allow any computer to access the device using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the device using this service. |
| SNMP Configuration | |
| Get Community | Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests. |
| Trap Community | Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |
| Trap Destination | Type the IP address of the station to send your SNMP traps to. |
| SNMP | |
| Service Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Service Access | Select the interface(s) through which a computer may access the device using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the device using this service.<br>Select **All** to allow any computer to access the device using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the device using this service. |
| DNS | |
| Server Port | The DNS service port number is 53 and cannot be changed here. |
| Service Access | Select the interface(s) through which a computer may send DNS queries to the device. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to send DNS queries to the device.<br>Select **All** to allow any computer to send DNS queries to the device.<br>Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the device. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART IV
# Building Block

# 24

# Building Blocks (BBs)

This chapter introduces building blocks and explains how to create and manage them.

## 24.1 Building Block (BB) Overview

A BB is a building block used to build a device configuration using Vantage CNM. A configuration BB is a template for a single configuration menu item, such as **Configuration** > **General** or **Configuration** > **Firewall**, for a specific type of device.

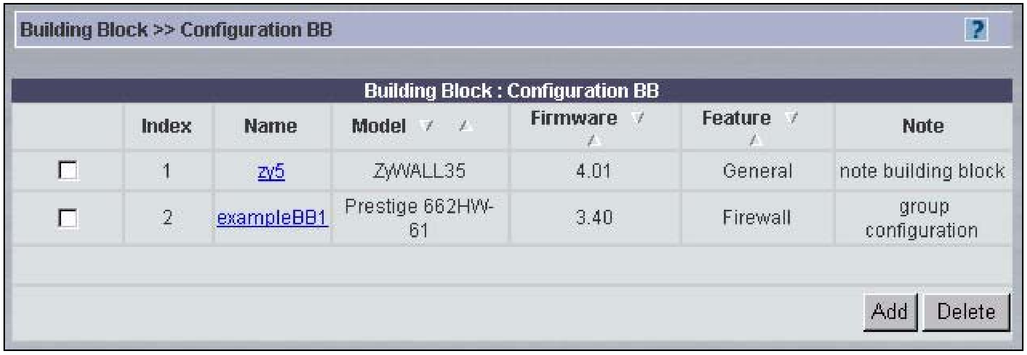
You can create a configuration BB from scratch or save the existing configuration of a device as a BB. In either case, you can then apply the BB to other devices of the same model type. If you modify the BB later, you have to reapply the BB to devices.

You can only view (and use) BBs in your own domain. You cannot view other administrator’s BBs, including BBs created by the root administrator. When creating new BBs from old ones use the save as icon to save as a new BB.

## 24.2 Configuration BB

Use this screen to create, edit, or delete building blocks. To open this screen, click **Building Block** > **Configuration BB**.

**Figure 140** Building Block > Configuration BB



Building Block >> Configuration BB

Building Block : Configuration BB

| | Index | Name | Model | Firmware | Feature | Note |
|---|---|---|---|---|---|---|
| □ | 1 | zy5 | ZyWALL35 | 4.01 | General | note building block |
| □ | 2 | exampleBB1 | Prestige 662HW-61 | 3.40 | Firewall | group configuration |

The following table describes the fields in this screen.

**Table 117** Building Block > Configuration BB

| TYPE | DESCRIPTION |
|---|---|
| Index | This field displays an index number for the building block. |
| Name | This field displays the name of the building block. Click this to edit the building block. |

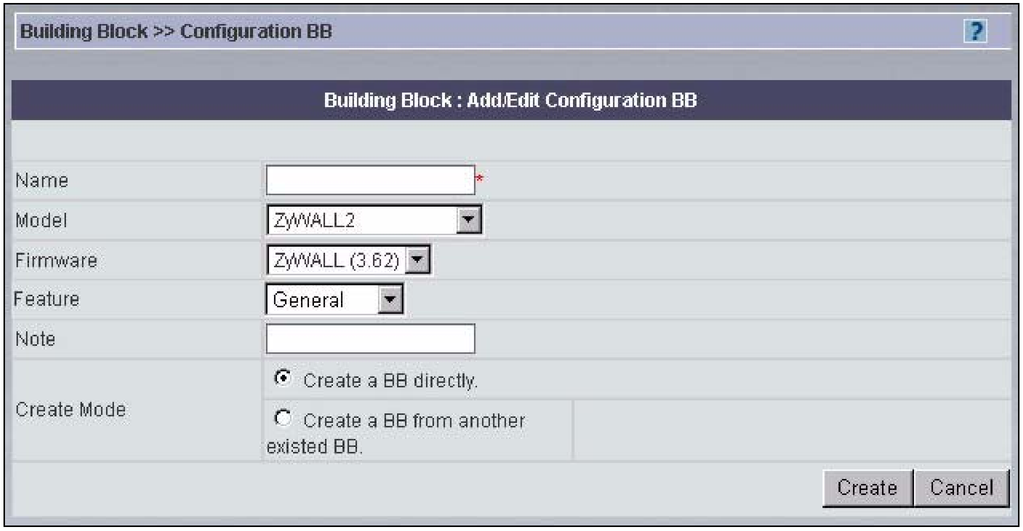
**Table 117** Building Block > Configuration BB (continued)

| TYPE | DESCRIPTION |
|---|---|
| Model | This field displays the type of device this building block is for. |
| Firmware | This field displays the firmware version this building block is for. |
| Feature | This field displays the menu item this building block is for. |
| Note | This field displays any description provided for the building block. |
| Add | Click to proceed to the next screen. |
| Delete | Click this to delete the selected building block(s). |

## 24.2.1 Adding/Editing a Configuration BB

Use this screen to create a new BB or edit an existing one. If you edit an existing BB, some fields are not available. To open this screen, click **Building Block > Configuration BB**, and then click **Add** or the name of an existing BB.

**Figure 141** Building Block > Configuration BB > Add



Building Block >> Configuration BB

Building Block : Add/Edit Configuration BB

| | |
|---|---|
| Name | * |
| Model | ZyWALL2 |
| Firmware | ZyWALL (3.62) |
| Feature | General |
| Note | |
| Create Mode | ● Create a BB directly.<br>○ Create a BB from another existed BB. |

The following table describes the fields in this screen.

**Table 118** Building Block > Configuration BB > Add

| TYPE | DESCRIPTION |
|---|---|
| Name | Enter a unique name for the building block. The name must be 1-32 alphanumeric characters or underscores (_). It cannot include spaces. The name is case-sensitive. |
| Model | Select the type of device the building block is for. |
| Firmware | Select the firmware version the building block is for. |
| Feature | Select the menu item the building block is for. |
| Note | Enter a description of the building block. You can enter up to 256 printable ASCII characters and spaces. |
| Create<br>Next | Click this to create the building block, if necessary, and edit the detailed configuration for the selected device type, firmware version, and menu item. See the corresponding **Configuration** menu item for details. |
| Cancel | Click this to return to the previous screen without saving changes. |

# PART V
# System

# 25

# System > Administrators

Use these screens to manage Vantage CNM administrators. An Administrator is associated with one management domain. After you create an Administrator, you have to associate the administrator with a domain before the Administrator can perform any functions in Vantage CNM.

## 25.1 Introduction to Administrators

There are four types of administrators: root, super, normal and custom. Only “root” can do everything including managing the Vantage CNM system. Super and normal are predefined administrator profiles that come with a default set of permissions. (You can alter the set of permissions for normal profiles in the **System > Preferences > User Group** screen. See Section 26.3.4 on page 294.) Custom administrators have no predefined permissions.

Administrators should periodically change their passwords. The “root” Administrator can also enforce periodic Administrator password changes in the **Force Administrator Password Change every** field in the **System > Preferences > User Access** screen.

### 25.1.1 “Root” Administrator

The default system name (and password) when you first log in is “root”. This is a default system Administrator account, which cannot be deleted by anyone from the system. root’s” details are viewable by others, but not editable.

1 Only one root administrator can exist.
2 Only root can change her own personal information except for UID (User Identification).
3 Only “root” can see all other Administrators. Other Administrators can only see Administrators within their domain.

### 25.1.2 “Super” Administrators

“Super” Administrators are Administrators created using the “Super” User Group. They are the next most powerful type Administrator next to “root”.

1 Super users have all permissions except System Management. System Management is defined as follows:

- Vantage CNM Upgrade
- License
- Preference
- Log option and purge log

- Certificate management
- Maintenance

2. Super permissions are pre-defined in Vantage CNM and are not editable by Vantage CNM Administrators.
3. A “super” Administrator cannot edit any Vantage CNM system settings, but can view (read only) Vantage CNM system status and Vantage CNM logs (but cannot purge or change log options).
4. “Super” Administrators at same management level can't disassociate each other from that management level.

### 25.1.3 “Normal” Administrators

These administrators have default permissions enabled as shown on the screen. Some permissions are not allowed. The Administrator who creates the “Normal” Administrator determines which of the enabled permissions to disable. Normal Administrators cannot create or manage other Administrators.

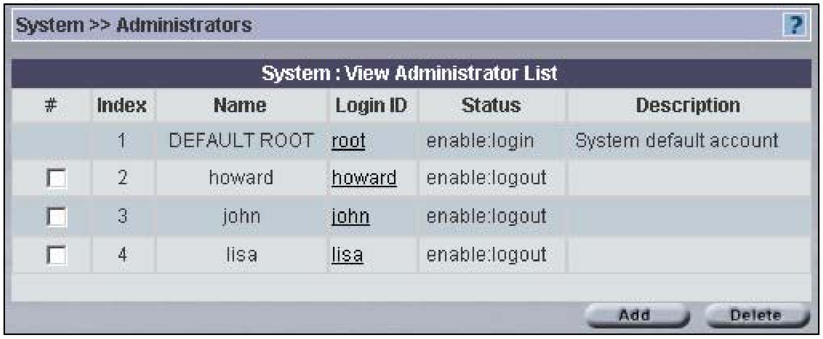
### 25.1.4 “Custom” Administrators

These administrators have no privileges enabled by default. Some permissions are not allowed. The Administrator who creates the “custom administrator” determines which of the allowable permissions to enable. Custom Administrators cannot create or manage other Administrators.

## 25.2 Configuring Administrators

Use this screen to display a list of all administrators configured for this domain and root. To open this screen, select a folder in the object pane and then click **System > Administrators**.

**Figure 142** System > Administrators



System >> Administrators

System : View Administrator List

| # | Index | Name | Login ID | Status | Description |
|---|---|---|---|---|---|
| | 1 | DEFAULT ROOT | root | enable:login | System default account |
| □ | 2 | howard | howard | enable:logout | |
| □ | 3 | john | john | enable:logout | |
| □ | 4 | lisa | lisa | enable:logout | |

The following table describes the fields in this screen.

**Table 119** System > Administrators

| LABEL | DESCRIPTION |
|---|---|
| # | Select the checkbox and enter a valid e-mail address of the person who should receive a report on logs that have been purged. |
| Index | This is the administrator index number. |
| Name | This is the administrator name for identification purposes. |

**Table 119** System > Administrators (continued)

| LABEL | DESCRIPTION |
|---|---|
| Login ID | This is the administrator login name associated with the password that you log into Vantage CNM with. The Login ID is displayed in the object tree when you associate an administrator to a folder. The Login ID cannot be changed after an Administrator account is created but her name can be. |
| Status | This field displays if this Administrator is currently logged in or not. |
| Description | This field displays extra information on this Administrator. |
| Add | Click **Add** to create a new Administrator if you have this permission. Only the “root” Administrator and “Super” Administrators can create (and manage) other Administrators within their domains. |
| Delete | Select an Administrator(s) and then click **Delete** to erase that Administrator account from Vantage CNM. You cannot delete an Administrator who is logged in or who has “child” Administrators. |

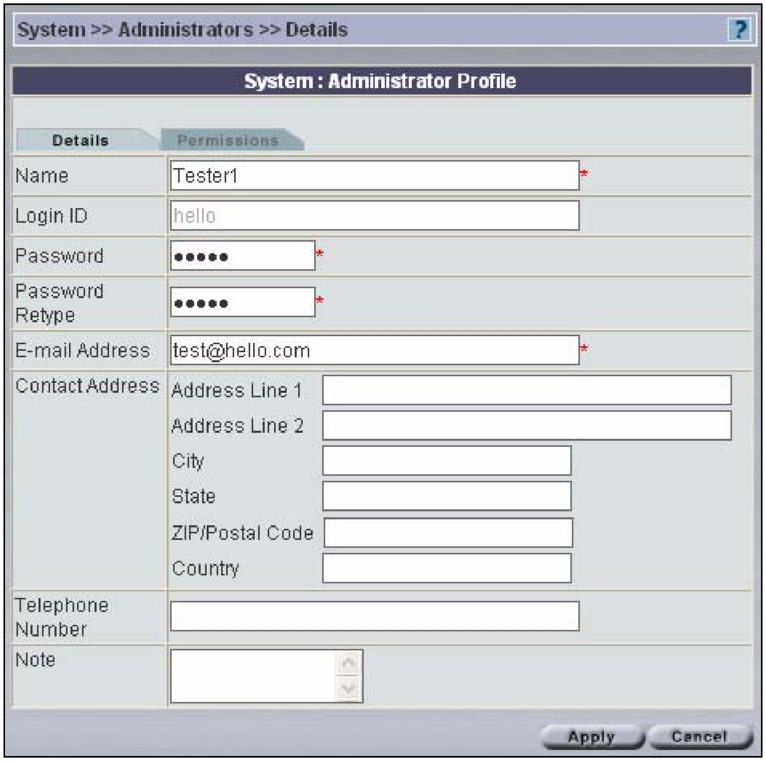
## 25.3 Creating an Administrator Account

Click **Add** to create a new Administrator account or select and existing Administrator account to edit it.

### 25.3.1 Administrator Details

Use this screen to edit the password, contact information, or permissions for an Administrator. Administrators can edit their own password and contact information but not permissions.

**Figure 143** System > Administrators > Add/Edit > Details


System >> Administrators >> Details
?
System : Administrator Profile
Details
Permissions
Apply
Cancel

| | |
|---|---|
| Name | Tester1 * |
| Login ID | hello |
| Password | ●●●●● * |
| Password Retype | ●●●●● * |
| E-mail Address | test@hello.com * |
| Contact Address | Address Line 1 |
| | Address Line 2 |
| | City |
| | State |
| | ZIP/Postal Code |
| | Country |
| Telephone Number | |
| Note | |

The following table describes the fields in this screen.

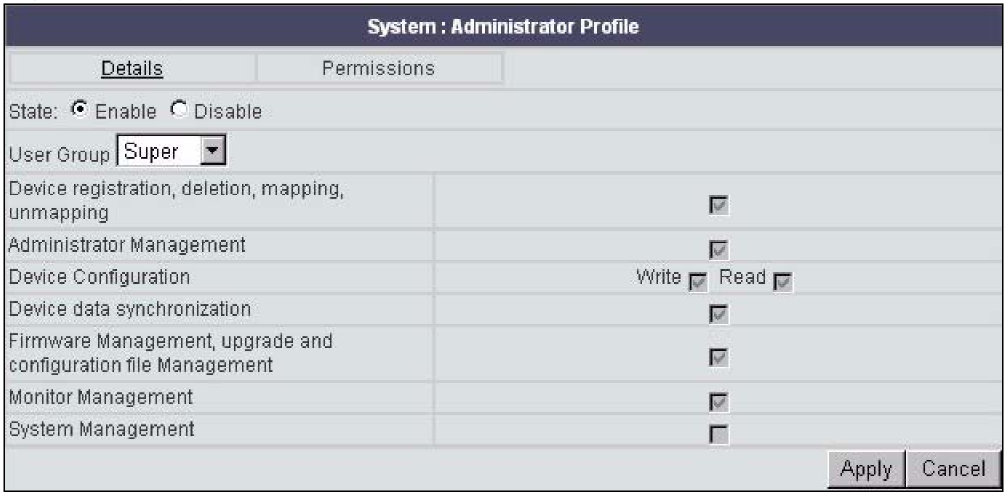
**Table 120** System > Administrators > Add/Edit > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | Type the administrator name used for identification purposes. |
| Login ID | Type the administrator login name associated with the password that you log into Vantage CNM with. The Login ID is displayed in the object tree when you associate an administrator to a folder. The Login ID cannot be changed after an Administrator account is created but her name can be. |
| Password | Type a password associated with the Login ID above. |
| Password Retype | Type the same password again here to make sure that the one you typed above was typed as intended. |
| E-mail Address | Type a valid e-mail address for this Administrator. |
| Contact Address | Type a mailing address for this Administrator. |
| Telephone Number | Type the complete telephone number including area codes for this Administrator. |
| Note | Type some extra information about this Administrator here. |
| Apply | Click **Apply** to save your settings in Vantage CNM. |
| Cancel | Click **Cancel** to go back to the previous screen without saving any changes. |

## 25.3.2 Administrator Permissions

You may select which permissions (privileges) an administrator may have from the next screen. Permissions can only be re-defined by the Administrator who created the Administrator account, and an Administrator's details cannot be changed while logged in.

**Figure 144** System > Administrator > Add/Edit > Permissions



System : Administrator Profile

Details | Permissions

State: ● Enable ○ Disable

User Group: Super

| | |
|---|---|
| Device registration, deletion, mapping, unmapping | ☑ |
| Administrator Management | ☑ |
| Device Configuration | Write ☑ Read ☑ |
| Device data synchronization | ☑ |
| Firmware Management, upgrade and configuration file Management | ☑ |
| Monitor Management | ☑ |
| System Management | □ |

The following table describes the fields in this screen.

**Table 121** System > Administrator > Add/Edit > Permissions

| LABEL | DESCRIPTION |
|---|---|
| State | Select **Disable** to prohibit Administrator access to Vantage CNM without deleting her profile. |
| User Group | Select a pre-defined set of permissions for this administrator, or select **Custom** to configure a specific set of permissions for this administrator. Pre-defined sets of permissions are maintained in the **System > Preferences > User Group** screen. See Section 26.3.4 on page 294. |
| Device registration, deletion, mapping, unmapping | This permission allows the Administrator to register and delete devices as well as associate and disassociate devices to a folder. |
| Administrator Management | This permission allows the Administrator to create, edit and delete Administrators as well as associate and disassociate Administrators to a folder. |
| Device Configuration | This permission allows the Administrator access to all the **System > Configuration** screens. |
| Device data synchronization | This permission allows the Administrator access to the Device > Synchronize screen. See that screen information in this User's Guide for more details. |
| Firmware Management, upgrade and configuration file Management | This permission allows the Administrator to upload device firmware and configuration files to Vantage CNM, download device firmware and configuration files as well as remove them from Vantage CNM. |
| Monitor Management | This permission allows the Administrator access to the Monitor screens. |
| System Management | System Management is defined as follows:<br>• Vantage CNM Upgrade<br>• License<br>• Preference<br>• Log option and purge log<br>• Certificate management<br>• Maintenance |
| Apply | Click **Apply** to save your settings in Vantage CNM. |
| Cancel | Click **Cancel** to begin configuring the screen afresh. |

# 26

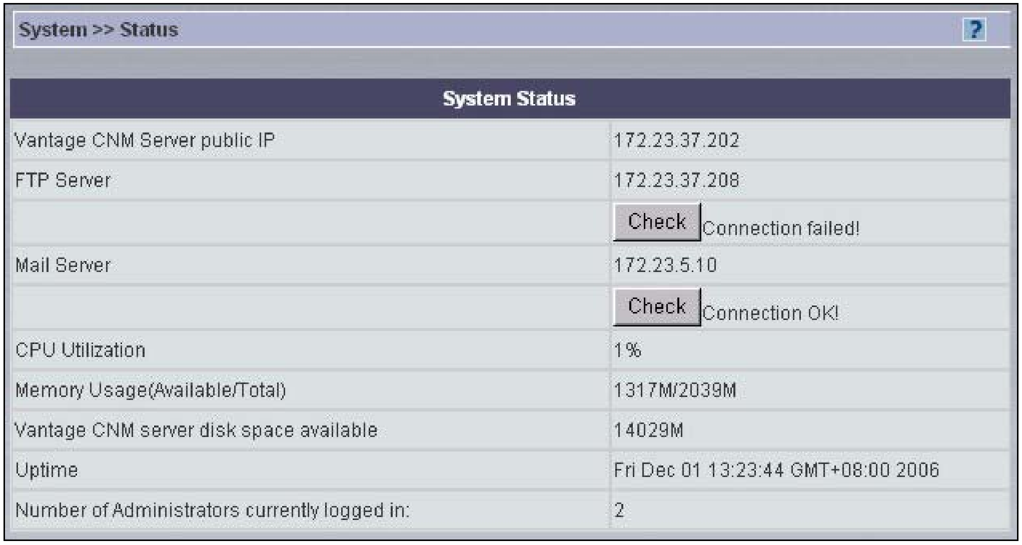
# Other System Screens

Only the root administrator can view the **System > Upgrade** to **System > Data Maintenance** screens as only the root administrator can perform these duties.

## 26.1 Status

Use this screen to view the current Vantage CNM system status. This is a read-only screen. To open this screen, click **System > Status**.

**Figure 145** System > Status



System >> Status

?

System Status

| | |
|---|---|
| Vantage CNM Server public IP | 172.23.37.202 |
| FTP Server | 172.23.37.208 |
| | Check Connection failed! |
| Mail Server | 172.23.5.10 |
| | Check Connection OK! |
| CPU Utilization | 1% |
| Memory Usage(Available/Total) | 1317M/2039M |
| Vantage CNM server disk space available | 14029M |
| Uptime | Fri Dec 01 13:23:44 GMT+08:00 2006 |
| Number of Administrators currently logged in: | 2 |

The following table describes the fields in this screen.

**Table 122** System > Status

| LABEL | DESCRIPTION |
|---|---|
| Vantage CNM Server public IP | This field displays the IP address of the communications server. If the COM server is on the same computer as Vantage CNM, then this address is the same IP address as that of the Vantage CNM server computer. You can change this value in **System > Preferences > Server**. See Section 26.3.1 on page 289. |
| FTP server | This field displays the IP address of the FTP server. You can change this value in **System > Preferences > Server**. See Section 26.3.1 on page 289. Click the **Check** button to test if the connection to the server is up. |
| Mail Server | This field displays the IP address of the Mail Server. You can change this value in **System > Preferences > Server**. See Section 26.3.1 on page 289. Click the **Check** button to test if the connection to the server is up. |

**Table 122** System > Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| CPU Utilization | This field displays the Vantage CNM server CPU processing power usage. Heavy usage may necessitate upgrading to a more powerful CPU. |
| Memory Usage | This field displays the Vantage CNM server memory usage. Heavy usage may necessitate installing more RAM. |
| Vantage CNM server disk space available | This field displays the Vantage CNM server computer hard drive free space. Heavy usage may necessitate buying another hard drive or purging old logs and alerts. |
| Uptime | This field displays how long Vantage CNM has been on since the last start up. |
| Number of Administrators currently logged in | This field displays the number of Administrators currently logged into Vantage CNM. |

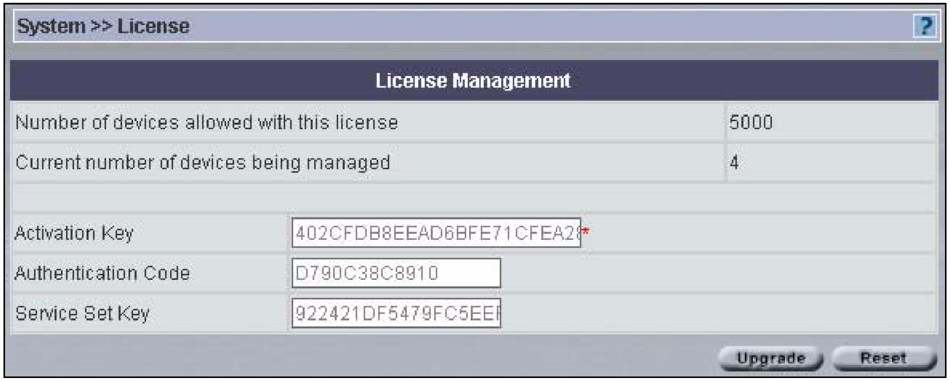
## 26.2 License

You need a license key to generate an **Activation Key** and **Server Set Key** in order to be able to use Vantage CNM. See the *Quick Start Guide* for more information on generating keys at www.myZyXEL.com.

You get an initial license key when you first buy Vantage CNM and after that you may buy expansion license keys in order to be able to manage more devices with Vantage CNM.

Click **System > License** to display the next screen.

**Figure 146** System > License > License Management



System >> License

License Management

| | |
|---|---|
| Number of devices allowed with this license | 5000 |
| Current number of devices being managed | 4 |
| Activation Key | 402CFDB8EEAD6BFE71CFEA2 * |
| Authentication Code | D790C38C8910 |
| Service Set Key | 922421DF5479FC5EE |

The following table describes the fields in this screen.

**Table 123** System > License > License Management

| LABEL | DESCRIPTION |
|---|---|
| Number of devices allowed with this license | This field displays the number of devices you are allowed to manage with this license. If you want to manage more devices, you need to purchase another license. |
| Current number of devices being managed | This field displays the number of devices currently registered with Vantage CNM. |
| Activation Key | This key is generated in the myZyXEL.com website from the **Authentication Code**. |

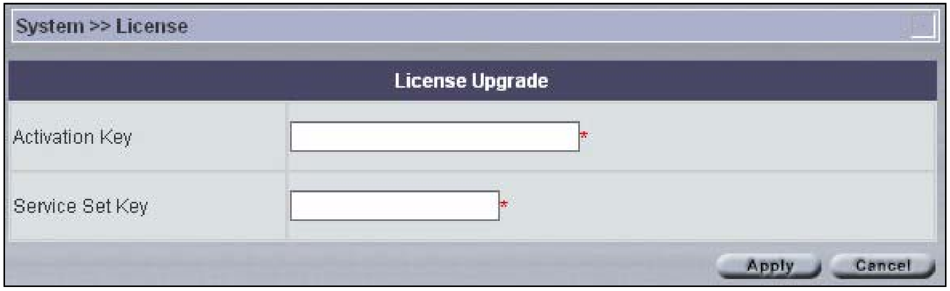
**Table 123** System > License > License Management (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Code | This read-only field displays an automatically generated code after you have installed Vantage CNM. Use this key to obtain an **Activation Key** and a **Service Set Key** from the myZyXEL.com website. |
| Service Set Key | This key is generated in the myZyXEL.com website. It identifies the set of licenses activated on a product. |
| Upgrade | Click **Upgrade** to proceed to the next screen. |
| Reset | Click **Reset** to begin configuring the screen afresh. |

### 26.2.1 License Upgrade

Click **Upgrade** in Figure 146 on page 288 to display this screen.

**Figure 147** System > License > License Upgrade



The following table describes the fields in this screen.

**Table 124** System > License > License Upgrade

| LABEL | DESCRIPTION |
|---|---|
| Activation Key | Copy and paste or type the **Activation Key** that is generated in the myZyXEL.com website. |
| Service Set Key | Copy and paste or type the **Service Set Key** that is generated in the myZyXEL.com website. |
| Apply | Click **Apply** to begin the license upgrade process. Vantage CNM must have an Internet connection. |
| Cancel | Click **Cancel** to return to the previous screen. |

## 26.3 System > Preferences

System preferences are global Vantage CNM server settings.

### 26.3.1 Server

You can configure these servers as you install Vantage CNM (in the installation wizard) or after you install it in this screen.

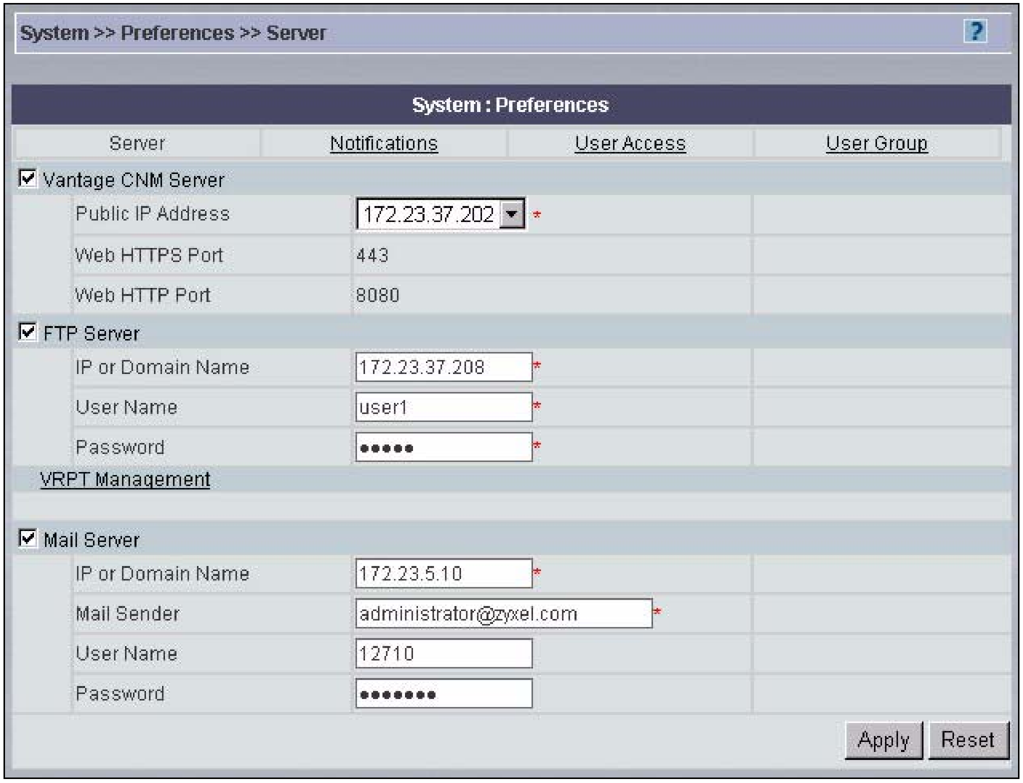
Configure the Vantage CNM public IP server address, FTP server (for firmware upload), and mail server (for Vantage CNM notifications and reports) in this screen. These IP addresses will be the same as the Vantage CNM server computer if they are all on the same computer.

The FTP server is used for file transfers, such as firmware upgrade.

The SMTP server is used for e-mail notifications.

You should know each server's IP address, username and password. File transfers (FTP) and e-mail notifications (SMTP) will not work in Vantage CNM if these are incorrectly configured.

**Figure 148** System > Preferences > Server



System >> Preferences >> Server

System : Preferences

Server | Notifications | User Access | User Group

☑ Vantage CNM Server

| | |
|---|---|
| Public IP Address | 172.23.37.202 * |
| Web HTTPS Port | 443 |
| Web HTTP Port | 8080 |

☑ FTP Server

| | |
|---|---|
| IP or Domain Name | 172.23.37.208 * |
| User Name | user1 * |
| Password | ●●●●● * |

VRPT Management

☑ Mail Server

| | |
|---|---|
| IP or Domain Name | 172.23.5.10 * |
| Mail Sender | administrator@zyxel.com * |
| User Name | 12710 |
| Password | ●●●●●●● |

Apply Reset

The following table describes the fields in this screen.

**Table 125** System > Preferences > Server

| LABEL | DESCRIPTION |
|---|---|
| Vantage CNM Server | Select the check box to make the IP address editable. |
| Public IP Address | Type the IP address of the communications server. |
| Web HTTPS Port | This field displays the port number the Vantage CNM server uses for HTTPS communication. |
| Web HTTP Port | This field displays the port number the Vantage CNM server uses for HTTP communication. |
| FTP Server | The FTP server is used for file uploads to and from Vantage CNM. Select the check box to activate the fields below. |
| IP or Domain Name | Type the IP address or domain name of the FTP server here. |
| User Name | Type your login name to this FTP server. |
| Password | Type the FTP server password associated with the login name. |
| VRPT Management | Click this to edit the settings for Vantage Report servers. See Section 26.8 on page 306. |
| Mail Server | The mail (SMTP) server is used to send Vantage CNM notifications. Select the check box to activate the fields below. |

**Table 125** System > Preferences > Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP or Domain Name | Type the IP address or the domain name of the mail server here. |
| Mail Sender | Type a name to identify the mail server. |
| User Name | Type your login name to this mail server. |
| Password | Type the mail server password associated with the login name. |
| Apply | Click **Apply** to save your settings in Vantage CNM. |
| Reset | Click **Reset** to begin configuring the screen afresh. |

### 26.3.1.1 Vantage CNM Server Public IP Address

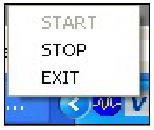
If you change the Vantage CNM server public IP address, then each (Vantage CNM-registered) device's Manager IP address must change too.

1. Go to the **System** > **Preferences** > **Server** screen.
2. Enter the new IP address in the **Vantage CNM Public IP** field and **Apply**.
3. To change all registered devices' Manager IP address to the new IP address, you must do *one* of the following:

- Manually restart each device and wait about 5 minutes until the device registers with Vantage CNM.
- Access each device's command line interface and enter "CNM managerIp x.x.x.x" where "x.x.x.x" is the new Vantage CNM public IP address.

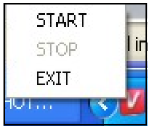
4. Restart Vantage CNM; you don't have to restart the computer on which Vantage CNM is installed. Right-click the Vantage CNM icon in the system tray and select **STOP**.

**Figure 149** Vantage CNM Icon - Stop



Right-click the icon again and select **START**.

**Figure 150** Vantage CNM Icon - Start

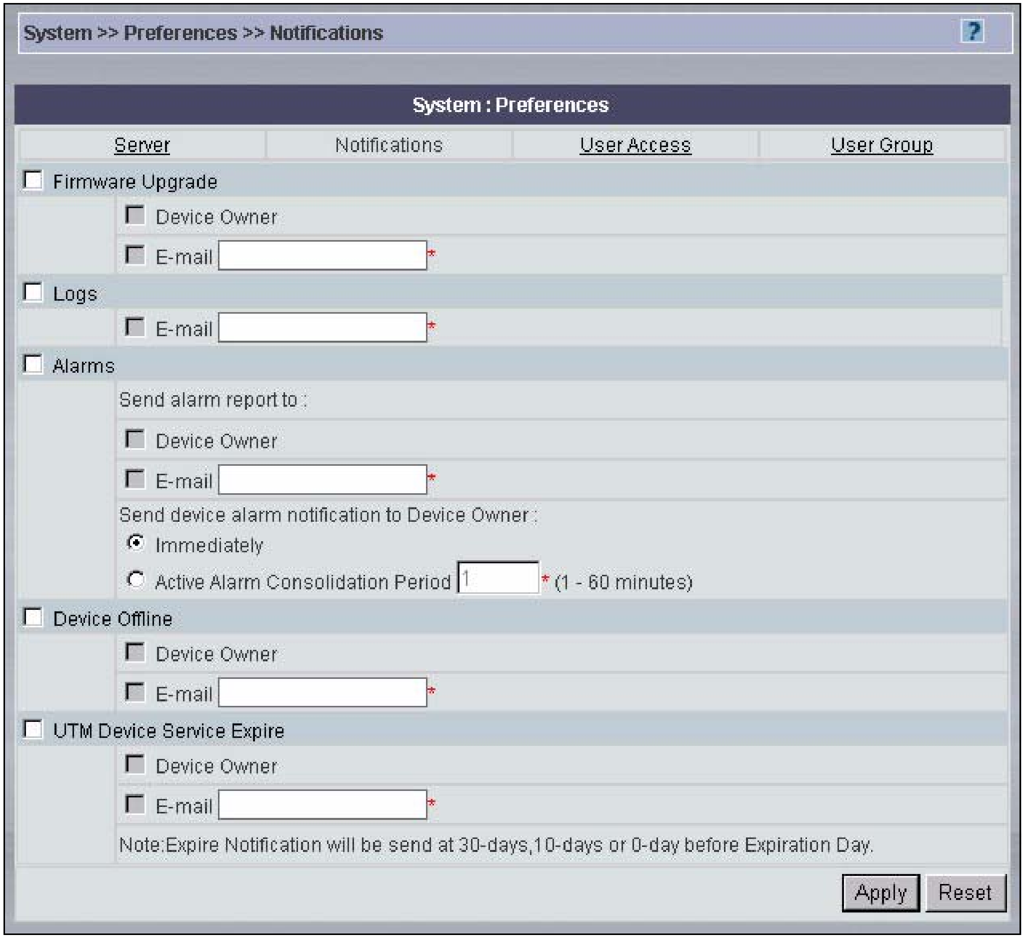


5. When you register new devices with Vantage CNM, make sure the new device can ping the Vantage CNM server (the new **Vantage CNM Public IP** address) and then set the device's Manager IP address correspondingly.

## 26.3.2 Notifications

Use this screen to decide who should receive e-mail for events that may warrant immediate attention such as firmware upgrade or device logs and/or alarms. **Device Owner** is a variable that refers to the e-mail address of the device owner (configured in the **Configuration** > **General** > **Owner Info** screen).

**Figure 151** System > Preferences > Notifications



System >> Preferences >> Notifications

System : Preferences

Server | Notifications | User Access | User Group

□ Firmware Upgrade
- □ Device Owner
- □ E-mail *

□ Logs
- □ E-mail *

□ Alarms
- Send alarm report to :
- □ Device Owner
- □ E-mail *
- Send device alarm notification to Device Owner :
- ● Immediately
- ○ Active Alarm Consolidation Period 1 * (1 - 60 minutes)

□ Device Offline
- □ Device Owner
- □ E-mail *

□ UTM Device Service Expire
- □ Device Owner
- □ E-mail *
- Note:Expire Notification will be send at 30-days,10-days or 0-day before Expiration Day.

The following table describes the fields in this screen.

**Table 126** System > Preferences > Notifications

| LABEL | DESCRIPTION |
|---|---|
| Firmware Upgrade | Set who should be notified when you upload firmware to a device. |
| Device Owner | Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**). |
| E-mail | Enter one or more e-mail addresses, separated by commas. |
| Logs | Set who should receive e-mailed logs. |
| E-mail | Enter one or more e-mail addresses, separated by commas. |
| Alarms | Set who should receive e-mailed alarms. |
| Device Owner | Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**). |
| E-mail | Enter one or more e-mail addresses, separated by commas. |
| Send device alarm notification to Device Owner : | Specify whether each alarm should be sent immediately or aggregated into one alarm for the specified interval (**Active Alarm Consolidation Period**). |
| Device Offline | Set who should be notified when a device that should be available to Vantage CNM becomes unavailable. |
| Device Owner | Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**). |

**Table 126** System > Preferences > Notifications (continued)

| LABEL | DESCRIPTION |
|---|---|
| E-mail | Enter one or more e-mail addresses, separated by commas. |
| UTM Device Service Expire | Set who should be notified when a license for subscription services such as IDP or anti-virus expires. These notices are sent 30 days before the expiration date, 10 days before the expiration date, and the expiration date itself. |
| Device Owner | Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**). |
| E-mail | Enter one or more e-mail addresses, separated by commas. |
| Apply | Click **Apply** to save your settings in Vantage CNM. |
| Reset | Click **Reset** to begin configuring the screen afresh. |

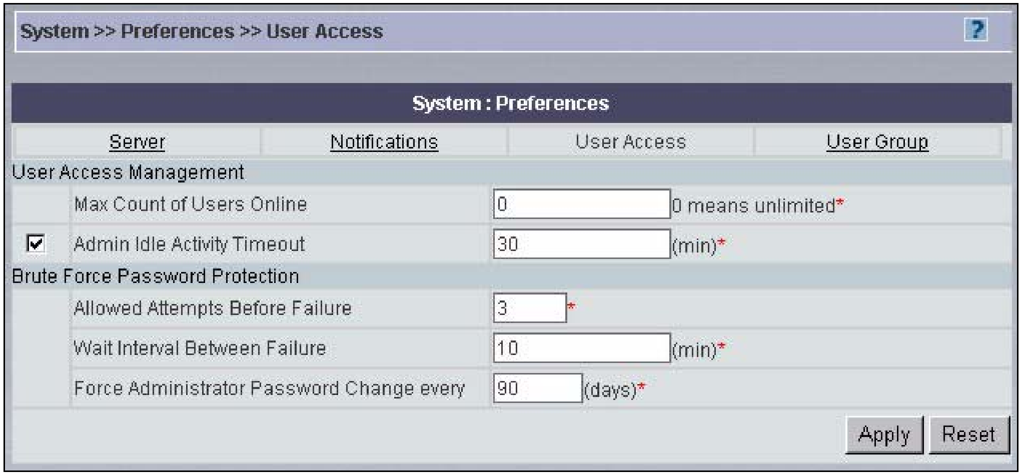
## 26.3.3 User Access

A User is an administrator. Set the maximum number of administrators allowed to log into Vantage CNM at one time, Vantage CNM idle time-out (so one administrator does not unwittingly hog resources by not logging out) and a brute force password protection mechanism in this screen.

Brute-Force Password Guessing Protection is a protection mechanism to discourage brute-force password guessing attacks on a device's management interface. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

You can also force all administrators to periodically change their passwords in this screen.

**Figure 152** System > Preferences > User Access



User Access Management

Max Count of Users Online: 0 — 0 means unlimited*

☑ Admin Idle Activity Timeout: 30 (min)*

Brute Force Password Protection

Allowed Attempts Before Failure: 3 *

Wait Interval Between Failure: 10 (min)*

Force Administrator Password Change every: 90 (days)*

The following table describes the fields in this screen.

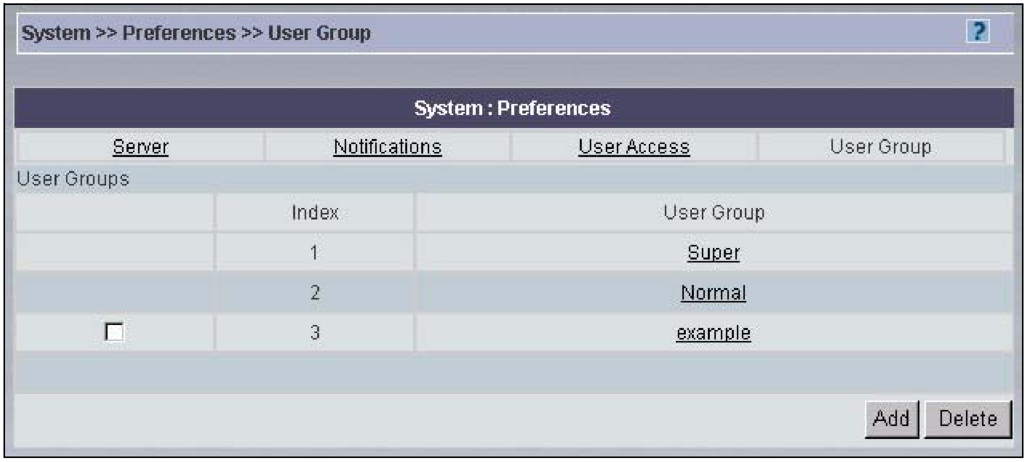
**Table 127** System > Preferences > User Access

| LABEL | DESCRIPTION |
|---|---|
| Max Count of Users Online | Type the maximum number of administrators allowed to log into Vantage CNM at any one time. |
| Admin Idle Activity Timeout | Select the check box next to this to activate the timeout, and type the length of time an Administrator can leave the Vantage CNM web configurator idle before he is automatically logged out. Clear the check box to disable the timeout. |
| Brute Force Password Protection | Configure the next two fields to apply this. |
| Allowed Attempts Before Failure | Type the number of times an incorrect password may be entered before a login failure is returned. |
| Wait Interval Between Failure | Type the wait time before allowing another login in after a login failure is returned. |
| Force Administrator Password Change every | Type how often all Administrators must change their Vantage CNM login passwords. If an Administrator does not change her password within this time, then the old password expires. |
| Apply | Click **Apply** to save your settings in Vantage CNM. |
| Reset | Click **Reset** to begin configuring the screen afresh. |

### 26.3.4 User Group

A “user group” is a pre-defined set of administrator permissions. **Super** pre-defined permissions are not editable. Root may choose what default permissions are associated with the **Normal** permissions template here. Root can also create and delete new permission templates here.

**Figure 153** System > Preferences > User Group



System >> Preferences >> User Group

System : Preferences

Server | Notifications | User Access | User Group

User Groups

| | Index | User Group |
|---|---|---|
| | 1 | Super |
| | 2 | Normal |
| □ | 3 | example |

The following table describes the fields in this screen.

**Table 128** System > Preferences > Permissions

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the template index number. 1 and 2 are default templates. |
| User Group | This field displays the template name (**User Group**). |

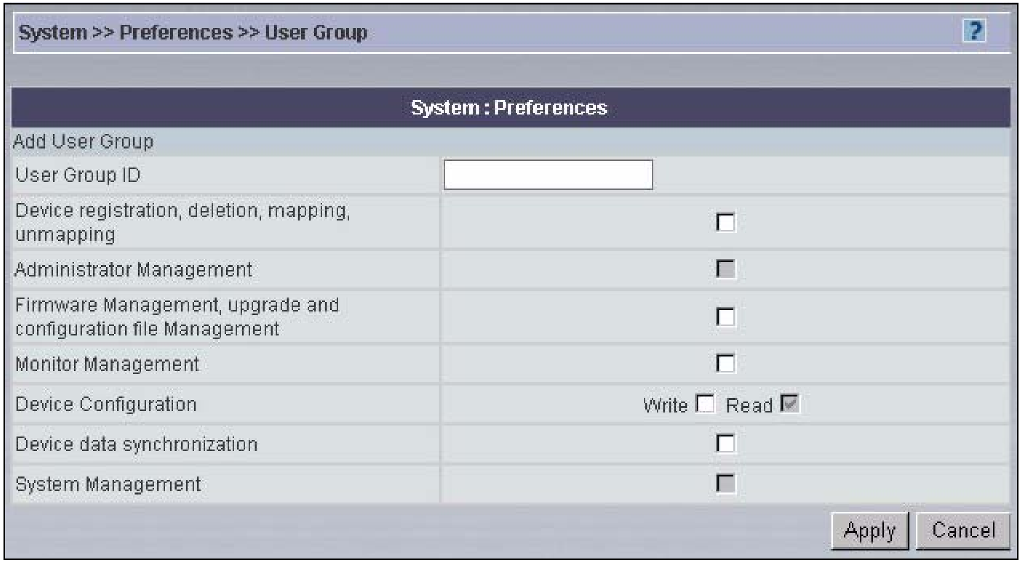
**Table 128** System > Preferences > Permissions (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add | Click **Add** to create a new template. |
| Delete | Select the check box next to a template, and click **Delete** to remove it. You cannot remove the **Super** and **Normal** templates. |

## 26.3.5 Add User Group

Use this screen to create or edit a "user group" (administrator permission template). To open this screen, click **Add** in the previous screen to display the next one as shown.

**Figure 154** System > Preferences > Permissions > Add



System >> Preferences >> User Group

System : Preferences

Add User Group

| | |
|---|---|
| User Group ID | |
| Device registration, deletion, mapping, unmapping | □ |
| Administrator Management | □ |
| Firmware Management, upgrade and configuration file Management | □ |
| Monitor Management | □ |
| Device Configuration | Write □ Read ☑ |
| Device data synchronization | □ |
| System Management | □ |

The following table describes the fields in this screen.

**Table 129** System > Preferences > Permissions > Add

| LABEL | DESCRIPTION |
|---|---|
| User Group ID | Enter the new template name (**User Group**) in this field. |
| Device registration, deletion, mapping, unmapping | This field allows the Administrator to register and delete devices as well as associate and disassociate devices to a folder. |
| Administrator Management | This field allows the Administrator to add, edit and delete the administrators. |
| Firmware Management, upgrade and configuration file Management | This field allows the Administrator to download configuration files and to manage and upload device firmware and configuration files. |
| Monitor Management | This field allows the Administrator access to the **Monitor** screens. |
| Device Configuration | |
| Read | This field allows the Administrator to read all the content in the **Configuration** menu. |
| Write | This field allows the Administrator to apply configuration changes in the **Configuration** menu. |
| Device data synchronization | This field allows the Administrator to synchronize data between Vantage CNM and devices. |

**Table 129** System > Preferences > Permissions > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Management | Only **root** can do system management. System Management is defined as follows:<br>• Vantage CNM Upgrade<br>• License<br>• Preference<br>• Log option and purge log<br>• Certificate management<br>• Maintenance |
| Apply | Click **Apply** to save your settings in Vantage CNM. |
| Cancel | Click **Cancel** to begin configuring the screen afresh. |

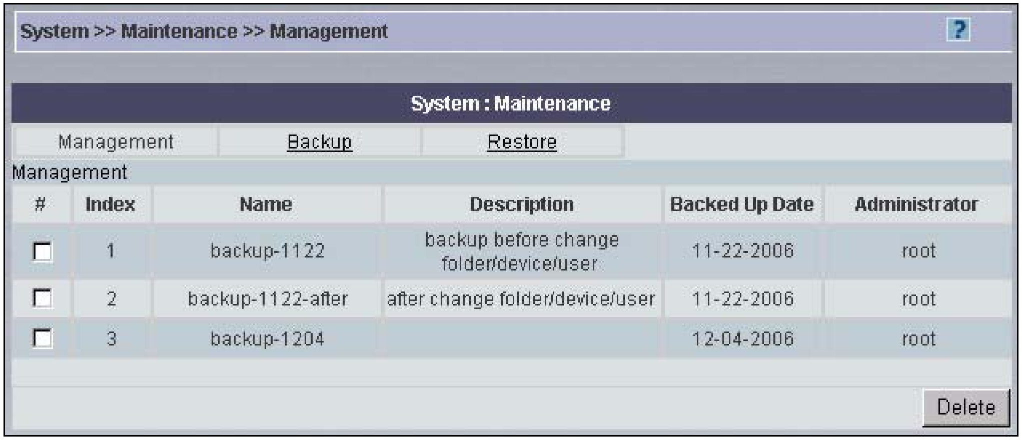
## 26.4 System Maintenance

Use the **Maintenance** screens to manage, back up and restore Vantage CNM system backup files. Data maintenance includes device firmware and configuration files you have uploaded to the Vantage CNM server. You can back up or restore to your computer or Vantage CNM. You can choose what domain to back up by selecting a folder in the object tree.

### 26.4.1 Management

Use this screen to delete previous (old) system backups.

**Figure 155** System > Maintenance > Management



| # | Index | Name | Description | Backed Up Date | Administrator |
|---|---|---|---|---|---|
| □ | 1 | backup-1122 | backup before change folder/device/user | 11-22-2006 | root |
| □ | 2 | backup-1122-after | after change folder/device/user | 11-22-2006 | root |
| □ | 3 | backup-1204 | | 12-04-2006 | root |

The following table describes the fields in this screen.

**Table 130** System > Maintenance > Management

| LABEL | DESCRIPTION |
|---|---|
| # | Select this and click **Delete** to remove the selected backup(s). |
| Index | This field displays the system backup file index number. |
| Name | This field displays the system backup file name. |
| Description | This field displays some extra description of the system backup file. |
| Backed Up Date | This field displays the date the system backup file was created. |

**Table 130** System > Maintenance > Management (continued)

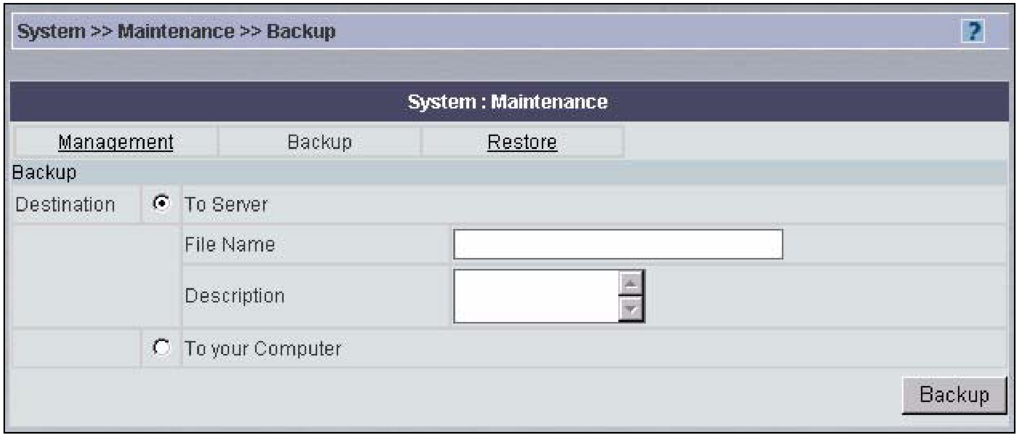
| LABEL | DESCRIPTION |
|---|---|
| Administrator | This field displays who created the system backup file. |
| Delete | Select a system backup file and then click **Delete** to remove it from Vantage CNM. |

## 26.4.2 Backup

Use this screen to save your current Vantage CNM system to the Vantage CNM server or your computer. You can enter extra information on the file in the **Description** text box.

Backup configuration allows you to back up (save) the current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings. You should perform system backup before you upgrade Vantage CNM software.

**Figure 156** System > Maintenance > Backup



The following table describes the fields in this screen.

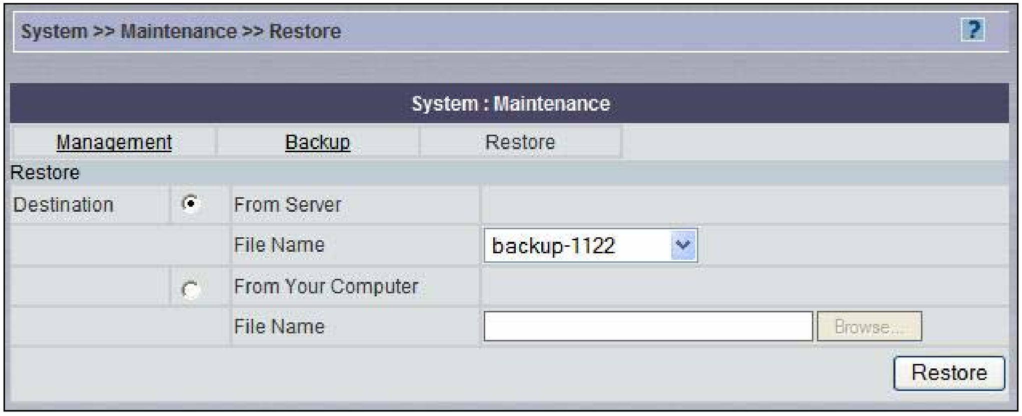
**Table 131** System > Maintenance > Backup

| LABEL | DESCRIPTION |
|---|---|
| Destination | |
| To Server | Select this option to back up the file to the Vantage CNM server. |
| File Name | Type in the location of the file you want to upload in this field. |
| Description | Type a description of the file backup. |
| To your Computer | Select the radio button to give the download destination to your computer. |
| Backup | Click this button to perform the file backup. |

## 26.4.3 Restore

Use this screen to restore a previously saved system backup (from your computer or Vantage CNM) to Vantage CNM.

**Figure 157** System > Maintenance > Restore



System >> Maintenance >> Restore

System : Maintenance

Management | Backup | Restore

Restore

| | | | |
|---|---|---|---|
| Destination | ● | From Server | |
| | | File Name | backup-1122 |
| | ○ | From Your Computer | |
| | | File Name | Browse... |

The following table describes the fields in this screen.

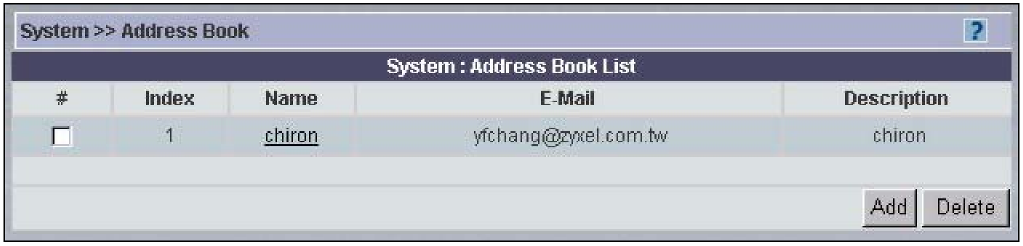
**Table 132** System > Maintenance > Restore

| LABEL | DESCRIPTION |
|---|---|
| Destination | Select this radio button to upload a configuration file **From Server**. |
| From Server | Select this option to restore the file from the Vantage CNM server. |
| File Name | Select a file from the drop-down list box. |
| From Your Computer | Select this radio button to upload a configuration file From **Your Computer**. |
| File Name | Type in the location of the file you want to upload in this field or click **Browse** ... to find it. |
| Restore | Click **Restore** to begin the upload process. |

## 26.5 Address Book

An address book is a list of personal details of people such as device owners and administrators. Click **System** > **Address Book** to display the next screen.

**Figure 158** System > Address Book



System >> Address Book

System : Address Book List

| # | Index | Name | E-Mail | Description |
|---|---|---|---|---|
| □ | 1 | chiron | yfchang@zyxel.com.tw | chiron |

The following table describes the labels in this screen.

**Table 133** System > Address Book

| LABEL | DESCRIPTION |
|---|---|
| # | This is a number defining an address book entry. |
| Index | This field displays the address book entry index number. |
| Name | This field displays the person’s name. |
| E-Mail | This field displays the person’s e-mail address. |

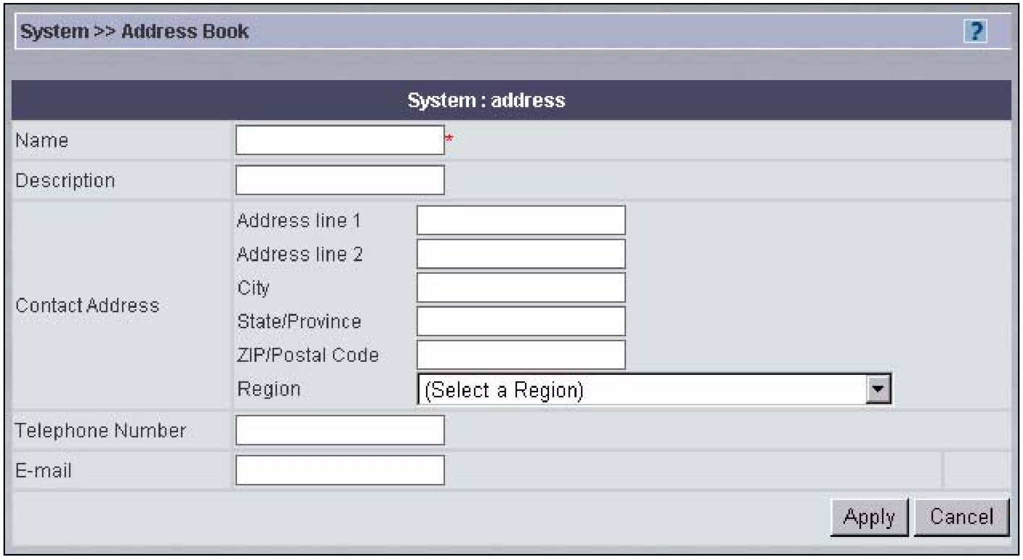
**Table 133** System > Address Book (continued)

| LABEL | DESCRIPTION |
|---|---|
| Description | This field displays some extra information about the person. |
| Add | Click **Add** to create a new customer record. |
| Delete | Select a system backup file and then click **Delete** to remove it from Vantage CNM. |

### 26.5.1 Address Book Add/Edit

Use this screen to add or edit an entry in the address book. From Figure 158 on page 298, click **Add** to create a new entry or click an existing entry hyperlink to edit it.

**Figure 159** System > Address Book > Add/Edit



The following table describes the labels in this screen.

**Table 134** System > Address Book > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Type the person’s name. |
| Description | Type some extra information about the person. |
| Contact Address | Type a mailing address for this person. |
| Telephone Number | Type the complete telephone number including area codes for this person. |
| E-mail | Type the person’s e-mail address. |
| Apply | Click **Apply** to create a new address book record. |
| Cancel | Click **Cancel** to return to the previous screen. |

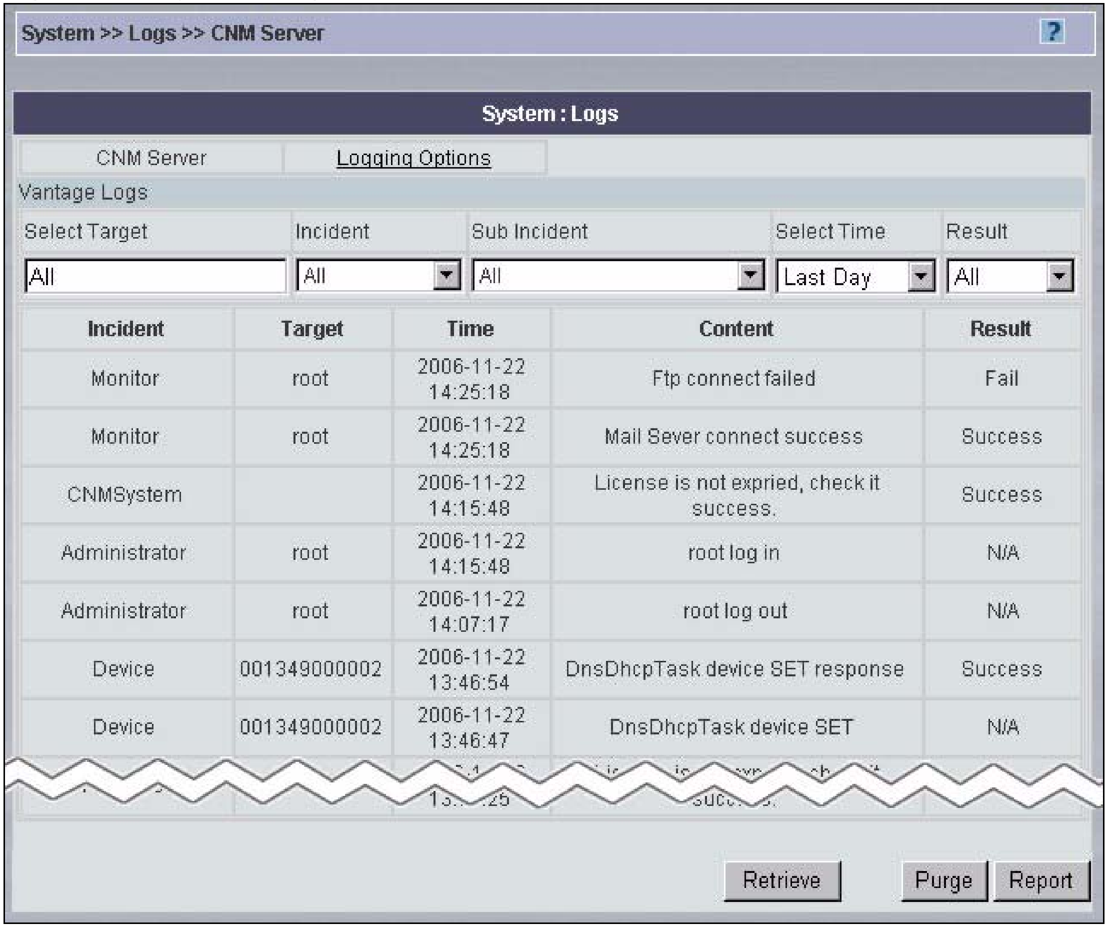
## 26.6 Vantage CNM Logs

Use these screens to view and configure Vantage CNM system log preferences.

## 26.6.1 CNM Server

You can view system logs for previous day, the last two days or up to one week here.

**Figure 160** System > Logs > CNM Server



| Select Target | Incident | Sub Incident | Select Time | Result |
|---|---|---|---|---|
| All | All | All | Last Day | All |

| Incident | Target | Time | Content | Result |
|---|---|---|---|---|
| Monitor | root | 2006-11-22 14:25:18 | Ftp connect failed | Fail |
| Monitor | root | 2006-11-22 14:25:18 | Mail Sever connect success | Success |
| CNMSystem | | 2006-11-22 14:15:48 | License is not expried, check it success. | Success |
| Administrator | root | 2006-11-22 14:15:48 | root log in | N/A |
| Administrator | root | 2006-11-22 14:07:17 | root log out | N/A |
| Device | 001349000002 | 2006-11-22 13:46:54 | DnsDhcpTask device SET response | Success |
| Device | 001349000002 | 2006-11-22 13:46:47 | DnsDhcpTask device SET | N/A |

The following table describes the labels in this screen.

**Table 135** System > Logs > CNM Server

| LABEL | DESCRIPTION |
|---|---|
| Select Target | Enter the source of the event. This must be **All**, the MAC address of a device (001122334455 format), or the user name of an account. **CNMSystem** events do not have a target. |
| Incident | Select one of the general categories of events whose logs you want to view. |
| Sub Incident | Select a more specific type of event whose logs you want to view. |
| Select Time | Select the time period for which you wish to view Vantage CNM logs |
| Result | Select whether or not the event was successful. In some cases, logs are informational, in which case you should select **All**. |
| Incident | This field displays the general category of the event. |
| Target | This field displays the source of the event. This might be the MAC address of a device, the user name of an account, or a blank value. **CNMSystem** events do not have a target. |
| Time | This field displays the date the Vantage CNM log occurred. |

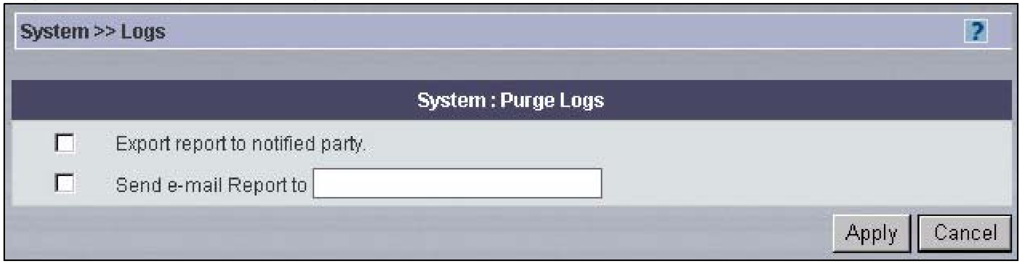
**Table 135** System > Logs > CNM Server (continued)

| LABEL | DESCRIPTION |
|---|---|
| Content | This field displays a message describing the log. |
| Result | This field indicates whether or not the event was successful. In some cases, logs are informational, in which case **N/A** is displayed. |
| Retrieve | Click **Retrieve** for Vantage CNM to pull the logs from the selected device. |
| Purge | Select **Purge** to delete system logs from the Vantage CNM server. |
| Report | Click **Report** to generate a report on the logs with the specified criteria. |

## 26.6.2 Purge Logs

Click **System** > **Logs** > **CNM Server** > **Purge** to remove logs from the Vantage CNM database. A report of purged logs can be e-mailed and/or downloaded to your computer.

**Figure 161** System > Logs > CNM Server > Purge



System >> Logs

System : Purge Logs

☐ Export report to notified party.

☐ Send e-mail Report to

The following table describes the labels in this screen.

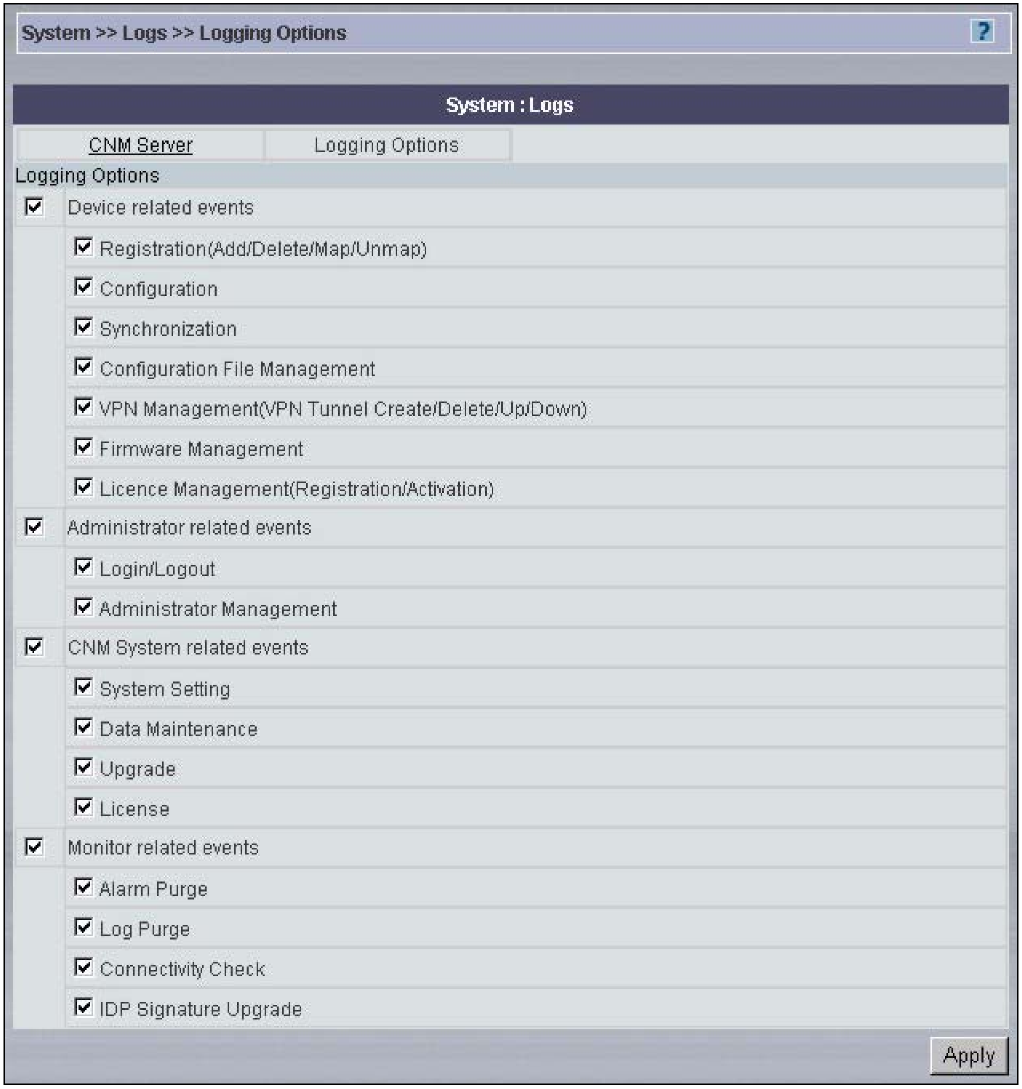
**Table 136** System > Logs > CNM Server > Purge

| LABEL | DESCRIPTION |
|---|---|
| Send e-mail Report to | Select the check box and enter valid e-mail address(es) of those who should receive a report on logs that have been purged. Separate more than one E-mail address by a comma. |
| Export report to notified party. | Select this check box to send a report on logs that have been purged to the e-mail addresses defined in notifications. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 26.6.3 Logging Options

Select what type of system logs you wish to log as shown in the following screen.

**Figure 162** System > Logs > Logging Options



Logging Options

- ☑ Device related events
  - ☑ Registration(Add/Delete/Map/Unmap)
  - ☑ Configuration
  - ☑ Synchronization
  - ☑ Configuration File Management
  - ☑ VPN Management(VPN Tunnel Create/Delete/Up/Down)
  - ☑ Firmware Management
  - ☑ Licence Management(Registration/Activation)
- ☑ Administrator related events
  - ☑ Login/Logout
  - ☑ Administrator Management
- ☑ CNM System related events
  - ☑ System Setting
  - ☑ Data Maintenance
  - ☑ Upgrade
  - ☑ License
- ☑ Monitor related events
  - ☑ Alarm Purge
  - ☑ Log Purge
  - ☑ Connectivity Check
  - ☑ IDP Signature Upgrade

## 26.7 Certificate Management Overview

Some devices can provide certificates (also called digital IDs) for users to authenticate the device. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.

2 Tim keeps the private key and makes the public key openly available.

3 Tim uses his private key to encrypt the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to decrypt it.

5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

### 26.7.1 Advantages of Certificates

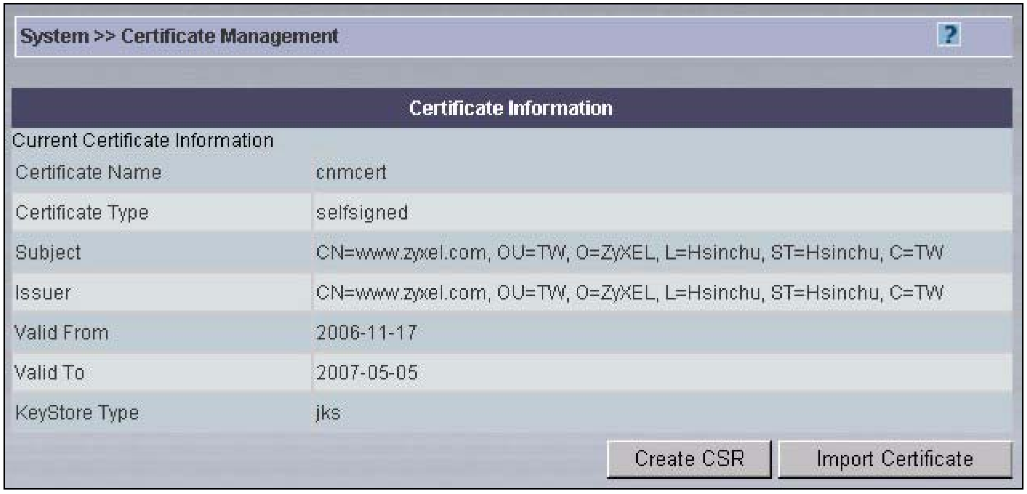
The device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.

Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

### 26.7.2 Current Certificate Information

You can view your current certificate information in this screen, including certificate name, type, origin and duration of validity.

**Figure 163** System > Certificate Management > Information



| Current Certificate Information | |
|---|---|
| Certificate Name | cnmcert |
| Certificate Type | selfsigned |
| Subject | CN=www.zyxel.com, OU=TW, O=ZyXEL, L=Hsinchu, ST=Hsinchu, C=TW |
| Issuer | CN=www.zyxel.com, OU=TW, O=ZyXEL, L=Hsinchu, ST=Hsinchu, C=TW |
| Valid From | 2006-11-17 |
| Valid To | 2007-05-05 |
| KeyStore Type | jks |

The following table describes the labels in this screen.

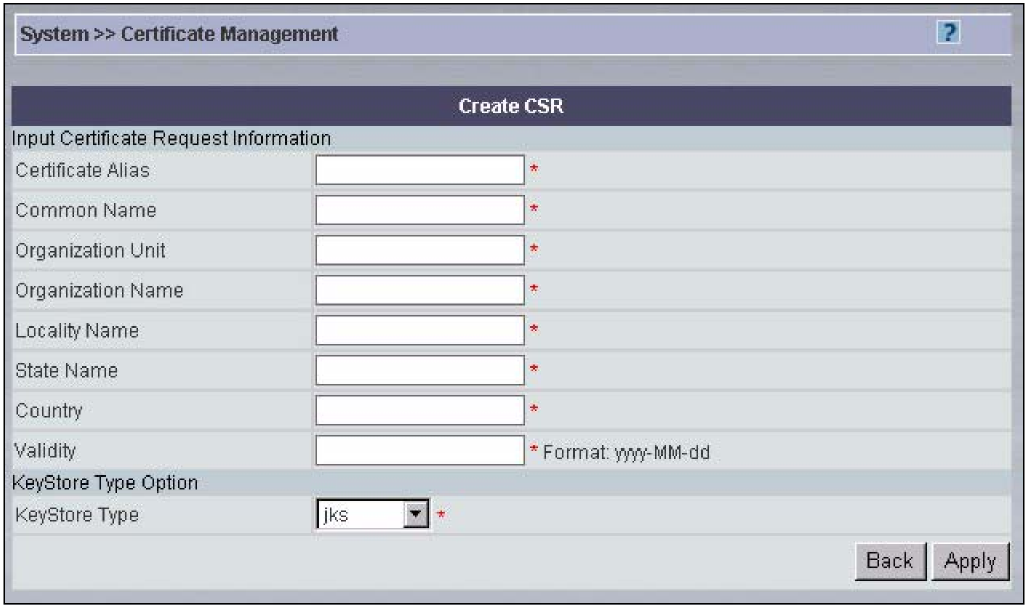
**Table 137** System > Certificate Management > Information

| LABEL | DESCRIPTION |
|---|---|
| Current Certificate Information | |
| Certificate Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| Certificate Type | This field displays what kind of certificate this is.<br>**REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate** Import screen to import the certificate and replace the request.<br>**SELF** represents a self-signed certificate.<br>***SELF** represents the default self-signed certificate, which the device uses to sign imported trusted remote host certificates.<br>**CERT** represents a certificate issued by a certification authority. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a "Not Yet Valid!" message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an "Expiring!" or "Expired!" message if the certificate is about to expire or has already expired. |
| KeyStore Type | This field specifies the format of the certificate. Possible formats include PKCS #12 (**pkcs12**) and Java Key Store (**jks**) |
| Create CSR | Click **Create CSR** to create a certificate. |
| Import Certificate | Click **Import Certificate** to go to the Import Certificate screen. |

## 26.7.3 Create CSR

You can create certificates by entering the requested information into the fields below. Then click **Apply**.

**Figure 164** System > Certificate Management > Create CSR



System >> Certificate Management

Create CSR

Input Certificate Request Information

| | |
|---|---|
| Certificate Alias | * |
| Common Name | * |
| Organization Unit | * |
| Organization Name | * |
| Locality Name | * |
| State Name | * |
| Country | * |
| Validity | * Format: yyyy-MM-dd |

KeyStore Type Option

| | |
|---|---|
| KeyStore Type | jks * |

The following table describes the labels in this screen.

**Table 138** System > Certificate Management > Create CSR

| LABEL | DESCRIPTION |
|---|---|
| Input Certificate Request Information | |
| Certificate Alias | Type a name to identify the certificate. You can use 1-32 alphanumeric characters, underscores (_), or dashes (-). |
| Common Name | Type the IP address or domain name used to identify the certificate's owner. You can use 1-32 printable ASCII characters. Spaces are not allowed. |
| Organization Unit | Type the organization unit (for example, department or division) in this field. You can use 1-32 alphanumeric characters, underscores (_), or dashes (-). |
| Organization Name | Type the name of the organization or company in this field. You can use 1-32 alphanumeric characters, underscores (_), or dashes (-). |
| Locality Name | Type the location (for example, city or town) of the organization or company; number, street etc. You can use 1-32 alphanumeric characters, underscores (_), or dashes (-). |
| State Name | Type the state or province where the organization or company is located. You can use 1-32 alphanumeric characters, underscores (_), or dashes (-). |
| Country | Type the country code where the organization or company is located. The country must be two letters long. |
| Validity | Type the date the certificate expires. This date cannot be in the past, and it cannot be more than fifty years from the current date. Use the specified format. |

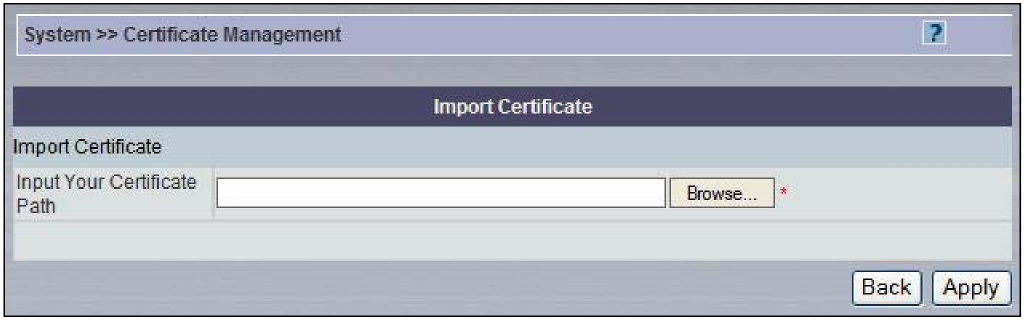
**Table 138** System > Certificate Management > Create CSR (continued)

| LABEL | DESCRIPTION |
|---|---|
| KeyStore Type Option | |
| KeyStore Type | Select what type of keystore file to use. Choices are PKCS #12 (**pkcs12**) and Java Key Store (**jks**). PKCS #12 is a common standard for X.509 certificates. Java Key Store may be used by standalone Java clients using SSL communication or WebLogic Server. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save these changes. |

### 26.7.4 Import Certificate

In this screen, you can **Browse** for a certificate that has already been downloaded to your computer. Select **Apply** to complete the certificate import.

**Figure 165** System > Certificate Management > Import Certificate



The following table describes the labels in this screen.

**Table 139** System > Certificate Management > Import Certificate

| LABEL | DESCRIPTION |
|---|---|
| Input Certificate | |
| Input Your Certificate Path | Type in the location of the certificate you want to upload in this field or click **Browse** ... to find it. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save these changes. |

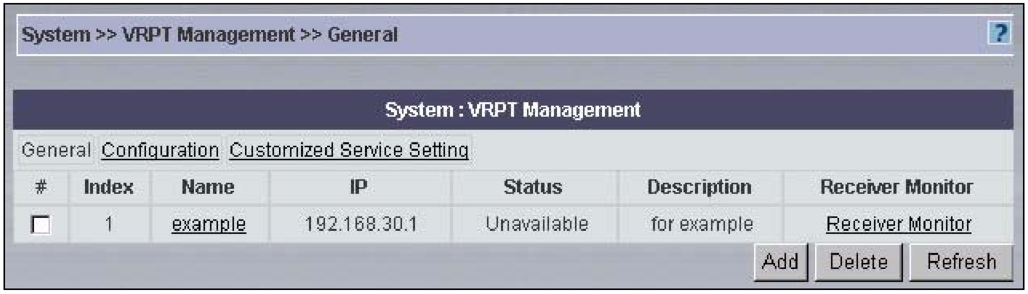
## 26.8 VRPT Management

Vantage CNM also includes Vantage Report. See Chapter 29 on page 333 for information about Vantage Report in Vantage CNM.

### 26.8.1 General

Use this screen to manage the Vantage Report instances in Vantage CNM. To open this screen, click **System** > **VRPT Management** > **General**.

**Figure 166** System > VRPT Management > General



System >> VRPT Management >> General

System : VRPT Management

General Configuration Customized Service Setting

| # | Index | Name | IP | Status | Description | Receiver Monitor |
|---|---|---|---|---|---|---|
| □ | 1 | example | 192.168.30.1 | Unavailable | for example | Receiver Monitor |

The following table describes the labels in this screen.

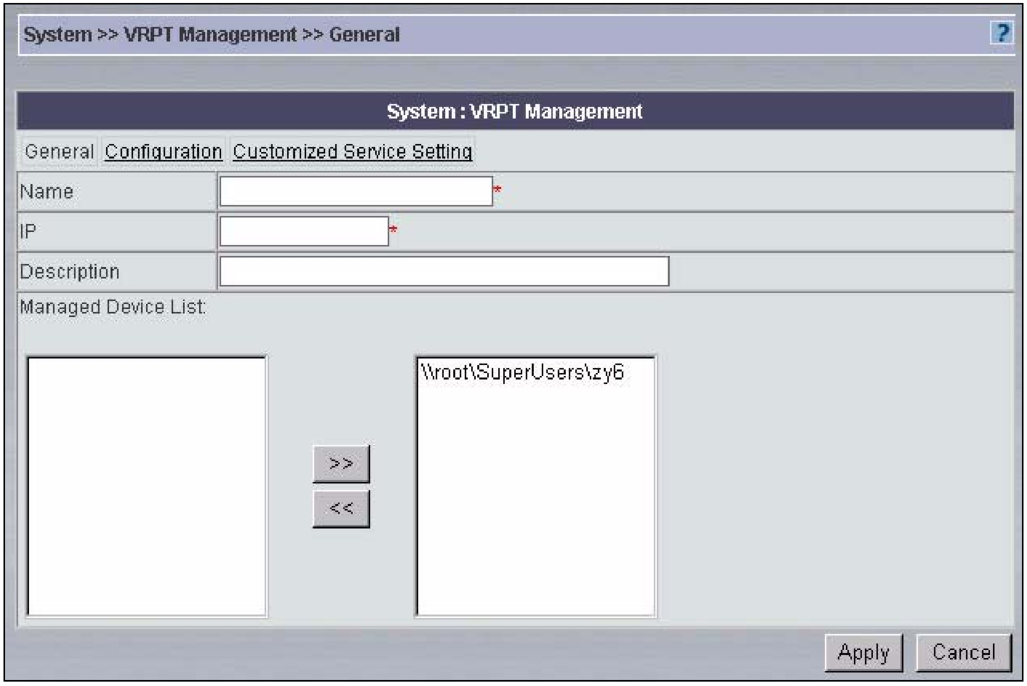
**Table 140** System > VRPT Management > General

| LABEL | DESCRIPTION |
|---|---|
| # | Select this and click **Delete** to remove the Vantage Report instance. |
| Index | This field displays the index number of each Vantage Report instance. |
| Name | This field displays the name of the Vantage Report instance in Vantage CNM. Click the name to edit it. |
| IP | This field displays the IP address of the Vantage Report instance. |
| Status | This field displays the status of the Vantage Report instance.<br>**Unavailable**: Vantage CNM is not able to connect to the Vantage Report server.<br>**Available**: Vantage CNM is able to connect to the Vantage Report server. |
| Description | This field displays any description of the Vantage Report instance. |
| Receiver Monitor | Click this to look at the total number of logs that Vantage Report received by day or from each device. |
| Add | Click this to set up a new Vantage Report instance in Vantage CNM. |
| Delete | Select the check box next to one or more Vantage Report instances and click **Delete** to remove it (them). |
| Refresh | Click this to update the information in this screen. |

## 26.8.2 Add/Edit VRPT Server

Use this screen to configure a VRPT server. To open this screen, click **System** > **VRPT Management** > **General**, and then click **Add** or an existing VRPT server.

**Figure 167** System > VRPT Management > General > Add/Edit



The following table describes the labels in this screen.

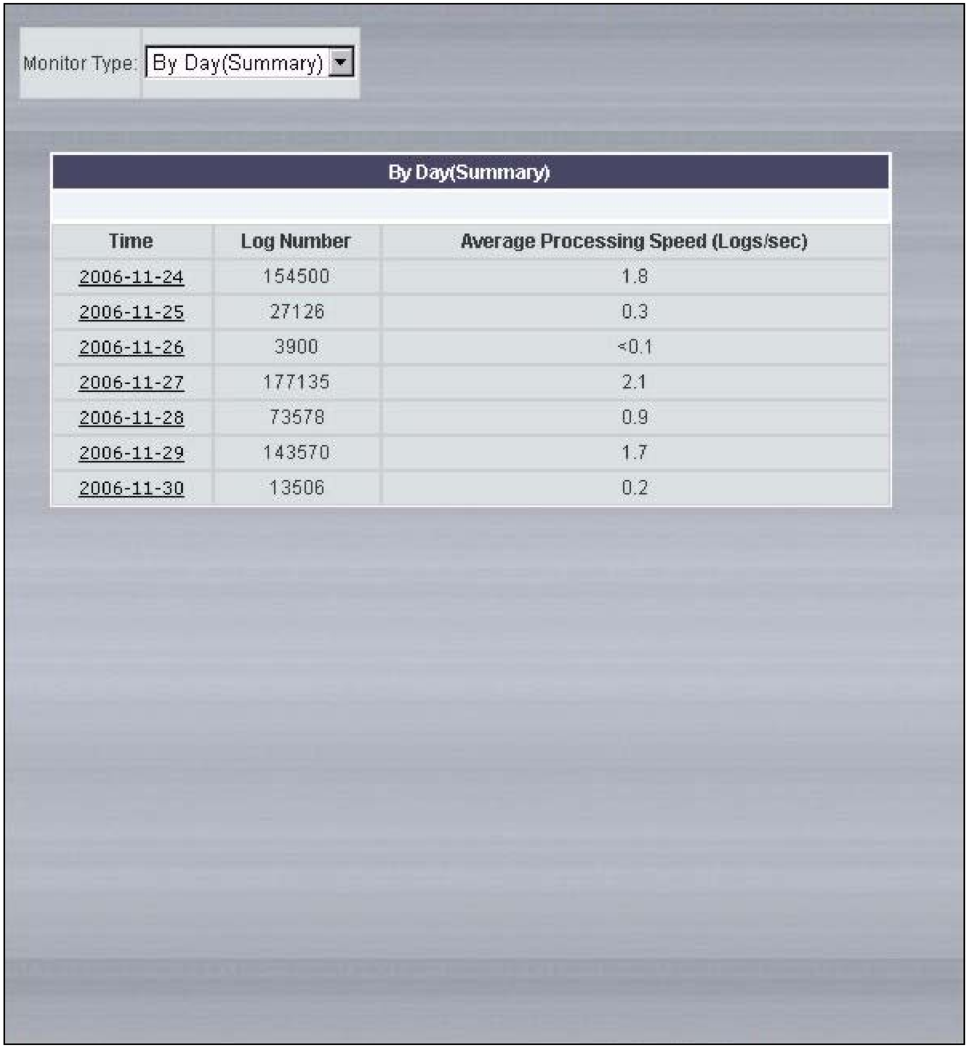
**Table 141** System > VRPT Management > General > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter a descriptive name of the Vantage Report instance in Vantage CNM. You must use 3-28 alphanumeric characters, underscores (_), dashes (-), or periods (.). |
| IP | Enter the IP address of the Vantage Report server. |
| Description | Type a description, if desired, for the Vantage Report instance. You can use up to 255 printable ASCII characters. |
| Managed Device List | Select the devices that are managed by the Vantage Report instance.<br>In the list on the left side, select the devices that are managed by the Vantage Report instance and click **>>**.<br>When you click **Apply**, Vantage CNM automatically configures these devices to send log messages to Vantage Report. It does not change any settings for log categories or traffic statistics, so you might have to change these manually. See Table 158 on page 339.<br>In the list on the right side, select the devices that are not managed by the Vantage Report instance and click **<<**. When you click **Apply**, Vantage CNM automatically resets the syslog settings to their default values for devices that previously used the specified Vantage Report server. It does not change any settings for log categories or traffic statistics. |
| Apply | Click **Apply** to save these changes. |
| Cancel | Click **Cancel** to return to the previous screen without saving changes. |

## 26.8.3 Log Receiver Monitor

Use this screen to look at the total number of logs that Vantage Report received by day or from each device. To open this screen, click **System > VRPT Management > General**, and then click **Receiver Monitor** next to the VRPT server whose reports you want to look at.

**Figure 168** System > VRPT Management > General > Receiver Monitor



Monitor Type: By Day(Summary)

By Day(Summary)

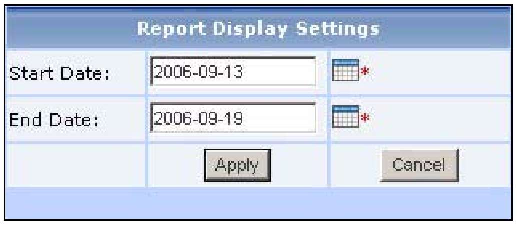
| Time | Log Number | Average Processing Speed (Logs/sec) |
|---|---|---|
| 2006-11-24 | 154500 | 1.8 |
| 2006-11-25 | 27126 | 0.3 |
| 2006-11-26 | 3900 | <0.1 |
| 2006-11-27 | 177135 | 2.1 |
| 2006-11-28 | 73578 | 0.9 |
| 2006-11-29 | 143570 | 1.7 |
| 2006-11-30 | 13506 | 0.2 |

The following table describes the labels in this screen.

**Table 142** System > VRPT Management > General > Receiver Monitor

| LABEL | DESCRIPTION |
|---|---|
| Monitor Type | Select whether you want to look at the total number of logs that Vantage Report received by day [**By Day(Summary)**] or from each device (**By Device**). |
| By Day(Summary) | These fields are displayed if **Monitor Type** is **By Day(Summary)**. |
| Time | This field displays the day for which the logs were collected. Click the date to go to a screen that lists how many logs were received from each device on that day. |
| Log Number | This field displays how many logs were received on each day. |

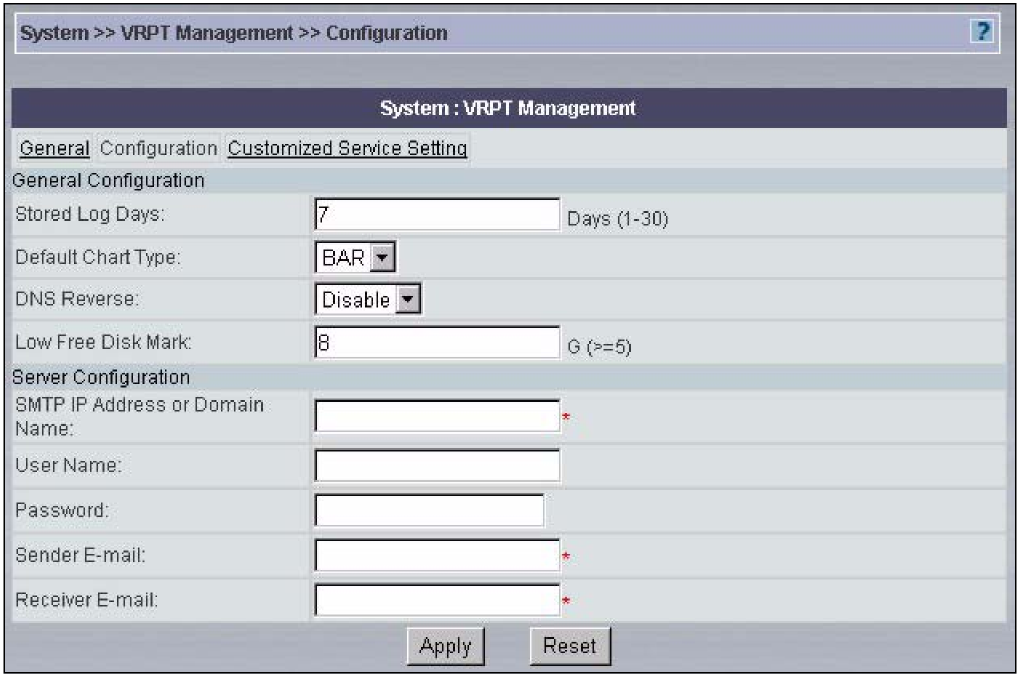
**Table 142** System > VRPT Management > General > Receiver Monitor (continued)

| LABEL | DESCRIPTION |
|---|---|
| Average Processing Speed (Logs/sec) | This field displays the average number of logs the Vantage Report server processed per second on each day. |
| By Device | These fields are displayed if **Monitor Type** is **By Device**. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use these fields to specify what historical information is included in the report. Click the settings icon. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2006-09-13 *<br>End Date: 2006-09-19 *<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System > General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes. |
| Device | This field displays the MAC addresses of the devices that sent logs on the days you selected. They are sorted by the number of logs from each. Click a device's MAC address to see details about the categories of logs that the device sent to Vantage Report on the selected days. |
| Log Number | This field displays how many logs Vantage Report received from each device. |
| % of Log Number | This field displays what percent of the selected time period's total logs came from each category. |

## 26.8.4 Configuration

Use this screen to maintain global reporting settings, such as how many days of logs to keep and default chart type, and to configure the mail server for Vantage Report. To open this screen, click **System > VRPT Management > Configuration**.

**Figure 169** System > VRPT Management > Configuration



System >> VRPT Management >> Configuration

System : VRPT Management

General Configuration

| | | |
|---|---|---|
| Stored Log Days: | 7 | Days (1-30) |
| Default Chart Type: | BAR | |
| DNS Reverse: | Disable | |
| Low Free Disk Mark: | 8 | G (>=5) |

Server Configuration

| | | |
|---|---|---|
| SMTP IP Address or Domain Name: | | * |
| User Name: | | |
| Password: | | |
| Sender E-mail: | | * |
| Receiver E-mail: | | * |

The following table describes the labels in this screen.

**Table 143** System > VRPT Management > Configuration

| LABEL | DESCRIPTION |
|---|---|
| General Configuration | |
| Stored Log Days | Enter the number of days that Vantage Report should keep logs and traffic information. Vantage Report automatically deletes logs and traffic information that are older than this. You cannot generate statistical reports or look at logs for information older than this. This affects scheduled reports too because they can only use whatever information is stored in Vantage Report. If you want scheduled reports to have a complete set of information, you should set this field accordingly.<br>When Vantage Report deletes data older than the time specified in this field, the raw data (raw logs) is exported as a CSV file (.csv) and compressed into a .zip file. These .zip files are stored in `<Vantage Report installation directory>\data\backup\csv`. |
| Default Chart Type | Select the default chart type in statistical report screens. |
| DNS Reverse | Select **Enable** if you want Vantage Report to do reverse DNS lookups in statistical reports. It has no effect in **Log Viewer**. In reverse DNS lookups, Vantage Report looks for the domain name associated with IP addresses that it displays. If Vantage Report finds the domain name, it displays the domain name and the IP address in the field. If it does not find the domain name, it only displays the IP address. This feature might increase the amount of time it takes to display statistical reports, however. |
| 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. |
| 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. |

**Table 143** System > VRPT Management > Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| User Name | Enter the user name for the Vantage Report account. If the user name is not required, leave this field blank. |
| Password | Enter the password for the Vantage Report account. If the password is not required, leave this field blank. |
| Sender E-mail | Enter the complete e-mail address for the Vantage Report account. |
| Receiver E-mail | Enter the e-mail address to which Vantage Report sends system notifications. See Section 30.2 on page 338 for more information about system notifications. |
| Apply | Click **Apply** to save these changes. |
| Reset | Click **Reset** to return to the values in this screen to their last-saved values. |

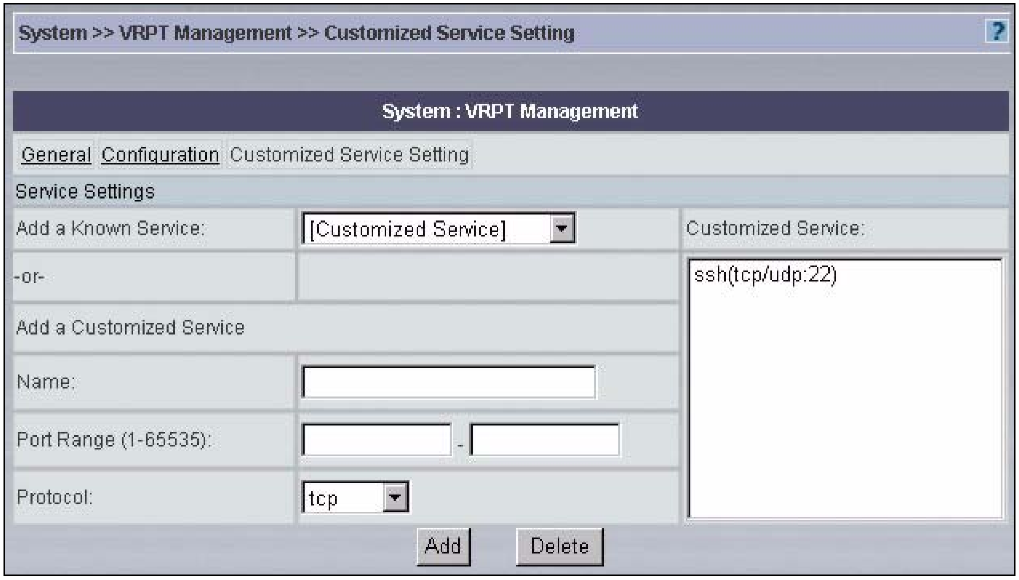
## 26.8.5 Customized Service Setting

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.

To open this screen, click **System > VRPT Management > Customized Service Setting**.

**Figure 170** System > VRPT Management > Customized Service Setting



The following table describes the labels in this screen.

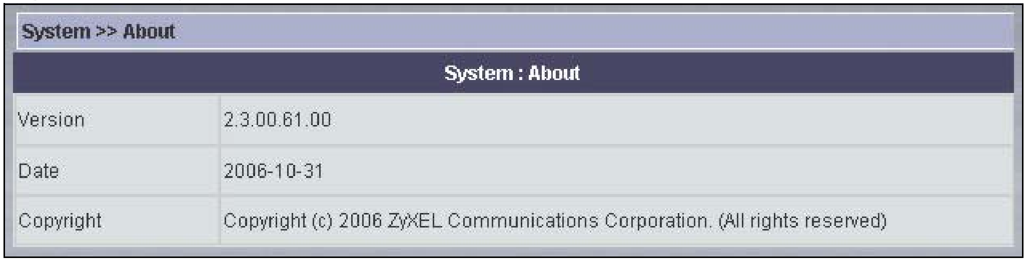
**Table 144** System > VRPT Management > Customized Service Setting

| LABEL | DESCRIPTION |
|---|---|
| Add a Known Service | Use this drop-down box to add a service to the **Customized Service** drop-down box.<br>Select a pre-defined service from the drop-down list box, and click the **Add** button; or<br>Select **[Customized Service]**, fill in the **Add a Customized Service** section, and click the **Add** button.<br>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.<br>To remove a service from the **Customized Service** drop-down box, click on the service in this list box, and click the **Delete** button.<br>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. |

## 26.9 About Vantage CNM

The **About** screen provides some basic information about Vantage CNM as shown in the following screen.

**Figure 171** System > About



System >> About

| System : About | |
|---|---|
| Version | 2.3.00.61.00 |
| Date | 2006-10-31 |
| Copyright | Copyright (c) 2006 ZyXEL Communications Corporation. (All rights reserved) |

# PART VI
# Monitor

# 27

# Monitor > Alarms

This chapter describes the monitor alarms.

## 27.1 Alarms

Alarms are time-critical information that the device automatically sends out at the time of occurrence. You may have administrators automatically e-mailed when an alarm occurs in the **System** > **Preferences** >**Notifications** screen. See Section 26.3.2 on page 291.

### 27.1.1 Alarm Types

There are three types of alarms.

**Table 145** Types of Alarms

| TYPE | DESCRIPTION |
|---|---|
| All | This displays all types of alarms. |
| Device | This is an alarm such as hardware failure or the network connection is down. |
| CNM | This is an alarm such as server communication error or illegal Vantage CNM login attempt. |

### 27.1.2 Alarm Classifications

There are four alarm severity classifications.

**Table 146** Alarm Severity

| SEVERITY | DESCRIPTION |
|---|---|
| All | This displays all alarm severities. |
| Fatal | This is an alarm such as unrecoverable hardware failure. |
| Major | This is an alarm such as an attack. |
| Minor | This is an alarm such as a recoverable hardware error. |
| Warning | This is an alarm such as an illegal Vantage CNM login attempt. |

## 27.1.3 Alarm States

When an alarm is received by Vantage CNM, it can be in one of three states:

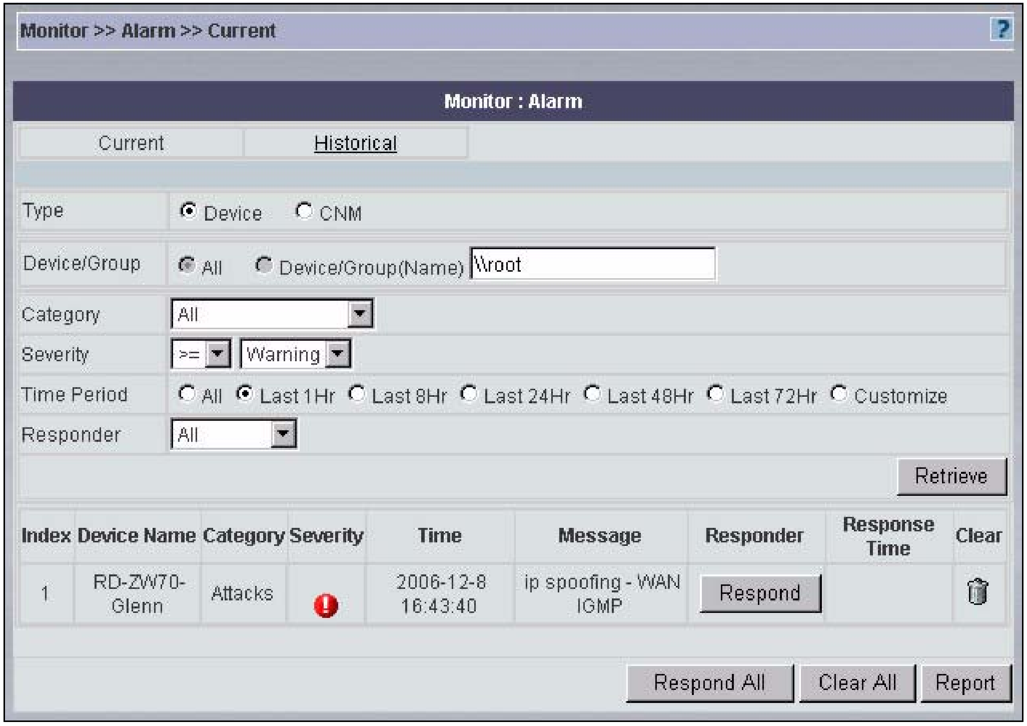
**Table 147** Alarm States

| STATE | DESCRIPTION |
|---|---|
| Active | This is the initial state of an alarm, which means this alarm is new and no one has assumed responsibility for handling it yet. |
| Acknowledged | This means that one administrator has decided to respond to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided. |
| Cleared | After the administrator has solved the cause of the alarm, he/she can clear the alarm. When an alarm is cleared, it is removed from the current alarm screen and becomes an historical alarm. |

## 27.1.4 Current Alarms

View recent alarms and who has taken care of or is taking care of them in this screen. An alarm becomes historical after selecting **Clear**.

**Figure 172** Monitor > Alarm > Current



Monitor >> Alarm >> Current

Monitor : Alarm

Current | Historical

Type ● Device ○ CNM

Device/Group ● All ○ Device/Group(Name) \\root

Category: All

Severity: >= Warning

Time Period ○ All ● Last 1Hr ○ Last 8Hr ○ Last 24Hr ○ Last 48Hr ○ Last 72Hr ○ Customize

Responder: All

Retrieve

| Index | Device Name | Category | Severity | Time | Message | Responder | Response Time | Clear |
|---|---|---|---|---|---|---|---|---|
| 1 | RD-ZW70-Glenn | Attacks | ! | 2006-12-8 16:43:40 | ip spoofing - WAN IGMP | Respond | | 🗑 |

Respond All | Clear All | Report

The following table describes the fields in this screen.

**Table 148** Monitor > Alarm > Current

| STATE | DESCRIPTION |
|---|---|
| Type | Select whether you want to look at device alarms (**Device**) or all alarms generated or received by Vantage CNM (**CNM**). |
| Device/Group | This field displays the selected device or folder. |
| Category | Select the type of alarm you wish to view. |

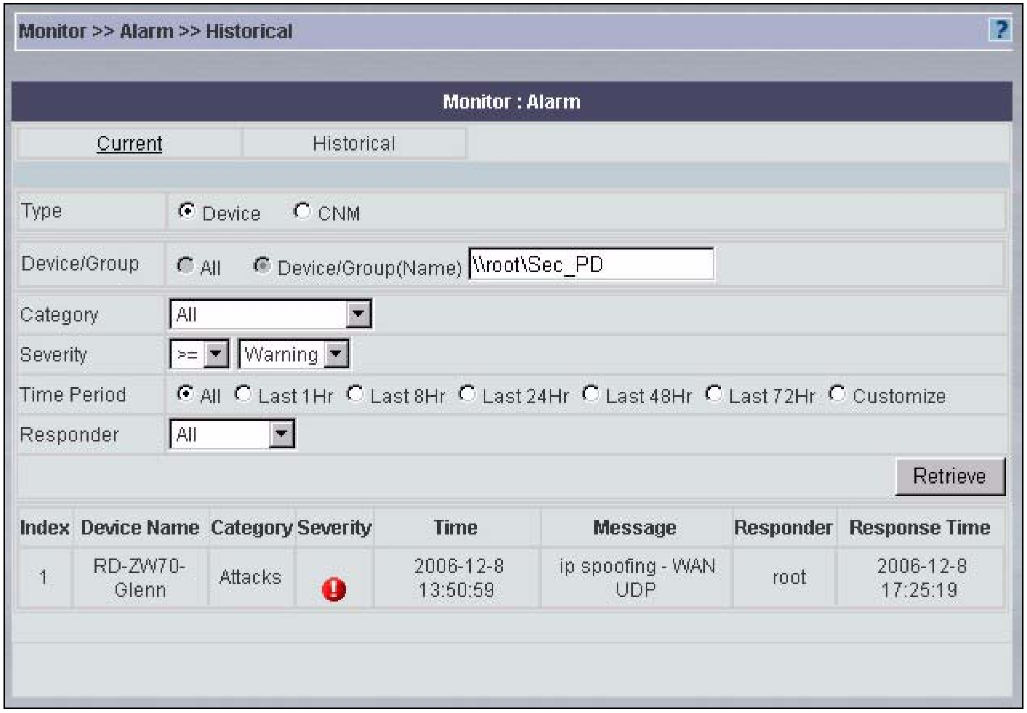
**Table 148** Monitor > Alarm > Current (continued)

| STATE | DESCRIPTION |
|---|---|
| Severity | Select the severity of alarm you wish to view. |
| Time Period | Select the time period for which you wish to view alarms. |
| Responder | Select alarms based on the administrator who is supposed to respond to them. |
| Retrieve | Click this to update the list of alarms based on the specified criteria. |
| Index | This field displays an alarm index number. |
| Device Name<br>Source | This field displays the name of the device or administrator that generated the alarm. |
| Category | This field displays the type of alarm. |
| Severity | This field displays the alarm severity. |
| Time | This field displays the time the alarm occurred. |
| Message | This field displays the reason the alarm occurred. |
| Responder | This field displays the administrator who responded to the alarm. If no administrator has responded, the **Respond** button is displayed. Click this to take responsibility for finding the cause of this alarm. |
| Response Time | This field displays the time the alarm occurred. |
| Clear | Click this to remove the alarm from the monitor. The alarm then appears in the **Monitor > Alarm > Historical** screen. See Section 27.1.5 on page 319. |
| Respond All | Click this to respond to all of the alarms in the list. |
| Clear All | Click this to remove all of the alarms in the list from the monitor. The alarms then appears in the **Monitor > Alarm > Historical** screen. See Section 27.1.5 on page 319. |
| Report | Click **Report** to generate a report on the alarms currently being viewed. |

## 27.1.5 Historical Alarms

Historical alarms are alarms that have been cleared by an administrator.

**Figure 173** Monitor > Historical Alarms



Monitor >> Alarm >> Historical

Monitor : Alarm

Current | Historical

| | |
|---|---|
| Type | ● Device ○ CNM |
| Device/Group | ○ All ● Device/Group(Name) \\root\Sec_PD |
| Category | All |
| Severity | >= Warning |
| Time Period | ● All ○ Last 1Hr ○ Last 8Hr ○ Last 24Hr ○ Last 48Hr ○ Last 72Hr ○ Customize |
| Responder | All |

Retrieve

| Index | Device Name | Category | Severity | Time | Message | Responder | Response Time |
|---|---|---|---|---|---|---|---|
| 1 | RD-ZW70-Glenn | Attacks | ! | 2006-12-8 13:50:59 | ip spoofing - WAN UDP | root | 2006-12-8 17:25:19 |

See Table 148 on page 318 for more information on fields in this table.

# 28

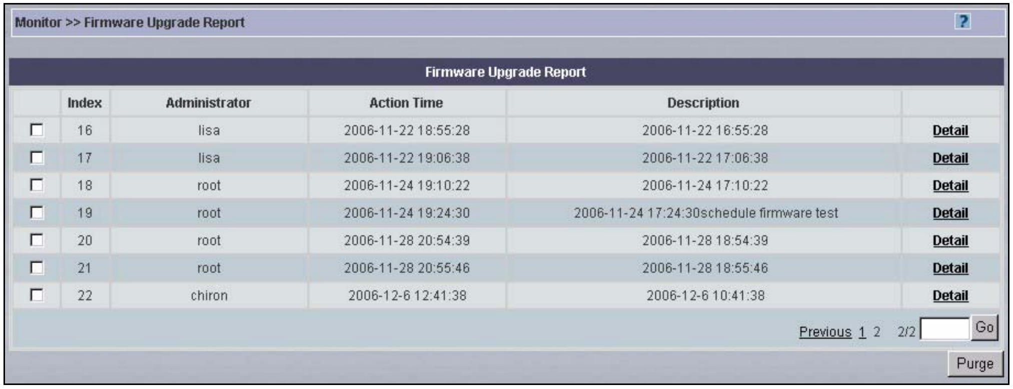
# Other Monitor Screens

Firmware Upgrade means that Vantage CNM signals the device to request a firmware FTP upload from Vantage CNM.

## 28.1 Firmware Report

This report shows a summary of firmware upgrades. See Section 3.6 on page 67. To open this report, click **Monitor > Firmware Report**.

**Figure 174** Monitor > Firmware Report



Monitor >> Firmware Upgrade Report

Firmware Upgrade Report

| | Index | Administrator | Action Time | Description | |
|---|---|---|---|---|---|
| □ | 16 | lisa | 2006-11-22 18:55:28 | 2006-11-22 16:55:28 | Detail |
| □ | 17 | lisa | 2006-11-22 19:06:38 | 2006-11-22 17:06:38 | Detail |
| □ | 18 | root | 2006-11-24 19:10:22 | 2006-11-24 17:10:22 | Detail |
| □ | 19 | root | 2006-11-24 19:24:30 | 2006-11-24 17:24:30schedule firmware test | Detail |
| □ | 20 | root | 2006-11-28 20:54:39 | 2006-11-28 18:54:39 | Detail |
| □ | 21 | root | 2006-11-28 20:55:46 | 2006-11-28 18:55:46 | Detail |
| □ | 22 | chiron | 2006-12-6 12:41:38 | 2006-12-6 10:41:38 | Detail |

The following table describes the labels in this screen.

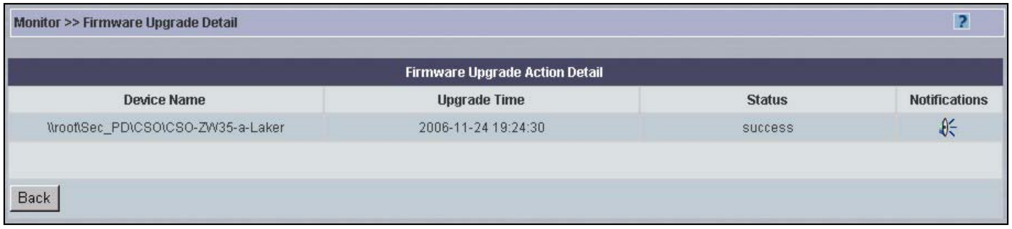
**Table 149** Monitor > Firmware Report

| LABEL | DESCRIPTION |
|---|---|
| Index | This is the upgrade list number. |
| Administrator | This displays the administrator who performed the upgrade. |
| Action Time | This displays the time at which the upgrade was performed. |
| Description | This displays the time at which the upgrade was requested and any description provided when the upgrade was scheduled. |
| Detail | Click this to look at more information about the request. |
| Purge | Select **Purge** to delete selected reports from the Vantage CNM server. |

### 28.1.1 Firmware Report Details

This report shows more information about a firmware upgrade. See Section 3.6 on page 67. To open this report, click **Monitor > Firmware Report > Detail**.

**Figure 175** Monitor > Firmware Report > Detail



Monitor >> Firmware Upgrade Detail

Firmware Upgrade Action Detail

| Device Name | Upgrade Time | Status | Notifications |
|---|---|---|---|
| \\root\Sec_PD\CSO\CSO-ZW35-a-Laker | 2006-11-24 19:24:30 | success | |

The following table describes the labels in this screen.

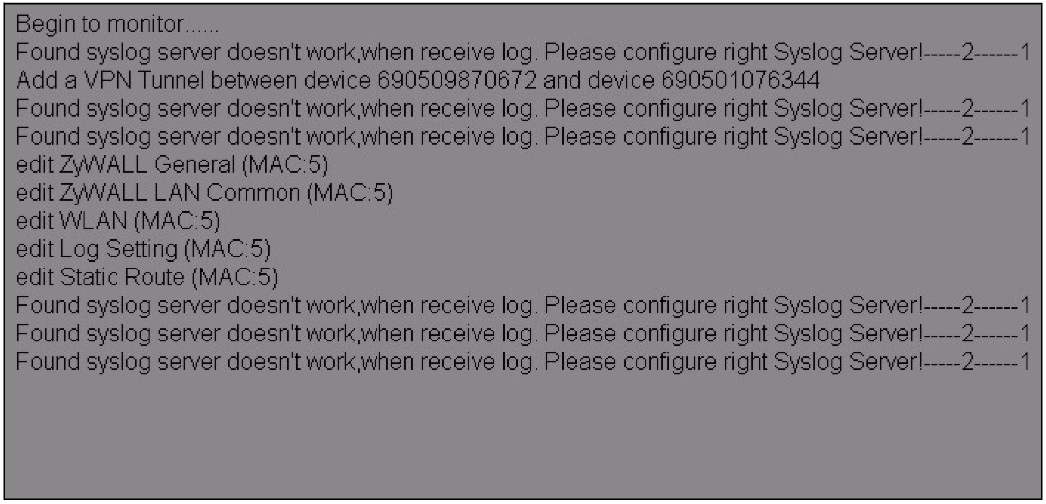
**Table 150** Monitor > Firmware Report > Detail

| LABEL | DESCRIPTION |
|---|---|
| Device Name | This field displays the name of each device that was upgraded. |
| Upgrade Time | This field displays the time at which the upgrade was performed. |
| Status | This field displays whether the upgrade was successful, failed, or timed out. |
| Notifications | Click this to send a notification to one or more administrators. A pop-up window appears to let you select the administrators. |
| Back | Click this to return to the previous screen. |

## 28.2 Status Monitor

This is a real-time message monitor that displays messages such as urgent alerts and when an administrator has logged in or logged out. Click **Monitor > Status Monitor** and wait for Vantage CNM to retrieve information and display it. Click it again to remove the monitor.

**Figure 176** Monitor > Status Monitor



```
Begin to monitor......
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Add a VPN Tunnel between device 690509870672 and device 690501076344
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
edit ZyWALL General (MAC:5)
edit ZyWALL LAN Common (MAC:5)
edit WLAN (MAC:5)
edit Log Setting (MAC:5)
edit Static Route (MAC:5)
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
```

## 28.3 VPN Editor

This is a graphical VPN editor screen where you can click and drag VPN tunnels (single-click VPN) and also view individual tunnel details.

The following table lists the icons that are used in the **Monitor** > **VPN Editor** screens.

Table 151 VPN Editor Icons

| ICON | DESCRIPTION |
|---|---|
| Edit | Edit the selected tunnel. |
| Delete | Delete the selected tunnel. |
| Save | Save a devices topology. |
| Force | Force delete the selected tunnel. |
| Refresh | Refresh the VPN monitor. |
| | A device that is turned on. |
| | A device that is turned off. |

## 28.3.1 One-Click VPN

Configure IPSec tunnels graphically in just one click.

1 Drag the device icons around the screen as you please (the icons are on top of each other in the top left corner of the screen in the beginning. Drag them apart to view each of them). Save this view by clicking **Save**.

2 Right-click a (local) device and select **VPN** in the popup menu. Click the device again and drag (you should see a red line) to another (remote) device, then release the mouse button.

3 You see the **Tunnel IPSec Detail** screen as shown next. Note that information in some fields has been automatically generated for you when you configure VPN this way. See Section 12.2.1 on page 166 for information on configuring this screen. At minimum, you must fill in the fields with the red asterisks. You can accept (or change) the automatically configured information in the other fields to set up the tunnel.

4 Click **Apply** to go to a tunnel summary screen.

The Tunnel Summary details are added to the top of the IPSec Summary, Figure 177 on page 324, in the order they are configured (last tunnel appears last in the list).

## 28.3.2 Tunnel Graphical Depictions

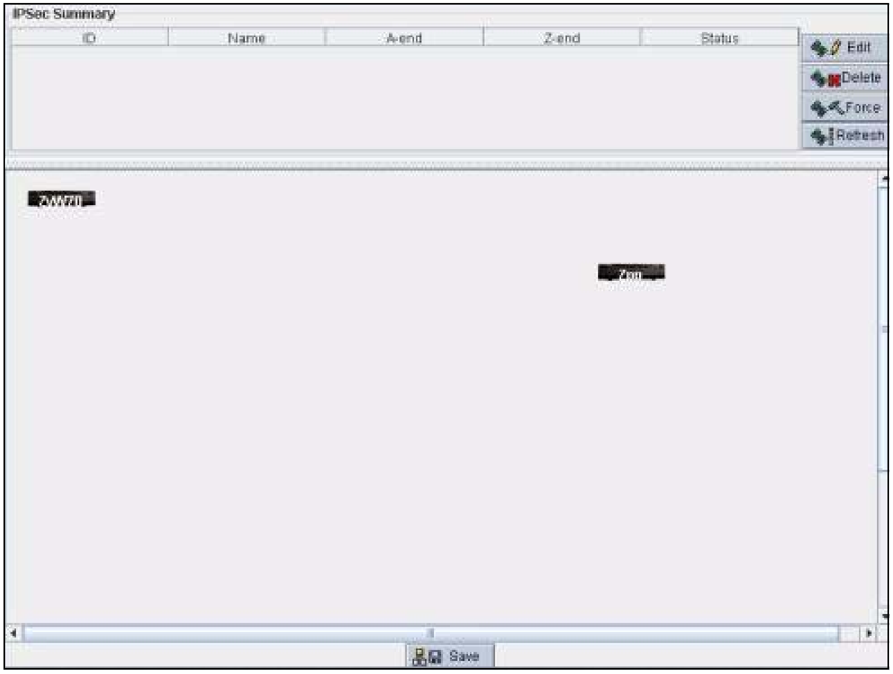
A gray dashed line means that the Vantage CNM server has not yet synchronized VPN tunnel information with both devices. This may be because Vantage CNM has not so far communicated with one of the devices.

A gray solid line means that the VPN tunnel is set up between the devices but the tunnel is not active yet (no traffic).

A green solid line means an active tunnel (with traffic) between the devices.

The icons are dragged apart and dashed lines indicating VPN Tunnels are created after configuring the **Tunnel IPSec Detail** screen.

**Figure 177** Monitor > VPN Monitor – Tunnel Graphics



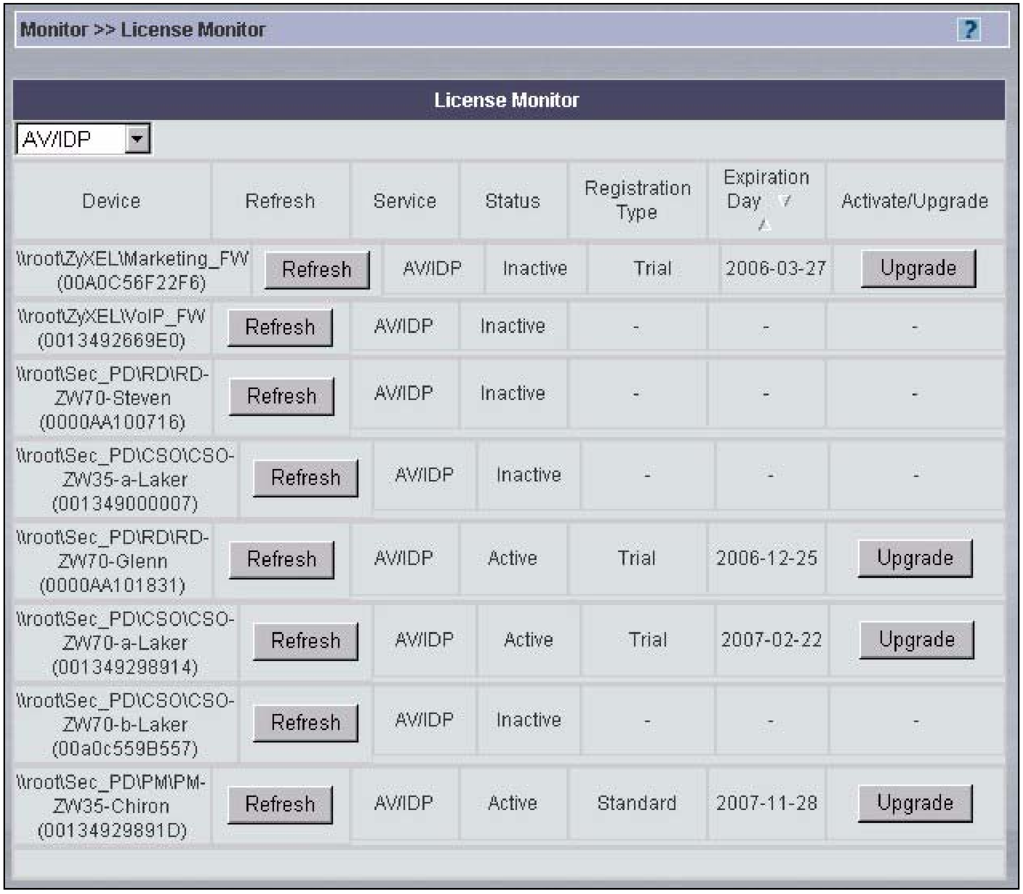
IPSec Summary

| ID | Name | A-end | Z-end | Status |
|---|---|---|---|---|

## 28.4 License Monitor

Use this screen to look at the current status of licenses for subscription services, such as IDP and content filtering. To open this screen, click **Monitor > License Monitor**.

**Figure 178** Monitor > License Monitor



Monitor >> License Monitor

License Monitor

AV/IDP

| Device | Refresh | Service | Status | Registration Type | Expiration Day | Activate/Upgrade |
|---|---|---|---|---|---|---|
| \\root\ZyXEL\Marketing_FW (00A0C56F22F6) | Refresh | AV/IDP | Inactive | Trial | 2006-03-27 | Upgrade |
| \\root\ZyXEL\VoIP_FW (0013492669E0) | Refresh | AV/IDP | Inactive | - | - | - |
| \\root\Sec_PD\RD\RD-ZW70-Steven (0000AA100716) | Refresh | AV/IDP | Inactive | - | - | - |
| \\root\Sec_PD\CSO\CSO-ZW35-a-Laker (001349000007) | Refresh | AV/IDP | Inactive | - | - | - |
| \\root\Sec_PD\RD\RD-ZW70-Glenn (0000AA101831) | Refresh | AV/IDP | Active | Trial | 2006-12-25 | Upgrade |
| \\root\Sec_PD\CSO\CSO-ZW70-a-Laker (001349298914) | Refresh | AV/IDP | Active | Trial | 2007-02-22 | Upgrade |
| \\root\Sec_PD\CSO\CSO-ZW70-b-Laker (00a0c559B557) | Refresh | AV/IDP | Inactive | - | - | - |
| \\root\Sec_PD\PM\PM-ZW35-Chiron (00134929891D) | Refresh | AV/IDP | Active | Standard | 2007-11-28 | Upgrade |

The following table describes the labels in this screen.

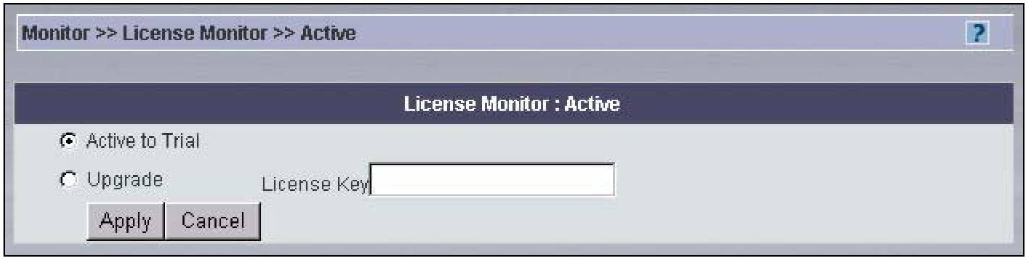
**Table 152** Monitor > License Monitor

| LABEL | DESCRIPTION |
|---|---|
| | Select the subscription service whose licensing status you want to view. |
| Device | This field displays the name (and location in Vantage CNM) of the device. |
| Refresh | Click this to update the license status of the selected service(s) for the device. |
| Service | This field displays the name of the selected service(s). |
| Status | This field displays the current status of the license for this service on this device.<br>**Active**: The service is currently available on the device.<br>**Inactive**: The service is not available (or has expired) on the device. |
| Registration Type | This field displays the type of license that is currently on the device. This is based on the last license that was set up on the device. For example, if you start with a trial version and upgrade to a standard license, this field shows the standard license. |
| Expiration Day | This field displays the date the subscription is scheduled to expire or already expired on the device. |
| Activate/Upgrade | Click **Activate** to activate a trial version of the service or to apply a license for the service to the device.<br>Click **Upgrade** to apply a license for the service to the device. |

### 28.4.1 Activate/Upgrade License

Use this screen to activate a trial version of the service, if available, or to apply a license for the service to the device. To open this screen, click **Monitor** > **License Monitor** > **Activate/ Upgrade**.

**Figure 179** Monitor > License Monitor > Activate/Upgrade



Monitor >> License Monitor >> Active

License Monitor : Active

● Active to Trial

○ Upgrade License Key

The following table describes the labels in this screen.

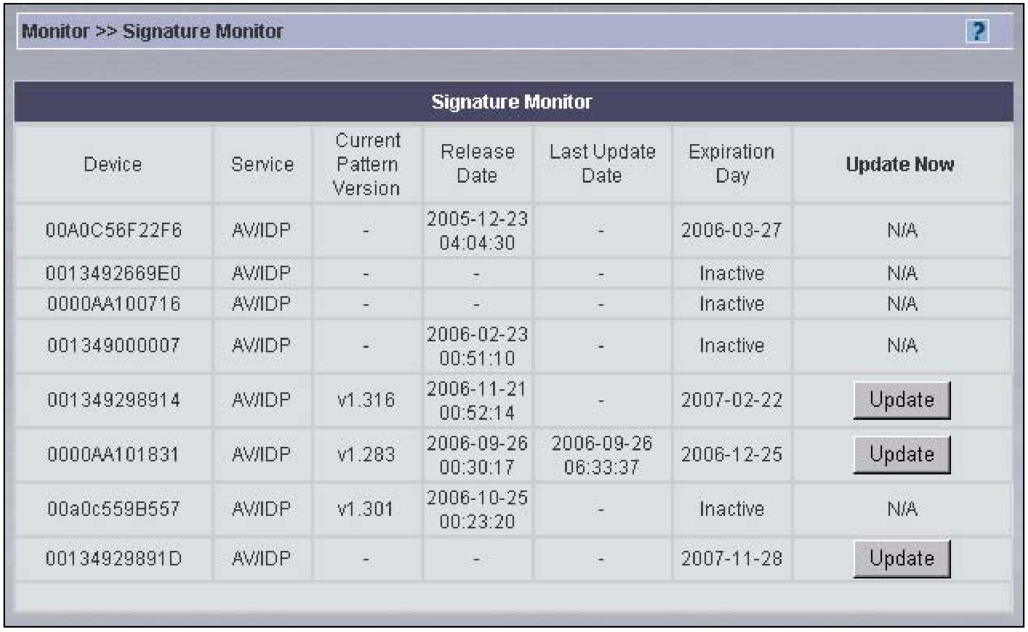
**Table 153** Monitor > License Monitor > Activate/Upgrade

| LABEL | DESCRIPTION |
|---|---|
| Active to Trial | This field is available if a trial version of the service is available for the device.<br>Select this and click **Apply** to activate a trial version of the service for the device. |
| Upgrade | Select this if you want to apply a license for the service to the device. |
| License Key | Enter your iCard's PIN number. If a standard service subscription runs out, you need to buy a new iCard (specific to your device) and enter the new PIN number to extend the service. |
| Apply | Click this to activate the trial version or apply the specified license to the device. |
| Cancel | Click this to return to the previous screen without making any changes. |

## 28.5 Signature Monitor

Use this screen to look at the current status of signatures for subscription services, such as IDP and anti-virus. To open this screen, click **Monitor** > **Signature Monitor**.

**Figure 180** Monitor > Signature Monitor



Monitor >> Signature Monitor

Signature Monitor

| Device | Service | Current Pattern Version | Release Date | Last Update Date | Expiration Day | Update Now |
|---|---|---|---|---|---|---|
| 00A0C56F22F6 | AV/IDP | - | 2005-12-23 04:04:30 | - | 2006-03-27 | N/A |
| 0013492669E0 | AV/IDP | - | - | - | Inactive | N/A |
| 0000AA100716 | AV/IDP | - | - | - | Inactive | N/A |
| 001349000007 | AV/IDP | - | 2006-02-23 00:51:10 | - | Inactive | N/A |
| 001349298914 | AV/IDP | v1.316 | 2006-11-21 00:52:14 | - | 2007-02-22 | Update |
| 0000AA101831 | AV/IDP | v1.283 | 2006-09-26 00:30:17 | 2006-09-26 06:33:37 | 2006-12-25 | Update |
| 00a0c559B557 | AV/IDP | v1.301 | 2006-10-25 00:23:20 | - | Inactive | N/A |
| 00134929891D | AV/IDP | - | - | - | 2007-11-28 | Update |

The following table describes the labels in this screen.

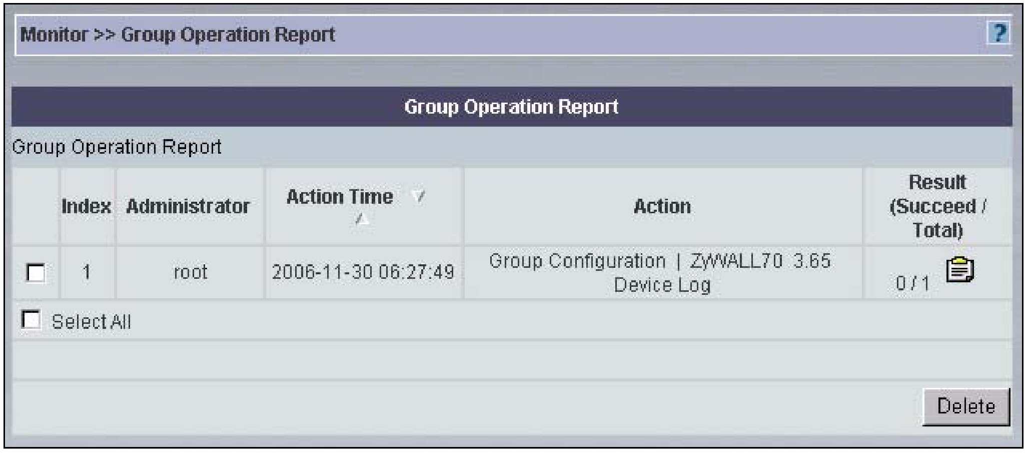
**Table 154** Monitor > Signature Monitor

| LABEL | DESCRIPTION |
|---|---|
| Device | This field displays the MAC address of the device. |
| Service | This field displays the name of the selected service(s). |
| Current Pattern Version | This field displays the signatures version number currently used by the device. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them.<br>This number increments as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications. |
| Release Date | This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created. |
| Last Update Date | This field displays the last date and time you downloaded new signatures to the device. |
| Expiration Day | This field displays the date the subscription is scheduled to expire. It displays **Inactive** if the service is not available on the device or has expired. |
| Update Now | Click this to begin downloading signatures immediately. |

## 28.6 Group Operation Report

Use this screen to look at a record of group configuration done using the **Group Config** menu item or the **Device > Signature Profile** menu item. See Section 2.1.2.8 on page 44 and Section 3.9 on page 77 for more information about these functions, respectively. To open this screen, click **Monitor > Group Operation Report**.

**Figure 181** Monitor > Group Operation Report



Monitor >> Group Operation Report

Group Operation Report

Group Operation Report

| | Index | Administrator | Action Time | Action | Result (Succeed / Total) |
|---|---|---|---|---|---|
| □ | 1 | root | 2006-11-30 06:27:49 | Group Configuration \| ZyWALL70 3.65 Device Log | 0 / 1 |

□ Select All

Delete

The following table describes the labels in this screen.

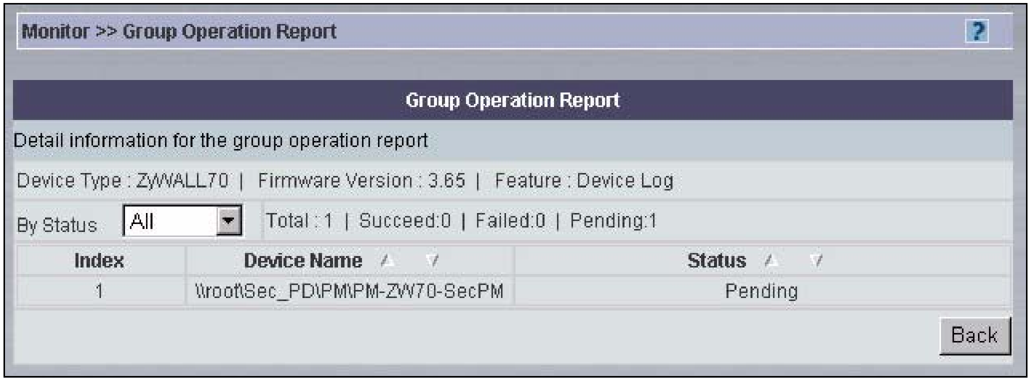
**Table 155** Monitor > Group Operation Report

| LABEL | DESCRIPTION |
|---|---|
| Index | This field displays an index number for the operation. |
| Administrator | This field displays the name of the administrator who performed the operation. |
| Action Time | This field displays the date and time the operation was requested. |
| Action | This field describes the operation. The information in the field depends on what type of operation was requested.<br>If the operation is a **Group Configuration**, this field displays the type of device, the firmware version, and the feature that is affected.<br>If the operation is a **Group Signature Restore**, this field identifies the set of signatures that is restored. |
| Result (Succeed / Total) | This field displays the number of devices on which the operation has been completed and the total number of devices to which the operation is supposed to be applied. Click **Details** to look at the detailed status of the operation. |
| Select All | Select this to select all of the operations in the report. |
| Delete | Click this to remove the selected operations from the report. This does not affect the operation itself. If the operation has not completed (or even started) on some devices, Vantage CNM tries to finish the operation anyway. The operation itself does not appear on the report anymore. |

## 28.6.1 Group Operation Details

Use this screen to look at the detailed status of a group operation. To open this screen, click **Monitor > Group Operation Report**, and then click the **Details** button next to the operation.

**Figure 182** Monitor > Group Operation Report > Details



Monitor >> Group Operation Report

Group Operation Report

Detail information for the group operation report

Device Type : ZyWALL70 | Firmware Version : 3.65 | Feature : Device Log

By Status: All | Total : 1 | Succeed:0 | Failed:0 | Pending:1

| Index | Device Name | Status |
|---|---|---|
| 1 | \\root\Sec_PD\PM\PM-ZW70-SecPM | Pending |

The following table describes the labels in this screen.

**Table 156** Monitor > Group Operation Report > Details

| LABEL | DESCRIPTION |
|---|---|
| Device Type | This field displays the model type of the device(s) to which the operation is applied. |
| Firmware Version | This field displays the firmware version of the device(s) to which the operation is applied. |
| Feature | This field displays the settings that are affected by the operation. |
| By Status | Select which devices you want to view in this report. |
| Total | This field displays the total number of devices to which the operation is applied. |
| Succeed | This field displays the total number of devices to which the operation was applied successfully. |
| Fail | This field displays the total number of devices to which the operation was not applied successfully. |
| Pending | This field displays the total number of devices to which the operation has not yet been applied. |
| Index | This field displays an index number for each device to which the operation is applied. |
| Device Name | This field displays the name (and location in Vantage CNM) of the device. |
| Status | This field displays the current status of the operation on the device. This corresponds to the **Succeed**, **Fail**, and **Pending** fields. |
| Back | Click this to return to the previous screen. |

# PART VII
# Vantage Report

# 29

# Report

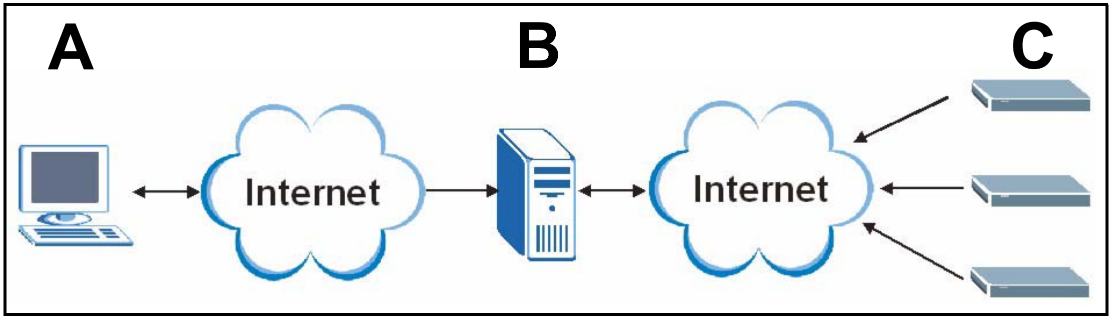
The **Report** menu activates Vantage Report. This chapter introduces Vantage Report and its role in Vantage CNM. Then, it explains how to set up and start Vantage Report.

## 29.1 Vantage Report Overview

This section introduces the standalone version of Vantage Report. See Section 29.2 on page 334 for more information about Vantage Report in Vantage CNM.

Vantage Report allows an administrator in any location to easily manage, monitor and gather statistics on devices located worldwide. With Vantage Report, you can monitor network access, enhance security, and anticipate future bandwidth needs. A typical application is illustrated in the following figure.

**Figure 183** Typical Vantage Report Application



In this example, you use the Vantage Report web configurator (**A**) to set up the Vantage Report server (**B**). You also configure the 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

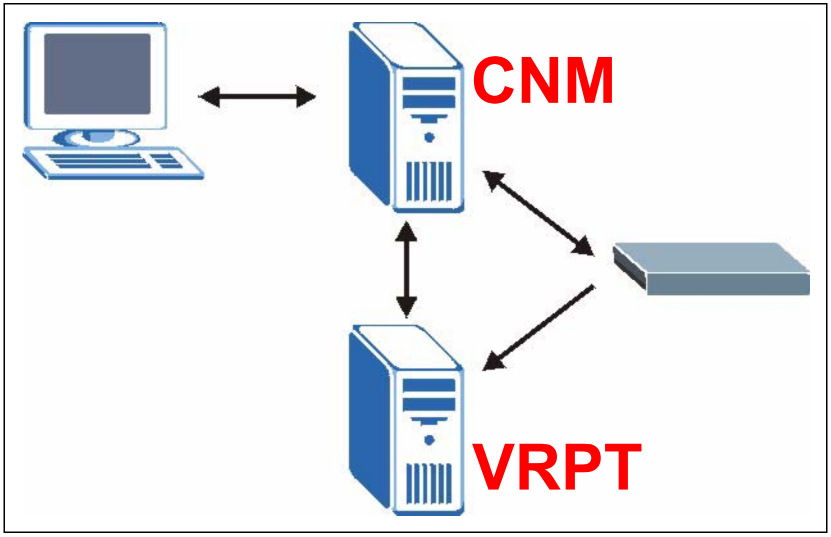
The Vantage Report server can also send statistical reports to you by e-mail.

## 29.2 Vantage Report in Vantage CNM

Vantage Report in Vantage CNM is a special release for Vantage CNM only. No additional license is required to use it. Vantage Report in Vantage CNM generally supports the capabilities available in the professional version of standalone Vantage Report, including drill-down reports, reverse DNS lookup, web usage by category, anti-virus, anti-spam, and HTML reports by e-mail. See Appendix A on page 515 for additional specifications.

Vantage Report in Vantage CNM does not have a separate web interface, so you have to use Vantage CNM to configure Vantage Report and to look at reports. This is illustrated below.

**Figure 184** Vantage Report and Vantage CNM Architecture



The Vantage Report server can be installed on the same machine as Vantage CNM or on a different machine. You can also set up multiple instances of Vantage Report in one instance of Vantage CNM (not shown in Figure 184 on page 334), but every instance of Vantage Report shares the same global configuration, SMTP settings, and list of customized services in Vantage CNM.

## 29.3 Setting Up Vantage Report in Vantage CNM

Follow these steps to set up each instance of Vantage Report and the devices that use it.

1 Install the Vantage Report server on a Windows or Linux system. The Vantage Report software for Vantage CNM is on the same CD as the Vantage CNM software.

2 Click **System** > **VRPT Management** > **General** > **Add**. Configure the Vantage Report instance in Vantage CNM, and select the devices that should send log messages to the Vantage Report instance.

When you click **Apply**, Vantage CNM automatically configures the selected devices to send log messages to the specified Vantage Report instance. It does not change any settings for log categories or traffic statistics.

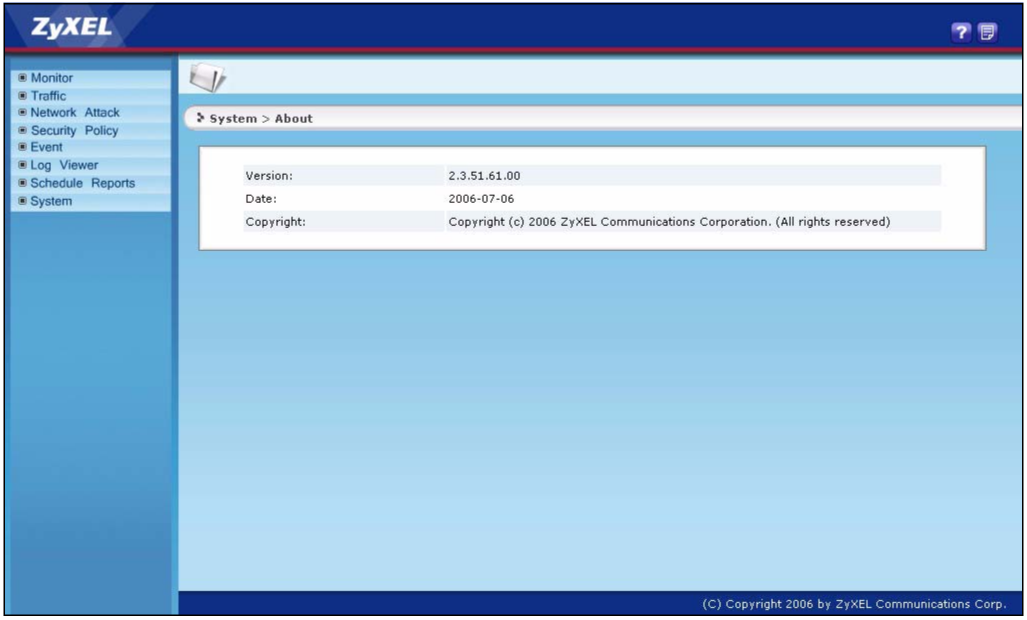
3 Click **Configuration** > **Device Log** for each device. Make sure the desired log categories are selected and that traffic statistics are sent to the Vantage Report server. See Table 158 on page 339 for more information.

## 29.4 Opening Vantage Report in Vantage CNM

Once you have set up Vantage Report in Vantage CNM (see Section 29.3 on page 334), select a device that is managed by Vantage Report, and click **Report > Report**.

Vantage Report opens in a new browser window.

**Figure 185** Report > Report (Vantage Report Main Screen)

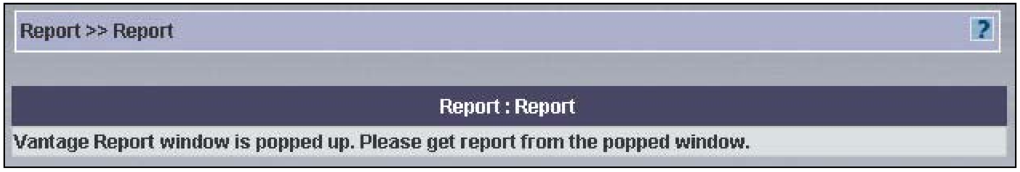


| | |
|---|---|
| Version: | 2.3.51.61.00 |
| Date: | 2006-07-06 |
| Copyright: | Copyright (c) 2006 ZyXEL Communications Corporation. (All rights reserved) |

(C) Copyright 2006 by ZyXEL Communications Corp.

The main window in Vantage CNM displays the following screen.

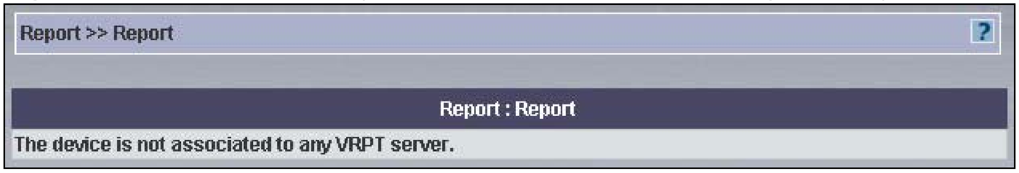
**Figure 186** Report > Report (Vantage CNM Screen)



Vantage Report window is popped up. Please get report from the popped window.

If the device is not managed by any Vantage Report instance yet, the Vantage Report window does not open, and the following screen appears.

**Figure 187** Report > Report (Device Not Associated with Vantage Report)



The device is not associated to any VRPT server.

30

# The Vantage Report Server

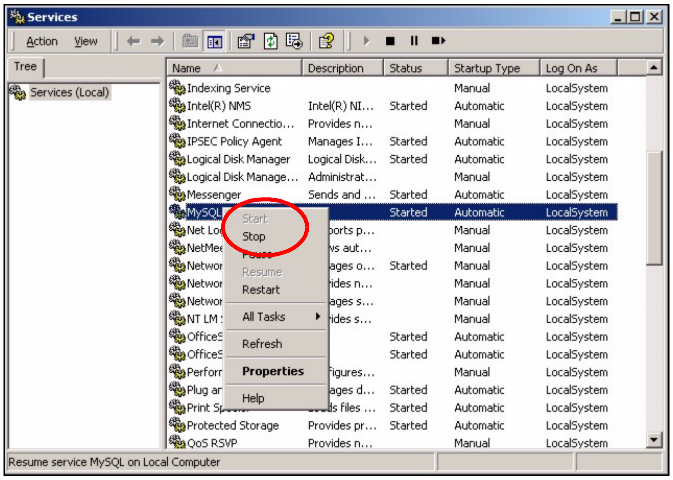
This chapter explains several characteristics of the Vantage Report server.

## 30.1 Starting and Stopping the Vantage Report Server

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

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

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



| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Indexing Service | | | Manual | LocalSystem |
| Intel(R) NMS | Intel(R) NI... | Started | Automatic | LocalSystem |
| Internet Connectio... | Provides n... | | Manual | LocalSystem |
| IPSEC Policy Agent | Manages I... | Started | Automatic | LocalSystem |
| Logical Disk Manager | Logical Disk... | Started | Automatic | LocalSystem |
| Logical Disk Manage... | Administrat... | | Manual | LocalSystem |
| Messenger | Sends and ... | Started | Automatic | LocalSystem |
| MySQL | | Started | Automatic | LocalSystem |
| Net Lo | ports p... | | Manual | LocalSystem |
| NetMee | ws aut... | | Manual | LocalSystem |
| Networ | ages o... | Started | Manual | LocalSystem |
| Networ | ides n... | | Manual | LocalSystem |
| Networ | ages s... | | Manual | LocalSystem |
| NT LM | ides s... | | Manual | LocalSystem |
| OfficeS | | Started | Automatic | LocalSystem |
| OfficeS | | Started | Automatic | LocalSystem |
| Perforr | figures... | | Manual | LocalSystem |
| Plug ar | ages d... | Started | Automatic | LocalSystem |
| Print Sp | ds files ... | Started | Automatic | LocalSystem |
| Protected Storage | Provides pr... | Started | Automatic | LocalSystem |
| QoS RSVP | Provides n... | | Manual | LocalSystem |

Resume service MySQL on Local Computer

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

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

## 30.2 E-mail in the Vantage Report Server

Before the Vantage Report server can send e-mail to anyone, you have to configure the SMTP mail server. See Section 26.8.4 on page 310 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 a specific e-mail address; 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 38 on page 497 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 **Receiver E-mail** field in the **System** > **VRPT Management** > **Configuration** screen. (See Section 26.8.4 on page 310.) Some of these messages are warnings; in some situations, however, the Vantage Report server starts or stops receive logs. See Appendix  on page 515 for a list of parameters and threshold values. One of the threshold values can be configured. See Section 26.8.4 on page 310.

## 30.3 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 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 157** Processing Times by Menu Item

| MENU ITEM | TIME (MIN) |
|---|---|
| Monitor | 5 |
| Traffic, Network Attack, Security Policy, Event | 5 |
| Log Viewer | 30 |

## 30.4 ZyXEL Device Configuration and Source Data

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

**Table 158** Configuration Requirements for ZyXEL Devices by Menu Item

| MENU ITEM(S) | SOURCE DATA | LOG SETTINGS* | ADDITIONAL |
|---|---|---|---|
| Monitor > Bandwidth | traffic statistics | -- | -- |
| Monitor > Service | traffic statistics | -- | -- |
| Monitor > Attack | log entries | Attack | -- |
| Monitor > Intrusion | log entries | IDP | IDP > Signature |
| Monitor > AntiVirus | log entries | Anti-Virus | Anti-Virus > General |
| Monitor > AntiSpam | log entries | Anti-Spam | -- |
| Traffic (except VPN) | traffic statistics | -- | -- |
| Traffic > VPN | log entries | IPSec | -- |
| Network Attack > Attack | log entries | Attack | -- |
| Network Attack > Intrusion | log entries | IDP | IDP > Signature |
| Network Attack > AntiVirus | log entries | Anti-Virus | Anti-Virus > General |
| Network Attack > AntiSpam | log entries | Anti-Spam | -- |
| Security Policy > WEB Blocked | log entries | Blocked Web Sites | -- |
| Security Policy > WEB Allowed | log entries | Forward Web Sites | -- |
| Event > Device Login | log entries | System Maintenance | -- |
| Log Viewer | 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 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 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 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 devices, it is possible to control what attack types are logged.

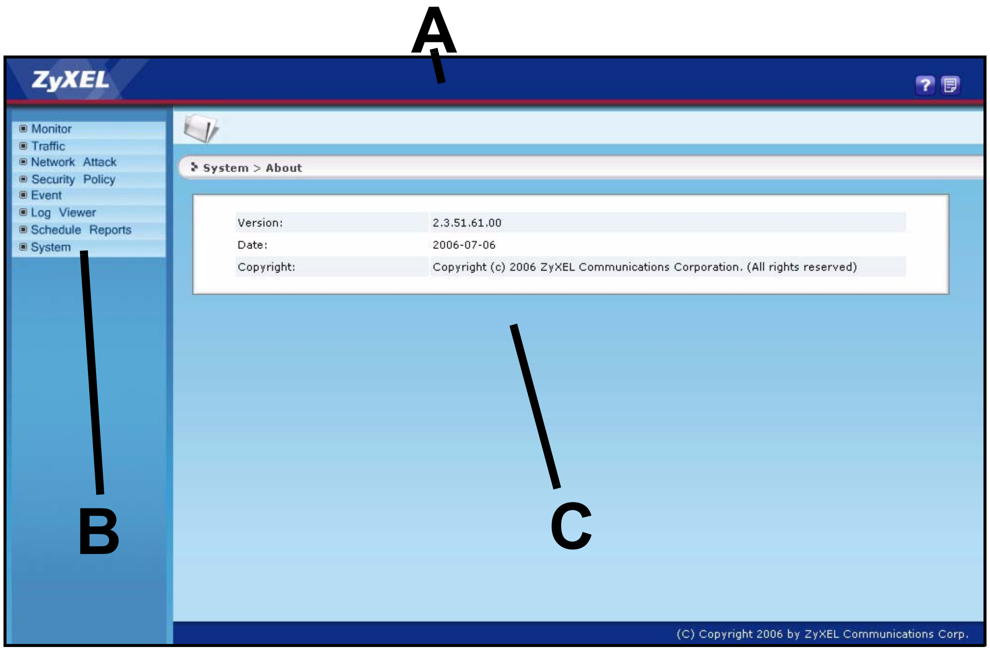
  For most devices, go to the screen indicated to select the appropriate log entries. You may also use the command-line interface.

# 31

# The Main Screen

This chapter explains each part of the main screen.

**Figure 188** Vantage Report Main Screen



System > About

|  |  |
|---|---|
| Version: | 2.3.51.61.00 |
| Date: | 2006-07-06 |
| Copyright: | Copyright (c) 2006 ZyXEL Communications Corporation. (All rights reserved) |

(C) Copyright 2006 by ZyXEL Communications Corp.

The main screen is divided into three parts: the title bar (**A**), the function window (**B**), and the report window (**C**). The title bar provides some icons that are useful anytime. The function window lists the reports you can generate and organizes these reports into categories. The report window shows the selected report for the selected device.

For security reasons, Vantage Report automatically times out when Vantage CNM times out.

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

## 31.1 Title Bar

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

**Table 159** Title Bar

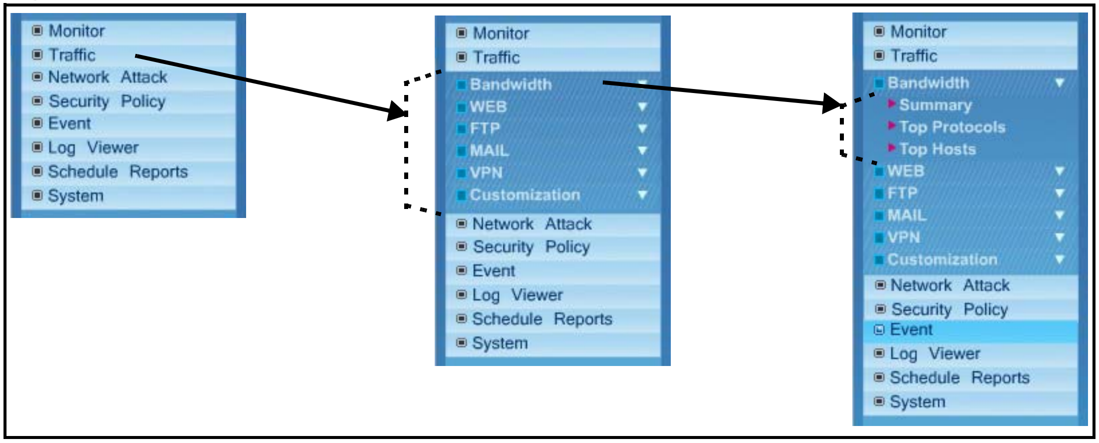
| ICON | DESCRIPTION |
|---|---|
| ? | This icon opens the help page for the current screen in Vantage Report. |
| ▤ | This icon provides the version of Vantage Report. |

## 31.2 Function Window

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

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 189.

**Figure 189** Function Window



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

Table 160 expands the function window and introduces each monitor, statistical report, and screen. In addition, it also indicates if you can drill down into each statistical report.

**Table 160** Function Window

| LEVEL 1/2 | LEVEL 3 | FUNCTION |
|---|---|---|
| Monitor | | Use monitors to check the status of devices. |
| Bandwidth | | Use this report to monitor the total amount of traffic handled by the selected device. |
| Service | | Use this report to monitor the amount of traffic generated by web, FTP, mail, or VPN services in the selected device. |
| Attack | | Use this report to monitor the number of Denial-of-Service (DoS) attacks detected by the selected device’s firewall. |
| Intrusion | | Use this report to monitor the number of intrusions detected by the selected device’s IDP feature. |
| AntiVirus | | Use this report to monitor the number of virus occurrences prevented by the selected device. |
| AntiSpam | | Use this report to monitor the number of spam messages stopped by the selected device. |
| Traffic | | Use these reports to look at how much traffic was handled by devices or who used the most bandwidth in a device. You can also look at traffic in various directions. |
| Bandwidth | Summary | Use this report to look at the amount of traffic handled by the selected device by time interval. You can also use this report to look at the top services in a specific time interval. |
| | Top Protocol | Use this report to look at the top services generating traffic through the selected device. You can also use this report to look at the top sources of traffic for any top service. |
| | Top Hosts | Use this report to look at the top sources of traffic in the selected device. You can also use this report to look at the top services for any top source. |
| WEB | Top Sites | Use this report to look at the top destinations of web traffic. You can also use this report to look at the top sources of web traffic for any top destination. |
| | Top Hosts | Use this report to look at the top sources of web traffic. You can also use this report to look at the top destinations of web traffic for any top source. |
| FTP | Top Sites | Use this report to look at the top destinations of FTP traffic. You can also use this report to look at the top sources of FTP traffic for any top destination. |
| | Top Hosts | Use this report to look at the top sources of FTP traffic. You can also use this report to look at the top destinations of FTP traffic for any top source. |
| MAIL | Top Sites | Use this report to look at the top destinations of mail traffic. You can also use this report to look at the top sources of mail traffic for any top destination. |
| | Top Hosts | Use this report to look at the top sources of mail traffic. You can also use this report to look at the top destinations of mail traffic for any top source. |
| VPN | Top Peer Gateways | Use this report to look at the top destinations of VPN traffic. You can also use this report to look at the top sources of VPN traffic for any top destination. |
| | Top Hosts | Use this report to look at the top sources of VPN traffic. You can also use this report to look at the top destinations of VPN traffic for any top source. |

**Table 160** Function Window (continued)

| LEVEL 1/2 | LEVEL 3 | FUNCTION |
|---|---|---|
| Customization | 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. |
| Network Attack | | Use these reports to look at Denial-of-Service (DoS) attacks that were detected by the device's firewall. |
| Attack | Summary | Use this report to look at the number of DoS attacks by time interval. You can also use this report to look at the top categories of DoS attacks in a specific time interval. |
| | Top Sources | Use this report to look at the top sources of DoS attacks by number of attacks. You can also use this report to look at the top categories of DoS attacks for any top source. |
| | By Category | Use this report to look at the top categories of DoS attacks by number of attacks. You can also use this report to look at the top sources of DoS attacks for any top category. |
| Intrusion | | Use these reports to look at intrusion signatures, types of intrusions, severity of intrusions, and the top sources and destinations of intrusions that are logged on the selected device. |
| | Summary | Use this report to look at the number of intrusions by time interval. You can also use this report to look at the top intrusion signatures in a specific time interval. |
| | Top Intrusions | Use this report to look at the top intrusion signatures by number of intrusions. You can also use this report to look at the top sources of intrusions for any top signature. |
| | Top Sources | Use this report to look at the top sources of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top source. |
| | Top Destinations | Use this report to look at the top destinations of intrusions by number of intrusions. You can also use this report to look at the top intrusion signatures for any top destination. |
| | By Severity | Use this report to look at the top severities (significance) of intrusions by number of intrusions. The levels of severity, in decreasing order of significance, are Emergency (system is unusable), Alert (immediate action is required), Critical, Error, Warning, Notice, Informational, and Debug. You can also use this report to look at the top intrusion signatures for any severity. |
| AntiVirus | | Use these reports to look at viruses that were detected by the device's anti-virus feature. |
| | Summary | Use this report to look at the number of virus occurrences by time interval. |
| | Top Viruses | Use this report to look at the top viruses by number of occurrences. |
| | Top Sources | Use this report to look at the top sources of virus occurrences by number of occurrences. |
| | Top Destinations | Use this report to look at the top destinations of virus occurrences by number of occurrences. |

**Table 160** Function Window (continued)

| LEVEL 1/2 | LEVEL 3 | FUNCTION |
|---|---|---|
| AntiSpam | | Use these reports to look at spam messages that were detected by the device's anti-spam feature. You can also look at the top senders and sources of spam messages. |
| | Summary | Use this report to look at the number of spam messages by time interval. You can also use this report to look at the top combinations of senders and first SMTP servers to which the spam was sent in a specific time interval. |
| | Top Senders | Use this report to look at the top combinations of senders and first SMTP servers to which the spam was sent by number of messages. |
| | Top Sources | Use this report to look at the top sources (last mail relay) of spam messages by number of messages. |
| | By Score | Use this report to look at the top scores calculated for spam messages by number of messages. |
| Security Policy | | Use these reports to look at the top sources and destinations of traffic that is forwarded or blocked based on each device's content filtering settings. You can also look at the amount of traffic forwarded or blocked by time interval. |
| WEB Blocked | Summary | Use this report to look at the number of attempts to access blocked web sites by time interval. You can also use this report to look at the top sources of attempts to access blocked web sites in a specific time interval. |
| | Top Sites | Use this report to look at the top destinations in attempts to access blocked web sites by number of attempts. You can also use this report to look at the top sources of attempts to access blocked web sites for any top destination. |
| | Top Hosts | Use this report to look at the top sources of attempts to access blocked web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access blocked web sites for any top source. |
| | By Category | Use this report to look at the top categories of destinations in attempts to access blocked web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access blocked web sites for any top category. |
| WEB Allowed | Summary | Use this report to look at the number of attempts to access allowed web sites by time interval. You can also use this report to look at the top sources of attempts to access allowed web sites in a specific time interval. |
| | Top Sites | Use this report to look at the top destinations of attempts to access allowed web sites by number of attempts. You can also use this report to look at the top sources of attempts to access allowed web sites for any top destination. |
| | Top Hosts | Use this report to look at the top sources of attempts to access allowed web sites by number of attempts. You can also use this report to look at the top destinations in attempts to access allowed web sites for any top source. |
| Event | | Use these screens to look at who successfully logged into the device (for management or monitoring purposes) or who tried to log in but failed. |
| Device Login | Successful Login | Use this screen to look at who successfully logged into the device (for management or monitoring purposes). |
| | Failed Login | Use this screen to look at who tried to log in into the device (for management or monitoring purposes) but failed. |
| Log Viewer | | Use these screens to look at all log entries for the selected device. |
| All Logs | | Use the log viewer screens to look at all the log entries for the selected device. |
| Schedule Reports | | |

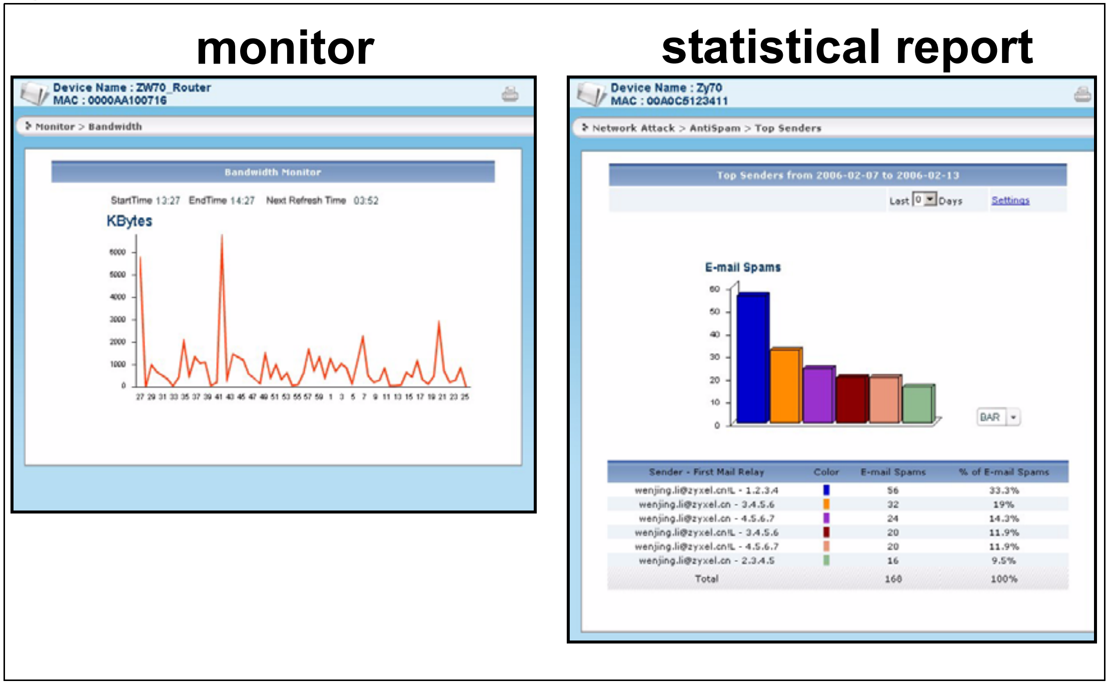
**Table 160** Function Window (continued)

| LEVEL 1/2 | LEVEL 3 | FUNCTION |
|---|---|---|
| Schedule Reports | | Use these screens to set up and maintain daily, weekly, and overtime (one-time) reports that Vantage Report sends by e-mail. |
| System | | The `root` account can use all of the following screens. Other users can use the **About** screen and some features in **User Maintenance**. |
| About | | Use this screen to get the current release and copyright for Vantage Report. |

## 31.3 Report Window

The report window displays the monitor, statistical report, or screen that you select in the device window and the function window. The layout in the report window is similar for all monitors. Similarly, the layout is similar for all statistical reports. Typical examples of monitors and statistical reports are shown in Figure 190.

**Figure 190** Report Window: Monitor and Statistical Report Examples



Device Name : ZW70_Router
MAC : 0000AA100716

Monitor > Bandwidth

Bandwidth Monitor

StartTime 13:27 EndTime 14:27 Next Refresh Time 03:52

Device Name : Zy70
MAC : 00A0C5123411

Network Attack > AntiSpam > Top Senders

Top Senders from 2006-02-07 to 2006-02-13

Last 0 Days Settings

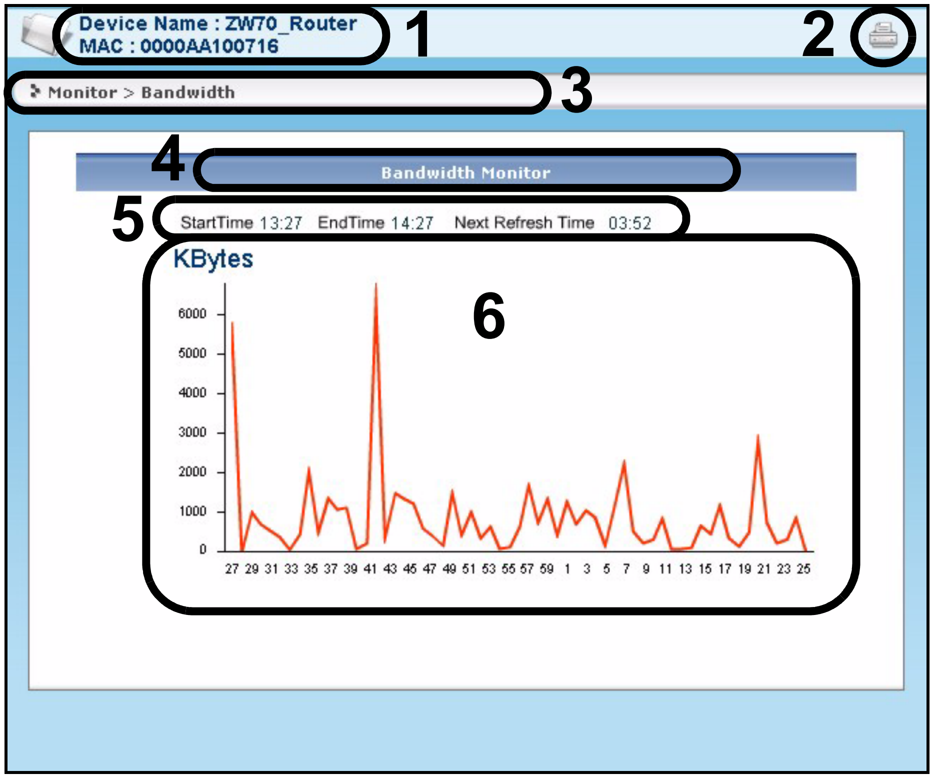
| Sender - First Mail Relay | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| wenjing.li@zyxel.cnIL - 1.2.3.4 | 🟦 | 56 | 33.3% |
| wenjing.li@zyxel.cn - 3.4.5.6 | 🟧 | 32 | 19% |
| wenjing.li@zyxel.cn - 4.5.6.7 | 🟪 | 24 | 14.3% |
| wenjing.li@zyxel.cnIL - 3.4.5.6 | 🟥 | 20 | 11.9% |
| wenjing.li@zyxel.cnIL - 4.5.6.7 | 🟧 | 20 | 11.9% |
| wenjing.li@zyxel.cn - 2.3.4.5 | 🟩 | 16 | 9.5% |
| Total | | 168 | 100% |

The following sections explain the layout for monitors and statistical reports in more detail. For other screens, the layout is different for each one, so see the appropriate screen description for more information.

### 31.3.1 Monitor Layout

A typical monitor is shown in Figure 191 on page 347.

**Figure 191** Typical Monitor Layout



Device Name : ZW70_Router
MAC : 0000AA100716

Monitor > Bandwidth

Bandwidth Monitor

StartTime 13:27 EndTime 14:27 Next Refresh Time 03:52

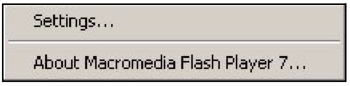
Each numbered section above is described in the following table.

**Table 161** Typical Monitor Features

| SECTION | DESCRIPTION |
|---|---|
| 1 | **Device Name**, **MAC**: These fields are the same ones you entered when you added the device. |
| 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<br>**End Time**: the time of the latest traffic information in the graph.<br>**Next Refresh Time**: This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again. This time is not the same as the processing time that is discussed in Section 30.3 on page 338. |
| 6 | The graph shows how the status changes over time. The X-axis (horizontal) is time. See Section 30.3 on page 338 for more information about clock time in Vantage Report. The Y-axis (vertical) depends on the type of monitor you select. In Figure 191, the y-axis is the number of kilobytes of traffic handled by the device each minute. See Section 30.4 on page 339 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 192** Report Window Right-Click Menu

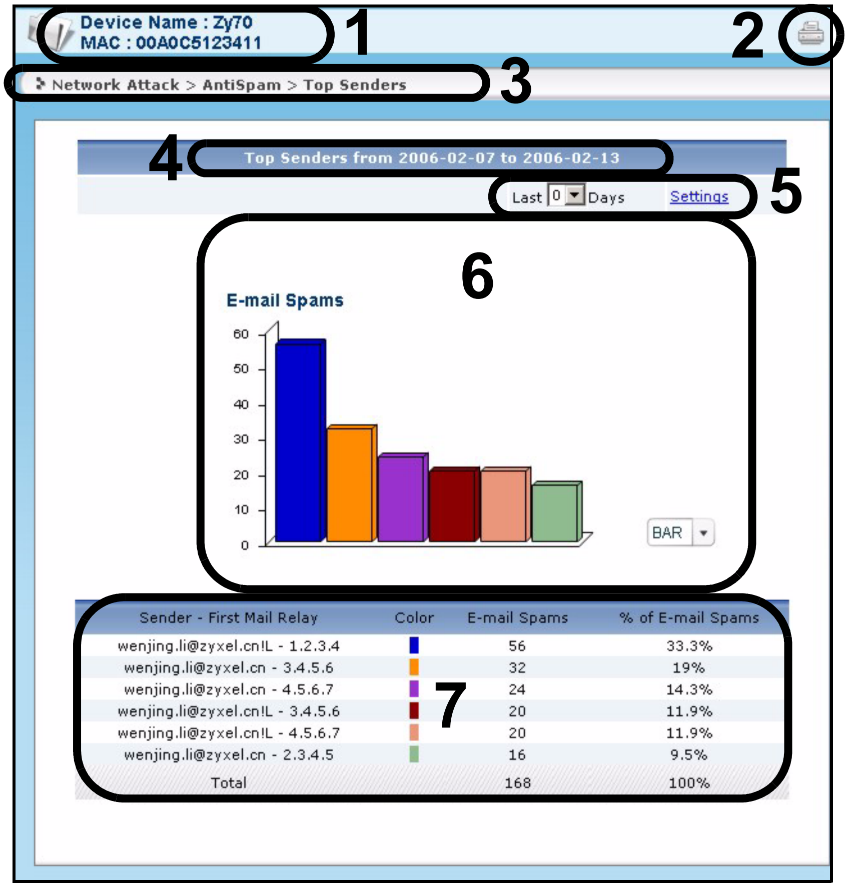


Click **Settings...** if you want to change the Flash settings on the Vantage Report server. In most cases, this is unnecessary. Click **About Macromedia Flash Player 7...** to get information about the current version of Flash.

## 31.3.2 Statistical Report Layout

A typical statistical report is shown in Figure 193.

**Figure 193** Typical Statistical Report Layout



Device Name : Zy70
MAC : 00A0C5123411

Network Attack > AntiSpam > Top Senders

Top Senders from 2006-02-07 to 2006-02-13

Last 0 Days Settings

| Sender - First Mail Relay | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| wenjing.li@zyxel.cn!L - 1.2.3.4 | 🟦 | 56 | 33.3% |
| wenjing.li@zyxel.cn - 3.4.5.6 | 🟧 | 32 | 19% |
| wenjing.li@zyxel.cn - 4.5.6.7 | 🟪 | 24 | 14.3% |
| wenjing.li@zyxel.cn!L - 3.4.5.6 | 🟥 | 20 | 11.9% |
| wenjing.li@zyxel.cn!L - 4.5.6.7 | 🟫 | 20 | 11.9% |
| wenjing.li@zyxel.cn - 2.3.4.5 | 🟩 | 16 | 9.5% |
| Total | | 168 | 100% |

Each numbered section above is described in the following table.

**Table 162** Typical Statistical Report Features

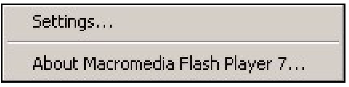
| SECTION | DESCRIPTION |
|---|---|
| 1 | **Device Name**, **MAC**: These fields are the same ones you entered when you added the device. |
| 2 | **Print** icon: Click this icon to **print** the current screen. |
| 3 | This field shows the menu items you selected to open this statistical report. |
| 4 | This field displays the title of the statistical report. The title includes the date(s) you specified in section 5. |

**Table 162** Typical Statistical Report Features (continued)

| SECTION | DESCRIPTION |
|---|---|
| 5 | **Last Days**, **Settings**: Use one of these fields to specify what historical information is included in the report.<br>• Select how many days, ending (and including) today, in the **Last Days** drop-down list.<br>• Click **Settings**, and select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days**. See Section 26.8.4 on page 310.<br>When you change any of these fields, the report updates automatically. The **Last Days** field returns to zero, regardless of your selection. This way, you can refresh the report by selecting **Last Days** again. You can see the current date range in the title (section 4). Both the **Last Days** and **Settings** fields reset to the default values when you click a menu item in the function window (including the menu item for the same report). They do not reset when you open or close drill-down reports.<br>These fields are not available in drill-down reports because these reports use the same historical information as the main report.<br>See Section 30.3 on page 338 for more information about time in these screens. |
| 6 | The graph displays the specified report visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little.<br>See Section 30.4 on page 339 for more information about the source data used by the statistical report. |
| 7 | In the table,<br>• 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.<br>• If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with IP addresses (for example, “www.yahoo.com/200.100.20.10”). See Section 26.8.4 on page 310.<br>• Some reports provide extra information (for example, number of traffic events) in the table. See each report for more information.<br>See Section 30.4 on page 339 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 194** Report Window Right-Click Menu



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

# 32

# Monitor

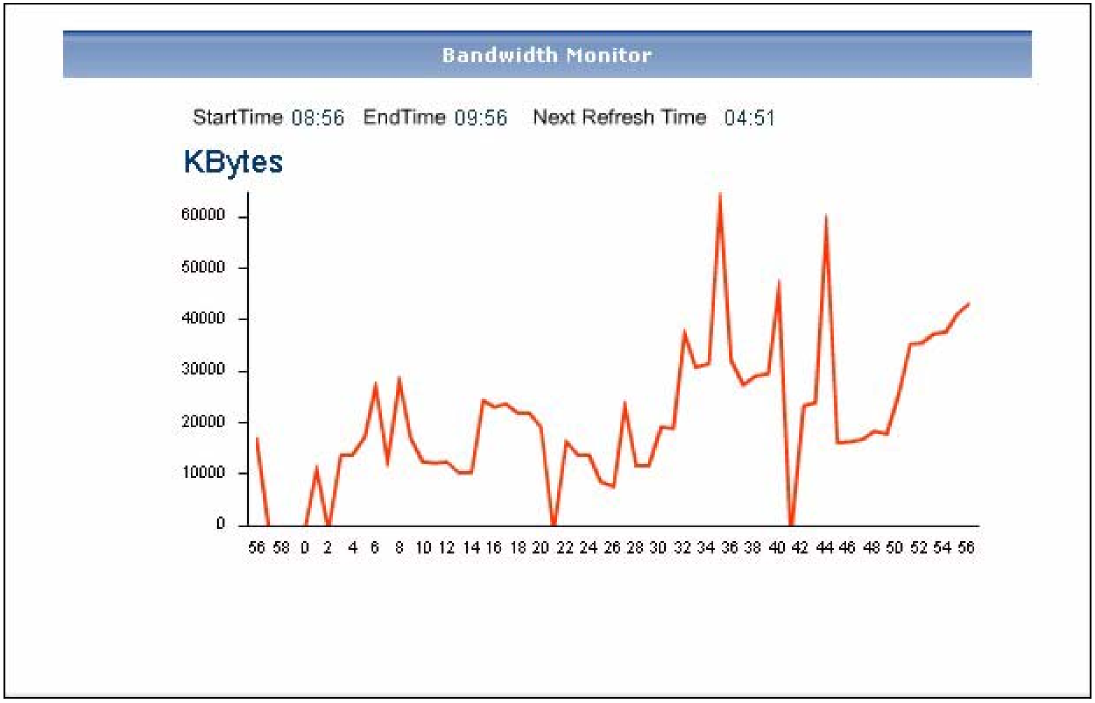
Use monitors to check the status of devices. See Section 30.3 on page 338 for a related discussion about time.

## 32.1 Bandwidth Monitor

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

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

**Figure 195** Monitor > Bandwidth



Bandwidth Monitor

StartTime 08:56 EndTime 09:56 Next Refresh Time 04:51

Each field is described in the following table.

**Table 163** Monitor > Bandwidth

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

**Table 163** Monitor > Bandwidth (continued)

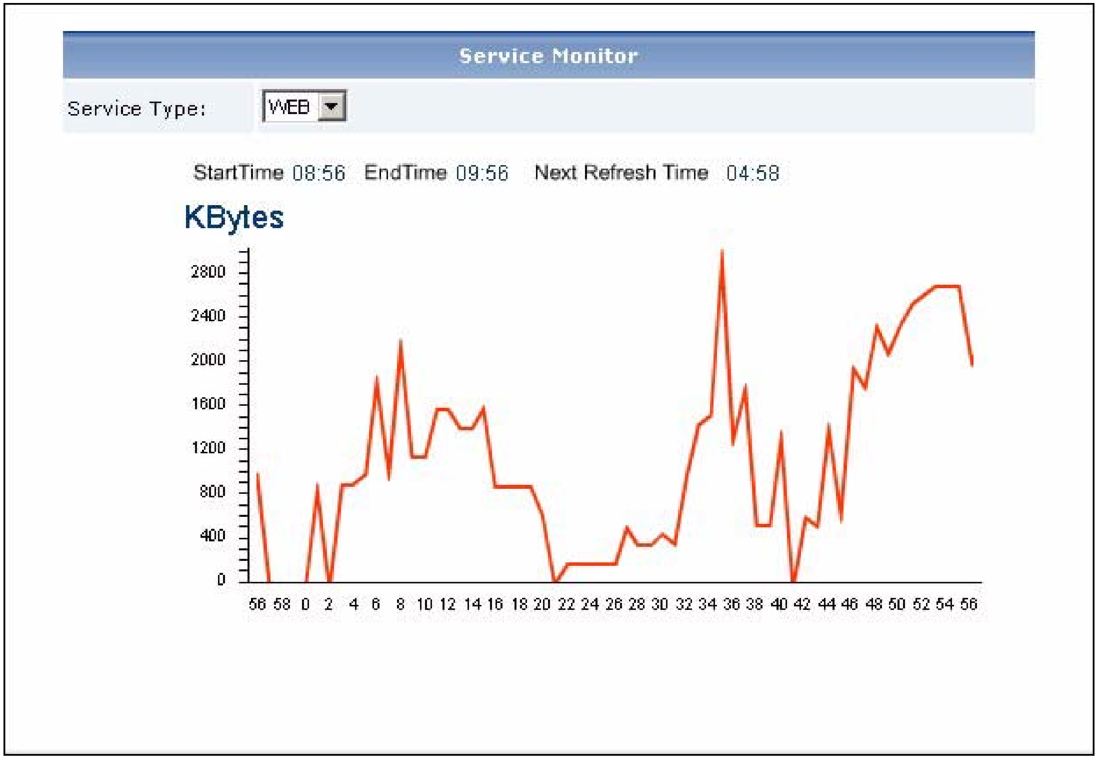
| LABEL | DESCRIPTION |
|---|---|
| Next Refresh Time | This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again.<br>This time is not the same as the processing time. |
| graph | The graph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

## 32.2 Service Monitor

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

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

**Figure 196** Monitor > Service



Service Monitor

Service Type: WEB

StartTime 08:56 EndTime 09:56 Next Refresh Time 04:58

Each field is described in the following table.

**Table 164** Monitor > Service

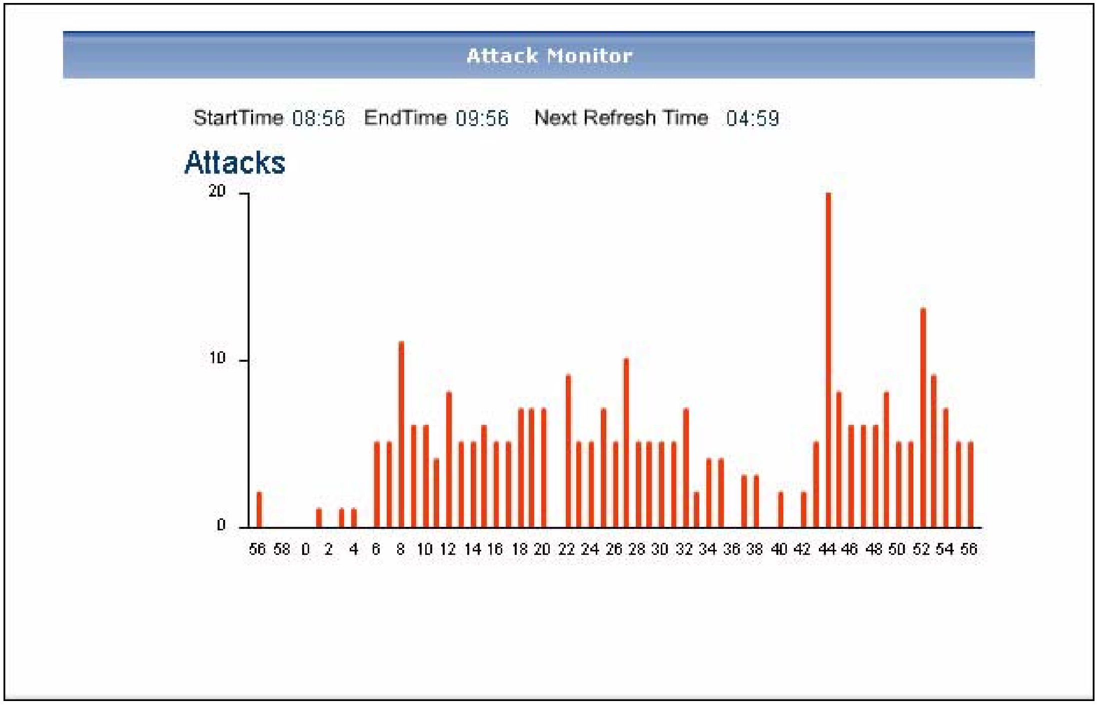
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the monitor. It does not include the service you select in the **Service Type** field. |
| Service Type | Select the service whose traffic you want to look at. Choices are:<br>**WEB** - Look at the amount of traffic generated by HTTP/HTTPS services.<br>**FTP** - Look at the amount of traffic generated by FTP services.<br>**MAIL** - Look at the amount of traffic generated by POP3/SMTP services.<br>**VPN** - Look at the amount of traffic generated by IPSec/VPN services. |
| Start Time | This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph. |
| End Time | This field displays the clock time (in 24-hour format) of the latest traffic statistics in the graph. |
| Next Refresh Time | This field displays how much time remains until Vantage Report automatically updates the screen. You can also update the screen immediately by clicking the menu item again.<br>This time is not the same as the processing time. |
| graph | The graph shows how the status changes over time.<br>Y-axis (vertical): how much traffic from the selected service is handled by the device each minute<br>X-axis (horizontal): clock time, minutes only. These minutes represent clock times between the **Start Time** and **End Time**. For example, if the start time is 13:27 and end time is 14:27, then “39” means 13:39 and “5” means 14:05. |

## 32.3 Attack Monitor

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

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

**Figure 197** Monitor > Attack



Each field is described in the following table.

**Table 165** Monitor > Attack

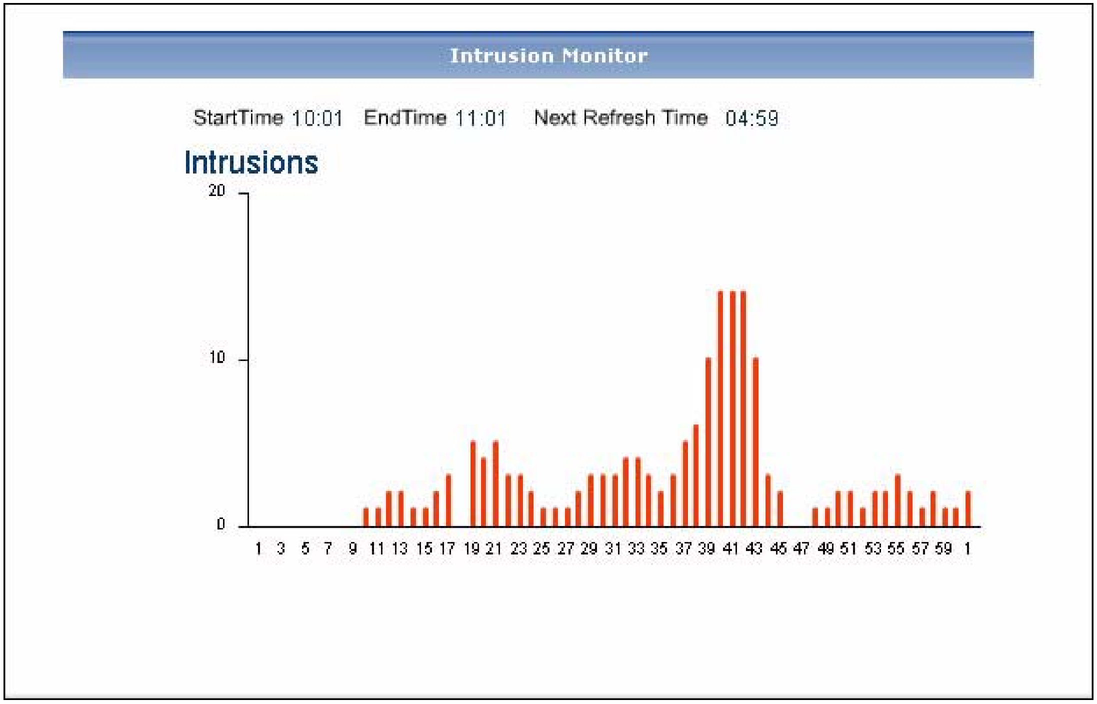
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the monitor. |
| Start Time | This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph. |
| End Time | This field displays the clock time (in 24-hour format) of the latest traffic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

## 32.4 Intrusion Monitor

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

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

**Figure 198** Monitor > Intrusion



Each field is described in the following table.

**Table 166** Monitor > Intrusion

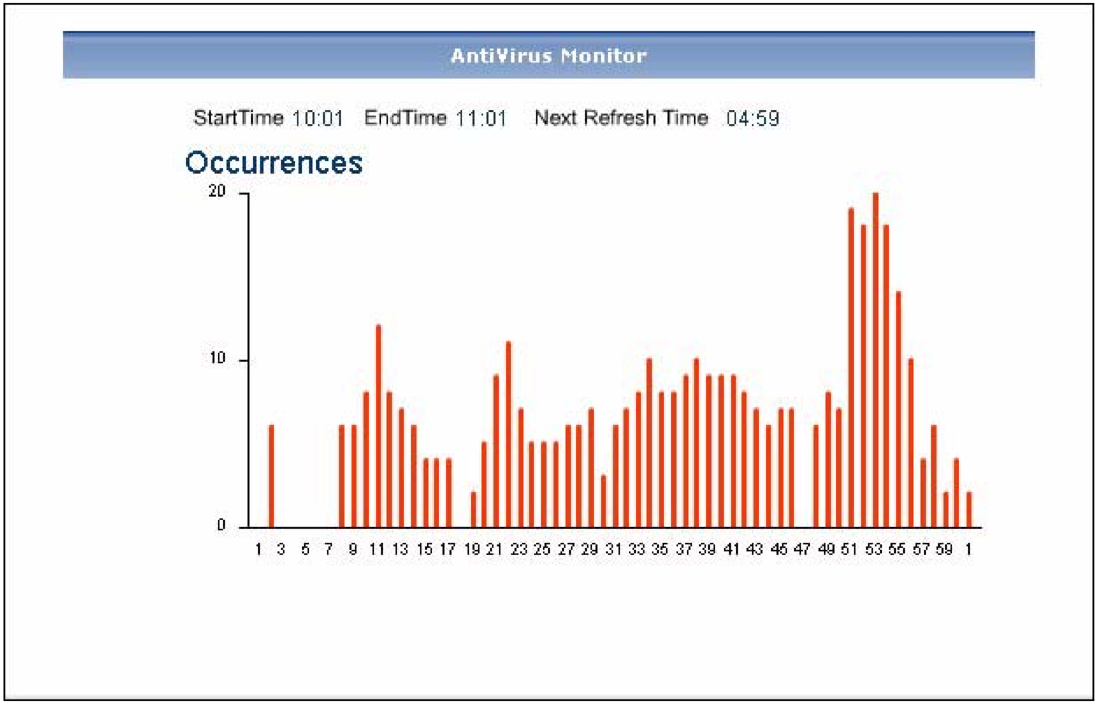
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the monitor. |
| Start Time | This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph. |
| End Time | This field displays the clock time (in 24-hour format) of the latest traffic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

## 32.5 Anti-Virus Monitor

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

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

**Figure 199** Monitor > AntiVirus



AntiVirus Monitor

StartTime 10:01 EndTime 11:01 Next Refresh Time 04:59

Each field is described in the following table.

**Table 167** Monitor > AntiVirus

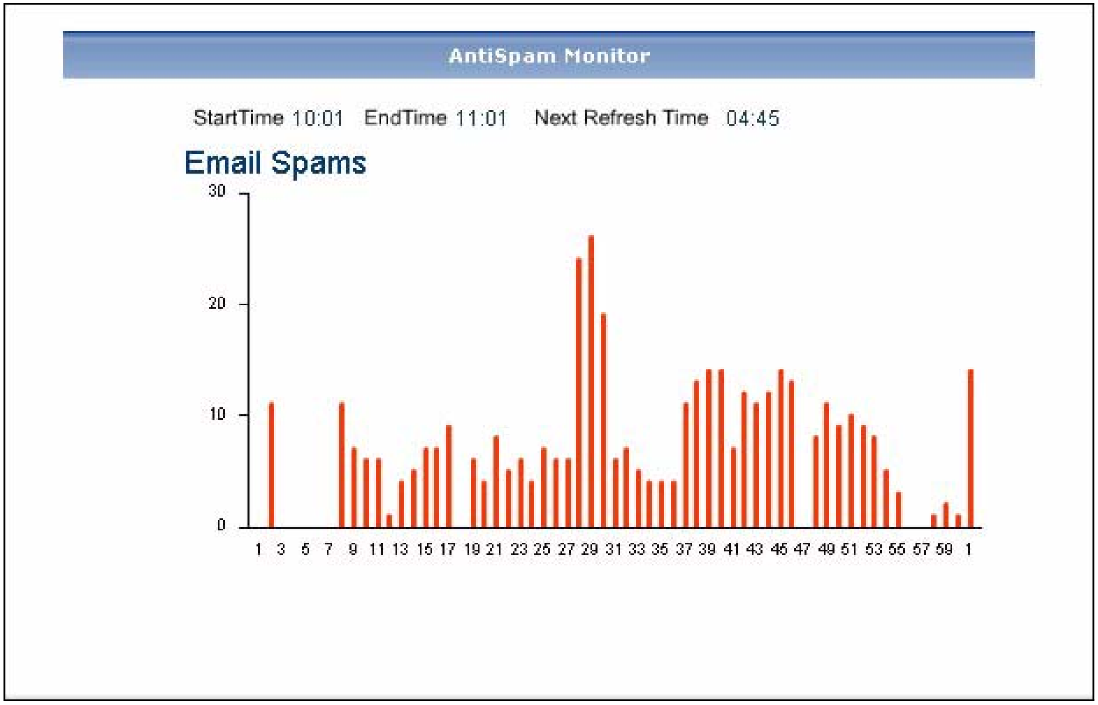
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the monitor. |
| Start Time | This field displays the clock time (in 24-hour format) of the earliest traffic statistics in the graph. |
| End Time | This field displays the clock time (in 24-hour format) of the latest traffic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

## 32.6 Anti-Spam Monitor

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

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

**Figure 200** Monitor > AntiSpam



Each field is described in the following table.

**Table 168** Monitor > AntiSpam

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

# 33

# Traffic

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

## 33.1 Bandwidth

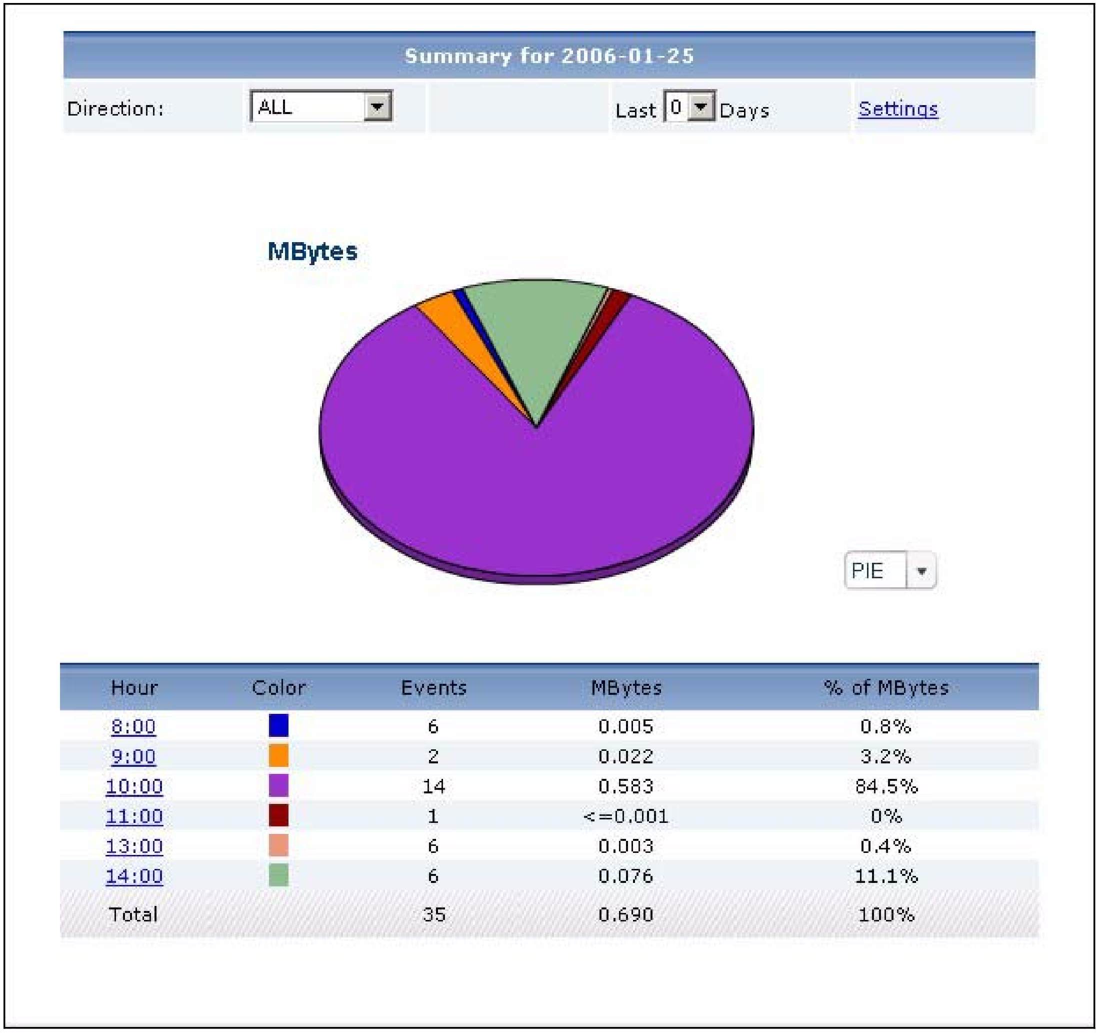
Use these reports to look at how much traffic was handled by devices, who used the most bandwidth in a device, and which protocols were used. You can also look at traffic in various directions.

### 33.1.1 Bandwidth Summary

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

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

**Figure 201** Traffic > Bandwidth > Summary



Summary for 2006-01-25

Direction: ALL    Last 0 Days    Settings

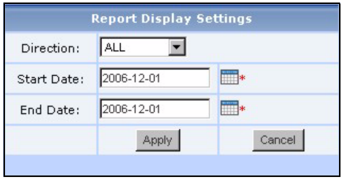
| Hour | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 8:00 | 🟦 | 6 | 0.005 | 0.8% |
| 9:00 | 🟧 | 2 | 0.022 | 3.2% |
| 10:00 | 🟪 | 14 | 0.583 | 84.5% |
| 11:00 | 🟥 | 1 | <=0.001 | 0% |
| 13:00 | 🟫 | 6 | 0.003 | 0.4% |
| 14:00 | 🟩 | 6 | 0.076 | 11.1% |
| Total | | 35 | 0.690 | 100% |

Each field is described in the following table.

**Table 169** Traffic > Bandwidth > Summary

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select. |
| Direction | This field is displayed if there are any traffic statistics for the selected report.<br>Select which kind of traffic, by direction, you want to look at. The options depend on which directions have traffic. If there is no traffic in a specific direction, the option is not available. In addition, the following options may appear.<br>**All** - all traffic, regardless of direction<br>**Inbound** - all traffic routed from the WAN<br>**Outbound** - all traffic routed to the WAN |

**Table 169** Traffic > Bandwidth > Summary (continued)

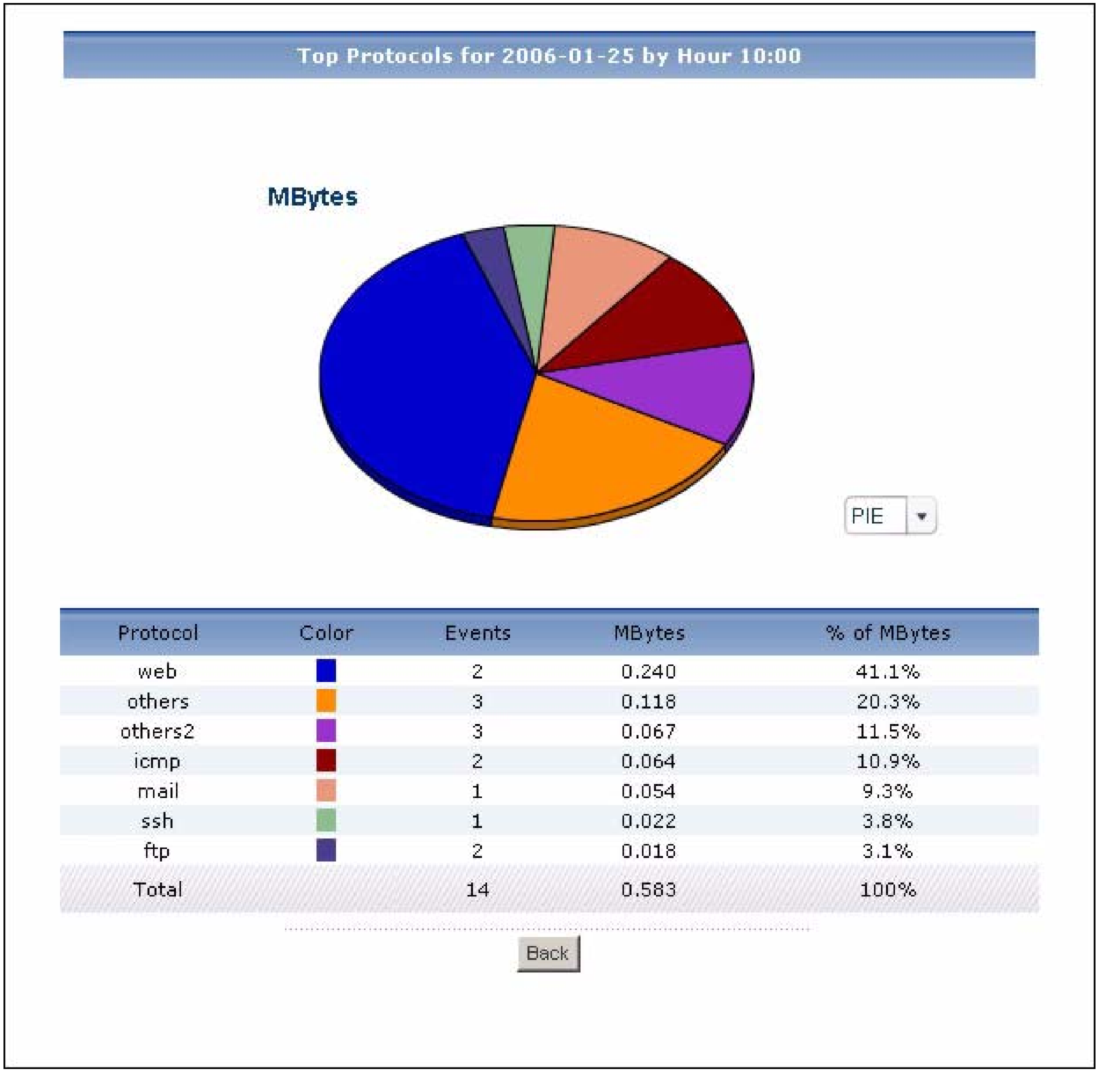
| LABEL | DESCRIPTION |
|---|---|
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Direction: ALL<br>Start Date: 2006-12-01<br>End Date: 2006-12-01<br> <br>Select a specific **Direction**, **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top services by amount of traffic in the selected time interval. The **Bandwidth Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| Events | This field displays the number of traffic events in each interval. |
| MBytes | This field displays how much traffic (in megabytes) the device handled in each time interval. |
| % of MBytes | This field displays what percentage of all traffic was handled in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

## 33.1.2 Bandwidth Summary Drill-Down

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

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

**Figure 202** Traffic > Bandwidth > Summary > Drill-Down



| Protocol | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| web | 🟦 | 2 | 0.240 | 41.1% |
| others | 🟧 | 3 | 0.118 | 20.3% |
| others2 | 🟪 | 3 | 0.067 | 11.5% |
| icmp | 🟥 | 2 | 0.064 | 10.9% |
| mail | 🟧 | 1 | 0.054 | 9.3% |
| ssh | 🟩 | 1 | 0.022 | 3.8% |
| ftp | 🟦 | 2 | 0.018 | 3.1% |
| Total | | 14 | 0.583 | 100% |

Each field is described in the following table.

**Table 170** Traffic > Bandwidth > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 **Customized Service Setting** screen (Section 26.8.5 on page 312). |
| Color | This field displays what color represents each service in the graph. |

**Table 170** Traffic > Bandwidth > Summary > Drill-Down (continued)

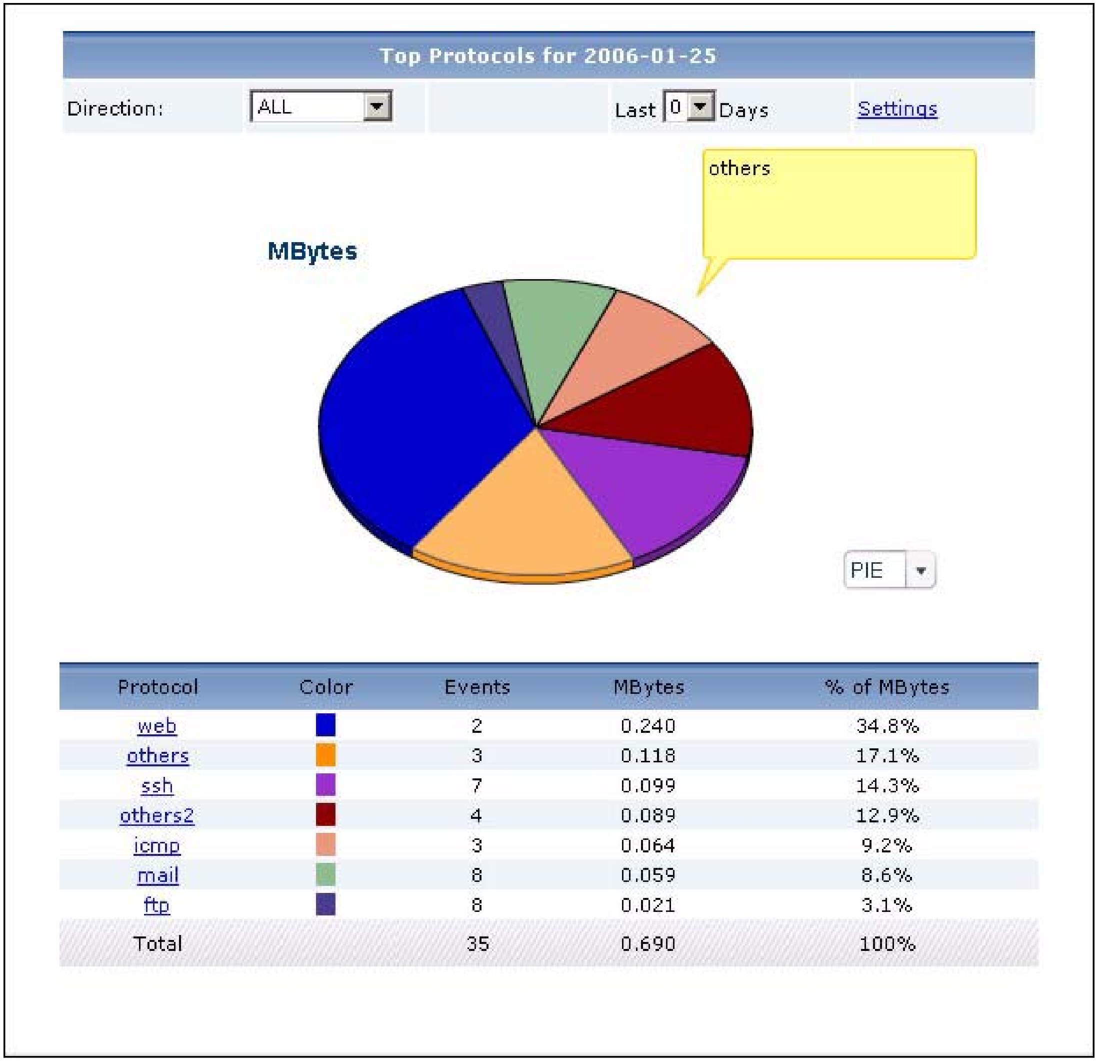
| LABEL | DESCRIPTION |
|---|---|
| Events | This field displays the number of traffic events for each service in the selected time interval. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each service in the selected time interval. |
| % of MBytes | This field displays what percentage of all traffic in the selected time interval was attributed to each service. |
| Total | This entry displays the totals for the services above. If the number of services in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report. |
| Back | Click this to return to the main report. |

### 33.1.3 Bandwidth Top Protocols

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

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

**Figure 203** Traffic > Bandwidth > Top Protocol



Top Protocols for 2006-01-25

Direction: ALL ▾ Last 0 ▾ Days Settings

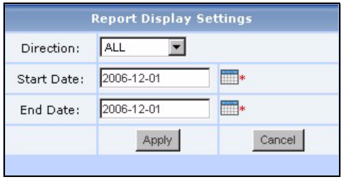
| Protocol | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| web | 🟦 | 2 | 0.240 | 34.8% |
| others | 🟧 | 3 | 0.118 | 17.1% |
| ssh | 🟪 | 7 | 0.099 | 14.3% |
| others2 | 🟥 | 4 | 0.089 | 12.9% |
| icmp | 🟧 | 3 | 0.064 | 9.2% |
| mail | 🟩 | 8 | 0.059 | 8.6% |
| ftp | 🟪 | 8 | 0.021 | 3.1% |
| Total | | 35 | 0.690 | 100% |

Each field is described in the following table.

**Table 171** Traffic > Bandwidth > Top Protocol

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select. |
| Direction | This field is displayed if there are any traffic statistics for the selected report.<br>Select which kind of traffic, by direction, you want to look at. The options depend on which directions have traffic. If there is no traffic in a specific direction, the option is not available. In addition, the following options may appear.<br>**All** - all traffic, regardless of direction<br>**Inbound** - all traffic routed from the WAN<br>**Outbound** - all traffic routed to the WAN |

**Table 171** Traffic > Bandwidth > Top Protocol (continued)

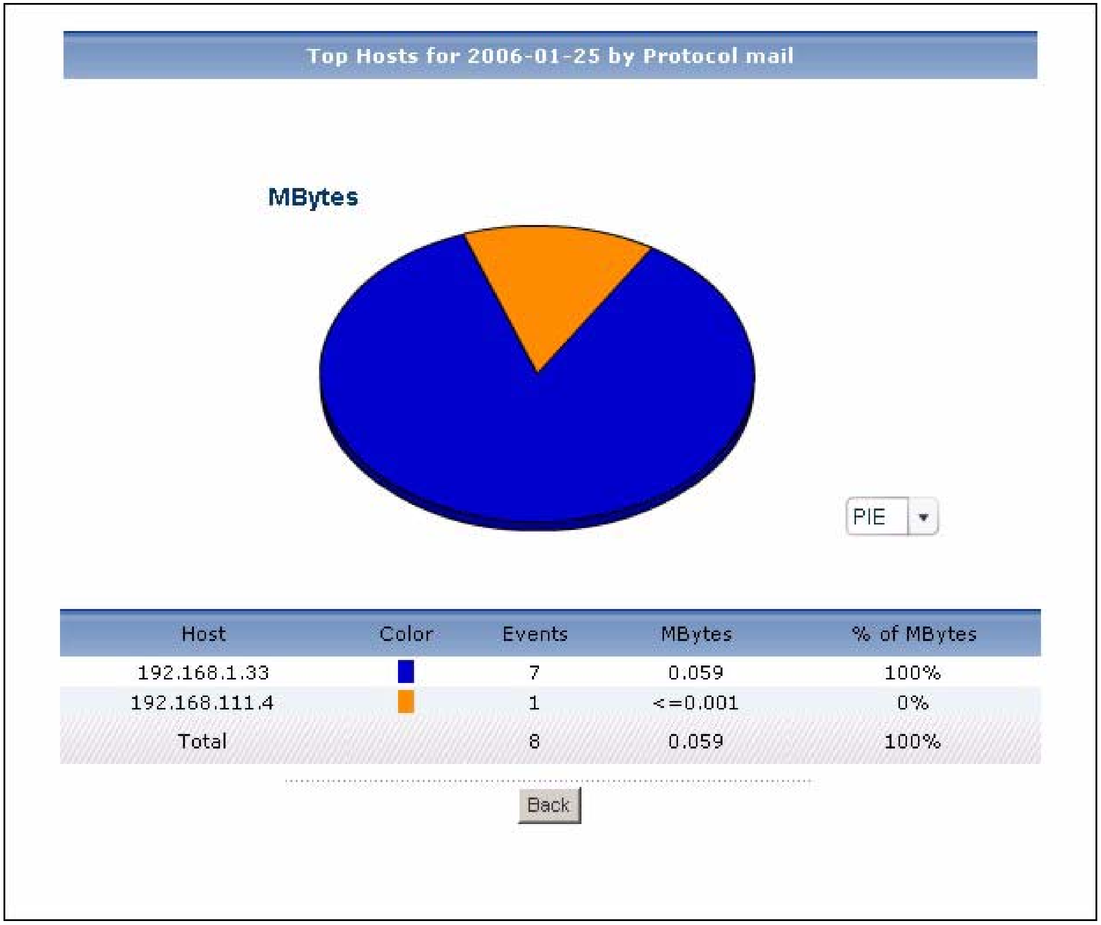
| LABEL | DESCRIPTION |
|---|---|
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Direction: ALL<br>Start Date: 2006-12-01<br>End Date: 2006-12-01<br> <br>Select a specific **Direction**, **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 sources may be different than the ones you manage in the **Customized Service Setting** screen (Section 26.8.5 on page 312).<br>Click on a service to look at the top sources of traffic for the selected service. The **Bandwidth Top Protocols Drill-Down** report appears. |
| Color | This field displays what color represents each service in the graph. |
| Events | This field displays the number of traffic events for each service. |
| MBytes | This field displays how much traffic (in megabytes) each service generated through the selected device. |
| % of MBytes | This field displays what percentage of all traffic each service generated through the selected device. |
| Total | This entry displays the totals for the services above. |

## 33.1.4 Bandwidth Top Protocols Drill-Down

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

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

**Figure 204** Traffic > Bandwidth > Top Protocol > Drill-Down



Top Hosts for 2006-01-25 by Protocol mail

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.33 | 🟦 | 7 | 0.059 | 100% |
| 192.168.111.4 | 🟧 | 1 | <=0.001 | 0% |
| Total | | 8 | 0.059 | 100% |

Each field is described in the following table.

**Table 172** Traffic > Bandwidth > Top Protocol > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Host | This field displays the top sources of traffic for the selected service, sorted by the amount of traffic generated by each one. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events each source generated using the selected service. |
| MBytes | This field displays how much traffic (in megabytes) each source generated using the selected service. |
| % of MBytes | This field displays what percentage of the selected service's traffic was generated by each source. |

**Table 172** Traffic > Bandwidth > Top Protocol > Drill-Down (continued)

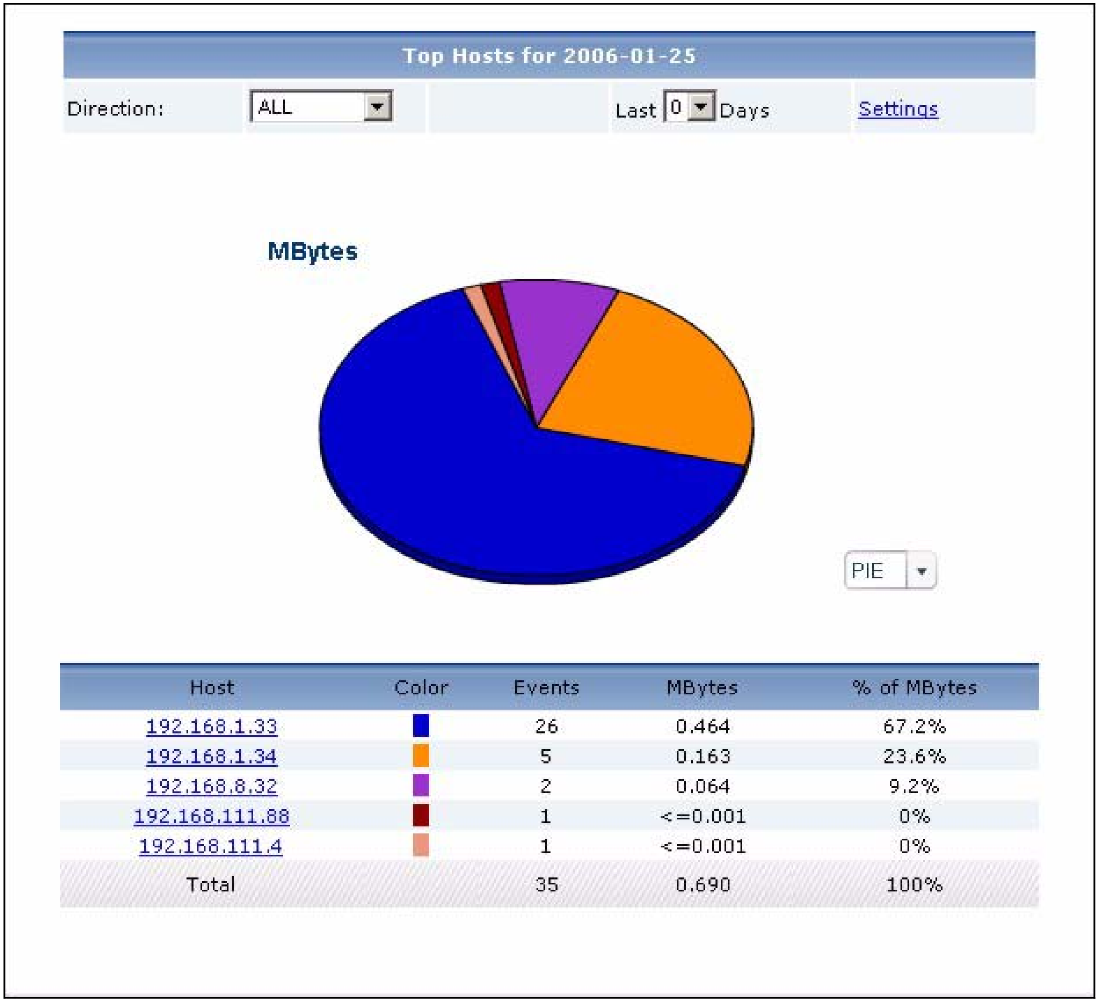
| LABEL | DESCRIPTION |
|---|---|
| Total | This entry displays the totals for the sources above. If the number of sources generating traffic using the selected service is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main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

### 33.1.5 Top Bandwidth Hosts

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

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

**Figure 205** Traffic > Bandwidth > Top Hosts



Top Hosts for 2006-01-25

Direction: ALL

Last 0 Days

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.33 | 🟦 | 26 | 0.464 | 67.2% |
| 192.168.1.34 | 🟧 | 5 | 0.163 | 23.6% |
| 192.168.8.32 | 🟪 | 2 | 0.064 | 9.2% |
| 192.168.111.88 | 🟥 | 1 | <=0.001 | 0% |
| 192.168.111.4 | 🟫 | 1 | <=0.001 | 0% |
| Total | | 35 | 0.690 | 100% |

Each field is described in the following table.

**Table 173** Traffic > Bandwidth > Top Hosts

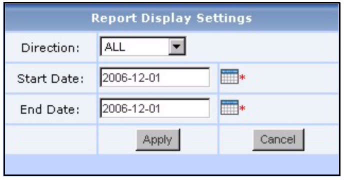
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select. |
| Direction | This field is displayed if there are any traffic statistics for the selected report.<br>Select which kind of traffic, by direction, you want to look at. The options depend on which directions have traffic. If there is no traffic in a specific direction, the option is not available. In addition, the following options may appear.<br>**All** - all traffic, regardless of direction<br>**Inbound** - all traffic routed from the WAN<br>**Outbound** - all traffic routed to the WAN |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Direction: ALL<br>Start Date: 2006-12-01<br>End Date: 2006-12-01<br> <br>Select a specific **Direction**, **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address.<br>Click on a source to look at the top services by amount of traffic for the selected source. The **Bandwidth Top Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events for each source. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each source. |

**Table 173** Traffic > Bandwidth > Top Hosts (continued)

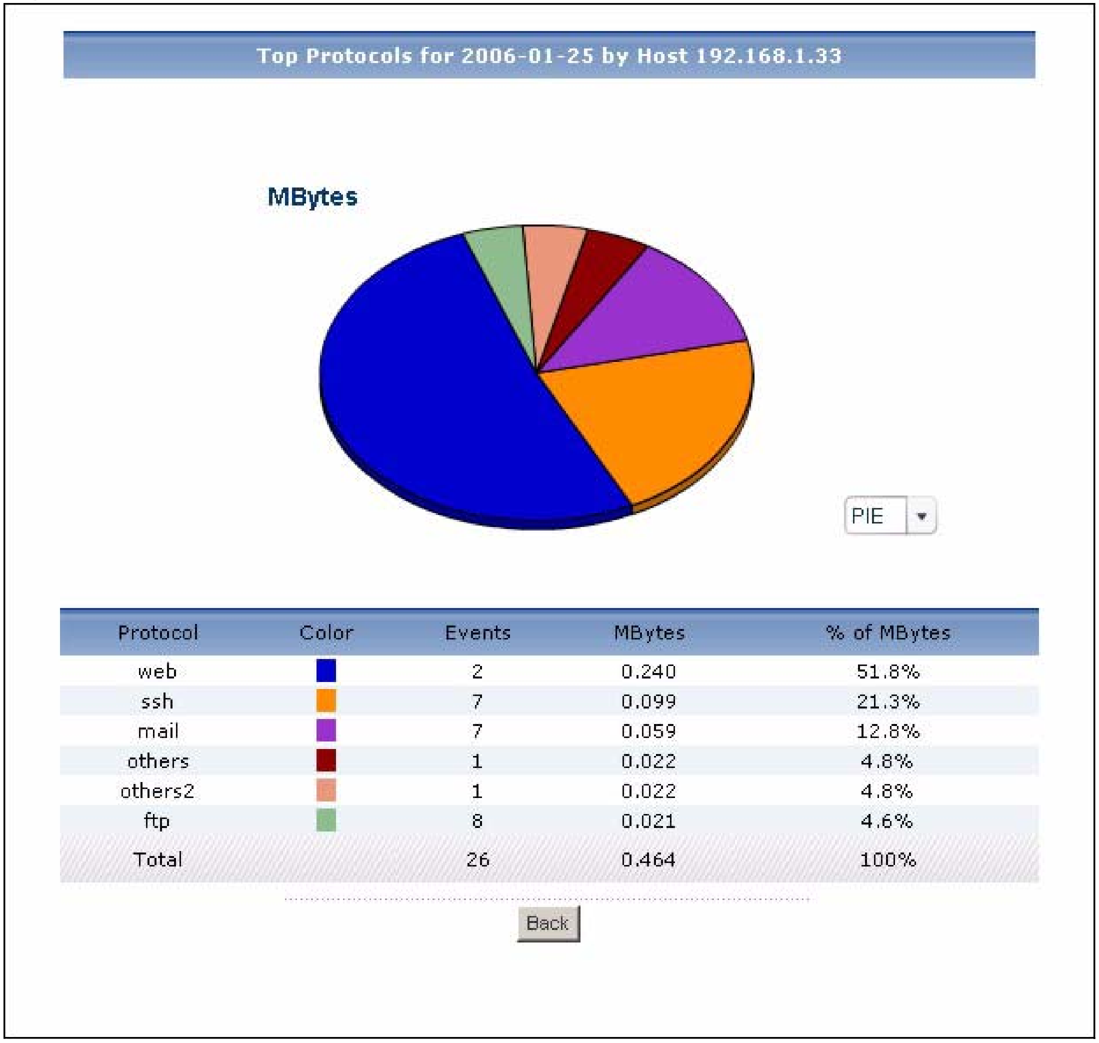
| LABEL | DESCRIPTION |
|---|---|
| % of MBytes | This field displays what percentage of all traffic the device handled for each source. |
| Total | This entry displays the totals for the sources above. |

### 33.1.6 Top Bandwidth Hosts Drill-Down

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

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

**Figure 206** Traffic > Bandwidth > Top Hosts > Drill-Down



Top Protocols for 2006-01-25 by Host 192.168.1.33

| Protocol | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| web | 🟦 | 2 | 0.240 | 51.8% |
| ssh | 🟧 | 7 | 0.099 | 21.3% |
| mail | 🟪 | 7 | 0.059 | 12.8% |
| others | 🟥 | 1 | 0.022 | 4.8% |
| others2 | 🟫 | 1 | 0.022 | 4.8% |
| ftp | 🟩 | 8 | 0.021 | 4.6% |
| Total | | 26 | 0.464 | 100% |

Each field is described in the following table.

**Table 174** Traffic > Bandwidth > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. It does not include the **Direction** you select. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 **Customized Service Setting** screen (Section 26.8.5 on page 312). |
| Color | This field displays what color represents each service in the graph. |
| Events | This field displays the number of traffic events the selected source generated using each service. |
| MBytes | This field displays how much traffic (in megabytes) the selected source generated using each service. |
| % of MBytes | This field displays what percentage of the selected source’s traffic was generated using each service. |
| Total | This entry displays the totals for the services above. If the number of services used by the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report. |
| Back | Click this to return to the main report. |

## 33.2 Web Traffic

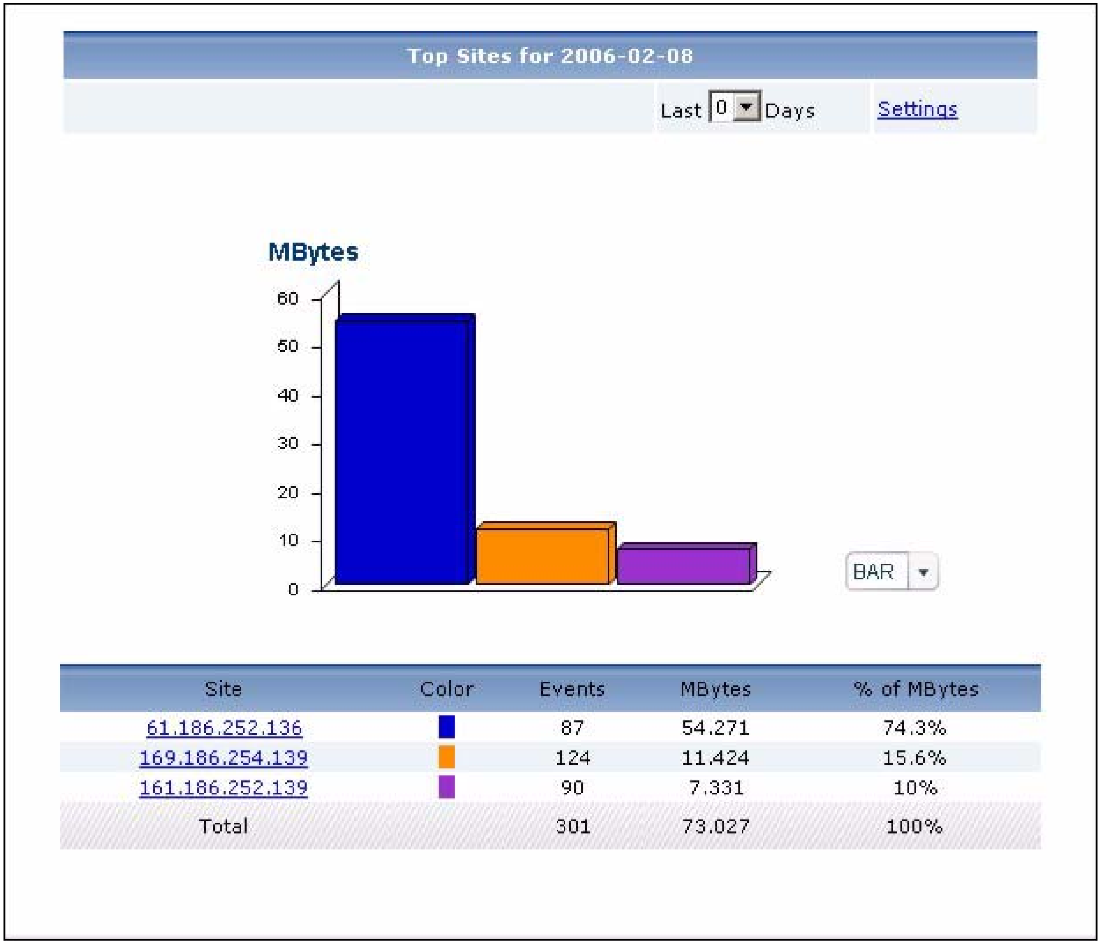
Use this report to look at the top destinations and sources of web traffic.

### 33.2.1 Top Web Sites

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

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

**Figure 207** Traffic > WEB > Top Sites



Top Sites for 2006-02-08

Last 0 Days Settings

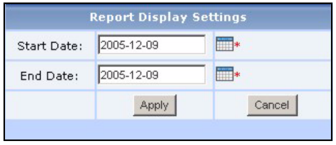
| Site | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 61.186.252.136 | 🟦 | 87 | 54.271 | 74.3% |
| 169.186.254.139 | 🟧 | 124 | 11.424 | 15.6% |
| 161.186.252.139 | 🟪 | 90 | 7.331 | 10% |
| Total | | 301 | 73.027 | 100% |

Each field is described in the following table.

**Table 175** Traffic > WEB > Top Sites

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

**Table 175** Traffic > WEB > Top Sites (continued)

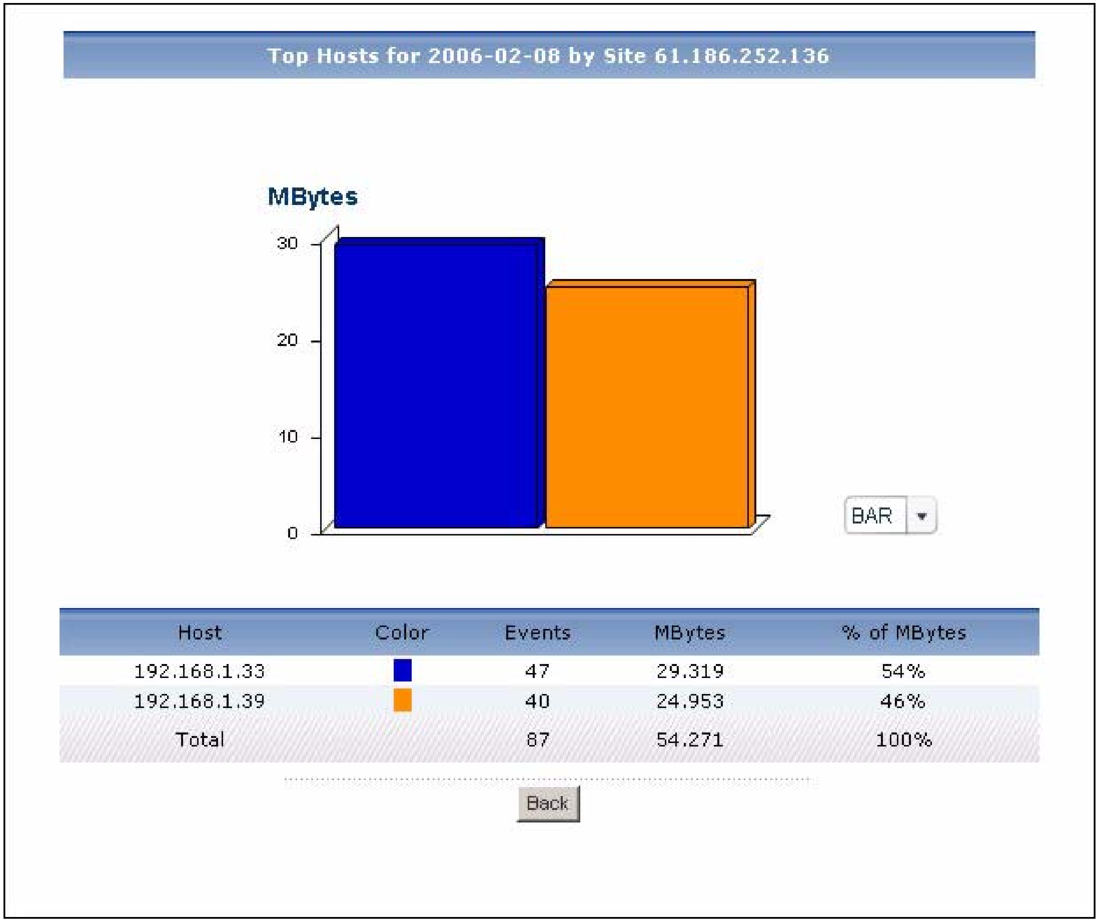
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”).<br>Click on a destination to look at the top sources of web traffic for the selected destination. The **Top Web Sites Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events for each destination. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each destination. |
| % of MBytes | This field displays what percentage of web traffic the device handled for each destination. |
| Total | This entry displays the totals for the destinations above. |

## 33.2.2 Top Web Sites Drill-Down

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

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

**Figure 208** Traffic > WEB > Top Sites > Drill-Down



Top Hosts for 2006-02-08 by Site 61.186.252.136

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.33 | 🟦 | 47 | 29.319 | 54% |
| 192.168.1.39 | 🟧 | 40 | 24.953 | 46% |
| Total |  | 87 | 54.271 | 100% |

Each field is described in the following table.

**Table 176** Traffic > WEB > Top Sites > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events from each source to the selected destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from each source to the selected destination. |
| % of MBytes | This field displays what percentage of the selected destination's web traffic was generated from each source. |

**Table 176** Traffic > WEB > Top Sites > Drill-Down (continued)

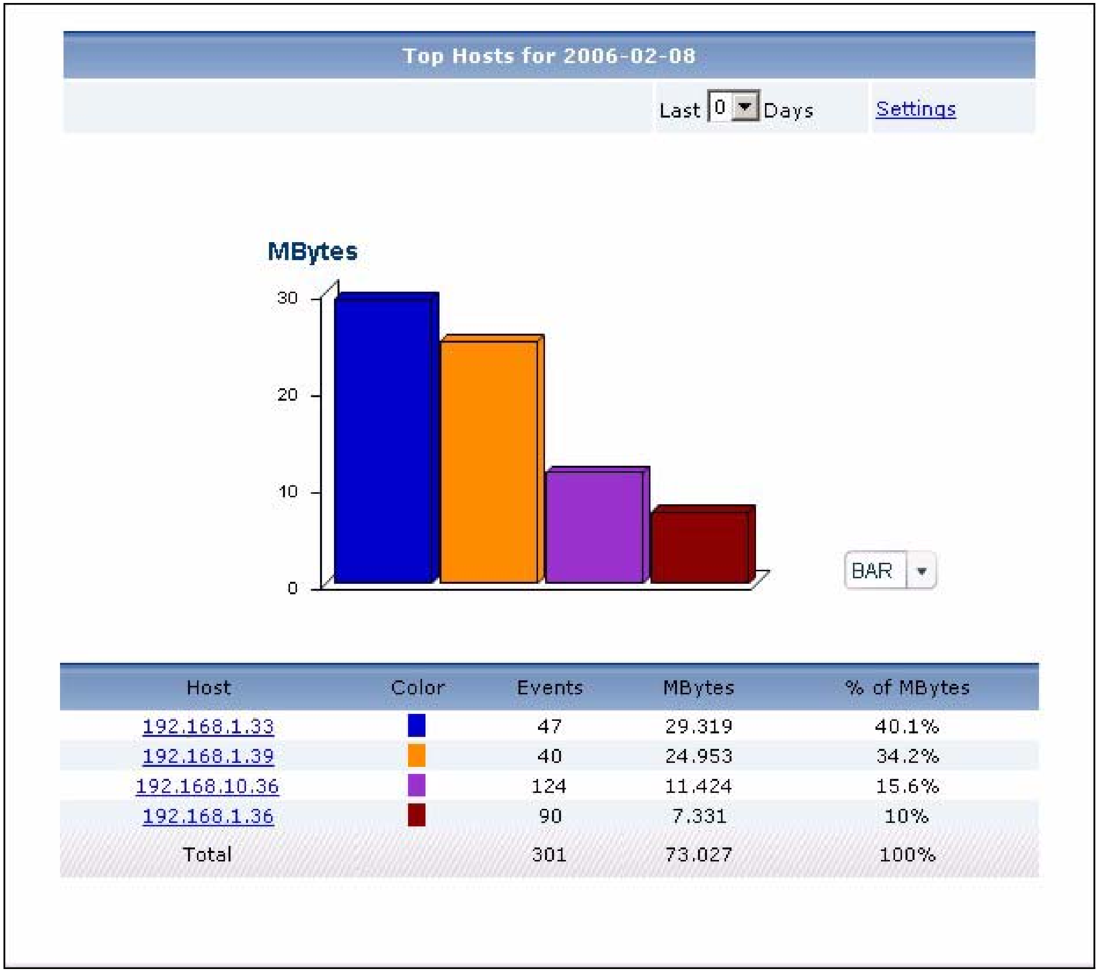
| LABEL | DESCRIPTION |
|---|---|
| Total | This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.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

## 33.2.3 Top Web Hosts

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

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

**Figure 209** Traffic > WEB > Top Hosts



Top Hosts for 2006-02-08

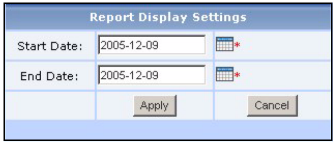
Last 0 Days

Settings

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.33 | 🟦 | 47 | 29.319 | 40.1% |
| 192.168.1.39 | 🟧 | 40 | 24.953 | 34.2% |
| 192.168.10.36 | 🟪 | 124 | 11.424 | 15.6% |
| 192.168.1.36 | 🟥 | 90 | 7.331 | 10% |
| Total | | 301 | 73.027 | 100% |

Each field is described in the following table.

**Table 177** Traffic > WEB > Top Hosts

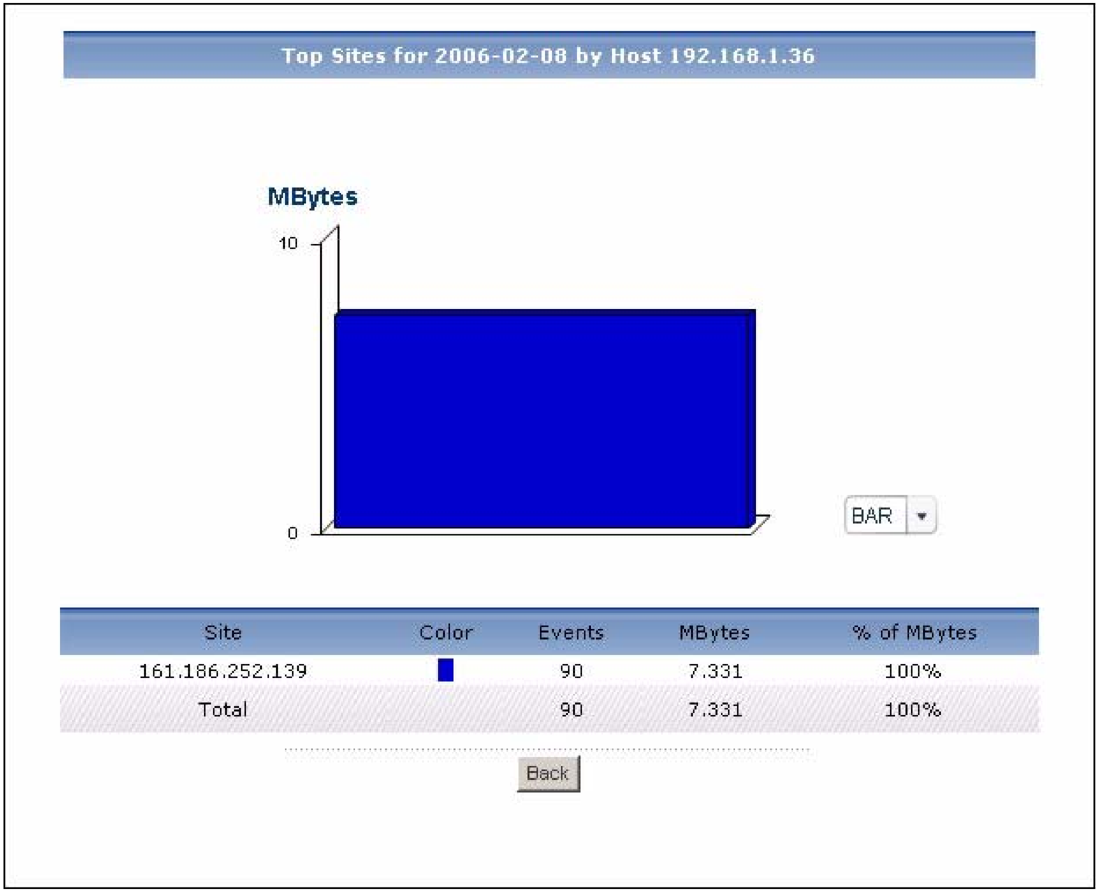
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of web traffic for the selected source. The **Top Web Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events for each source. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of MBytes | This field displays what percentage of web traffic the device handled for each source. |
| Total | This entry displays the totals for the sources above. |

## 33.2.4 Top Web Hosts Drill-Down

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

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

**Figure 210** Traffic > WEB > Top Hosts > Drill-Down



Top Sites for 2006-02-08 by Host 192.168.1.36

| Site | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 161.186.252.139 | ■ | 90 | 7.331 | 100% |
| Total | | 90 | 7.331 | 100% |

Each field is described in the following table.

**Table 178** Traffic > WEB > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), 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. |
| Events | This field displays the number of traffic events from the selected source to each destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from the selected source to each destination. |

**Table 178** Traffic > WEB > Top Hosts > Drill-Down (continued)

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

## 33.3 FTP Traffic

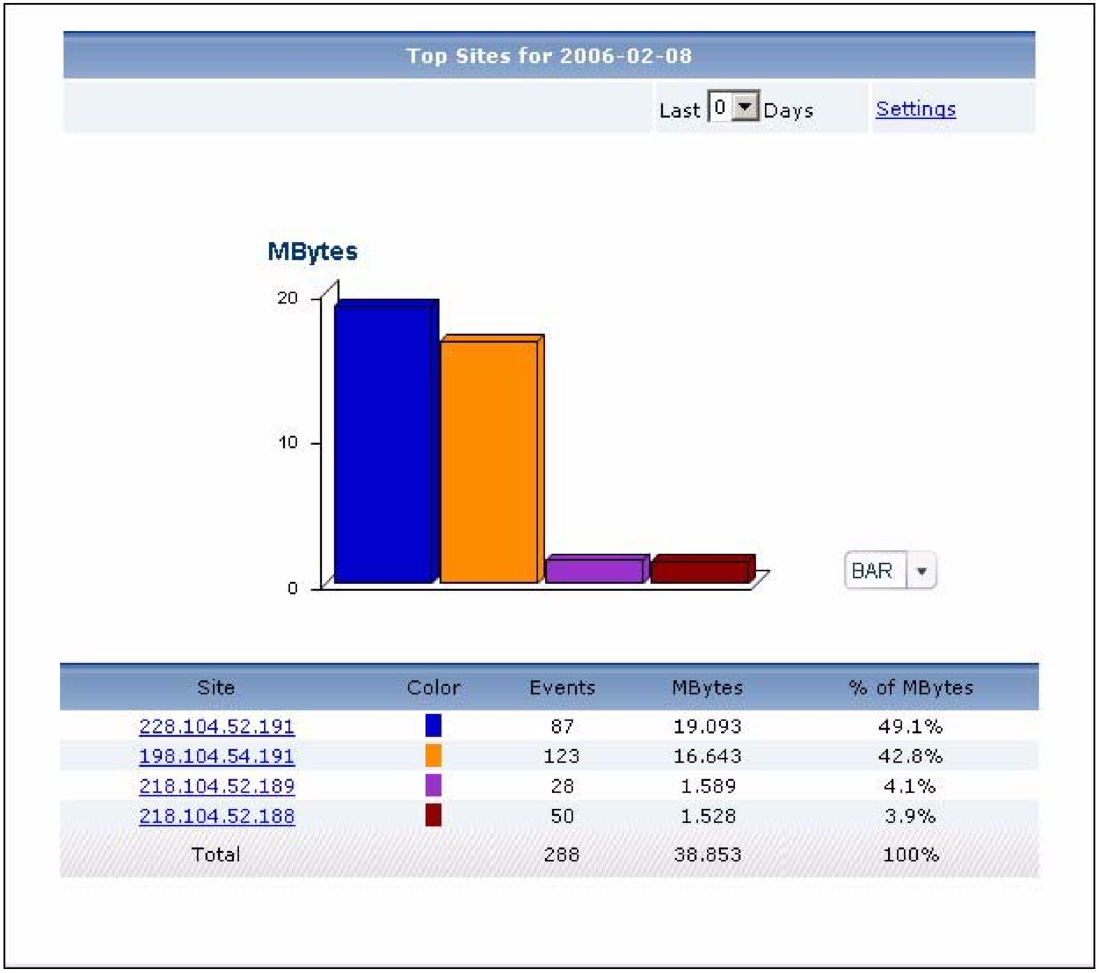
Use this report to look at the top destinations and sources of FTP traffic.

### 33.3.1 Top FTP Sites

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

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

**Figure 211** Traffic > FTP > Top Sites



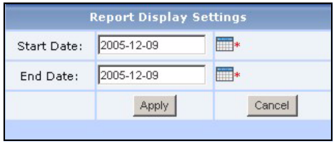
Top Sites for 2006-02-08

Last 0 Days

| Site | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 228.104.52.191 | 🟦 | 87 | 19.093 | 49.1% |
| 198.104.54.191 | 🟧 | 123 | 16.643 | 42.8% |
| 218.104.52.189 | 🟪 | 28 | 1.589 | 4.1% |
| 218.104.52.188 | 🟥 | 50 | 1.528 | 3.9% |
| Total | | 288 | 38.853 | 100% |

Each field is described in the following table.

**Table 179** Traffic > FTP > Top Sites

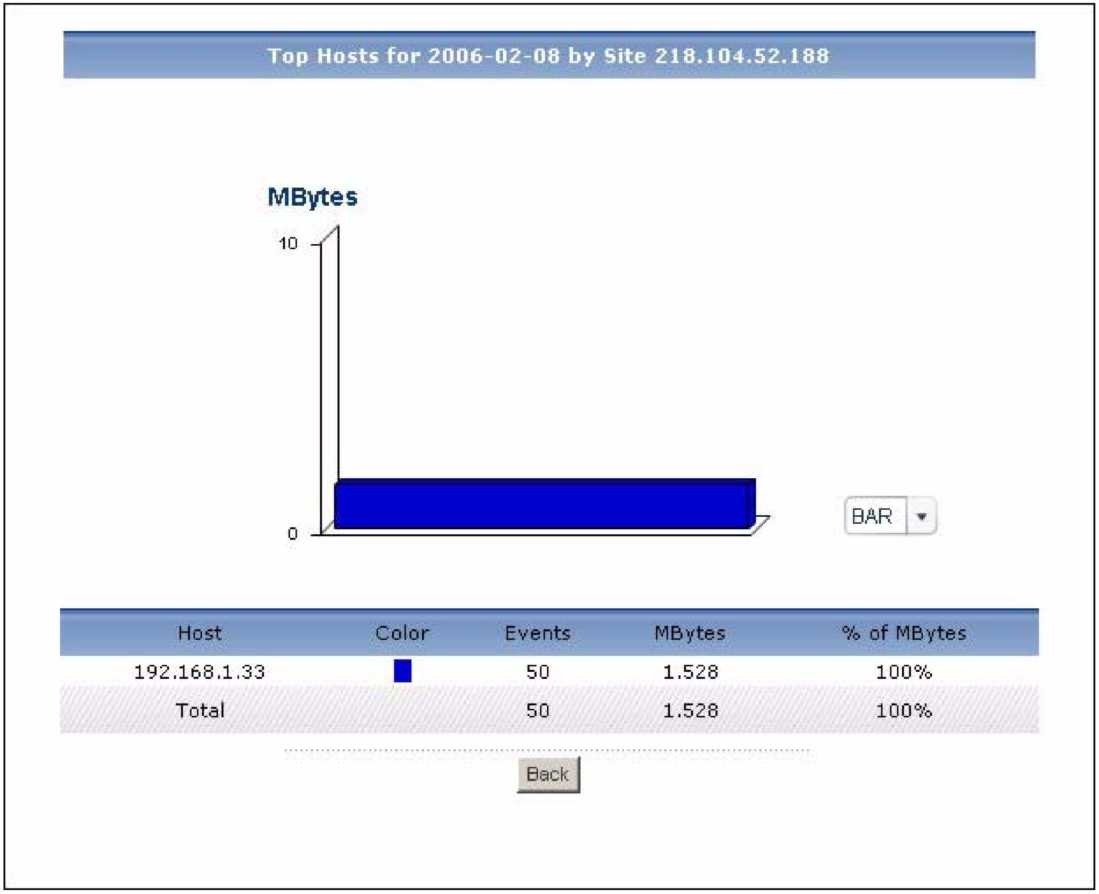
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br> <br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”).<br>Click on a destination to look at the top sources of FTP traffic for the selected destination. The **Top FTP Sites Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events for each destination. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each destination. |
| % of MBytes | This field displays what percentage of FTP traffic the device handled for each destination. |
| Total | This entry displays the totals for the destinations above. |

### 33.3.2 Top FTP Sites Drill-Down

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

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

**Figure 212** Traffic > FTP > Top Sites > Drill-Down



Top Hosts for 2006-02-08 by Site 218.104.52.188

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.33 | 🟦 | 50 | 1.528 | 100% |
| Total | | 50 | 1.528 | 100% |

Each field is described in the following table.

**Table 180** Traffic > FTP > Top Sites > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events from each source to the selected destination. |

**Table 180** Traffic > FTP > Top Sites > Drill-Down (continued)

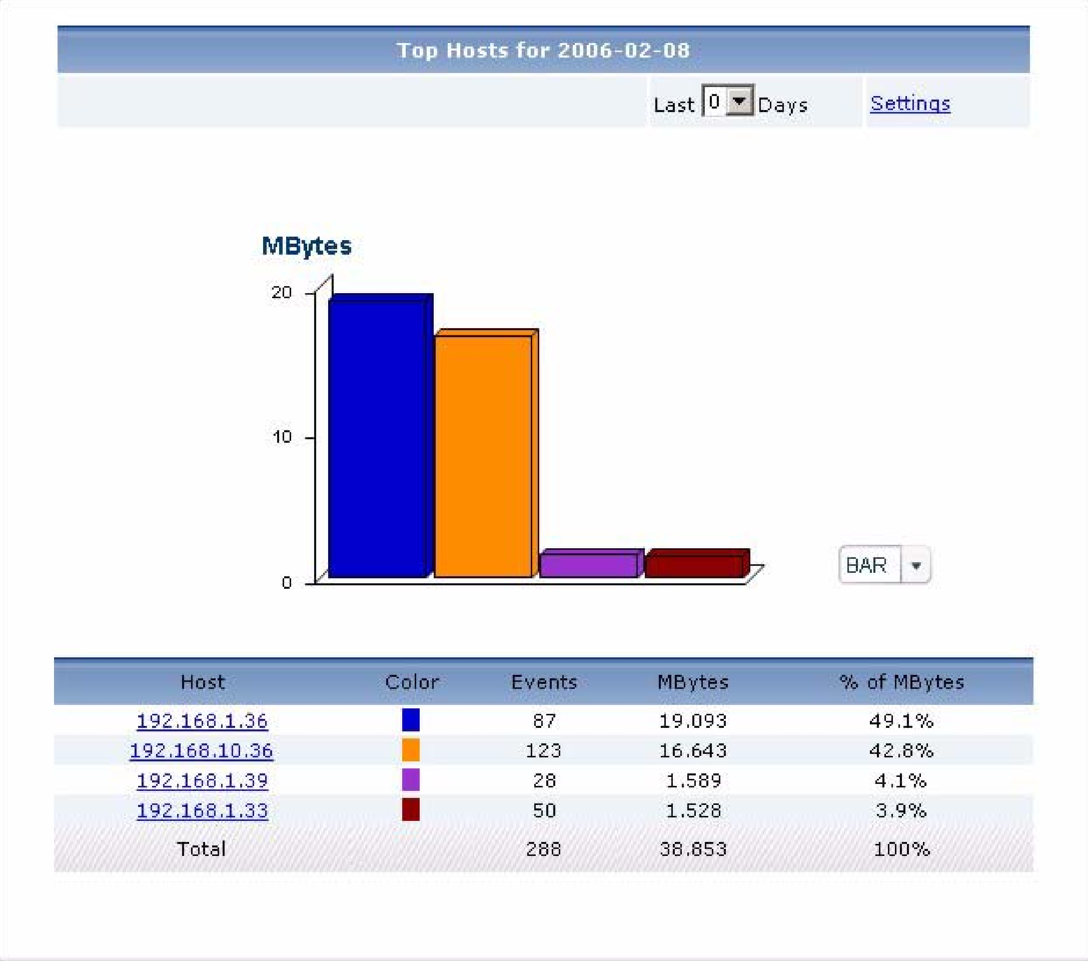
| LABEL | DESCRIPTION |
|---|---|
| MBytes | This field displays how much traffic (in megabytes) was generated from each source to the selected destination. |
| % of MBytes | This field displays what percentage of the selected destination's FTP traffic was generated from each source. |
| Total | This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

## 33.3.3 Top FTP Hosts

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

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

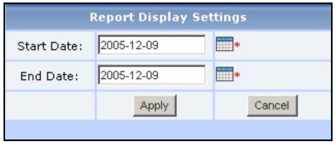
**Figure 213** Traffic > FTP > Top Hosts



| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.36 | 🟦 | 87 | 19.093 | 49.1% |
| 192.168.10.36 | 🟧 | 123 | 16.643 | 42.8% |
| 192.168.1.39 | 🟪 | 28 | 1.589 | 4.1% |
| 192.168.1.33 | 🟥 | 50 | 1.528 | 3.9% |
| Total | | 288 | 38.853 | 100% |

Each field is described in the following table.

**Table 181** Traffic > FTP > Top Hosts

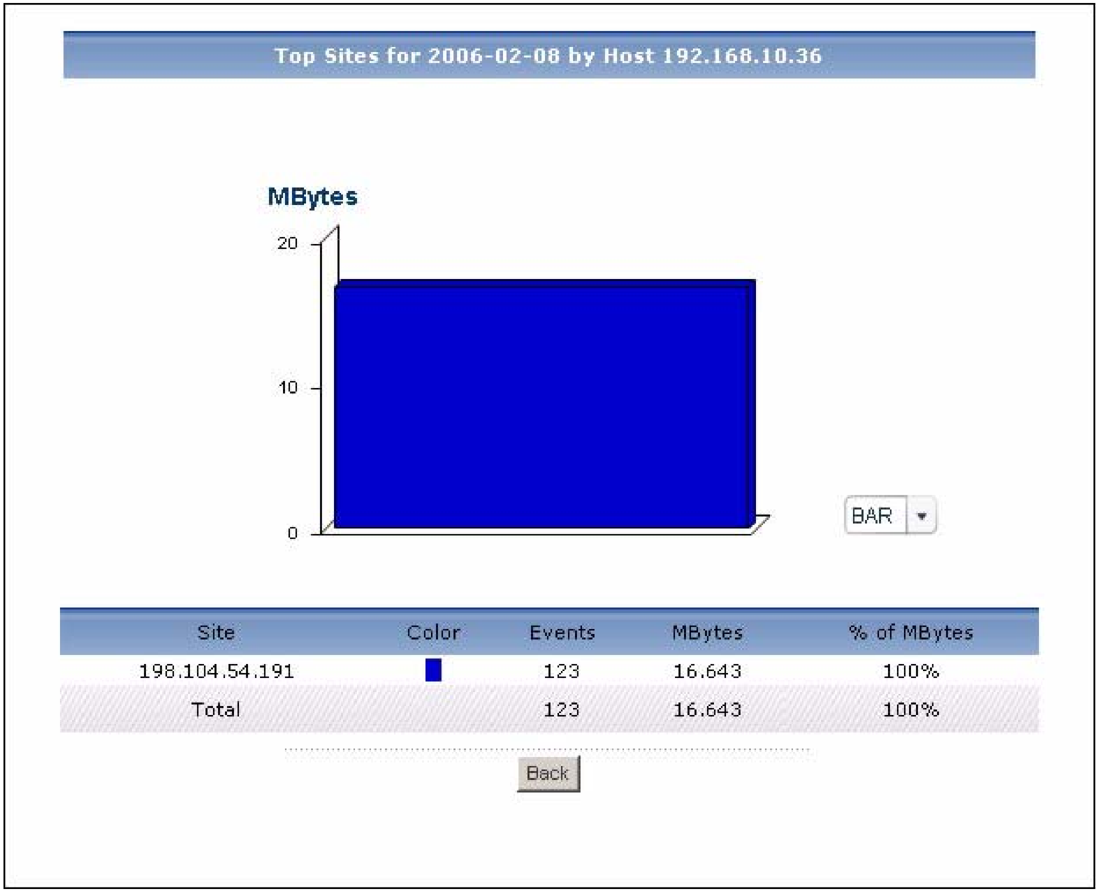
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br> Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of FTP traffic for the selected source. The **Top FTP Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events for each source. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of MBytes | This field displays what percentage of FTP traffic the device handled for each source. |
| Total | This entry displays the totals for the sources above. |

## 33.3.4 Top FTP Hosts Drill-Down

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

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

**Figure 214** Traffic > FTP > Top Hosts > Drill-Down



Top Sites for 2006-02-08 by Host 192.168.10.36

| Site | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 198.104.54.191 | 🟦 | 123 | 16.643 | 100% |
| Total | | 123 | 16.643 | 100% |

Each field is described in the following table.

**Table 182** Traffic > FTP > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), 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. |
| Events | This field displays the number of traffic events from the selected source to each destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from the selected source to each destination. |

**Table 182** Traffic > FTP > Top Hosts > Drill-Down (continued)

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

## 33.4 Mail Traffic

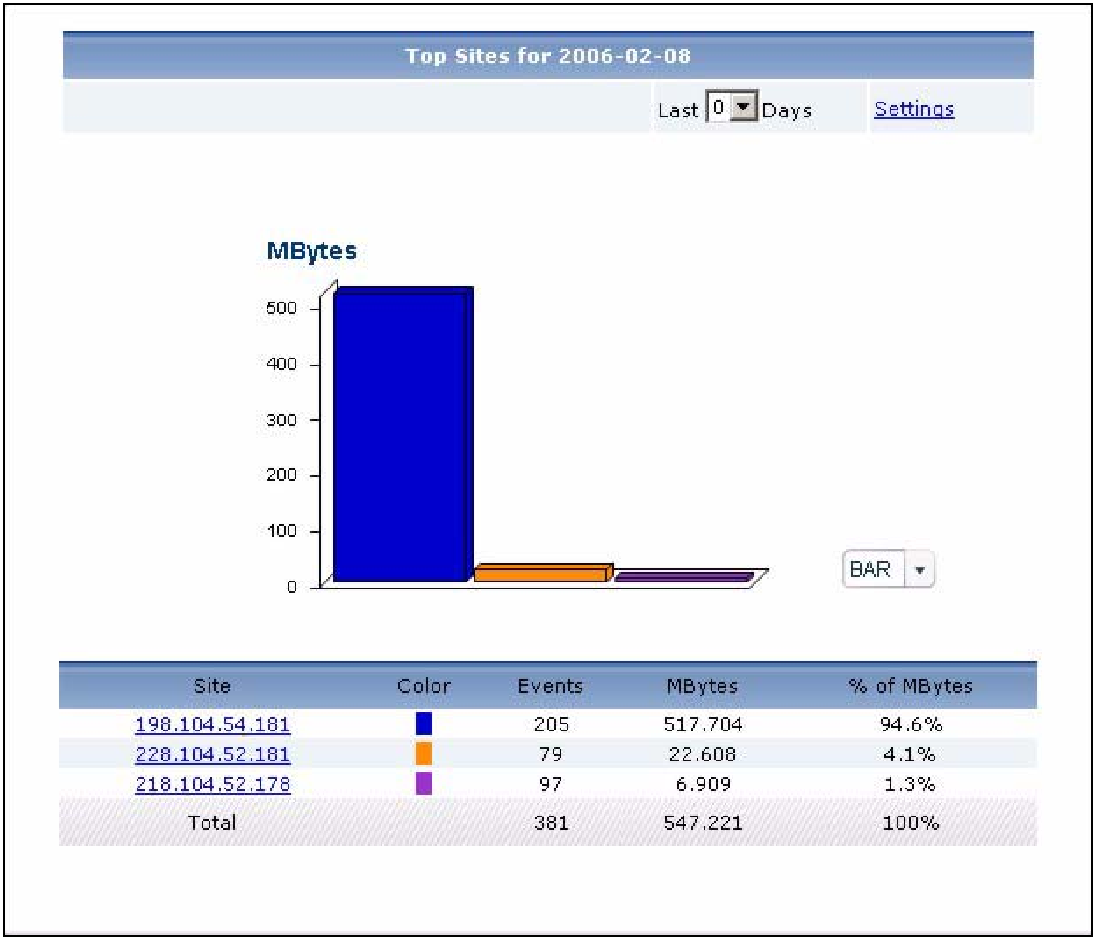
Use this report to look at the top destinations and sources of mail traffic.

### 33.4.1 Top Mail Sites

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

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

**Figure 215** Traffic > MAIL > Top Sites



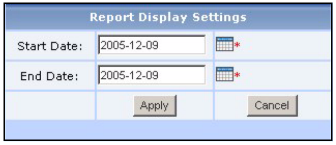
Top Sites for 2006-02-08

Last 0 Days Settings

| Site | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 198.104.54.181 | 🟦 | 205 | 517.704 | 94.6% |
| 228.104.52.181 | 🟧 | 79 | 22.608 | 4.1% |
| 218.104.52.178 | 🟪 | 97 | 6.909 | 1.3% |
| Total | | 381 | 547.221 | 100% |

Each field is described in the following table.

**Table 183** Traffic > MAIL > Top Sites

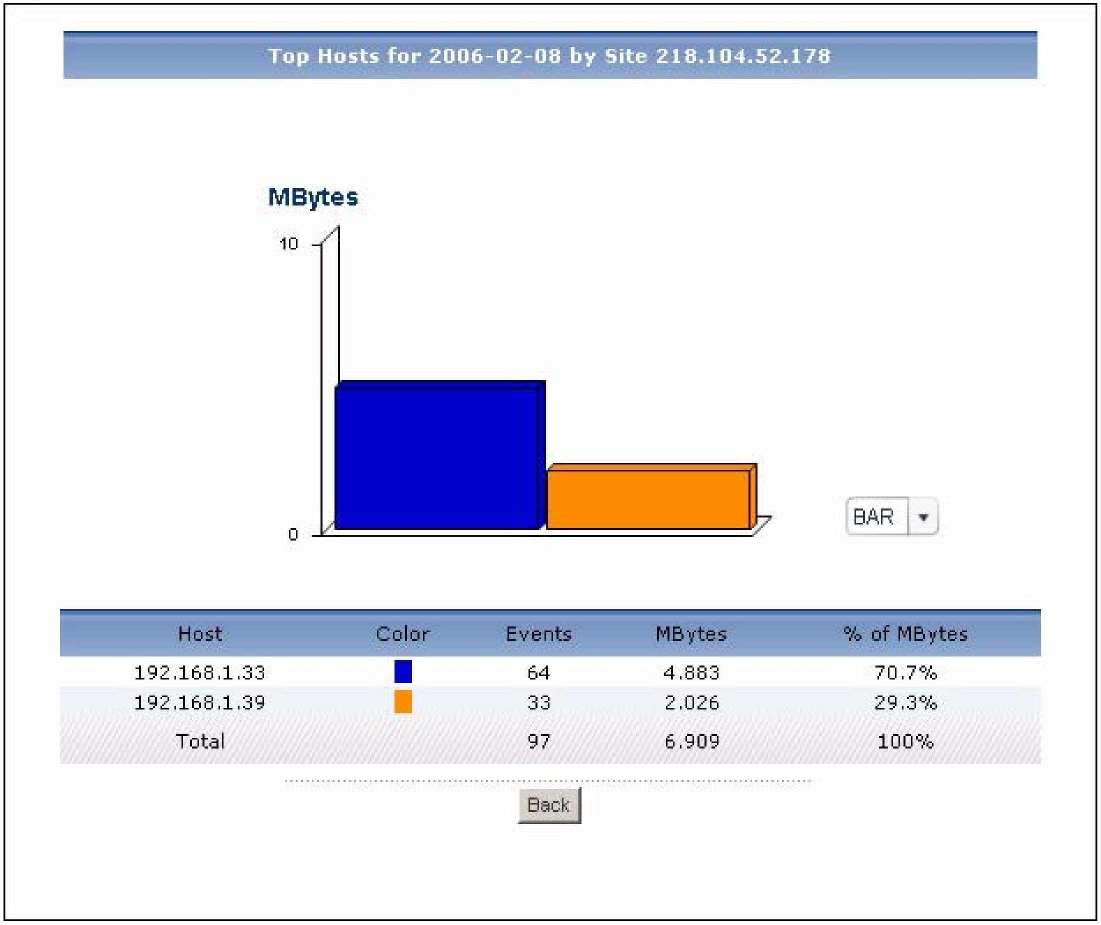
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”).<br>Click on a destination to look at the top sources of mail traffic for the selected destination. The **Top Mail Sites Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events for each destination. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each destination. |
| % of MBytes | This field displays what percentage of mail traffic the device handled for each destination. |
| Total | This entry displays the totals for the destinations above. |

## 33.4.2 Top Mail Sites Drill-Down

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

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

**Figure 216** Traffic > MAIL > Top Sites > Drill-Down



Top Hosts for 2006-02-08 by Site 218.104.52.178

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.1.33 | 🟦 | 64 | 4.883 | 70.7% |
| 192.168.1.39 | 🟧 | 33 | 2.026 | 29.3% |
| Total | | 97 | 6.909 | 100% |

Each field is described in the following table.

**Table 184** Traffic > MAIL > Top Sites > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |

**Table 184** Traffic > MAIL > Top Sites > Drill-Down (continued)

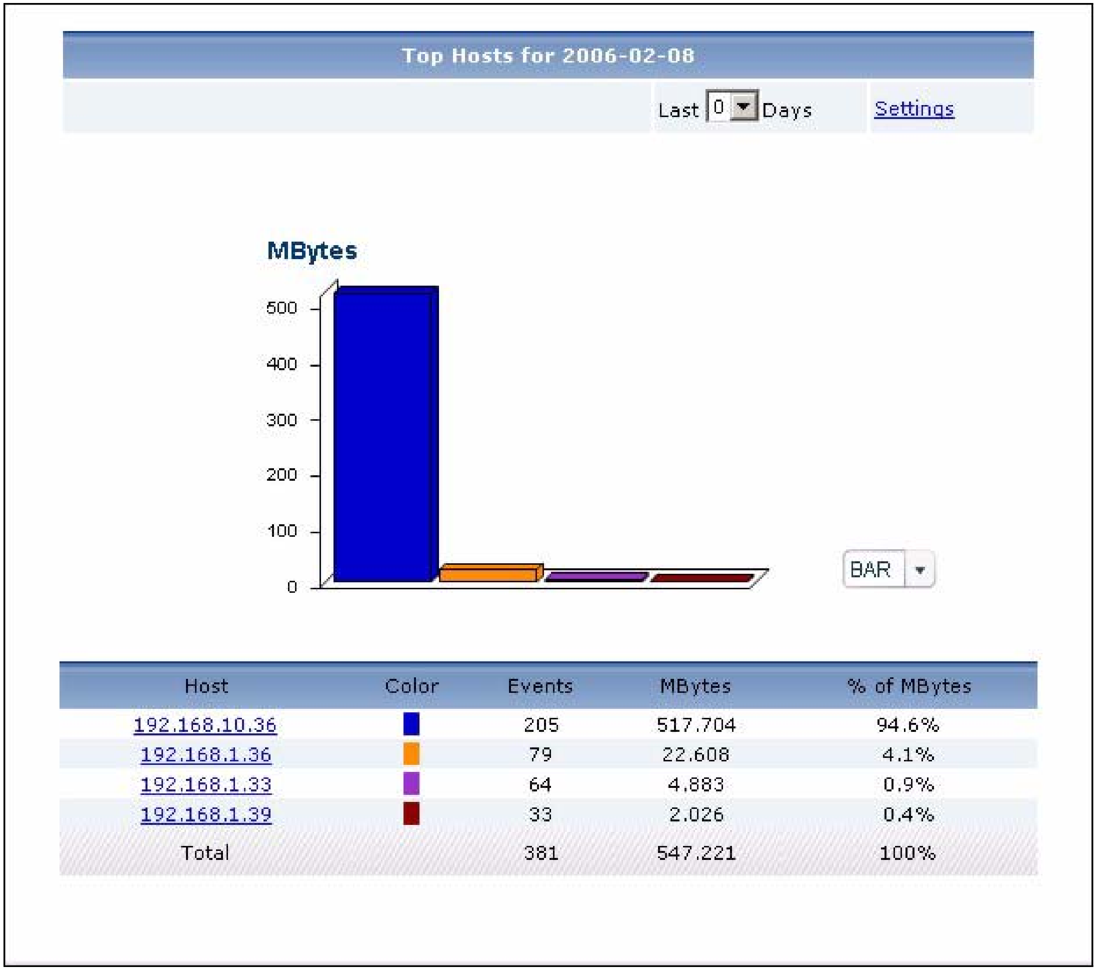
| LABEL | DESCRIPTION |
|---|---|
| Events | This field displays the number of traffic events from each source to the selected destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from each source to the selected destination. |
| % of MBytes | This field displays what percentage of the selected destination’s mail traffic was generated from each source. |
| Total | This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report. |
| Back | Click this to return to the main report. |

## 33.4.3 Top Mail Hosts

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

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

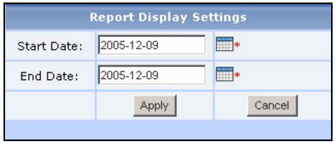
**Figure 217** Traffic > MAIL > Top Hosts



| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.10.36 | 🟦 | 205 | 517.704 | 94.6% |
| 192.168.1.36 | 🟧 | 79 | 22.608 | 4.1% |
| 192.168.1.33 | 🟪 | 64 | 4.883 | 0.9% |
| 192.168.1.39 | 🟥 | 33 | 2.026 | 0.4% |
| Total | | 381 | 547.221 | 100% |

Each field is described in the following table.

**Table 185** Traffic > MAIL > Top Hosts

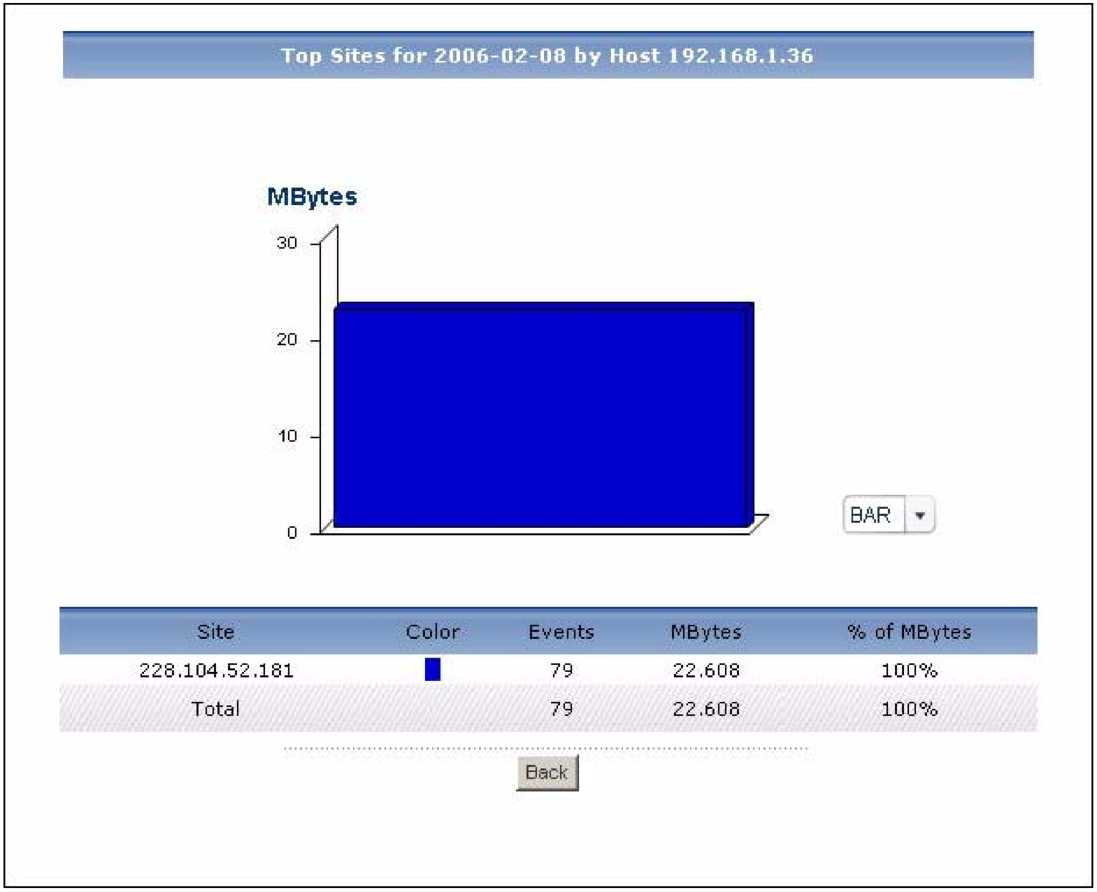
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of mail traffic for the selected source. The **Top Mail Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events for each source. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of MBytes | This field displays what percentage of mail traffic the device handled for each source. |
| Total | This entry displays the totals for the sources above. |

## 33.4.4 Top Mail Hosts Drill-Down

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

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

**Figure 218** Traffic > MAIL > Top Hosts > Drill-Down



Top Sites for 2006-02-08 by Host 192.168.1.36

| Site | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 228.104.52.181 | 🟦 | 79 | 22.608 | 100% |
| Total | | 79 | 22.608 | 100% |

Each field is described in the following table.

**Table 186** Traffic > MAIL > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), 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. |
| Events | This field displays the number of traffic events from the selected source to each destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from the selected source to each destination. |

**Table 186** Traffic > MAIL > Top Hosts > Drill-Down (continued)

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

## 33.5 VPN Traffic

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

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

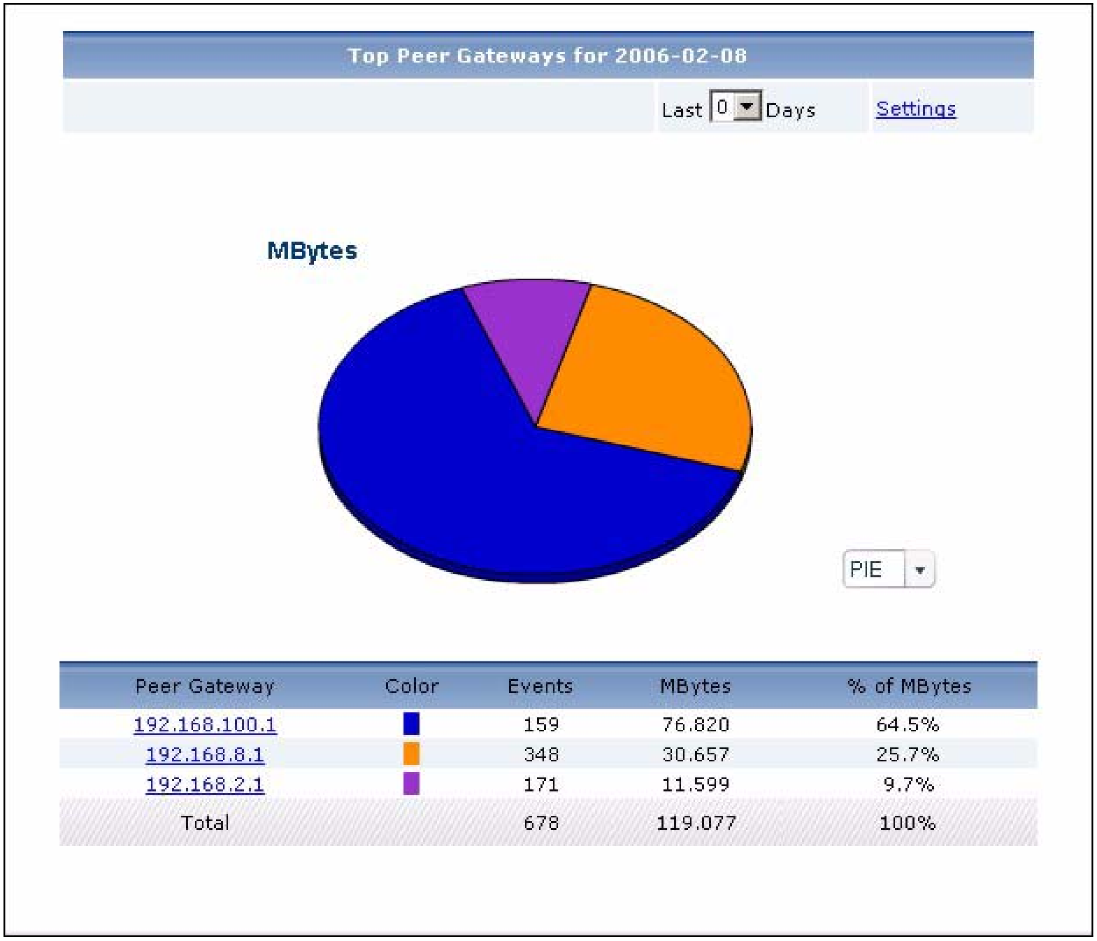
### 33.5.1 Top VPN Peer Gateways

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

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

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

**Figure 219** Traffic > VPN > Top Peer Gateways



Top Peer Gateways for 2006-02-08

Last 0 Days Settings

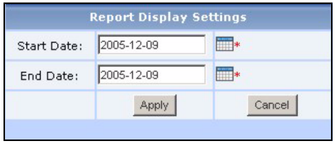
| Peer Gateway | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.100.1 | 🟦 | 159 | 76.820 | 64.5% |
| 192.168.8.1 | 🟧 | 348 | 30.657 | 25.7% |
| 192.168.2.1 | 🟪 | 171 | 11.599 | 9.7% |
| Total | | 678 | 119.077 | 100% |

Each field is described in the following table.

**Table 187** Traffic > VPN > Top Peer Gateways

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

**Table 187** Traffic > VPN > Top Peer Gateways (continued)

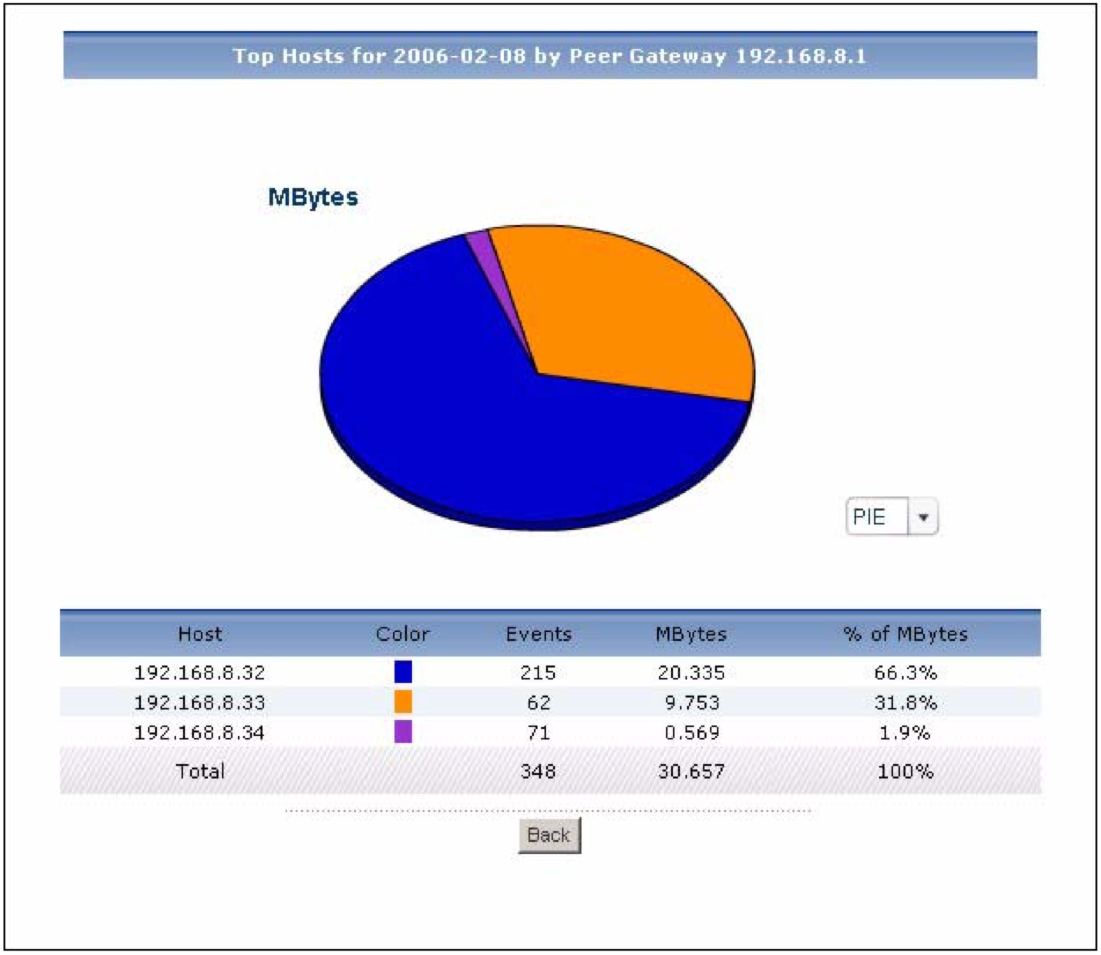
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Peer Gateway | This field displays the top destinations of VPN traffic in the selected device, sorted by the amount of traffic for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed.<br>Each destination is identified by the IP address of the remote gateway. Click on a destination to look at the top sources of VPN traffic for the selected destination. The **Top VPN Peer Gateways Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events for each destination. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each destination. |
| % of MBytes | This field displays what percentage of VPN traffic the device handled for each destination. |
| Total | This entry displays the totals for the destinations above. |

## 33.5.2 Top VPN Peer Gateways Drill-Down

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

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

**Figure 220** Traffic > VPN > Top Peer Gateways > Drill-Down



Top Hosts for 2006-02-08 by Peer Gateway 192.168.8.1

| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.8.32 | 🟦 | 215 | 20.335 | 66.3% |
| 192.168.8.33 | 🟧 | 62 | 9.753 | 31.8% |
| 192.168.8.34 | 🟪 | 71 | 0.569 | 1.9% |
| Total |  | 348 | 30.657 | 100% |

Each field is described in the following table.

**Table 188** Traffic > VPN > Top Peer Gateways > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Host | This field displays the top sources of VPN traffic to the selected destination, sorted by the amount of traffic attributed to each one.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events from each source to the selected destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from each source to the selected destination. |

**Table 188** Traffic > VPN > Top Peer Gateways > Drill-Down (continued)

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

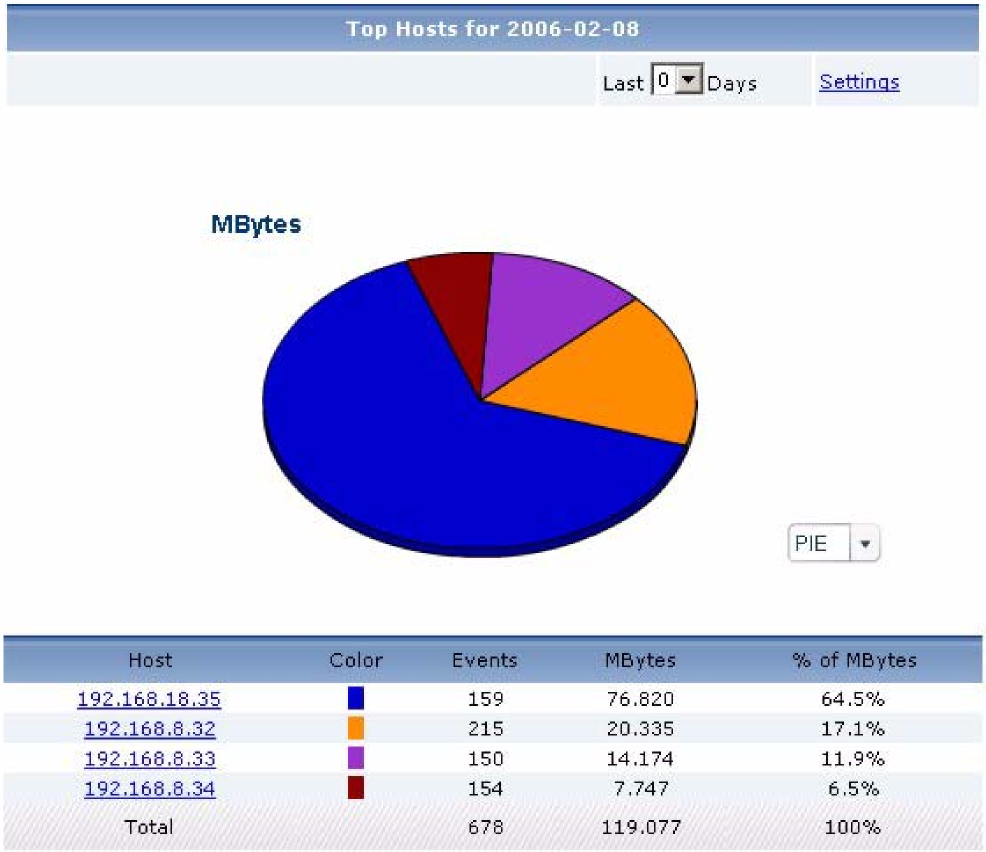
### 33.5.3 Top VPN Hosts

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

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

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

**Figure 221** Traffic > VPN > Top Hosts



Top Hosts for 2006-02-08

Last 0 Days Settings

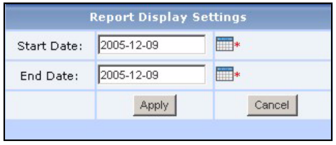
| Host | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.18.35 | 🟦 | 159 | 76.820 | 64.5% |
| 192.168.8.32 | 🟧 | 215 | 20.335 | 17.1% |
| 192.168.8.33 | 🟪 | 150 | 14.174 | 11.9% |
| 192.168.8.34 | 🟥 | 154 | 7.747 | 6.5% |
| Total | | 678 | 119.077 | 100% |

Each field is described in the following table.

**Table 189** Traffic > VPN > Top Hosts

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

**Table 189** Traffic > VPN > Top Hosts (continued)

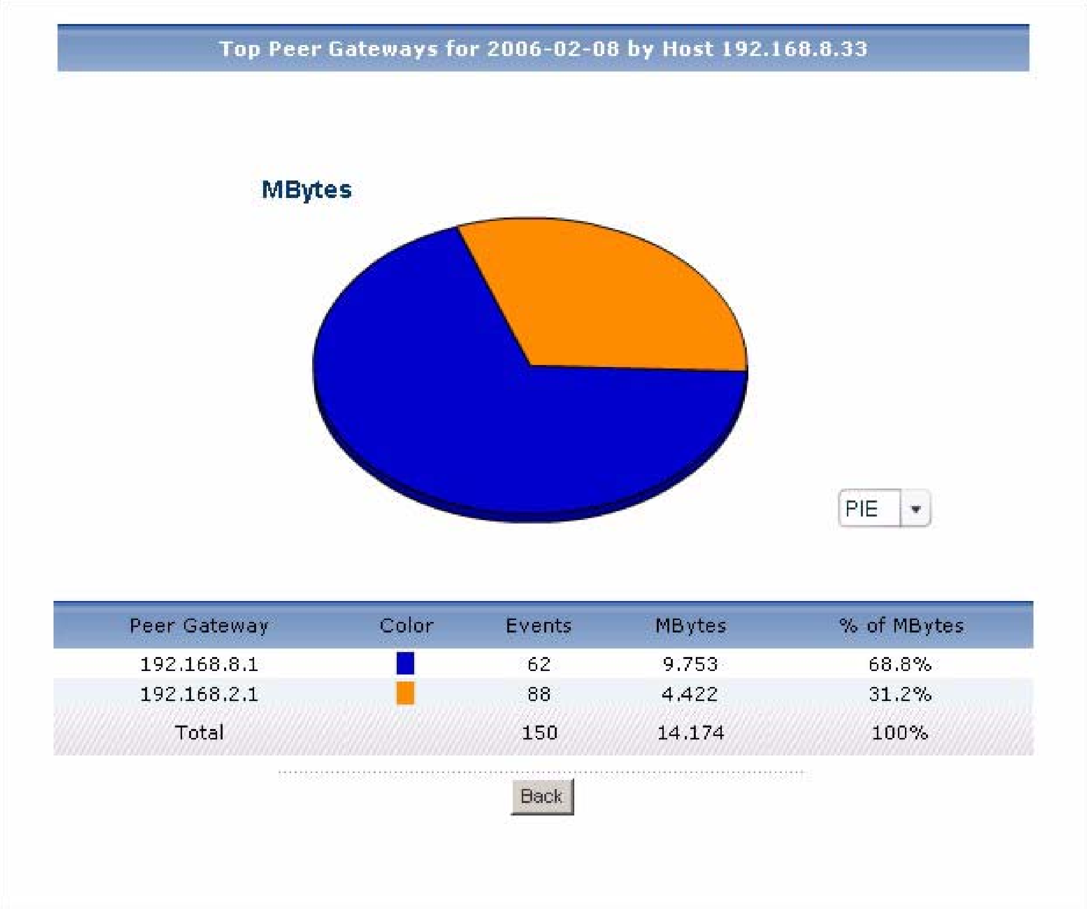
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Host | This field displays the top sources of VPN traffic 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.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of VPN traffic for the selected source. The **Top VPN Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events for each source. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of MBytes | This field displays what percentage of VPN traffic the device handled for each source. |
| Total | This entry displays the totals for the sources above. |

## 33.5.4 Top VPN Hosts Drill-Down

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

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

**Figure 222** Traffic > VPN > Top Hosts > Drill-Down



Top Peer Gateways for 2006-02-08 by Host 192.168.8.33

| Peer Gateway | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 192.168.8.1 | 🟦 | 62 | 9.753 | 68.8% |
| 192.168.2.1 | 🟧 | 88 | 4.422 | 31.2% |
| Total | | 150 | 14.174 | 100% |

Each field is described in the following table.

**Table 190** Traffic > VPN > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Peer Gateway | This field displays the top destinations of VPN traffic from the selected source, sorted by the amount of traffic attributed to each one.<br>Each destination is identified by its IP address. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events from the selected source to each destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from the selected source to each destination. |
| % of MBytes | This field displays what percentage of the selected source’s VPN traffic was sent to each destination. |

**Table 190** Traffic > VPN > Top Hosts > Drill-Down (continued)

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

## 33.6 Other Traffic

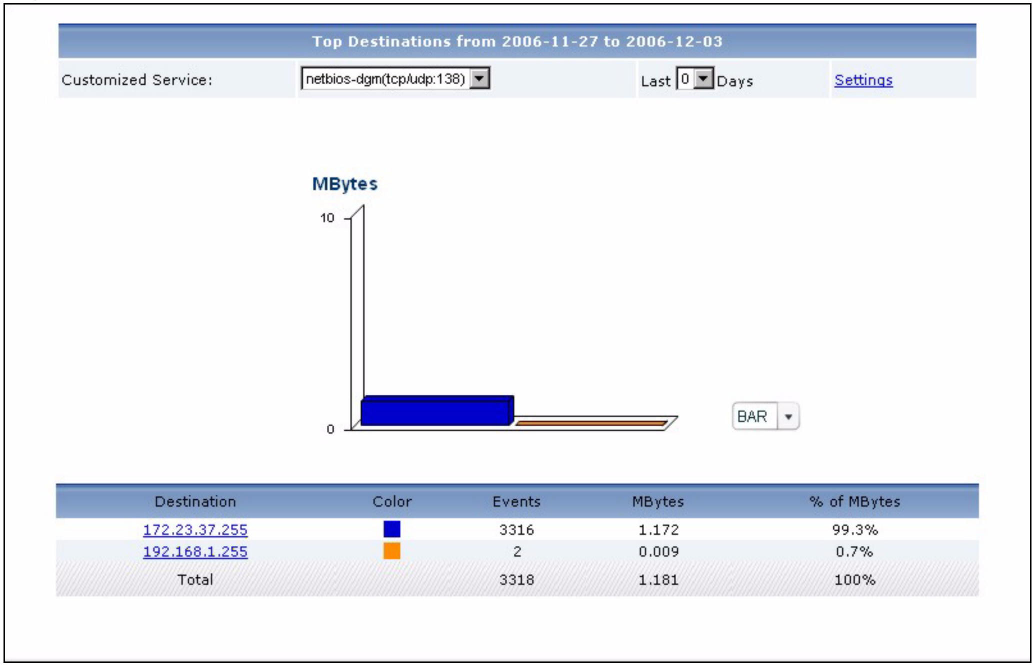
Use these reports to look at the top sources and destinations of any kind of traffic.

### 33.6.1 Top Destinations of Other Traffic

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

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

**Figure 223** Traffic > Customization > Top Destinations



Top Destinations from 2006-11-27 to 2006-12-03

Customized Service: netbios-dgm(tcp/udp:138) Last 0 Days Settings

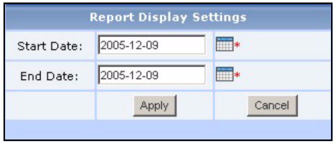
| Destination | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 172.23.37.255 | 🟦 | 3316 | 1.172 | 99.3% |
| 192.168.1.255 | 🟧 | 2 | 0.009 | 0.7% |
| Total | | 3318 | 1.181 | 100% |

Each field is described in the following table.

**Table 191** Traffic > Customization > Top Destinations

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Customized Service | Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the **Customized Service Setting** screen. See Section 26.8.5 on page 312. |

**Table 191** Traffic > Customization > Top Destinations (continued)

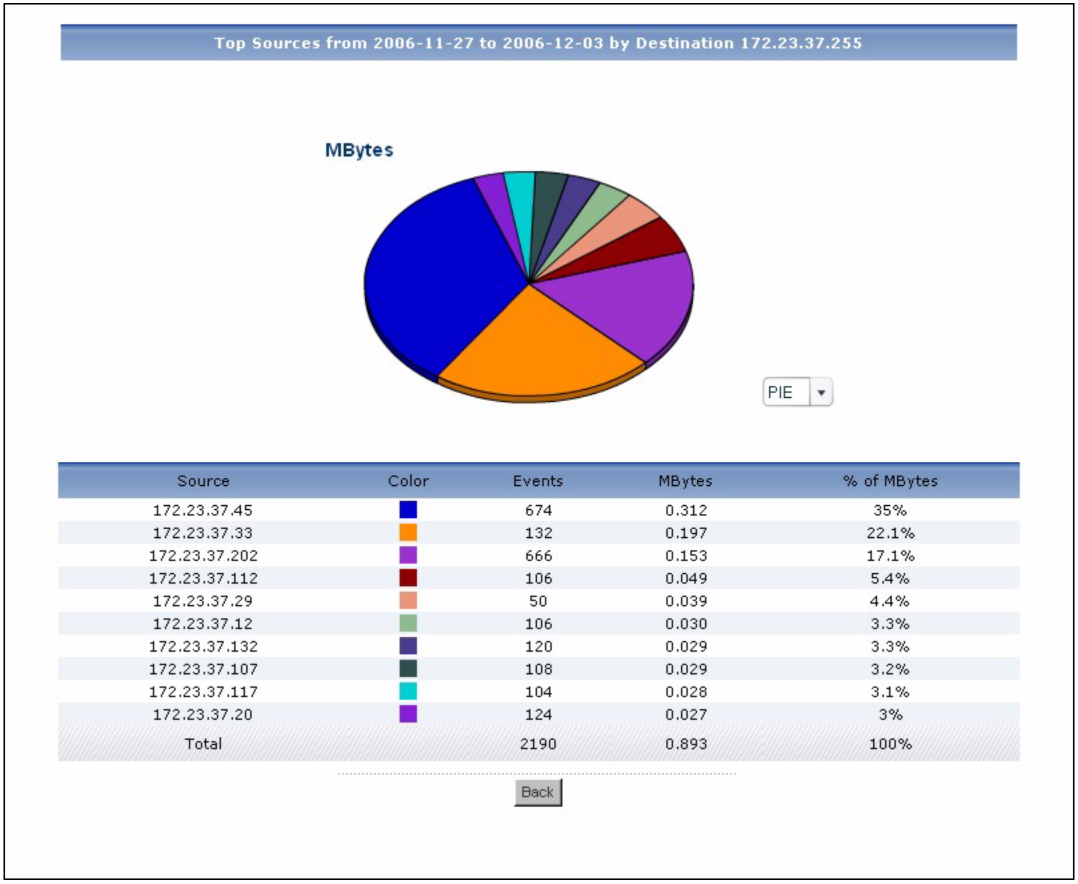
| LABEL | DESCRIPTION |
|---|---|
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. Click on a destination to look at the top sources of the selected service's traffic for the selected destination. The **Top Sites for Other Services Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events for each destination. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each destination. |
| % of MBytes | This field displays what percentage of the selected service's traffic the device handled for each destination. |
| Total | This entry displays the totals for the destinations above. |

## 33.6.2 Top Destinations of Other Traffic Drill-Down

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

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

**Figure 224** Traffic > Customization > Top Destinations > Drill-Down



Top Sources from 2006-11-27 to 2006-12-03 by Destination 172.23.37.255

| Source | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 172.23.37.45 | 🟦 | 674 | 0.312 | 35% |
| 172.23.37.33 | 🟧 | 132 | 0.197 | 22.1% |
| 172.23.37.202 | 🟪 | 666 | 0.153 | 17.1% |
| 172.23.37.112 | 🟥 | 106 | 0.049 | 5.4% |
| 172.23.37.29 | 🟧 | 50 | 0.039 | 4.4% |
| 172.23.37.12 | 🟩 | 106 | 0.030 | 3.3% |
| 172.23.37.132 | 🟪 | 120 | 0.029 | 3.3% |
| 172.23.37.107 | ⬛ | 108 | 0.029 | 3.2% |
| 172.23.37.117 | 🟦 | 104 | 0.028 | 3.1% |
| 172.23.37.20 | 🟪 | 124 | 0.027 | 3% |
| Total | | 2190 | 0.893 | 100% |

Each field is described in the following table.

**Table 192** Traffic > Customization > Top Destinations > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 service's traffic to the selected destination, sorted by the amount of traffic attributed to each one.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events from each source to the selected destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from each source to the selected destination. |
| % of MBytes | This field displays what percentage of the selected destination's traffic using the selected service was generated from each source. |

**Table 192** Traffic > Customization > Top Destinations > Drill-Down (continued)

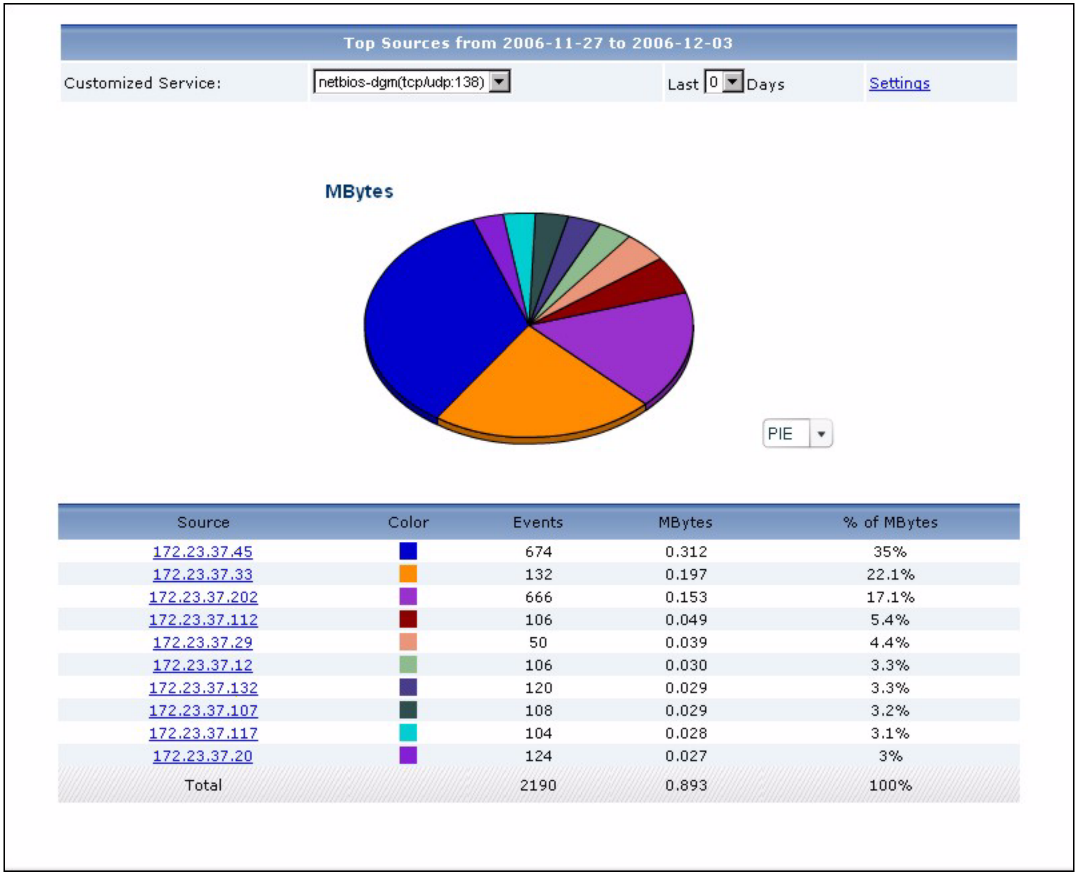
| LABEL | DESCRIPTION |
|---|---|
| Total | This entry displays the totals for the sources above. If the number of sources of traffic to the selected destination is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report.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

## 33.6.3 Top Sources of Other Traffic

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

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

**Figure 225** Traffic > Customization > Top Sources



Top Sources from 2006-11-27 to 2006-12-03

Customized Service: netbios-dgm(tcp/udp:138)

Last 0 Days

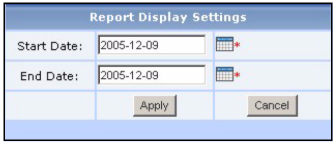
| Source | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 172.23.37.45 | 🟦 | 674 | 0.312 | 35% |
| 172.23.37.33 | 🟧 | 132 | 0.197 | 22.1% |
| 172.23.37.202 | 🟪 | 666 | 0.153 | 17.1% |
| 172.23.37.112 | 🟥 | 106 | 0.049 | 5.4% |
| 172.23.37.29 | 🟧 | 50 | 0.039 | 4.4% |
| 172.23.37.12 | 🟩 | 106 | 0.030 | 3.3% |
| 172.23.37.132 | 🟪 | 120 | 0.029 | 3.3% |
| 172.23.37.107 | ⬛ | 108 | 0.029 | 3.2% |
| 172.23.37.117 | 🟦 | 104 | 0.028 | 3.1% |
| 172.23.37.20 | 🟪 | 124 | 0.027 | 3% |
| Total | | 2190 | 0.893 | 100% |

Each field is described in the following table.

**Table 193** Traffic > Customization > Top Sources

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Customized Service | Select the service whose traffic you want to view. You can add, edit, or remove the services in this drop-down list in the **Customized Service Setting** screen. See Section 26.8.5 on page 312. |

**Table 193** Traffic > Customization > Top Sources (continued)

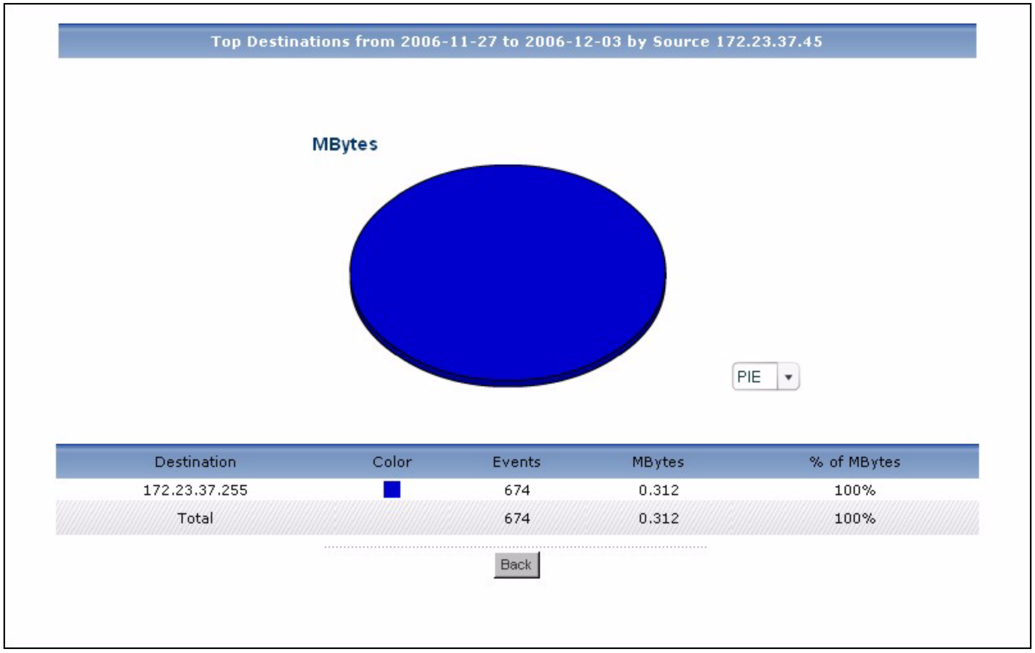
| LABEL | DESCRIPTION |
|---|---|
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 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.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of the selected service’s traffic for the selected source. The **Top Hosts for Other Services Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Events | This field displays the number of traffic events for each source. |
| MBytes | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of MBytes | This field displays what percentage of the selected service’s traffic the device handled for each source. |
| Total | This entry displays the totals for the sources above. |

## 33.6.4 Top Sources of Other Traffic Drill-Down

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

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

**Figure 226** Traffic > Customization > Top Sources > Drill-Down



Top Destinations from 2006-11-27 to 2006-12-03 by Source 172.23.37.45

| Destination | Color | Events | MBytes | % of MBytes |
|---|---|---|---|---|
| 172.23.37.255 | 🟦 | 674 | 0.312 | 100% |
| Total | | 674 | 0.312 | 100% |

Each field is described in the following table.

**Table 194** Traffic > Customization > Top Sources > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its IP address. |
| Color | This field displays what color represents each destination in the graph. |
| Events | This field displays the number of traffic events from the selected source to each destination. |
| MBytes | This field displays how much traffic (in megabytes) was generated from the selected source to each destination. |
| % of MBytes | This field displays what percentage of the selected source's traffic using the selected service was sent to each destination. |
| Total | This entry displays the totals for the destinations above. If the number of destinations of traffic from the selected source is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report. |
| Back | Click this to return to the main report. |

# 34

# Network Attack

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

## 34.1 Attack

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

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

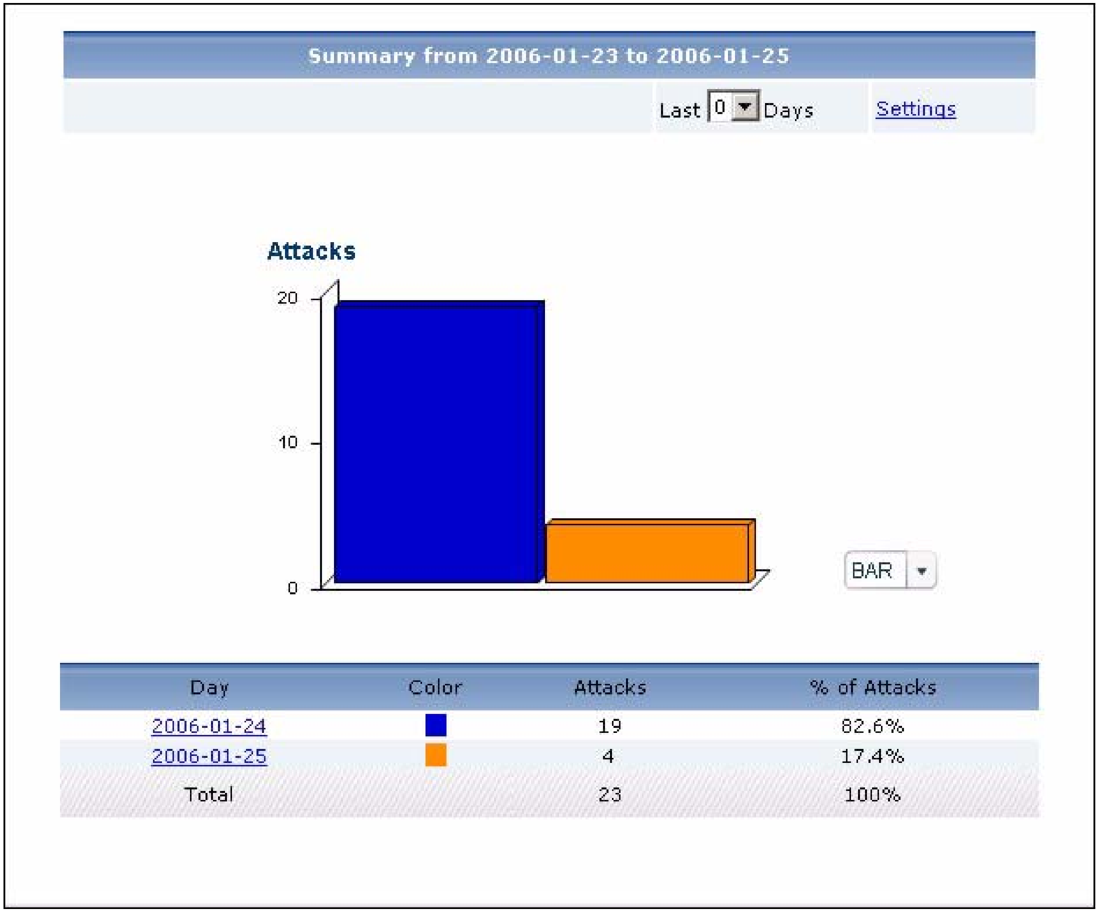
### 34.1.1 Attack Summary

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

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

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

**Figure 227** Network Attack > Attack > Summary



Summary from 2006-01-23 to 2006-01-25

Last 0 Days Settings

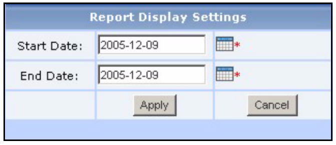
| Day | Color | Attacks | % of Attacks |
|---|---|---|---|
| 2006-01-24 | 🟦 | 19 | 82.6% |
| 2006-01-25 | 🟧 | 4 | 17.4% |
| Total |  | 23 | 100% |

Each field is described in the following table.

**Table 195** Network Attack > Attack > Summary

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

**Table 195** Network Attack > Attack > Summary (continued)

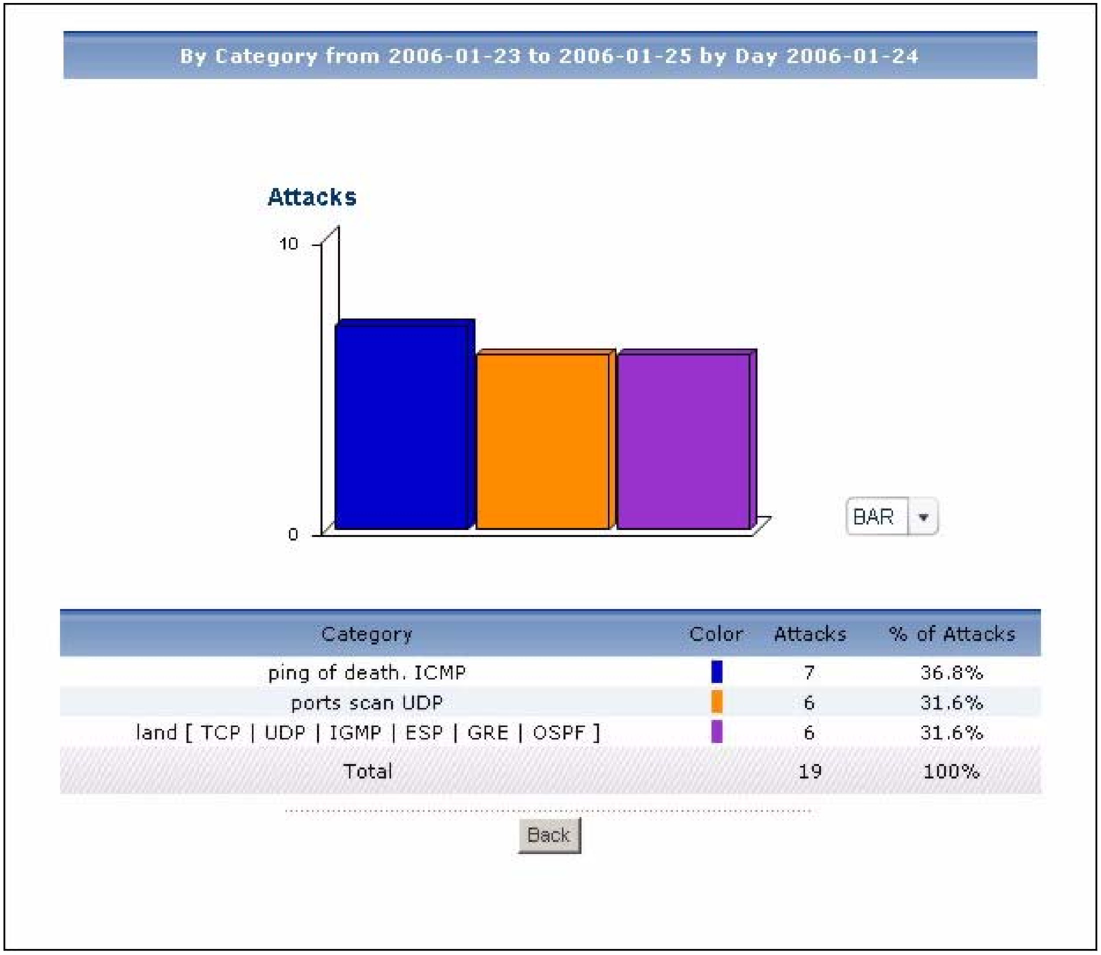
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top categories of attacks in the selected time interval. The **Attack Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| Attacks | This field displays the number of DoS attacks in the selected time interval. |
| % of Attacks | This field displays what percentage of all DoS attacks was handled in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

### 34.1.2 Attack Summary Drill-Down

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

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

Figure 228 Network Attack > Attack > Summary > Drill-Down



By Category from 2006-01-23 to 2006-01-25 by Day 2006-01-24

| Category | Color | Attacks | % of Attacks |
|---|---|---|---|
| ping of death, ICMP | 🟦 | 7 | 36.8% |
| ports scan UDP | 🟧 | 6 | 31.6% |
| land [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | 🟪 | 6 | 31.6% |
| Total | | 19 | 100% |

Each field is described in the following table.

Table 196 Network Attack > Attack > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Category | This field displays the top categories of DoS attacks in the selected time interval, sorted by the number of attacks by each one. |
| Color | This field displays what color represents each category in the graph. |
| Attacks | This field displays how many DoS attacks by each category occurred in the selected time interval. |
| % of Attacks | This field displays what percentage of all DoS attacks in the selected time interval comes from each category. |

**Table 196** Network Attack > Attack > Summary > Drill-Down (continued)

| 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. |

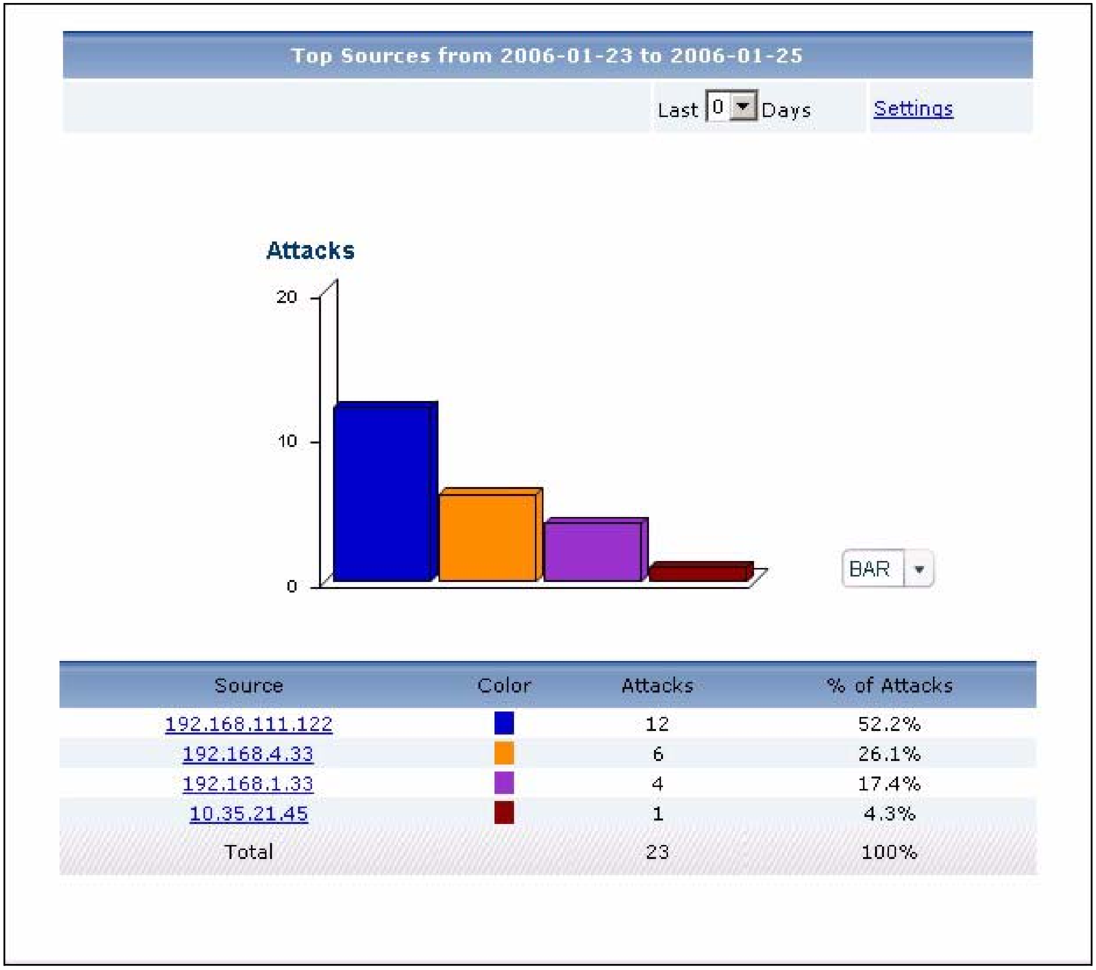
### 34.1.3 Top Attack Sources

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

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

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

**Figure 229** Network Attack > Attack > Top Sources



Top Sources from 2006-01-23 to 2006-01-25

Last 0 Days Settings

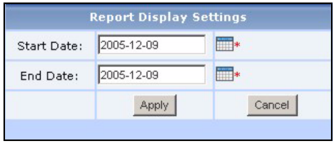
| Source | Color | Attacks | % of Attacks |
|---|---|---|---|
| 192.168.111.122 | 🟦 | 12 | 52.2% |
| 192.168.4.33 | 🟧 | 6 | 26.1% |
| 192.168.1.33 | 🟪 | 4 | 17.4% |
| 10.35.21.45 | 🟥 | 1 | 4.3% |
| Total | | 23 | 100% |

Each field is described in the following table.

**Table 197** Network Attack > Attack > Top Sources

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

**Table 197** Network Attack > Attack > Top Sources (continued)

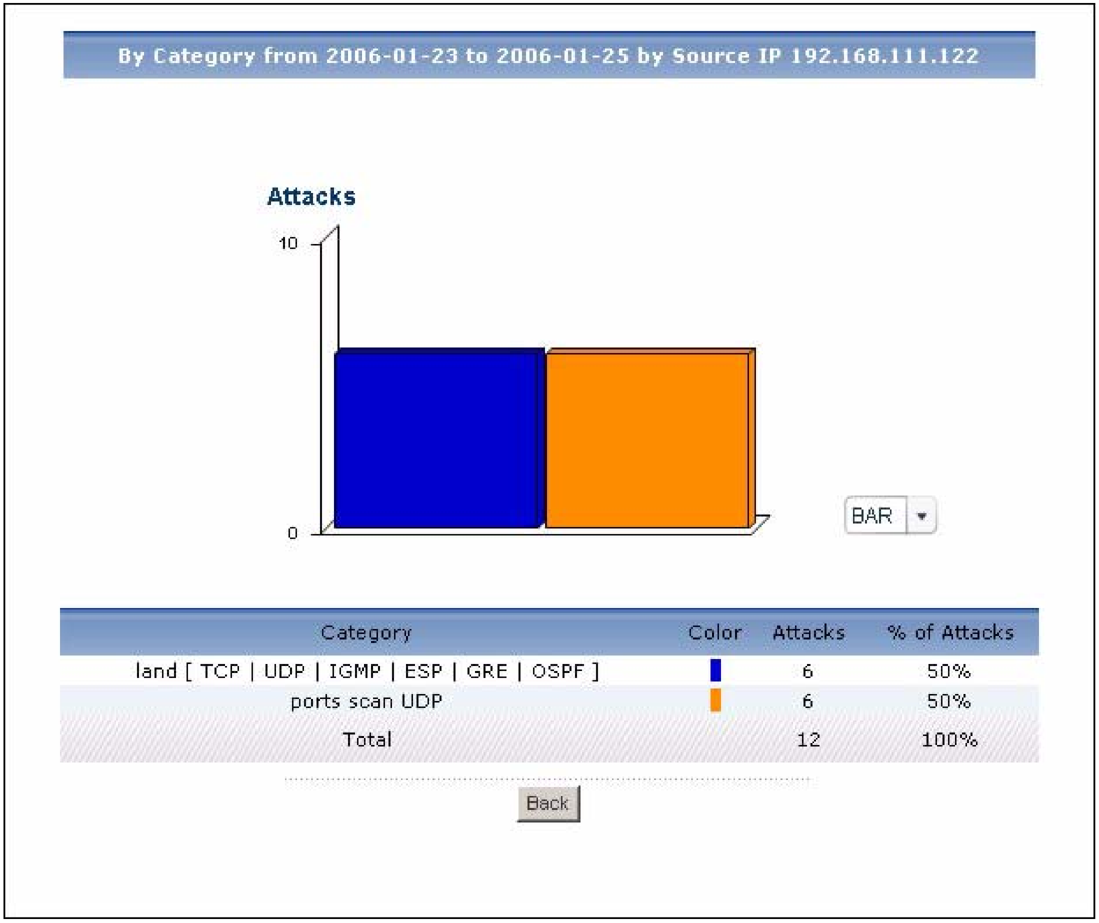
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”).<br>Click on a source to look at the top categories of DoS attacks by the selected source. The **Top Attack Sources Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Attacks | This field displays the number of DoS attacks by each source. |
| % of Attacks | This field displays what percentage of all DoS attacks was made by each source. |
| Total | This entry displays the totals for the sources above. |

## 34.1.4 Top Attack Sources Drill-Down

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

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

**Figure 230** Network Attack > Attack > Top Sources > Drill-Down



By Category from 2006-01-23 to 2006-01-25 by Source IP 192.168.111.122

| Category | Color | Attacks | % of Attacks |
|---|---|---|---|
| land [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | 🟦 | 6 | 50% |
| ports scan UDP | 🟧 | 6 | 50% |
| Total | | 12 | 100% |

Each field is described in the following table.

**Table 198** Network Attack > Attack > Top Sources > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Category | This field displays the top categories of DoS attacks from the selected source, sorted by the number of attacks by each one. |
| Color | This field displays what color represents each category in the graph. |
| Attacks | This field displays the number of DoS attacks in each category that occurred from the selected source. |
| % of Attacks | This field displays what percentage of all DoS attacks from the selected source comes from each category. |

**Table 198** Network Attack > Attack > Top Sources > Drill-Down (continued)

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

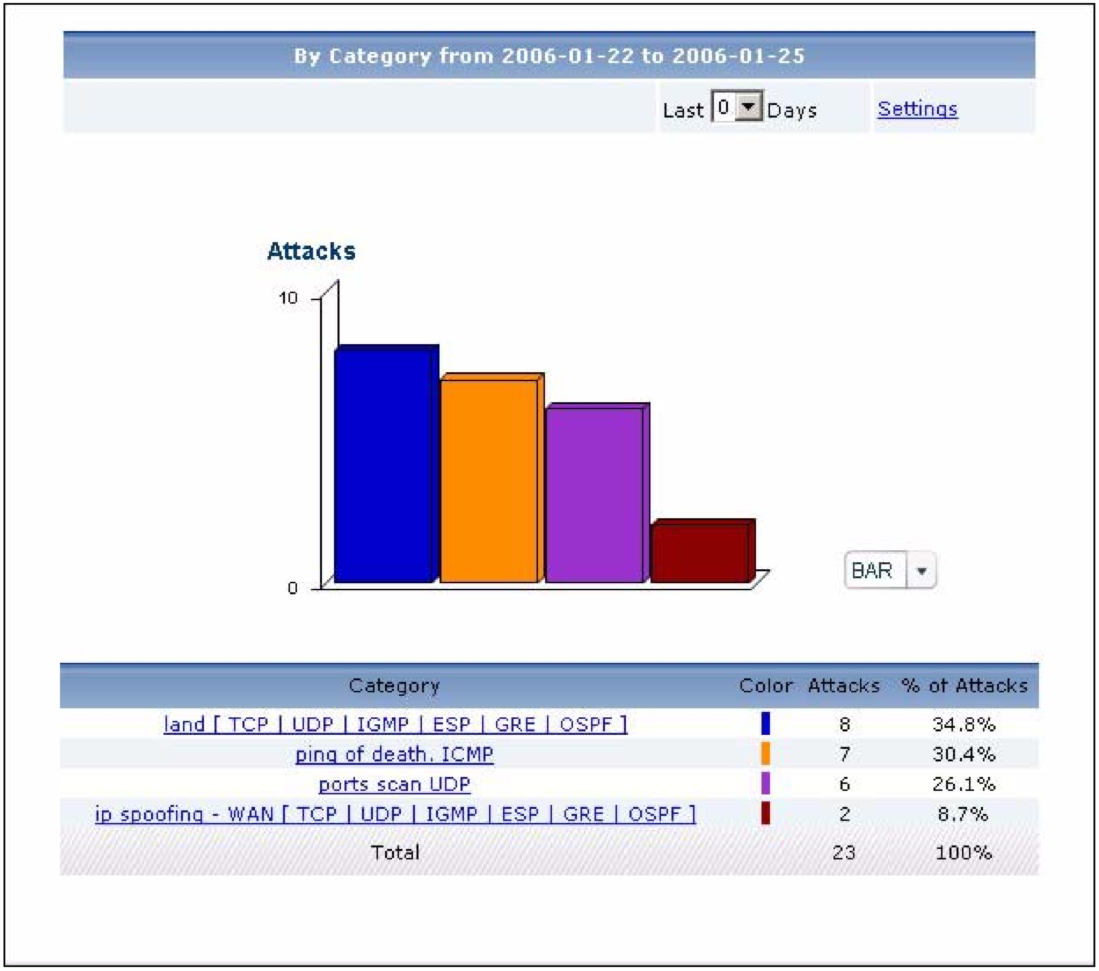
## 34.1.5 Top Attack Categories

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

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

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

**Figure 231** Network Attack > Attack > By Category



By Category from 2006-01-22 to 2006-01-25

Last 0 Days Settings

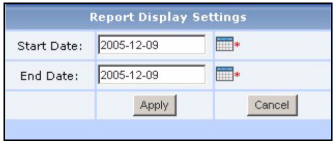
| Category | Color | Attacks | % of Attacks |
|---|---|---|---|
| land [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | 🟦 | 8 | 34.8% |
| ping of death, ICMP | 🟧 | 7 | 30.4% |
| ports scan UDP | 🟪 | 6 | 26.1% |
| ip spoofing - WAN [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | 🟥 | 2 | 8.7% |
| Total |  | 23 | 100% |

Each field is described in the following table.

**Table 199** Network Attack > Attack > By Category

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

**Table 199** Network Attack > Attack > By Category (continued)

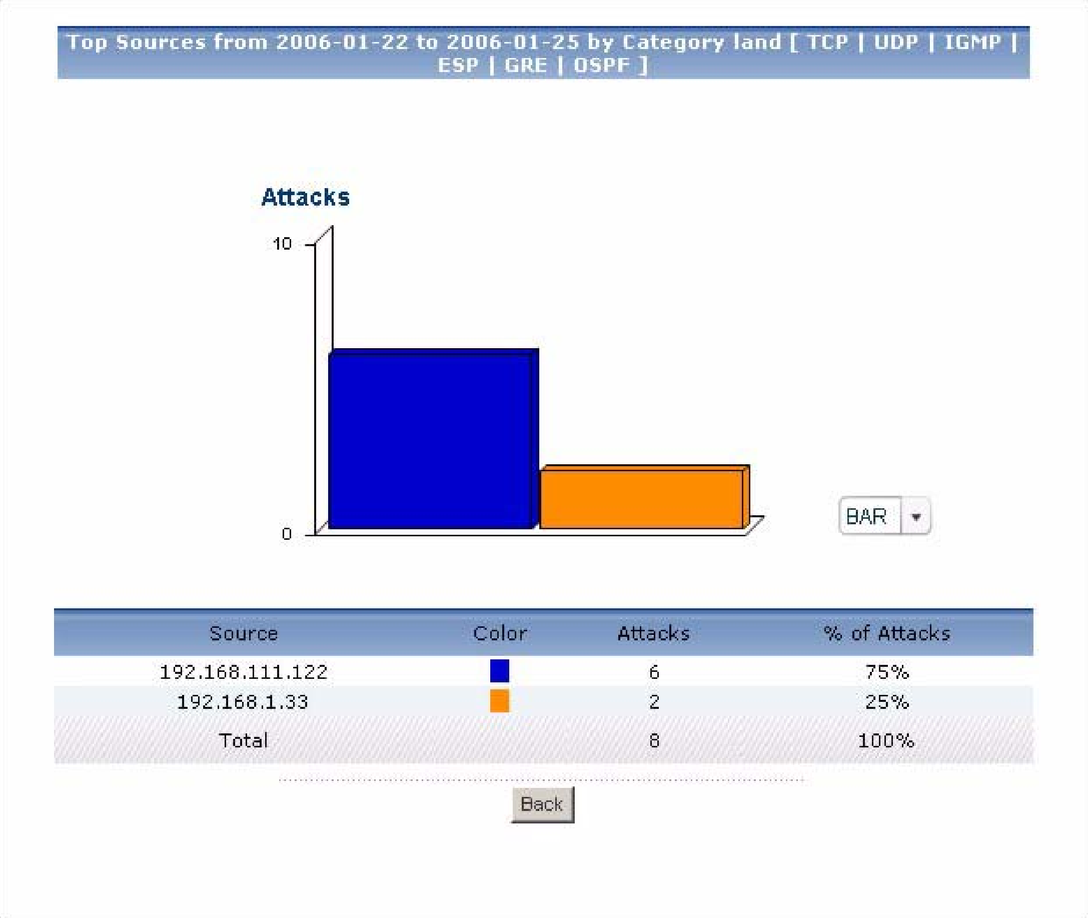
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Category | This field displays the top categories of DoS attacks in the selected device, sorted by the number of attacks by each one. If the number of categories is less than the maximum number of records displayed in this table, every category is displayed.<br>Click on a category to look at the top sources of DoS attacks in the selected category. The **Top Attack Categories Drill-Down** report appears. |
| Color | This field displays what color represents each category in the graph. |
| Attacks | This field displays how many DoS attacks in each category the device stopped. |
| % of Attacks | This field displays what percentage of all DoS attacks come from each category. |
| Total | This entry displays the totals for the categories above. |

## 34.1.6 Top Attack Categories Drill-Down

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

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

**Figure 232** Network Attack > Attack > By Category > Drill-Down



Top Sources from 2006-01-22 to 2006-01-25 by Category land [ TCP | UDP | IGMP | ESP | GRE | OSPF ]

| Source | Color | Attacks | % of Attacks |
|---|---|---|---|
| 192.168.111.122 | 🟦 | 6 | 75% |
| 192.168.1.33 | 🟧 | 2 | 25% |
| Total | | 8 | 100% |

Each field is described in the following table.

**Table 200** Network Attack > Attack > By Category > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Source | This field displays the top sources of DoS attacks in the selected category, sorted by the number of attacks by each one.<br>Each source is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). |
| Color | This field displays what color represents each source in the graph. |
| Attacks | This field displays the number of DoS attacks by each source in the selected category. |
| % of Attacks | This field displays what percentage of all DoS attacks in the selected category were made by each source. |

**Table 200** Network Attack > Attack > By Category > Drill-Down (continued)

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

## 34.2 Intrusion

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

To look at intrusion reports, each device must record intrusions in its log. See the User’s Guide for each 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 device logs each **Attack Type** you want to see in Vantage Report.

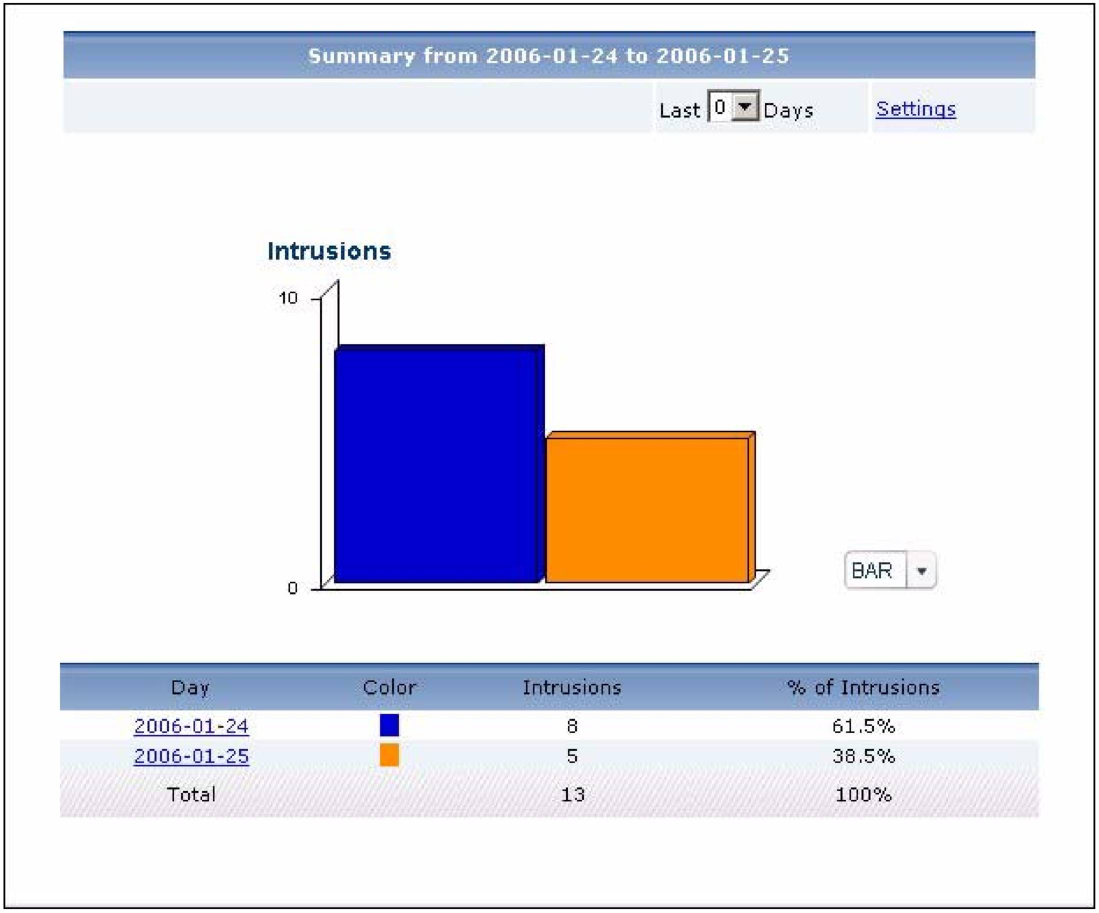
### 34.2.1 Intrusion Summary

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

To look at intrusion reports, each device must record intrusions in its log. See the User’s Guide for each 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 device logs each **Attack Type** you want to see in Vantage Report.

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

**Figure 233** Network Attack > Intrusion > Summary



Summary from 2006-01-24 to 2006-01-25

Last 0 Days Settings

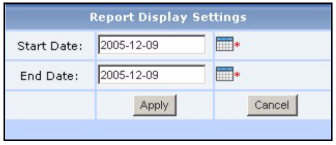
| Day | Color | Intrusions | % of Intrusions |
|---|---|---|---|
| 2006-01-24 | 🟦 | 8 | 61.5% |
| 2006-01-25 | 🟧 | 5 | 38.5% |
| Total | | 13 | 100% |

Each field is described in the following table.

**Table 201** Network Attack > Intrusion > Summary

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

**Table 201** Network Attack > Intrusion > Summary (continued)

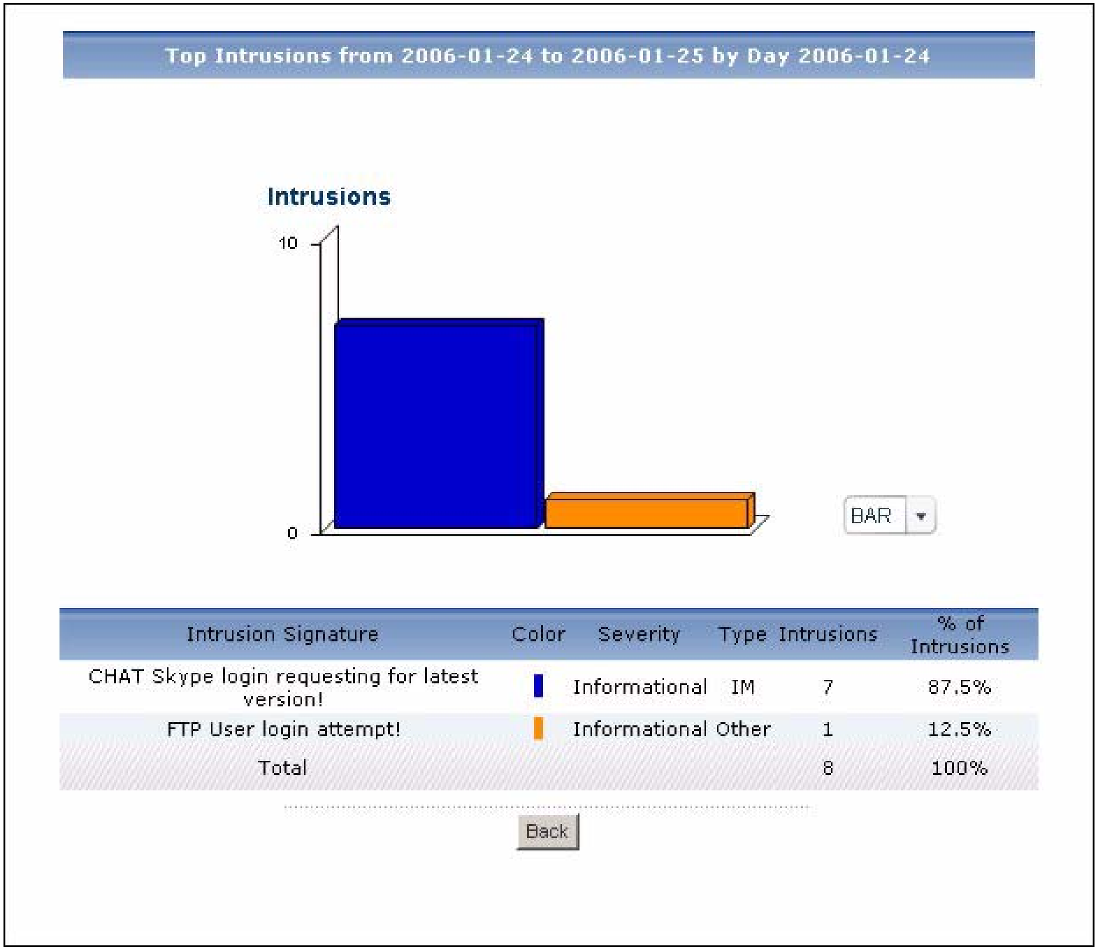
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top intrusion signatures in the selected time interval. The **Intrusion Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| Intrusions | This field displays the number of intrusions in the selected time interval. |
| % of Intrusions | This field displays what percentage of all intrusions was made in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

## 34.2.2 Intrusion Summary Drill-Down

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

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

**Figure 234** Network Attack > Intrusion > Summary > Drill-Down



Top Intrusions from 2006-01-24 to 2006-01-25 by Day 2006-01-24

| Intrusion Signature | Color | Severity | Type | Intrusions | % of Intrusions |
|---|---|---|---|---|---|
| CHAT Skype login requesting for latest version! | 🟦 | Informational | IM | 7 | 87.5% |
| FTP User login attempt! | 🟧 | Informational | Other | 1 | 12.5% |
| Total | | | | 8 | 100% |

Each field is described in the following table.

**Table 202** Network Attack > Intrusion > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Intrusion Signature | This field displays the top categories of intrusions in the selected time interval, sorted by the number of attempts by each one. |
| Color | This field displays what color represents each intrusion signature in the graph. |
| Severity | This field displays the severity of each intrusion signature. |
| Type | This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most 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 202** Network Attack > Intrusion > Summary > Drill-Down (continued)

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

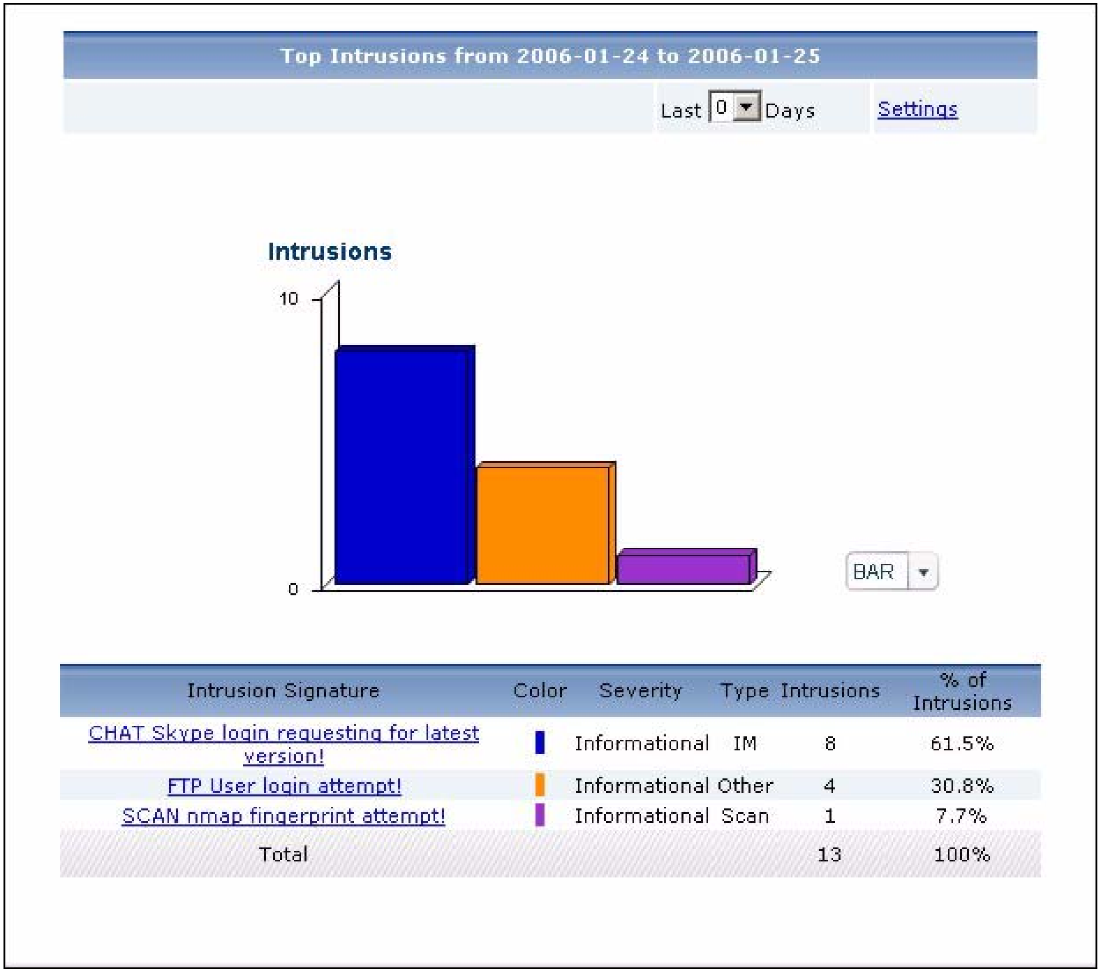
### 34.2.3 Top Intrusion Signatures

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

✍ To look at intrusion reports, each device must record intrusions in its log. See the User’s Guide for each 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 device logs each **Attack Type** you want to see in Vantage Report.

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

**Figure 235** Network Attack > Intrusion > Top Intrusions



Top Intrusions from 2006-01-24 to 2006-01-25

Last 0 Days Settings

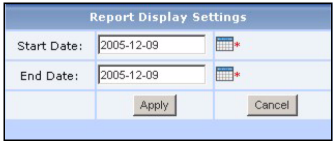
| Intrusion Signature | Color | Severity | Type | Intrusions | % of Intrusions |
|---|---|---|---|---|---|
| CHAT Skype login requesting for latest version! | 🟦 | Informational | IM | 8 | 61.5% |
| FTP User login attempt! | 🟧 | Informational | Other | 4 | 30.8% |
| SCAN nmap fingerprint attempt! | 🟪 | Informational | Scan | 1 | 7.7% |
| Total | | | | 13 | 100% |

Each field is described in the following table.

**Table 203** Network Attack > Intrusion > Top Intrusions

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

**Table 203** Network Attack > Intrusion > Top Intrusions (continued)

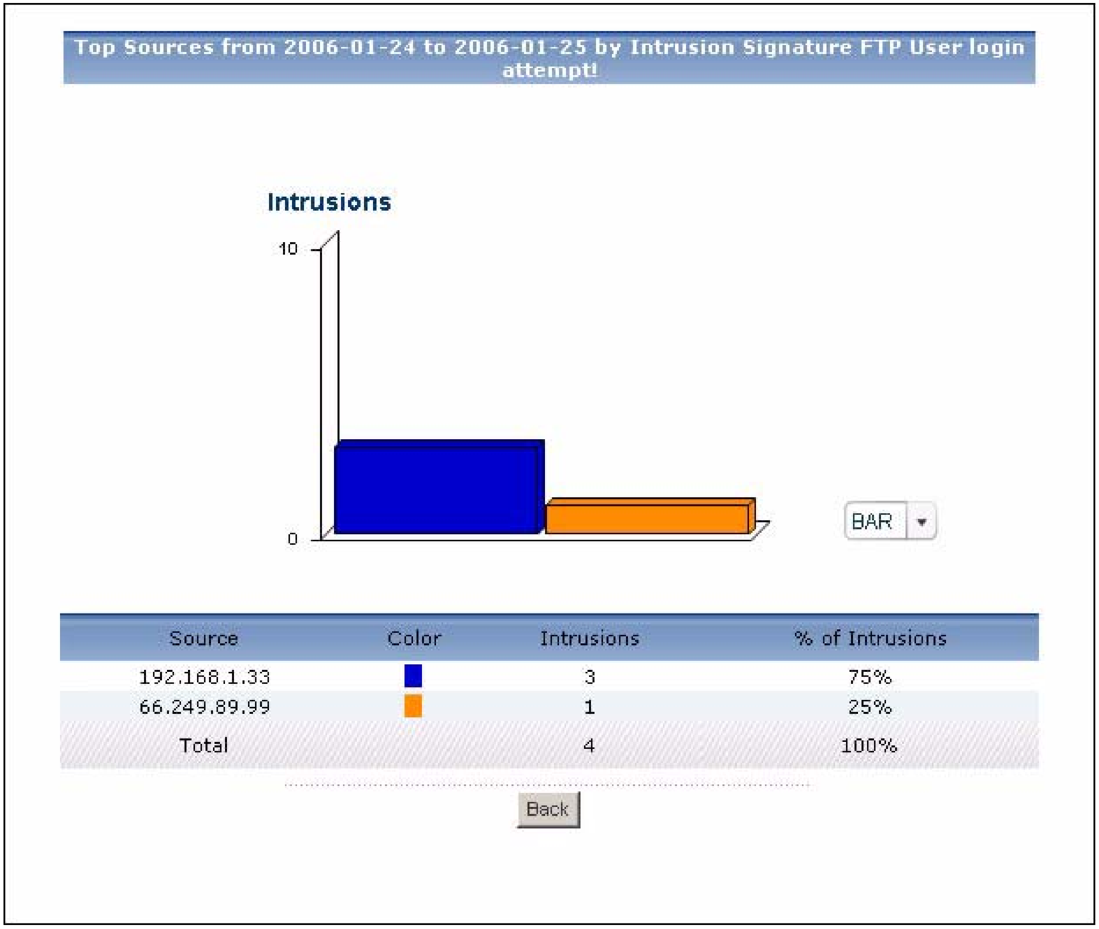
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br> <br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Click on an intrusion signature to look at the top sources for the selected signature. The **Top Intrusion Signatures Drill-Down** report appears. |
| Color | This field displays what color represents each intrusion signature in the graph. |
| Severity | This field displays the severity of each intrusion signature. |
| Type | This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most devices. |
| Intrusions | This field displays the number of intrusions by each intrusion signature. |
| % of Intrusions | This field displays what percentage of all intrusions was made by each intrusion signature. |
| Total | This entry displays the totals for the intrusion signatures above. |

## 34.2.4 Top Intrusion Signatures Drill-Down

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

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

**Figure 236** Network Attack > Intrusion > Top Intrusions > Drill-Down



Top Sources from 2006-01-24 to 2006-01-25 by Intrusion Signature FTP User login attempt!

| Source | Color | Intrusions | % of Intrusions |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 3 | 75% |
| 66.249.89.99 | 🟧 | 1 | 25% |
| Total | | 4 | 100% |

Each field is described in the following table.

**Table 204** Network Attack > Intrusion > Top Intrusions > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), 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. |

**Table 204** Network Attack > Intrusion > Top Intrusions > Drill-Down (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

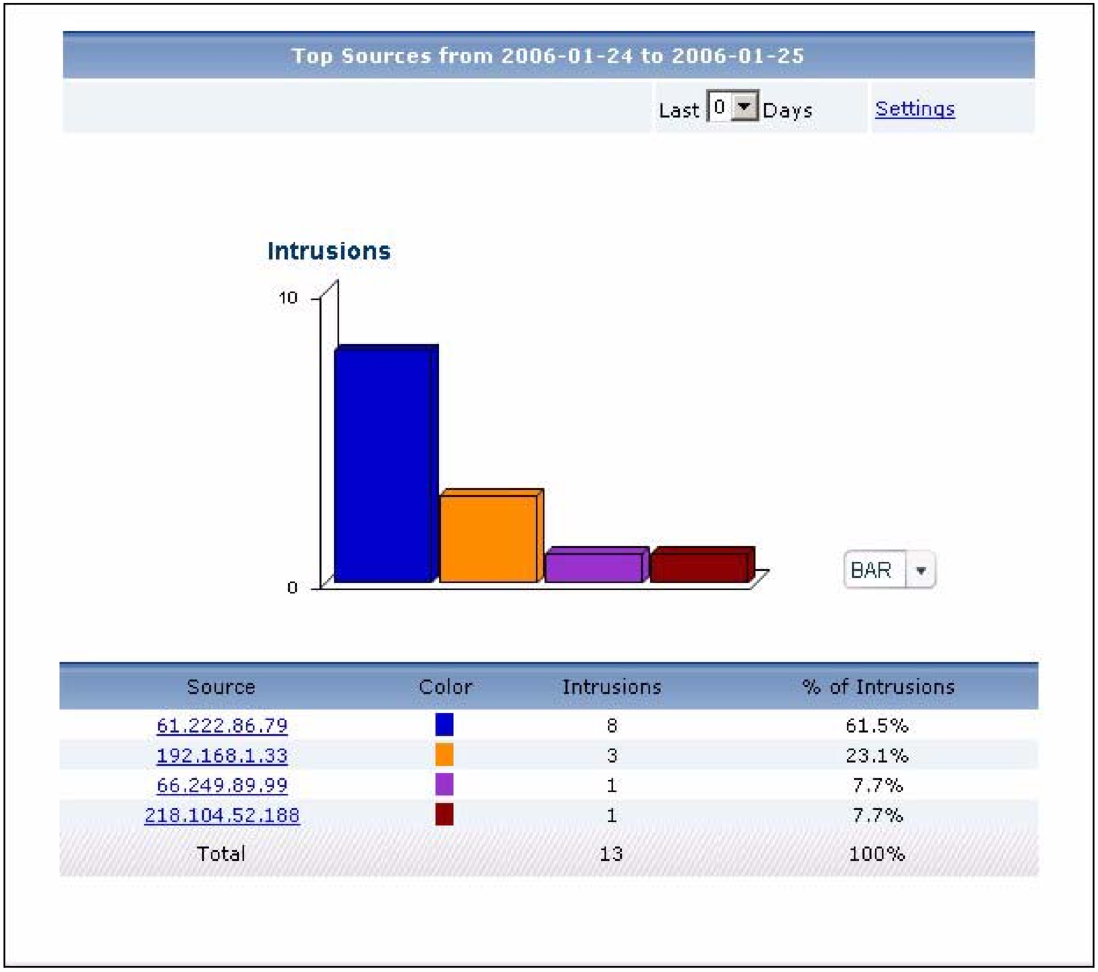
### 34.2.5 Top Intrusion Sources

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

To look at intrusion reports, each device must record intrusions in its log. See the User's Guide for each 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 device logs each **Attack Type** you want to see in Vantage Report.

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

**Figure 237** Network Attack > Intrusion > Top Sources



Top Sources from 2006-01-24 to 2006-01-25

Last 0 Days Settings

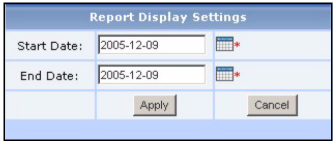
| Source | Color | Intrusions | % of Intrusions |
|---|---|---|---|
| 61.222.86.79 | 🟦 | 8 | 61.5% |
| 192.168.1.33 | 🟧 | 3 | 23.1% |
| 66.249.89.99 | 🟪 | 1 | 7.7% |
| 218.104.52.188 | 🟥 | 1 | 7.7% |
| Total | | 13 | 100% |

Each field is described in the following table.

**Table 205** Network Attack > Intrusion > Top Sources

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

**Table 205** Network Attack > Intrusion > Top Sources (continued)

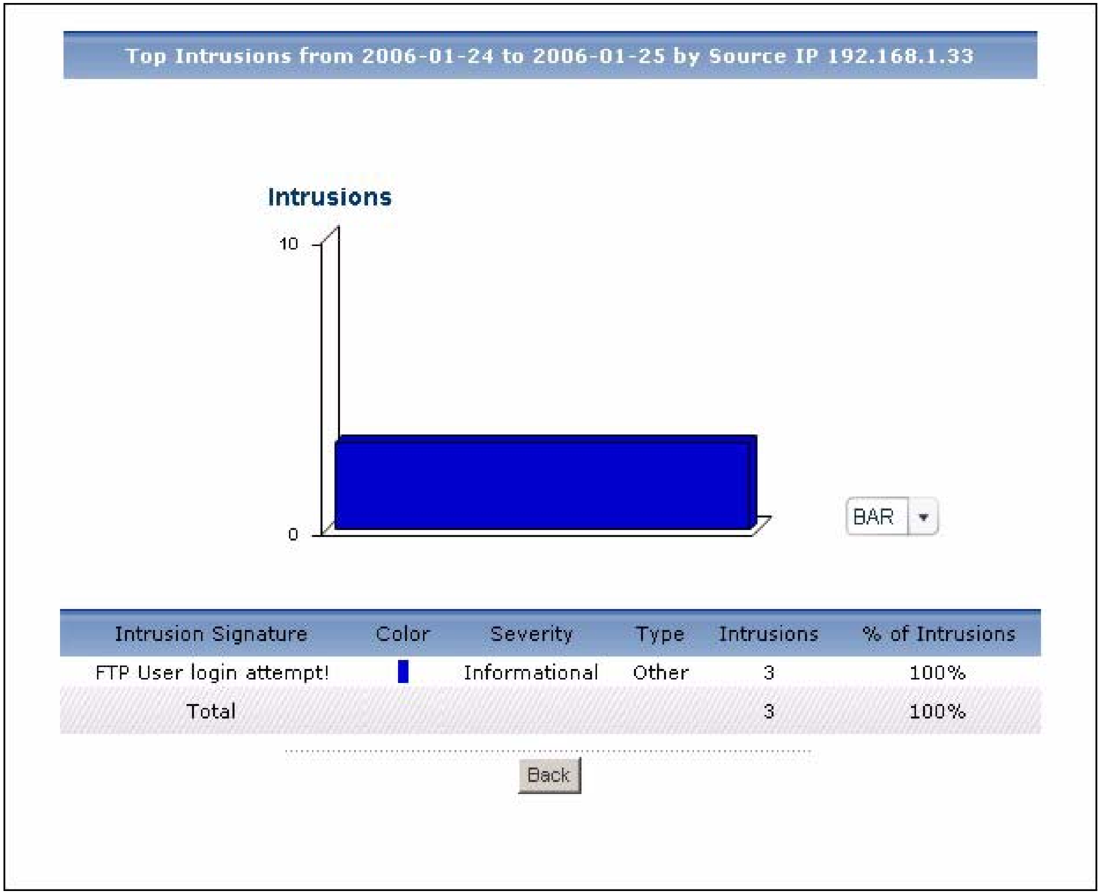
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10").<br>Click on a source to look at the top intrusion signatures for the selected source. The **Top Intrusion Sources Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Intrusions | This field displays the number of intrusions by each source. |
| % of Intrusions | This field displays what percentage of all intrusions was made by each source. |
| Total | This entry displays the totals for the sources above. |

## 34.2.6 Top Intrusion Sources Drill-Down

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

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

**Figure 238** Network Attack > Intrusion > Top Sources > Drill-Down



Top Intrusions from 2006-01-24 to 2006-01-25 by Source IP 192.168.1.33

| Intrusion Signature | Color | Severity | Type | Intrusions | % of Intrusions |
|---|---|---|---|---|---|
| FTP User login attempt! | 🟦 | Informational | Other | 3 | 100% |
| Total | | | | 3 | 100% |

Each field is described in the following table.

**Table 206** Network Attack > Intrusion > Top Sources > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 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 206** Network Attack > Intrusion > Top Sources > Drill-Down (continued)

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

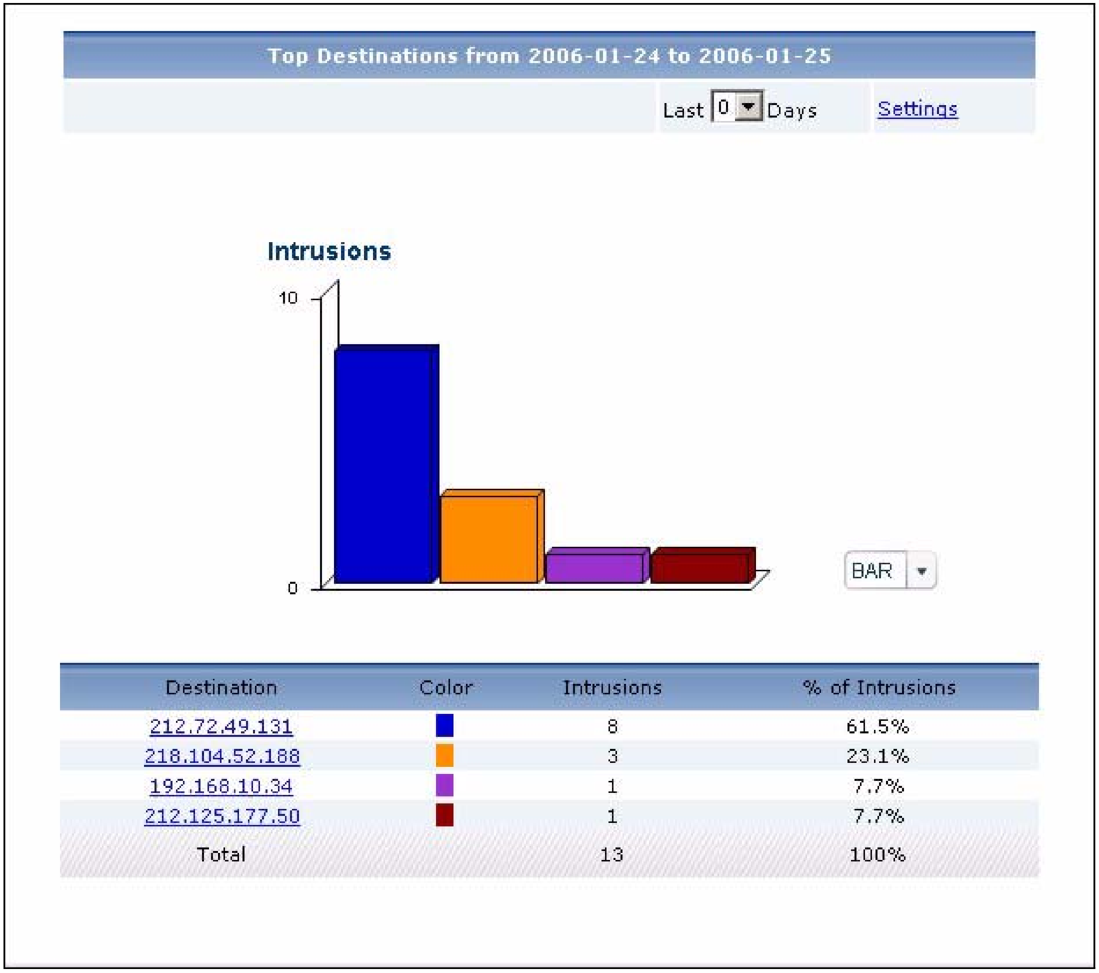
### 34.2.7 Top Intrusion Destinations

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

To look at intrusion reports, each device must record intrusions in its log. See the User’s Guide for each 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 device logs each **Attack Type** you want to see in Vantage Report.

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

**Figure 239** Network Attack > Intrusion > Top Destinations



Top Destinations from 2006-01-24 to 2006-01-25

Last 0 ▾ Days Settings

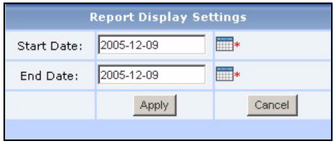
| Destination | Color | Intrusions | % of Intrusions |
|---|---|---|---|
| 212.72.49.131 | 🟦 | 8 | 61.5% |
| 218.104.52.188 | 🟧 | 3 | 23.1% |
| 192.168.10.34 | 🟪 | 1 | 7.7% |
| 212.125.177.50 | 🟥 | 1 | 7.7% |
| Total | | 13 | 100% |

Each field is described in the following table.

**Table 207** Network Attack > Intrusion > Top Destinations

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

**Table 207** Network Attack > Intrusion > Top Destinations (continued)

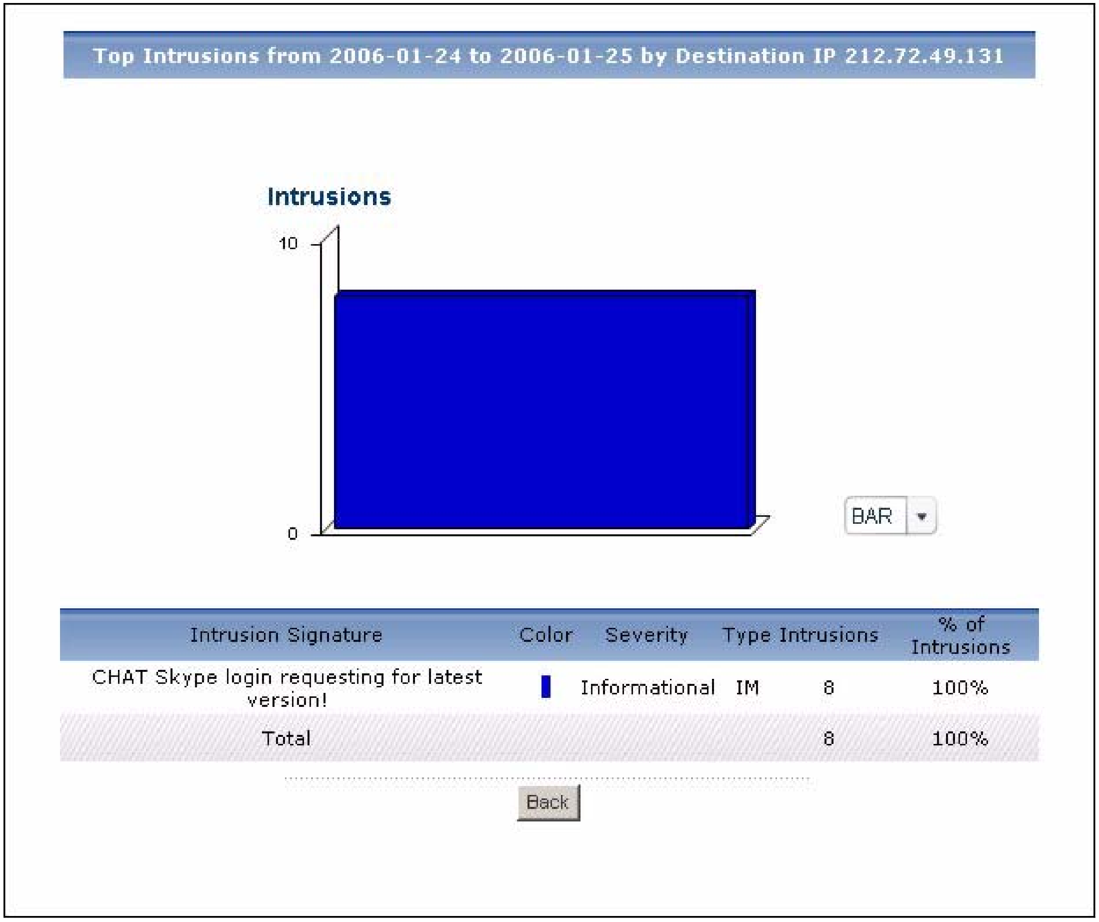
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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 at each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed.<br>Each destination is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”).<br>Click on a destination to look at the top intrusion signatures for the selected destination. The **Top Intrusion Destinations Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Intrusions | This field displays the number of intrusions at each destination. |
| % of Intrusions | This field displays what percentage of all intrusions went to each destination. |
| Total | This entry displays the totals for the destinations above. |

## 34.2.8 Top Intrusion Destinations Drill-Down

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

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

**Figure 240** Network Attack > Intrusion > Top Destinations > Drill-Down



Top Intrusions from 2006-01-24 to 2006-01-25 by Destination IP 212.72.49.131

| Intrusion Signature | Color | Severity | Type | Intrusions | % of Intrusions |
|---|---|---|---|---|---|
| CHAT Skype login requesting for latest version! | 🟦 | Informational | IM | 8 | 100% |
| Total | | | | 8 | 100% |

Each field is described in the following table.

**Table 208** Network Attack > Intrusion > Top Destinations > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Intrusion Signature | This field displays the top intrusion signatures at the selected destination, sorted by the number of intrusions at each one. |
| Color | This field displays what color represents each intrusion signature in the graph. |
| Severity | This field displays the severity of each intrusion signature. |
| Type | This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most devices. |
| Intrusions | This field displays the number of intrusions at the selected destination using each intrusion signature. |
| % of Intrusions | This field displays what percentage of all intrusions at the selected destination was made by each intrusion signature. |

**Table 208** Network Attack > Intrusion > Top Destinations > Drill-Down (continued)

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

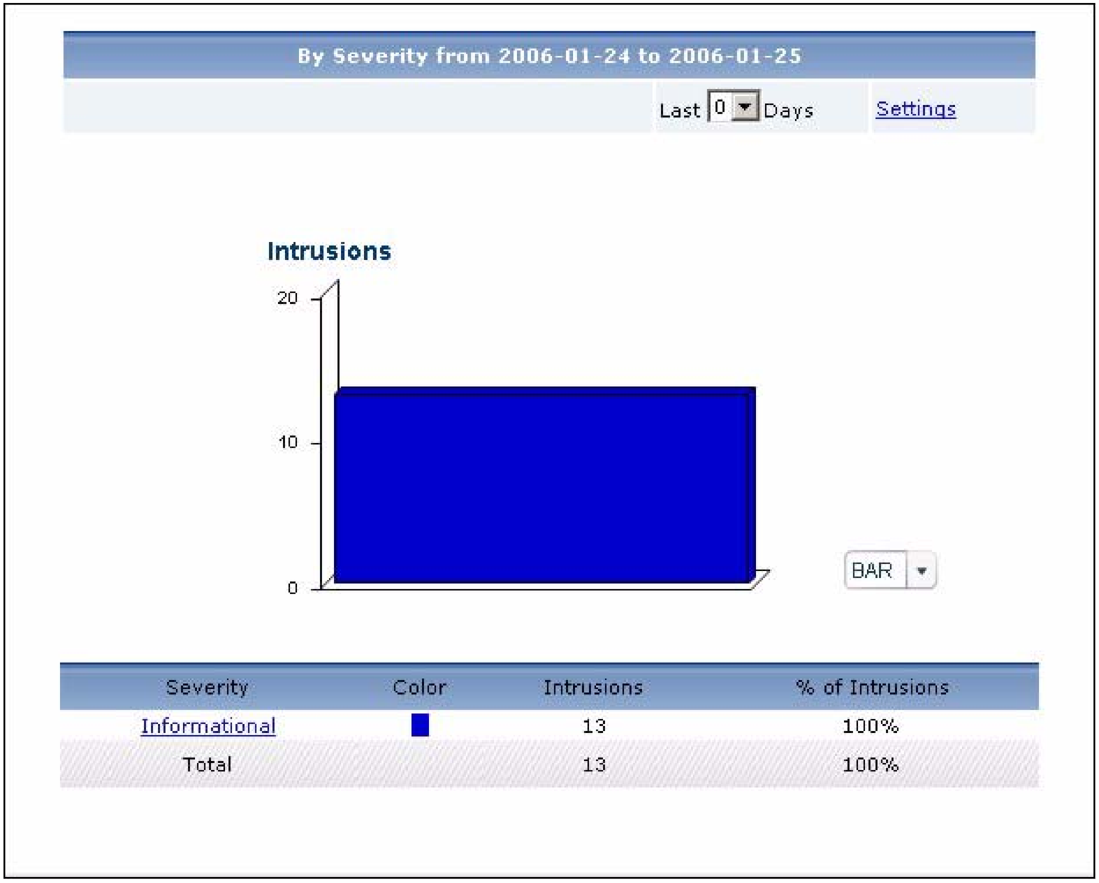
### 34.2.9 Intrusion Severities

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

✍ To look at intrusion reports, each device must record intrusions in its log. See the User’s Guide for each 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 device logs each **Attack Type** you want to see in Vantage Report.

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

**Figure 241** Network Attack > Intrusion > By Severity



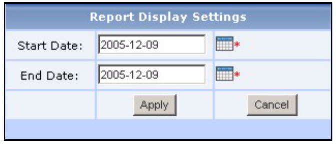
| Severity | Color | Intrusions | % of Intrusions |
|---|---|---|---|
| Informational | 🟦 | 13 | 100% |
| Total | | 13 | 100% |

Each field is described in the following table.

**Table 209** Network Attack > Intrusion > By Severity

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

**Table 209** Network Attack > Intrusion > By Severity (continued)

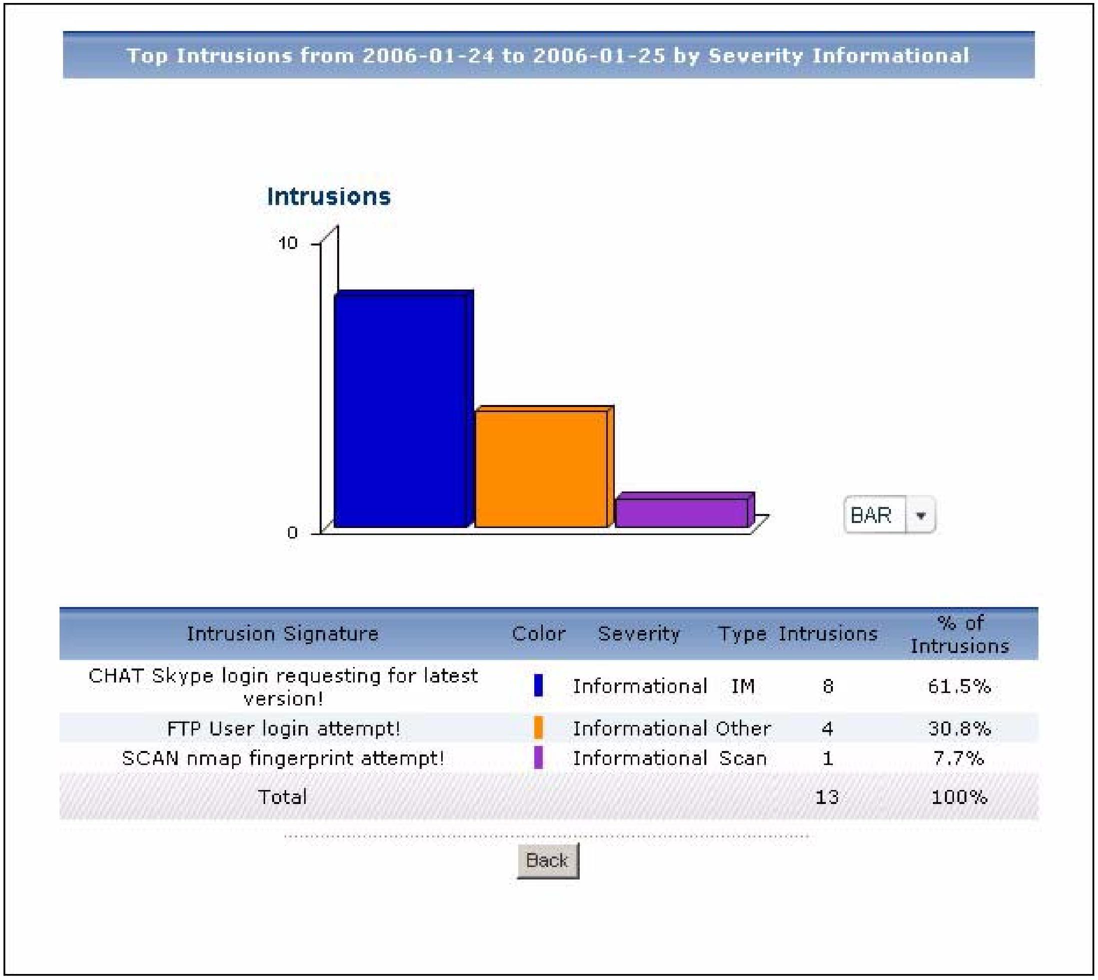
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Click on a severity to look at the top intrusion signatures for the selected severity. The **Intrusion Severities Drill-Down** report appears. |
| Color | This field displays what color represents each level of severity in the graph. |
| Intrusions | This field displays the number of intrusions of each level of severity. |
| % of Intrusions | This field displays what percentage of all intrusions are at each level of severity. |
| Total | This entry displays the totals for the severities above. |

## 34.2.10 Intrusion Severities Drill-Down

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

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

**Figure 242** Network Attack > Intrusion > By Severity > Drill-Down



Top Intrusions from 2006-01-24 to 2006-01-25 by Severity Informational

| Intrusion Signature | Color | Severity | Type | Intrusions | % of Intrusions |
|---|---|---|---|---|---|
| CHAT Skype login requesting for latest version! | 🟦 | Informational | IM | 8 | 61.5% |
| FTP User login attempt! | 🟧 | Informational | Other | 4 | 30.8% |
| SCAN nmap fingerprint attempt! | 🟪 | Informational | Scan | 1 | 7.7% |
| Total | | | | 13 | 100% |

Each field is described in the following table.

**Table 210** Network Attack > Intrusion > By Severity > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Intrusion Signature | This field displays the top intrusion signatures of the selected severity, sorted by the number of intrusions by each one. |
| Color | This field displays what color represents each intrusion signature in the graph. |
| Severity | This field displays the severity of each intrusion signature. |
| Type | This field displays what kind of intrusion each intrusion signature is. This corresponds to **IDP > Signature > Attack Type** in most devices. |
| Intrusions | This field displays the number of intrusions of the selected severity using each intrusion signature. |

**Table 210** Network Attack > Intrusion > By Severity > Drill-Down (continued)

| LABEL | DESCRIPTION |
|---|---|
| % of Intrusions | This field displays what percentage of all intrusions of the selected severity was made by each intrusion signature. |
| Total | This entry displays the totals for the intrusion signatures above. If the number of intrusion signatures of the selected severity is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report. |
| Back | Click this to return to the main report. |

## 34.3 AntiVirus

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

To look at anti-virus reports, each device must record anti-virus messages in its log. See the User's Guide for each 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**. Devices can log viruses based on the **Service** the virus was using. Make sure the device logs viruses you want to include in Vantage Report.

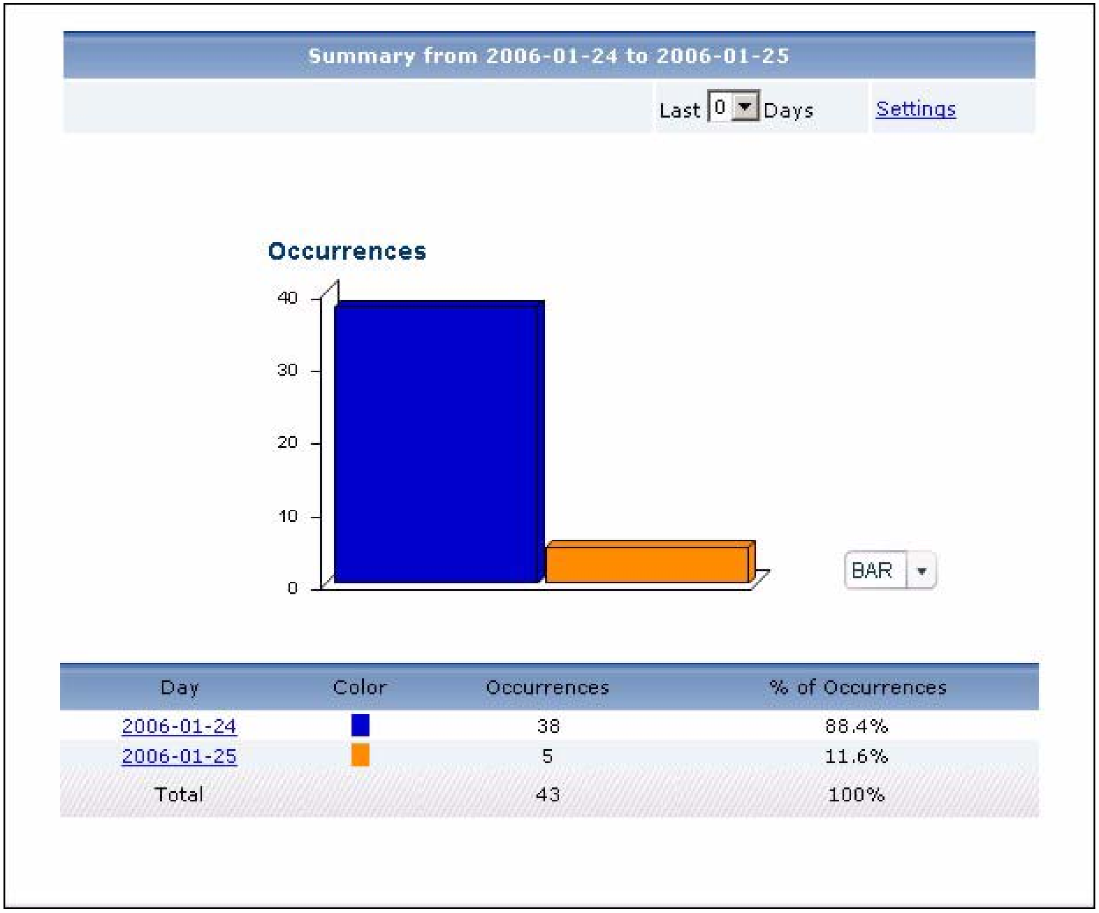
### 34.3.1 Virus Summary

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

To look at anti-virus reports, each device must record anti-virus messages in its log. See the User's Guide for each 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**. Devices can log viruses based on the **Service** the virus was using. Make sure the device logs viruses you want to include in Vantage Report.

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

**Figure 243** Network Attack > AntiVirus > Summary



Summary from 2006-01-24 to 2006-01-25

Last 0 Days Settings

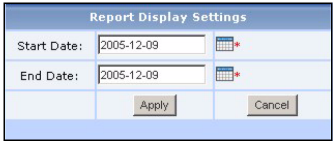
| Day | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| 2006-01-24 | 🟦 | 38 | 88.4% |
| 2006-01-25 | 🟧 | 5 | 11.6% |
| Total | | 43 | 100% |

Each field is described in the following table.

**Table 211** Network Attack > AntiVirus > Summary

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

**Table 211** Network Attack > AntiVirus > Summary (continued)

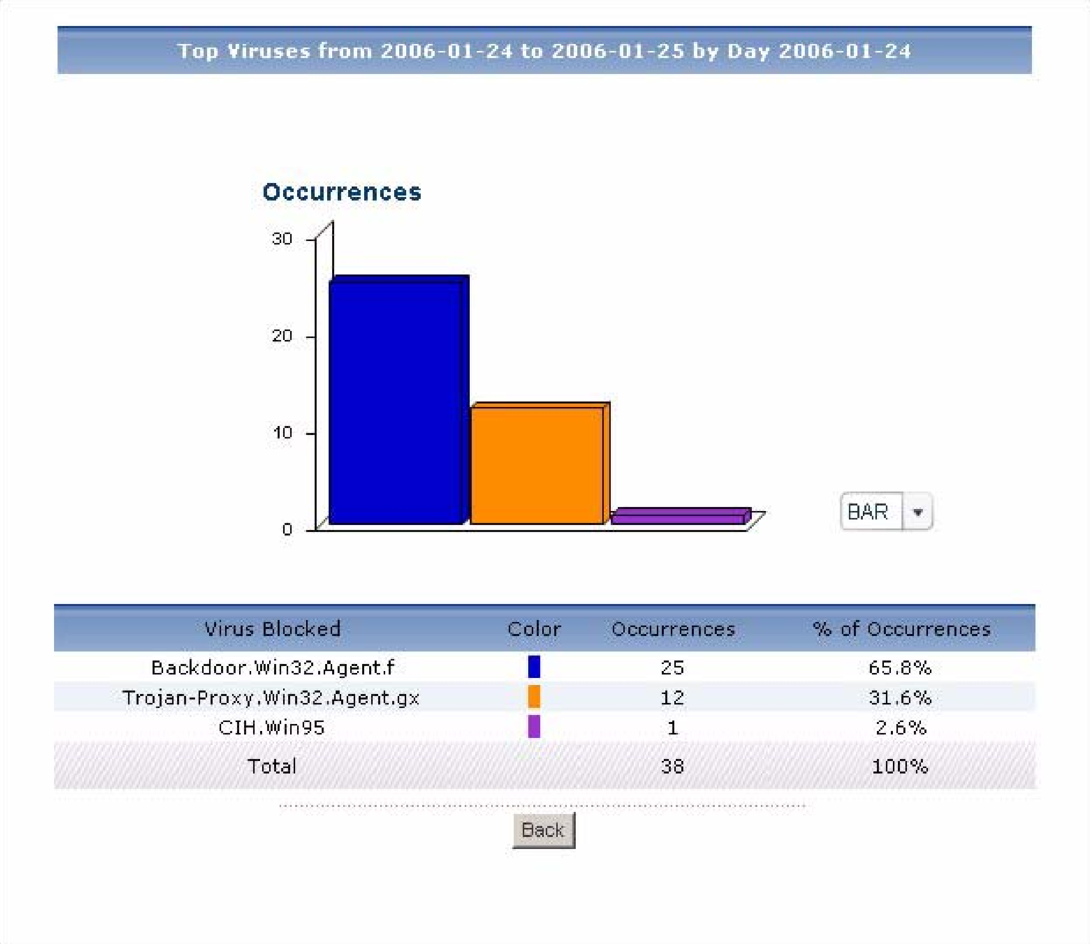
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br> <br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top viruses in the selected time interval. The **Virus Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| Occurrences | This field displays the number of occurrences in the selected time interval. |
| % of Occurrences | This field displays what percentage of all occurrences was made in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

## 34.3.2 Virus Summary Drill-Down

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

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

**Figure 244** Network Attack > AntiVirus > Summary > Drill-Down



Top Viruses from 2006-01-24 to 2006-01-25 by Day 2006-01-24

| Virus Blocked | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| Backdoor.Win32.Agent.f | 🟦 | 25 | 65.8% |
| Trojan-Proxy.Win32.Agent.gx | 🟧 | 12 | 31.6% |
| CIH.Win95 | 🟪 | 1 | 2.6% |
| Total | | 38 | 100% |

Each field is described in the following table.

**Table 212** Network Attack > AntiVirus > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Virus Blocked | This field displays the top viruses stopped in the selected time interval, sorted by the number of occurrences by each one. |
| Color | This field displays what color represents each virus in the graph. |
| Occurrences | This field displays the number of occurrences by each virus in the selected time interval. |
| % of Occurrences | This field displays what percentage of all occurrences in the selected time interval was made by each virus. |

**Table 212** Network Attack > AntiVirus > Summary > Drill-Down (continued)

| 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. |

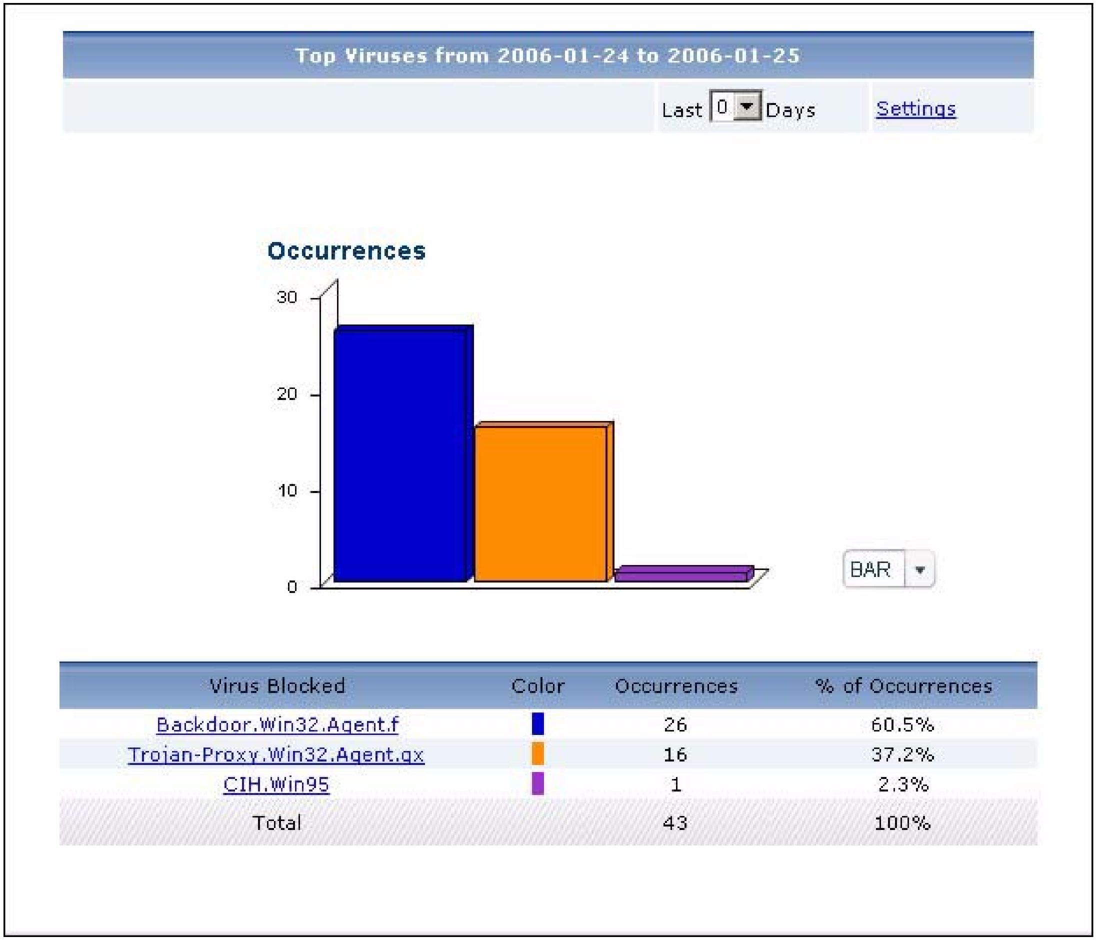
### 34.3.3 Top Viruses

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

To look at anti-virus reports, each device must record anti-virus messages in its log. See the User's Guide for each 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**. Devices can log viruses based on the **Service** the virus was using. Make sure the device logs viruses you want to include in Vantage Report.

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

**Figure 245** Network Attack > AntiVirus > Top Viruses



Top Viruses from 2006-01-24 to 2006-01-25

Last 0 Days Settings

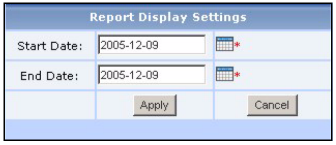
| Virus Blocked | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| Backdoor.Win32.Agent.f | 🟦 | 26 | 60.5% |
| Trojan-Proxy.Win32.Agent.gx | 🟧 | 16 | 37.2% |
| CIH.Win95 | 🟪 | 1 | 2.3% |
| Total | | 43 | 100% |

Each field is described in the following table.

**Table 213** Network Attack > AntiVirus > Top Viruses

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

**Table 213** Network Attack > AntiVirus > Top Viruses (continued)

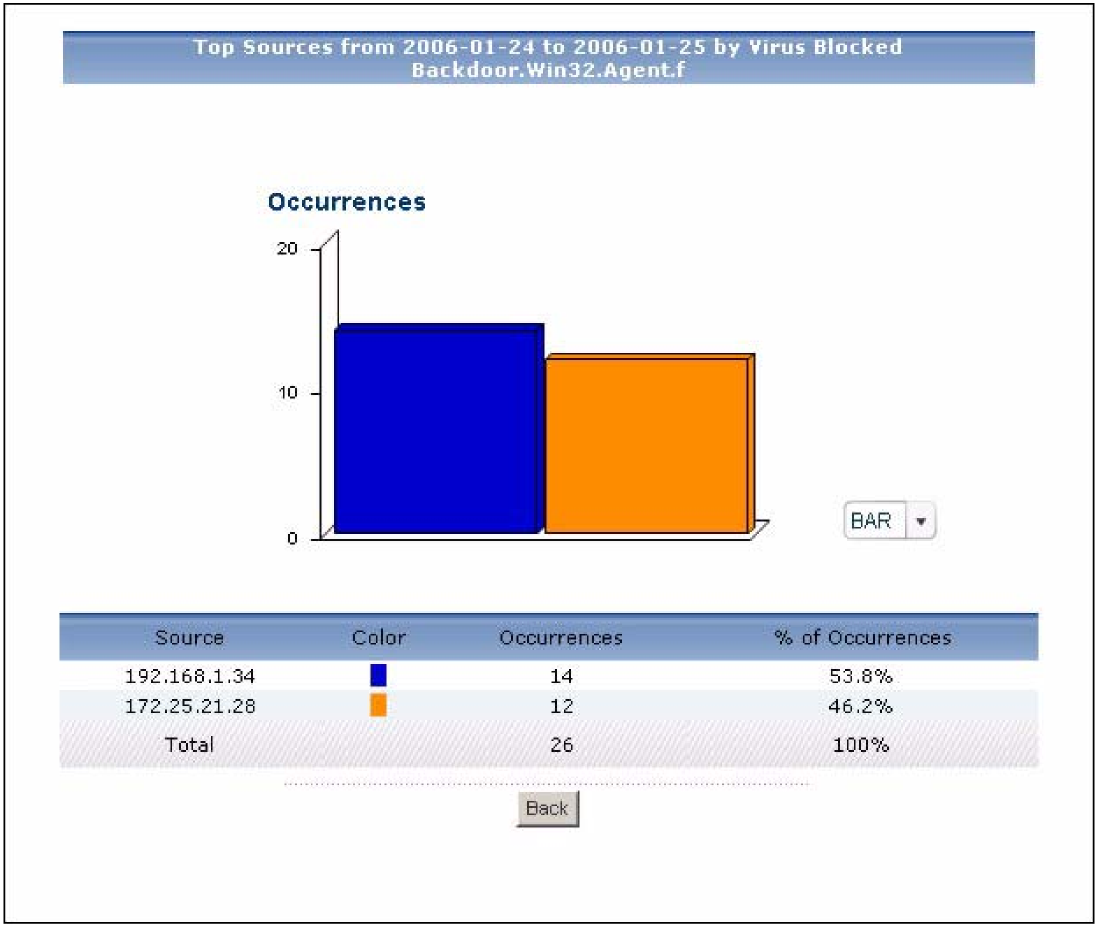
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Click on a virus to look at the top sources for the selected virus. The **Top Viruses Drill-Down** report appears. |
| Color | This field displays what color represents each virus in the graph. |
| Occurrences | This field displays the number of occurrences by each virus. |
| % of Occurrences | This field displays what percentage of all occurrences was made by each virus. |
| Total | This entry displays the totals for the viruses above. |

## 34.3.4 Top Viruses Drill-Down

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

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

**Figure 246** Network Attack > AntiVirus > Top Viruses > Drill-Down



Top Sources from 2006-01-24 to 2006-01-25 by Virus Blocked Backdoor.Win32.Agent.f

| Source | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| 192.168.1.34 | 🟦 | 14 | 53.8% |
| 172.25.21.28 | 🟧 | 12 | 46.2% |
| Total | | 26 | 100% |

Each field is described in the following table.

**Table 214** Network Attack > AntiVirus > Top Viruses > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). |
| Color | This field displays what color represents each source in the graph. |
| Occurrences | This field displays the number of occurrences of the selected virus from each source. |

**Table 214** Network Attack > AntiVirus > Top Viruses > Drill-Down (continued)

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

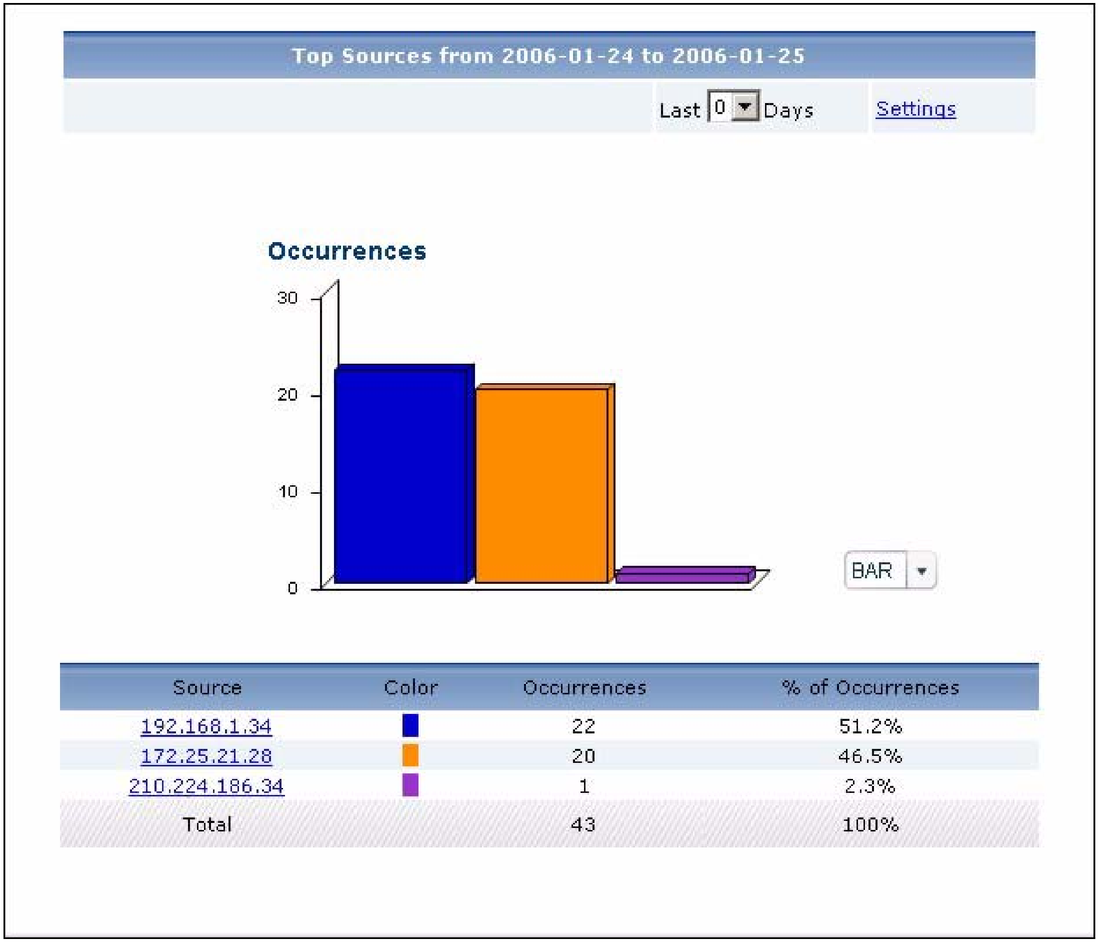
## 34.3.5 Top Virus Sources

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

To look at anti-virus reports, each device must record anti-virus messages in its log. See the User's Guide for each 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**. Devices can log viruses based on the **Service** the virus was using. Make sure the device logs viruses you want to include in Vantage Report.

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

**Figure 247** Network Attack > AntiVirus > Top Sources



Top Sources from 2006-01-24 to 2006-01-25

Last 0 Days Settings

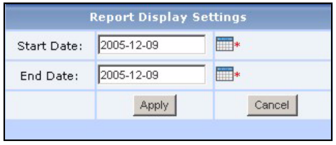
| Source | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| 192.168.1.34 | 🟦 | 22 | 51.2% |
| 172.25.21.28 | 🟧 | 20 | 46.5% |
| 210.224.186.34 | 🟪 | 1 | 2.3% |
| Total | | 43 | 100% |

Each field is described in the following table.

**Table 215** Network Attack > AntiVirus > Top Sources

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

**Table 215** Network Attack > AntiVirus > Top Sources (continued)

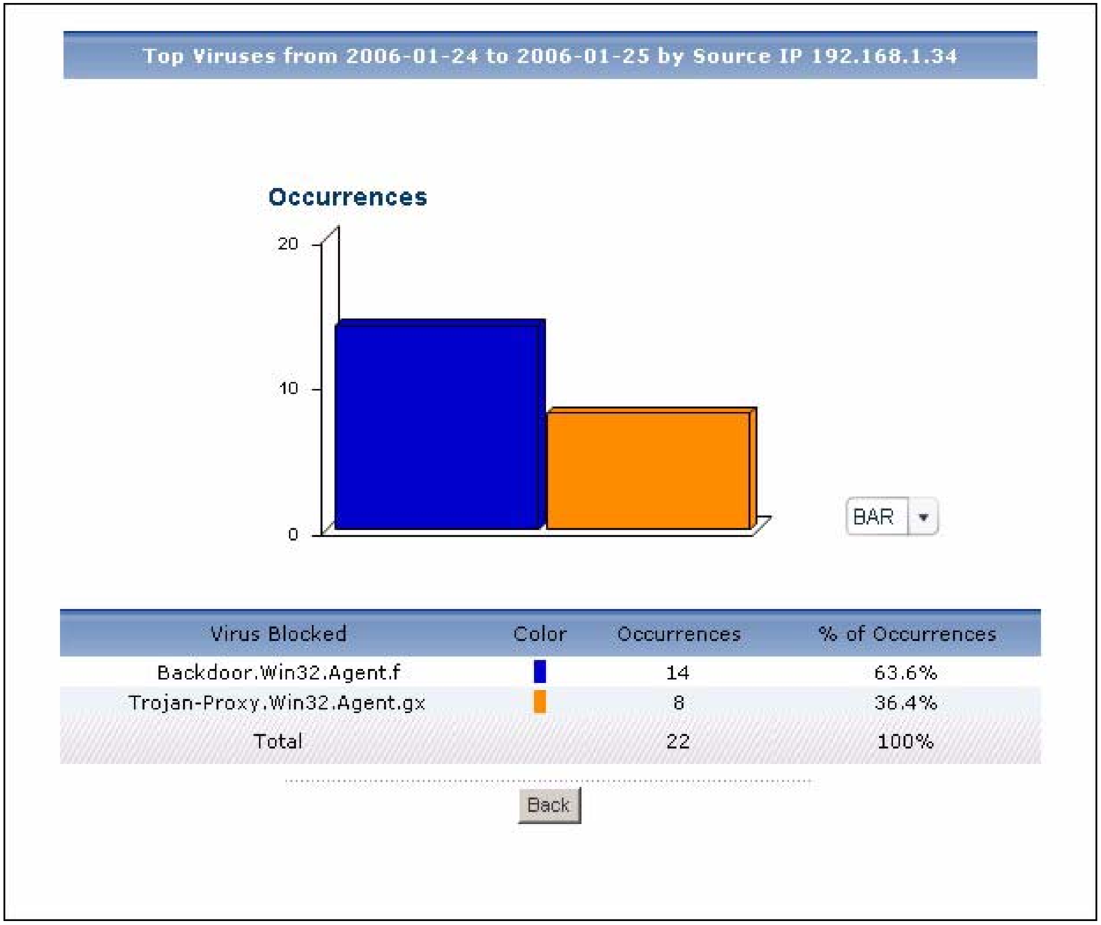
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”).<br>Click on a source to look at the top viruses for the selected source. The **Top Virus Sources Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Occurrences | This field displays the number of occurrences from each source. |
| % of Occurrences | This field displays what percentage of all occurrences comes from each source. |
| Total | This entry displays the totals for the sources above. |

## 34.3.6 Top Virus Sources Drill-Down

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

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

**Figure 248** Network Attack > AntiVirus > Top Sources > Drill-Down



Top Viruses from 2006-01-24 to 2006-01-25 by Source IP 192.168.1.34

| Virus Blocked | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| Backdoor.Win32.Agent.f | 🟦 | 14 | 63.6% |
| Trojan-Proxy.Win32.Agent.gx | 🟧 | 8 | 36.4% |
| Total | | 22 | 100% |

Each field is described in the following table.

**Table 216** Network Attack > AntiVirus > Top Sources > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Virus Blocked | This field displays the top viruses stopped from the selected source, sorted by the number of occurrences by each one. |
| Color | This field displays what color represents each virus in the graph. |
| Occurrences | This field displays the number of occurrences from the selected source by each virus. |
| % of Occurrences | This field displays what percentage of all occurrences from the selected source was made by each virus. |

**Table 216** Network Attack > AntiVirus > Top Sources > Drill-Down (continued)

| 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. |

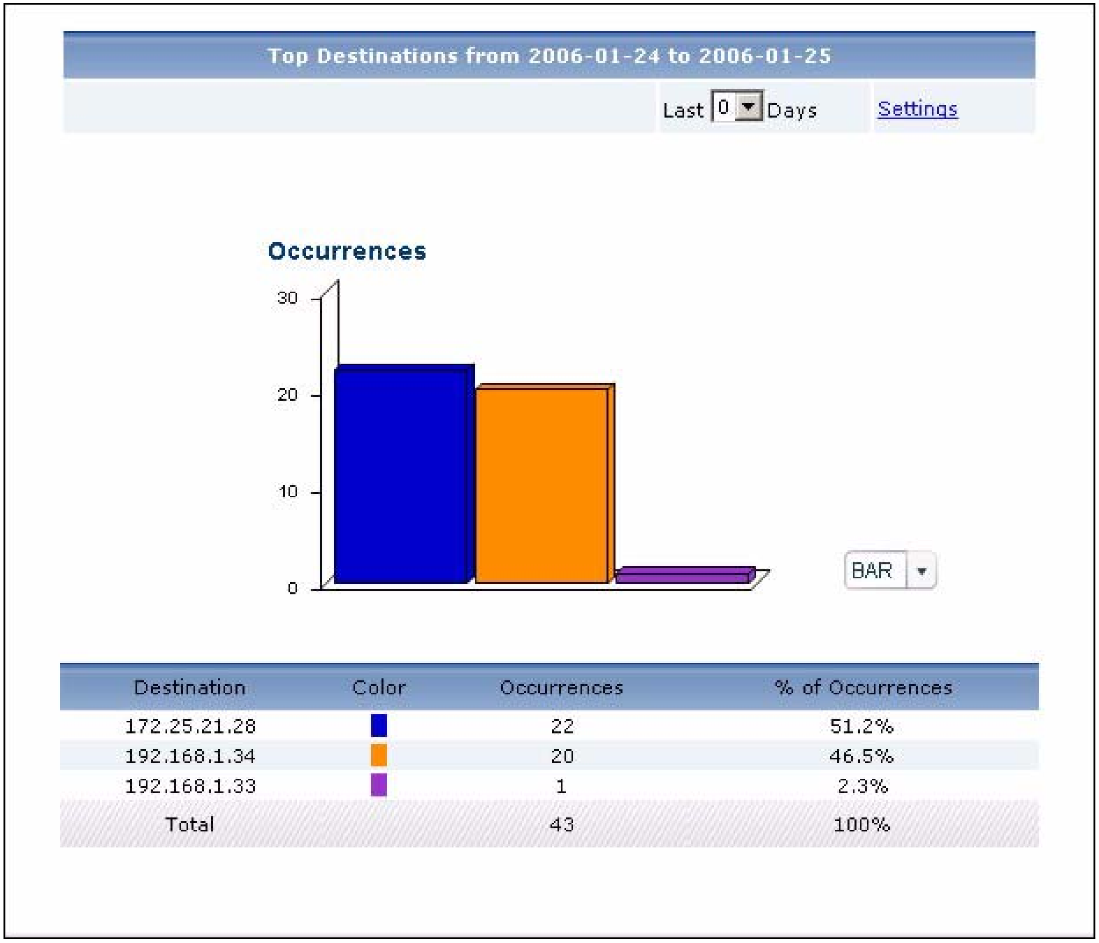
### 34.3.7 Top Virus Destinations

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

To look at anti-virus reports, each device must record anti-virus messages in its log. See the User’s Guide for each 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**. Devices can log viruses based on the **Service** the virus was using. Make sure the device logs viruses you want to include in Vantage Report.

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

**Figure 249** Network Attack > AntiVirus > Top Destinations



Top Destinations from 2006-01-24 to 2006-01-25

Last 0 Days Settings

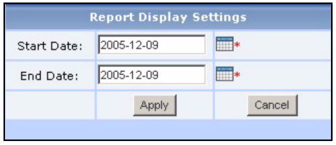
| Destination | Color | Occurrences | % of Occurrences |
|---|---|---|---|
| 172.25.21.28 | 🟦 | 22 | 51.2% |
| 192.168.1.34 | 🟧 | 20 | 46.5% |
| 192.168.1.33 | 🟪 | 1 | 2.3% |
| Total |  | 43 | 100% |

Each field is described in the following table.

**Table 217** Network Attack > AntiVirus > Top Destinations

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |

**Table 217** Network Attack > AntiVirus > Top Destinations (continued)

| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>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. |
| Total | This entry displays the totals for the destinations above. |

## 34.4 AntiSpam

Use these reports to look at spam messages that were detected by the device’s anti-spam feature. You can also look at the top senders and sources of spam messages.

To look at anti-spam reports, each device must record anti-spam messages in its log. See the User’s Guide for each device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Spam** is enabled.

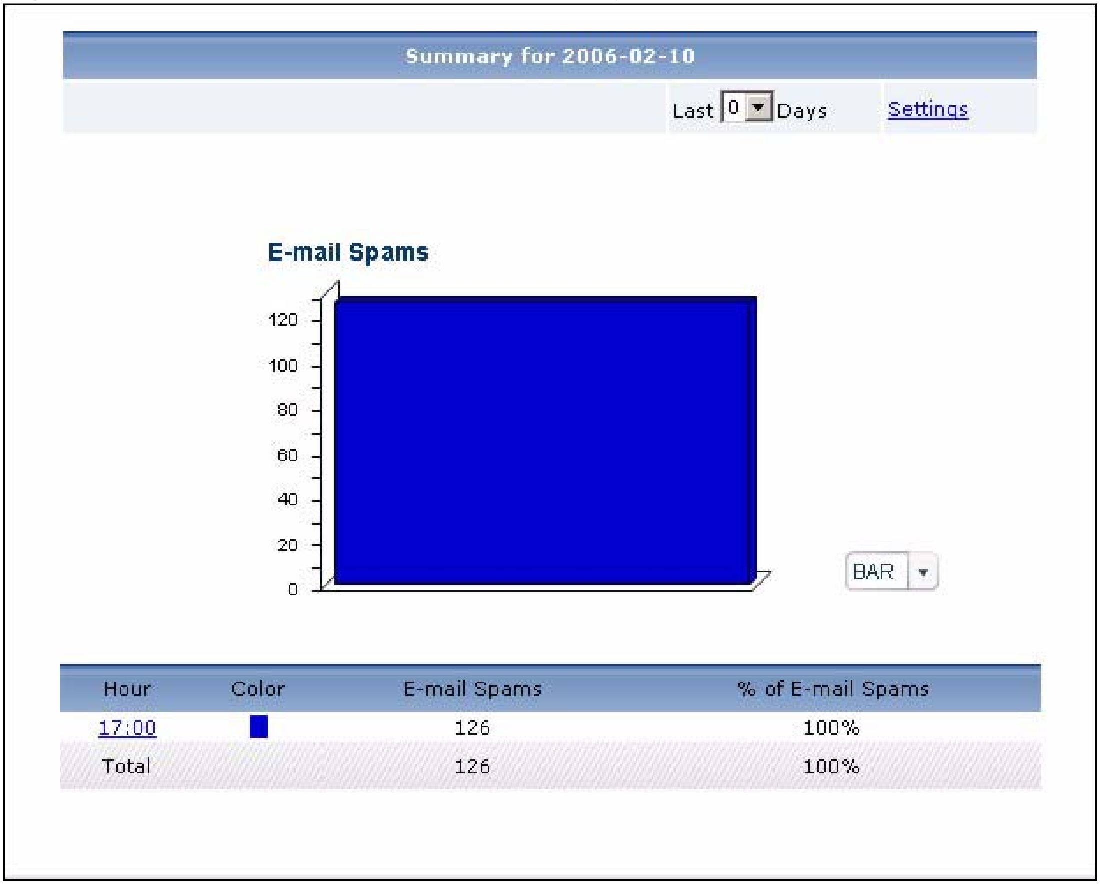
### 34.4.1 Spam Summary

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

To look at anti-spam reports, each device must record anti-spam messages in its log. See the User’s Guide for each device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Spam** is enabled.

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

**Figure 250** Network Attack > AntiSpam > Summary



Summary for 2006-02-10

Last 0 Days Settings

E-mail Spams

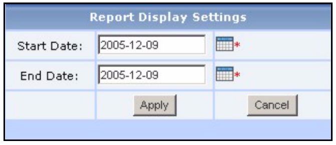
| Hour | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| 17:00 | 🟦 | 126 | 100% |
| Total | | 126 | 100% |

Each field is described in the following table.

**Table 218** Network Attack > AntiSpam > Summary

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

**Table 218** Network Attack > AntiSpam > Summary (continued)

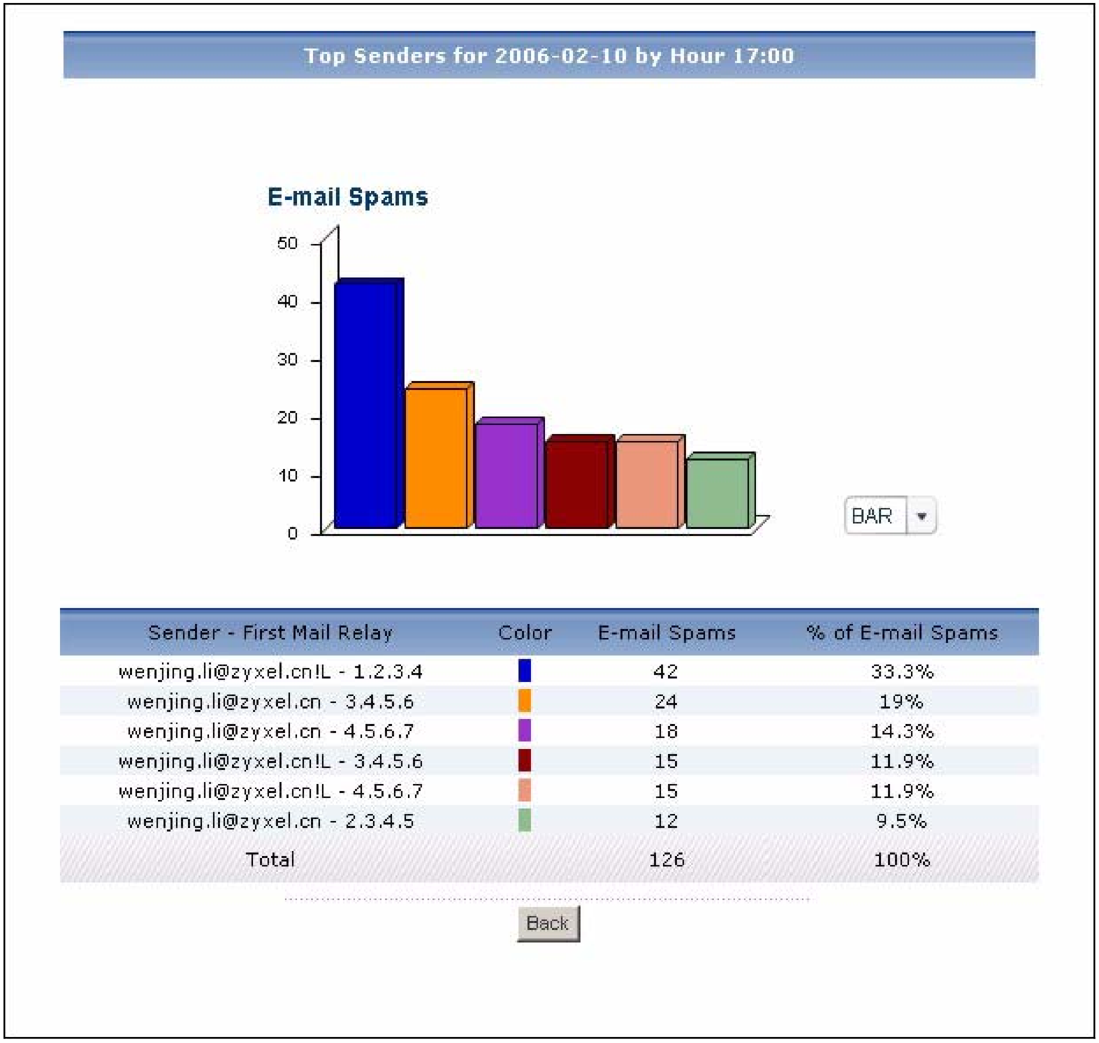
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top spam messages in the selected time interval. The **Spam Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| E-mail Spams | This field displays the number of spam messages in the selected time interval. |
| % of E-mail Spams | This field displays what percentage of all spam messages was made in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

## 34.4.2 Spam Summary Drill-Down

Use this report to look at the top combinations of senders of spam messages and the first SMTP server to which the sender sends spam in a specific time interval. For example, if a sender sends spam through two SMTP servers, there are two entries for the sender, one with each SMTP server.

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

**Figure 251** Network Attack > AntiSpam > Summary > Drill-Down



Top Senders for 2006-02-10 by Hour 17:00

| Sender - First Mail Relay | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| wenjing.li@zyxel.cn!L - 1.2.3.4 | 🟦 | 42 | 33.3% |
| wenjing.li@zyxel.cn - 3.4.5.6 | 🟧 | 24 | 19% |
| wenjing.li@zyxel.cn - 4.5.6.7 | 🟪 | 18 | 14.3% |
| wenjing.li@zyxel.cn!L - 3.4.5.6 | 🟥 | 15 | 11.9% |
| wenjing.li@zyxel.cn!L - 4.5.6.7 | 🟧 | 15 | 11.9% |
| wenjing.li@zyxel.cn - 2.3.4.5 | 🟩 | 12 | 9.5% |
| Total | | 126 | 100% |

Each field is described in the following table.

**Table 219** Network Attack > AntiSpam > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Sender - First Mail Relay | This field displays the top combinations of senders of spam and the first SMTP server to which spam is sent in the selected time interval, sorted by the number of spam messages sent for each combination.<br>Each sender is identified by its e-mail address.<br>Each SMTP server is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). |

**Table 219** Network Attack > AntiSpam > Summary > Drill-Down (continued)

| LABEL | DESCRIPTION |
|---|---|
| Color | This field displays what color represents each sender in the graph. |
| E-mail Spams | This field displays how many spam messages each sender sent. |
| % of E-mail Spams | This field displays what percentage of all spam messages in the selected time interval was sent by each sender. |
| Total | This entry displays the totals for the senders above. If the number of senders in the selected time interval is greater than the maximum number of records displayed in this table, this total might be a little lower than the total in the main report. |
| Back | Click this to return to the main report. |

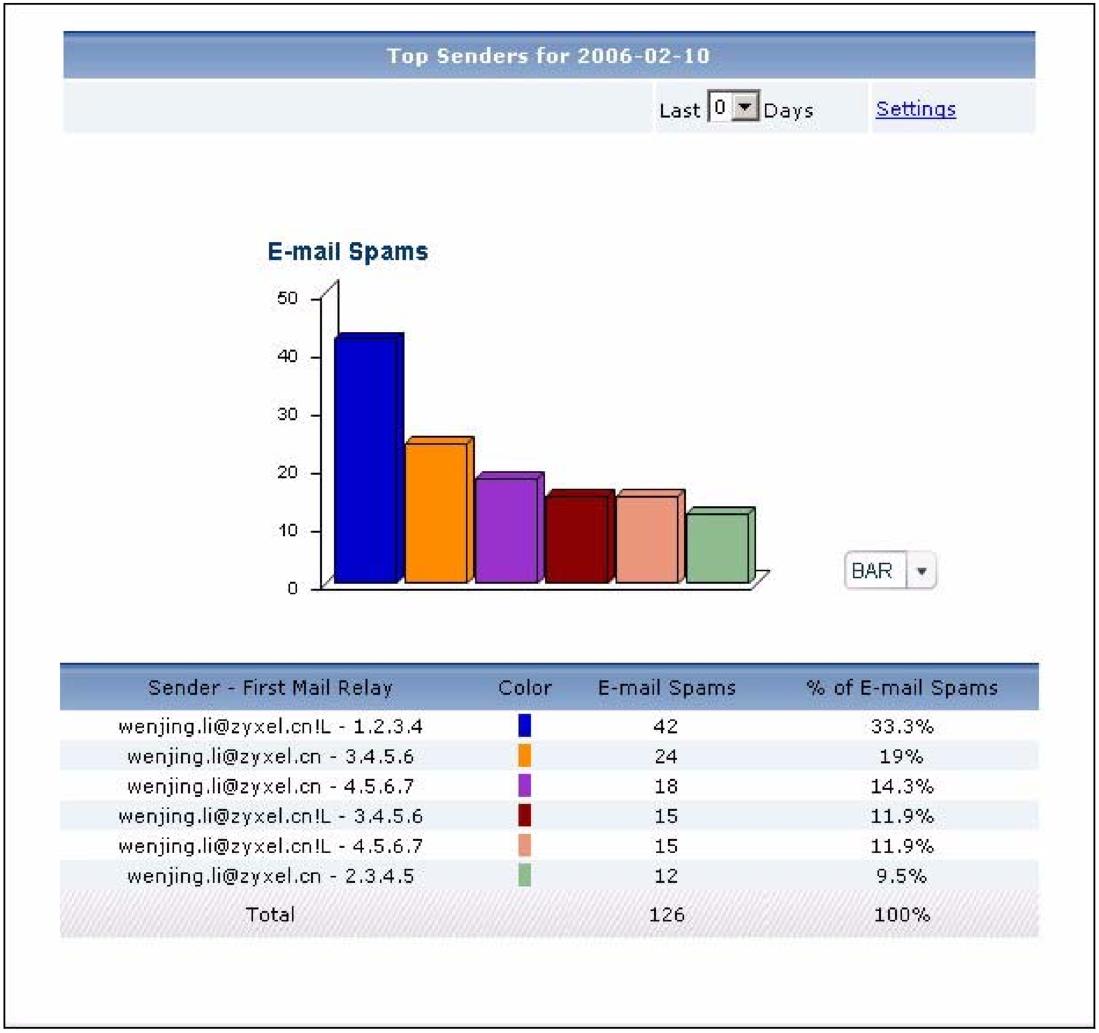
### 34.4.3 Top Spam Senders

Use this report to look at the top combinations of senders of spam messages and the first SMTP server to which the sender sends spam. For example, if a sender sends spam through two SMTP servers, there are two entries for the sender, one with each SMTP server.

To look at anti-spam reports, each device must record anti-spam messages in its log. See the User’s Guide for each device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Spam** is enabled.

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

**Figure 252** Network Attack > AntiSpam > Top Senders



Top Senders for 2006-02-10

Last 0 ▾ Days Settings

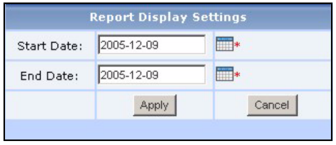
| Sender - First Mail Relay | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| wenjing.li@zyxel.cn!L - 1.2.3.4 | 🟦 | 42 | 33.3% |
| wenjing.li@zyxel.cn - 3.4.5.6 | 🟧 | 24 | 19% |
| wenjing.li@zyxel.cn - 4.5.6.7 | 🟪 | 18 | 14.3% |
| wenjing.li@zyxel.cn!L - 3.4.5.6 | 🟥 | 15 | 11.9% |
| wenjing.li@zyxel.cn!L - 4.5.6.7 | 🟥 | 15 | 11.9% |
| wenjing.li@zyxel.cn - 2.3.4.5 | 🟩 | 12 | 9.5% |
| Total | | 126 | 100% |

Each field is described in the following table.

**Table 220** Network Attack > AntiSpam > Top Senders

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |

**Table 220** Network Attack > AntiSpam > Top Senders (continued)

| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Sender - First Mail Relay | This field displays the top combinations of senders of spam and the first SMTP server to which spam is sent using the selected device, sorted by the number of spam messages sent for each combination.<br>Each sender is identified by its e-mail address.<br>Each SMTP server is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, “www.yahoo.com/200.100.20.10”). |
| Color | This field displays what color represents each sender in the graph. |
| E-mail Spams | This field displays how many spam messages each sender sent. |
| % of E-mail Spams | This field displays what percentage of all spam messages was sent by each sender. |
| Total | This entry displays the totals for the senders above. |

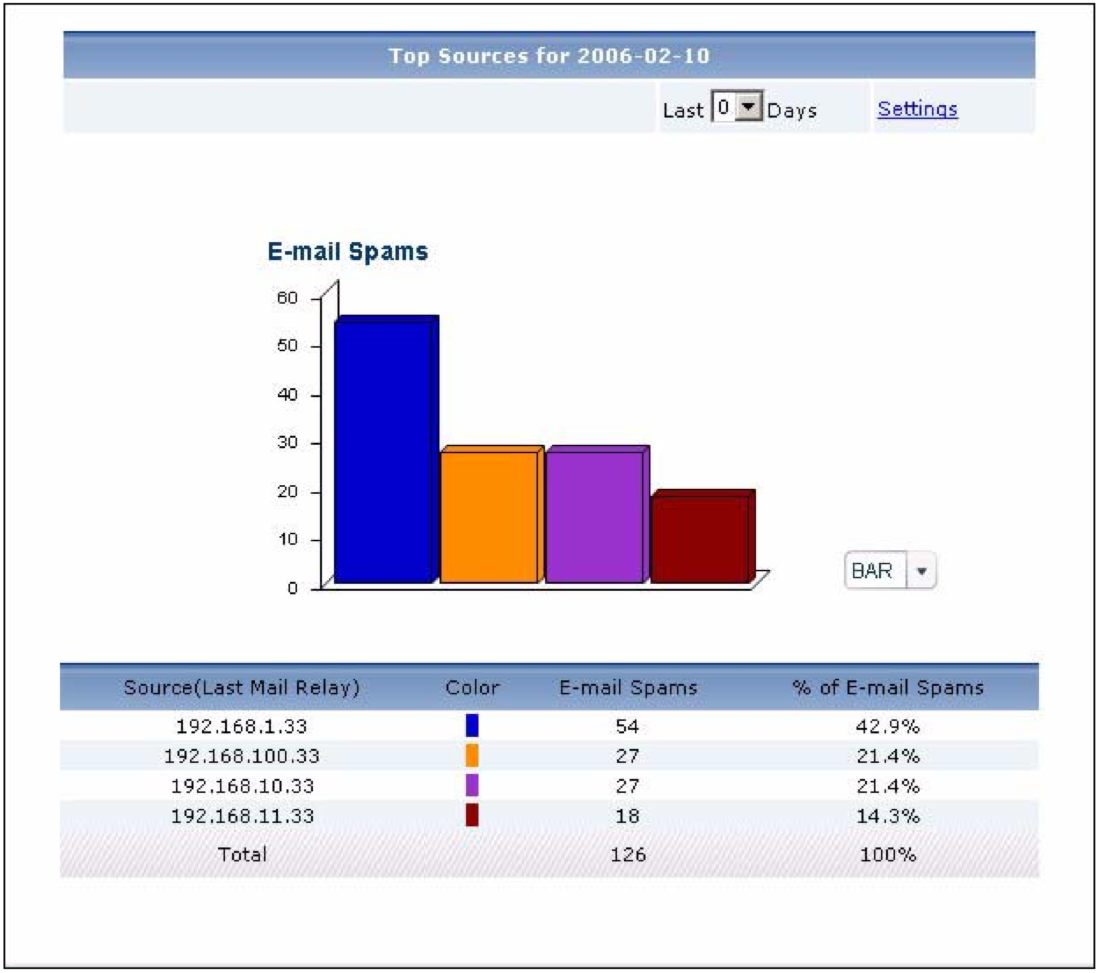
## 34.4.4 Top Spam Sources

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

To look at anti-spam reports, each device must record anti-spam messages in its log. See the User’s Guide for each device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **Anti-Spam** is enabled.

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

**Figure 253** Network Attack > AntiSpam > Top Sources



Top Sources for 2006-02-10

Last 0 Days Settings

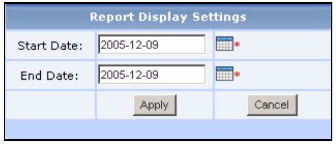
| Source(Last Mail Relay) | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 54 | 42.9% |
| 192.168.100.33 | 🟧 | 27 | 21.4% |
| 192.168.10.33 | 🟪 | 27 | 21.4% |
| 192.168.11.33 | 🟥 | 18 | 14.3% |
| Total | | 126 | 100% |

Each field is described in the following table.

**Table 221** Network Attack > AntiSpam > Top Sources

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |

**Table 221** Network Attack > AntiSpam > Top Sources (continued)

| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Source (Last Mail Relay) | This field displays the top SMTP servers that sent spam blocked by the selected device, sorted by the number of spam messages from each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed.<br>Each SMTP server is identified by its IP address. If **DNS Reverse** is enabled in **System > VRPT Management > Configuration** (Section 26.8.4 on page 310), the table displays the domain name, if identifiable, with the IP address (for example, "www.yahoo.com/200.100.20.10"). |
| Color | This field displays what color represents each source in the graph. |
| E-mail Spams | This field displays the number of spam messages from each source. |
| % of E-mail Spams | This field displays what percentage of all spam messages came from each source. |
| Total | This entry displays the totals for the sources above. |

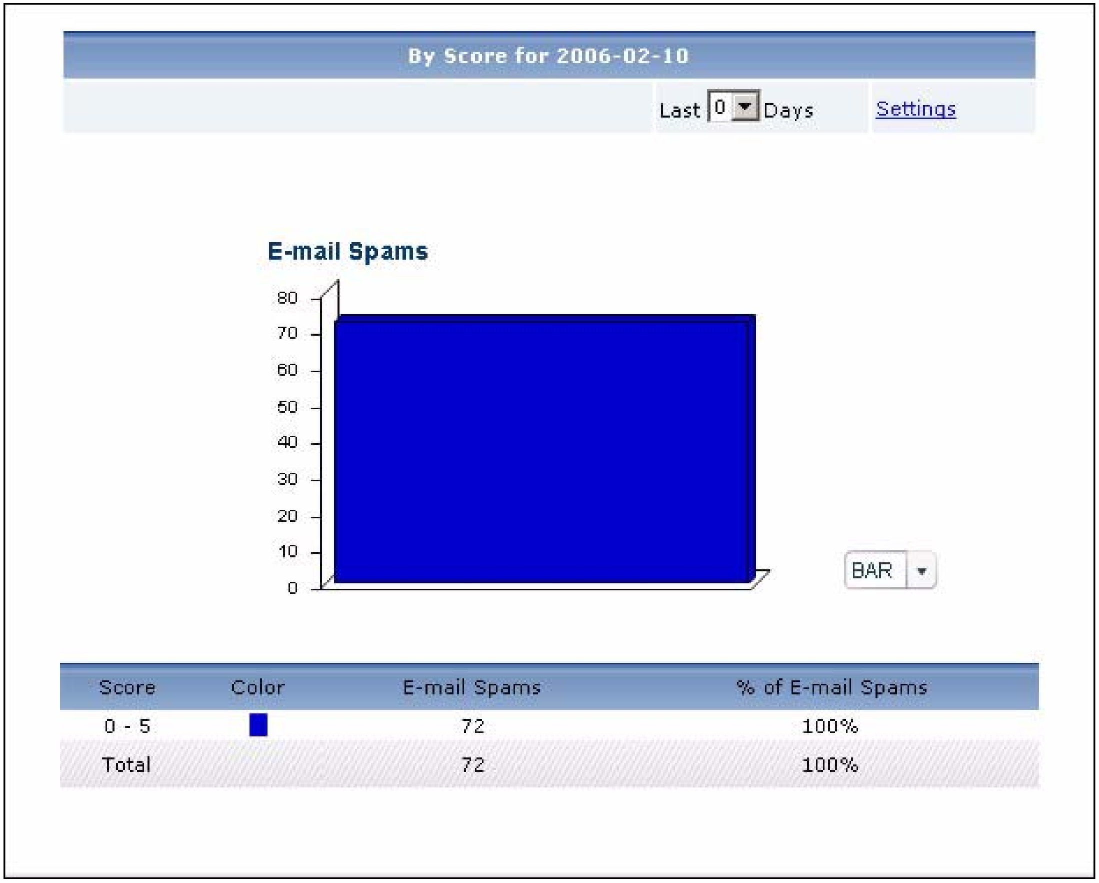
## 34.4.5 Top Spam Scores

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

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

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

**Figure 254** Network Attack > AntiSpam > By Score



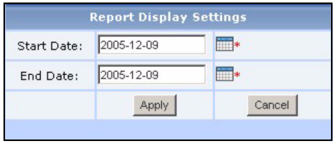
| Score | Color | E-mail Spams | % of E-mail Spams |
|---|---|---|---|
| 0 - 5 | 🟦 | 72 | 100% |
| Total | | 72 | 100% |

Each field is described in the following table.

**Table 222** Network Attack > AntiSpam > By Score

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |

**Table 222** Network Attack > AntiSpam > By Score (continued)

| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br>Apply Cancel<br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Score | This field displays the top scores calculated for spam messages by the selected device, sorted by the number of spam messages from each score. If the number of scores is less than the maximum number of records displayed in this table, every score is displayed. |
| Color | This field displays what color represents each score in the graph. |
| E-mail Spams | This field displays the number of spam messages from each score. |
| % of E-mail Spams | This field displays what percentage of all spam messages came from each score. |
| Total | This entry displays the totals for the scores above. |

# 35

# Security Policy

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

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

## 35.1 Blocked Web Accesses

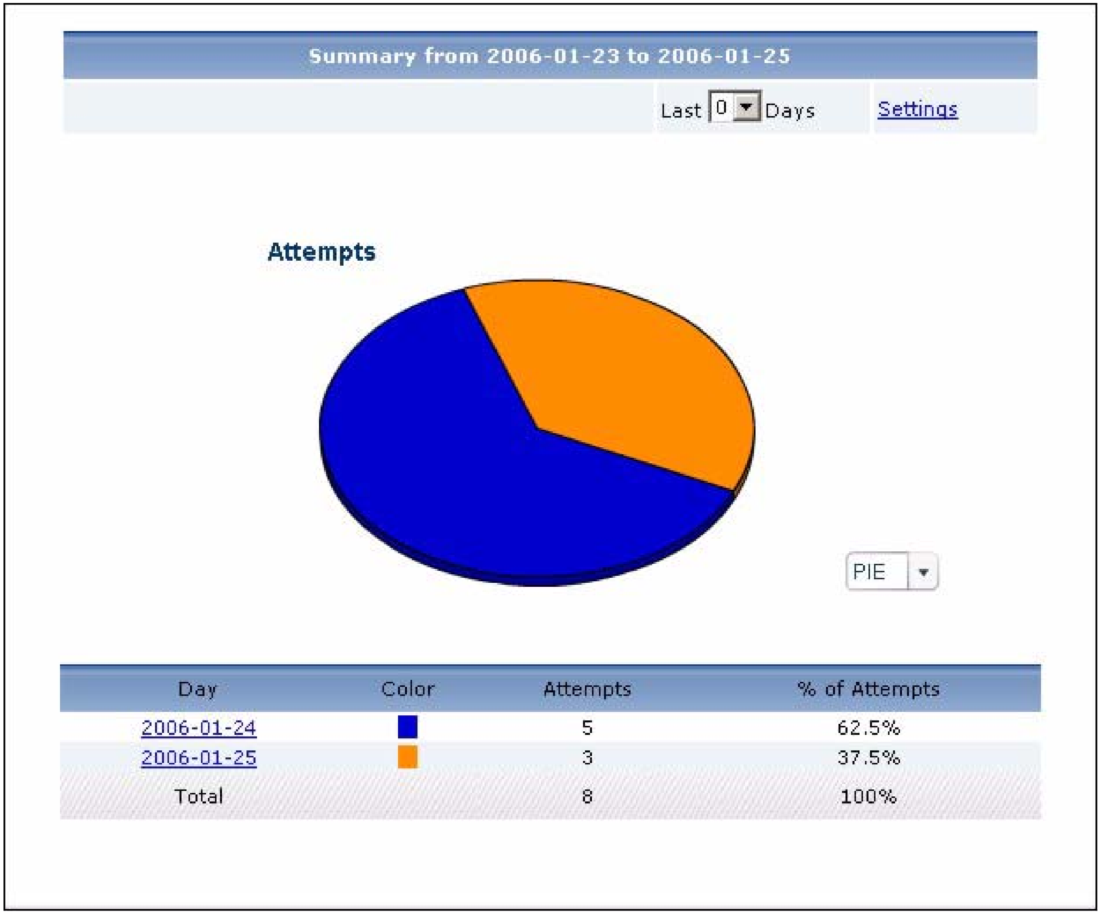
Use this report to look at the number of attempts to access blocked web sites by time interval as well as top blocked sites and hosts.

### 35.1.1 Web Block Summary

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

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

**Figure 255** Security Policy > WEB Blocked > Summary



Summary from 2006-01-23 to 2006-01-25

Last 0 Days Settings

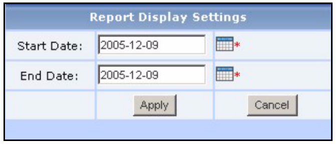
| Day | Color | Attempts | % of Attempts |
|---|---|---|---|
| 2006-01-24 | 🟦 | 5 | 62.5% |
| 2006-01-25 | 🟧 | 3 | 37.5% |
| Total | | 8 | 100% |

Each field is described in the following table.

**Table 223** Security Policy > WEB Blocked > Summary

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

**Table 223** Security Policy > WEB Blocked > Summary (continued)

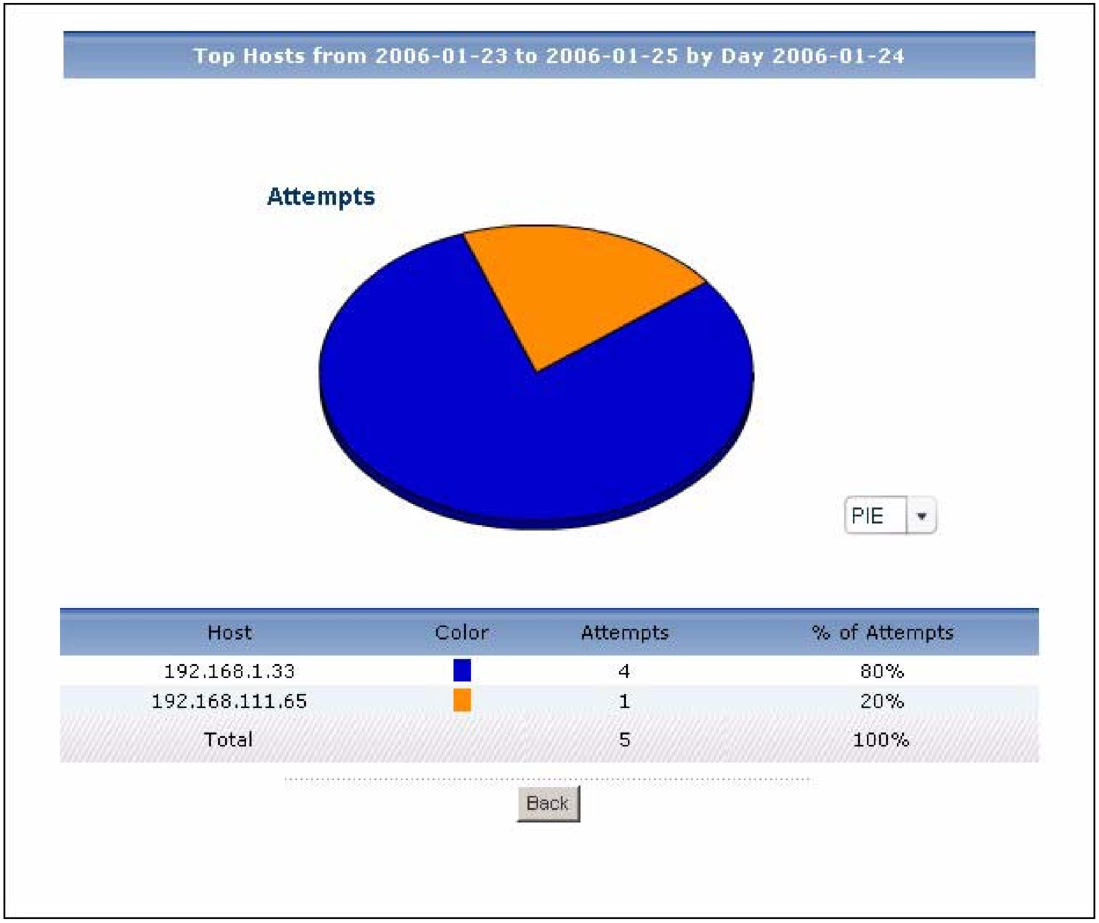
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09 *<br>End Date: 2005-12-09 *<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top sources of attempts to access blocked web sites in the selected time interval. The **Web Block Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| Attempts | This field displays the number of attempts by each source to access blocked web sites in the selected time interval. |
| % of Attempts | This field displays what percentage of all attempts was handled in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

### 35.1.2 Web Block Summary Drill-Down

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

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

**Figure 256** Security Policy > WEB Blocked > Summary > Drill-Down



Top Hosts from 2006-01-23 to 2006-01-25 by Day 2006-01-24

| Host | Color | Attempts | % of Attempts |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 4 | 80% |
| 192.168.111.65 | 🟧 | 1 | 20% |
| Total | | 5 | 100% |

Each field is described in the following table.

**Table 224** Security Policy > WEB Blocked > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Attempts | This field displays how much traffic (in megabytes) the device handled for each source in the selected time interval. |
| % of Attempts | This field displays what percentage of all traffic in the selected time interval was attributed to each source. |

**Table 224** Security Policy > WEB Blocked > Summary > Drill-Down (continued)

| 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. |

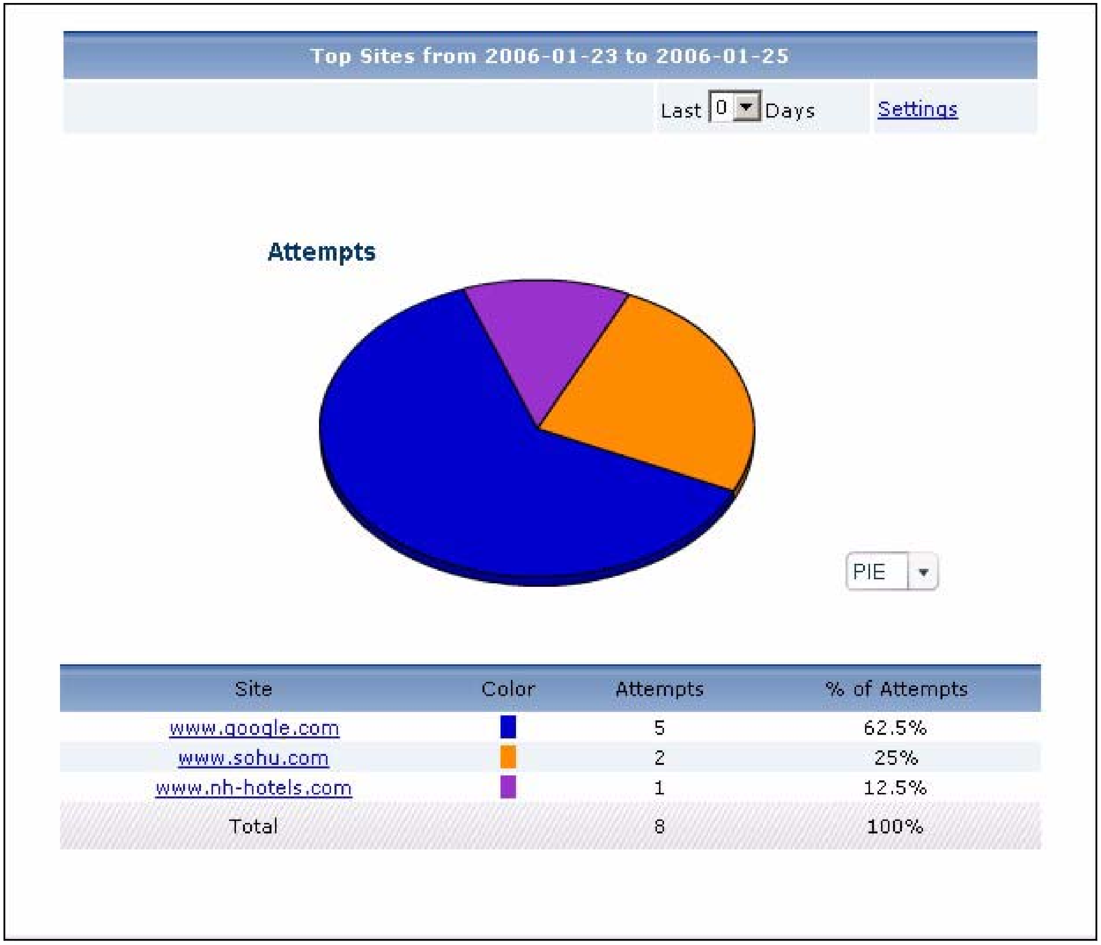
### 35.1.3 Top Blocked Web Sites

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

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

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

**Figure 257** Security Policy > WEB Blocked > Top Sites



Top Sites from 2006-01-23 to 2006-01-25

Last 0 Days Settings

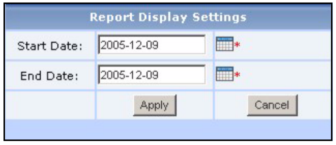
| Site | Color | Attempts | % of Attempts |
|---|---|---|---|
| www.google.com | 🟦 | 5 | 62.5% |
| www.sohu.com | 🟧 | 2 | 25% |
| www.nh-hotels.com | 🟪 | 1 | 12.5% |
| Total | | 8 | 100% |

Each field is described in the following table.

**Table 225** Security Policy > WEB Blocked > Top Sites

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

**Table 225** Security Policy > WEB Blocked > Top Sites (continued)

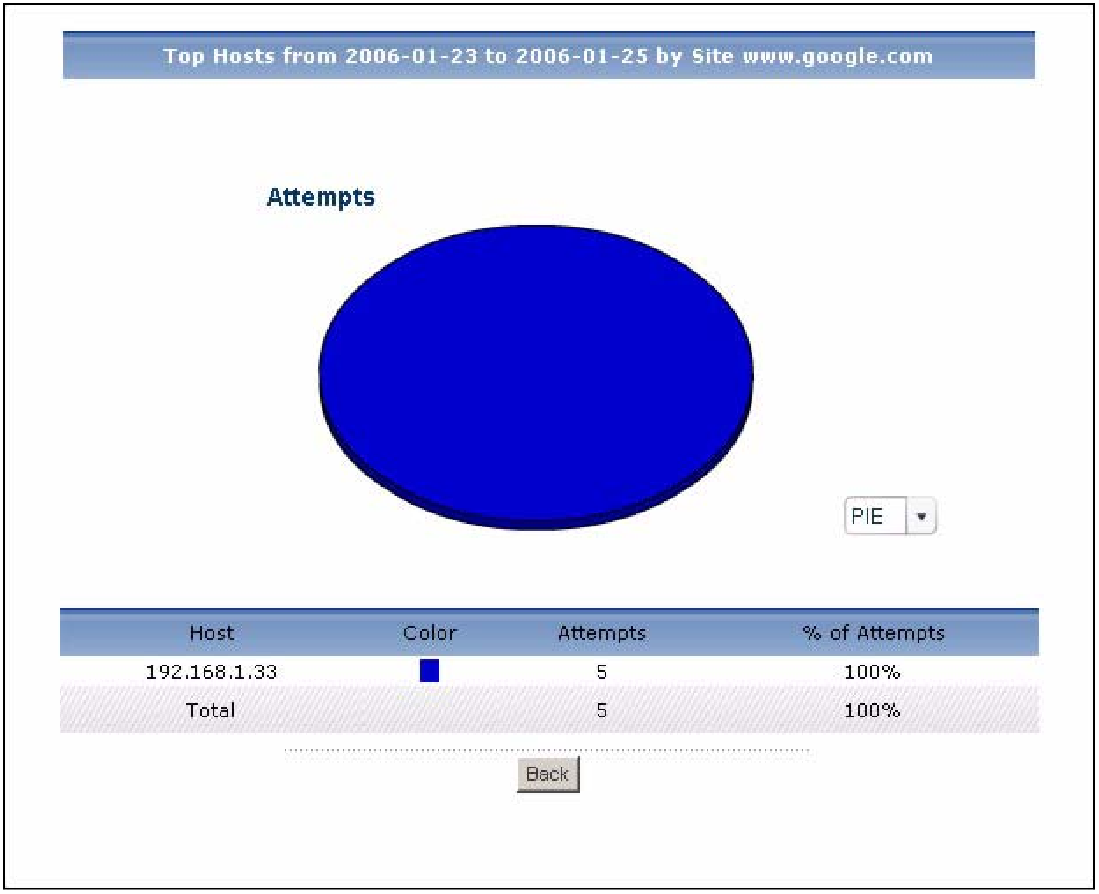
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each destination is identified by its domain name. Click on a destination to look at the top sources of blocked web traffic for the selected destination. The **Top Blocked Web Sites Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Attempts | This field displays how much traffic (in megabytes) the device handled for each destination. |
| % of Attempts | This field displays what percentage of all attempts to access blocked web sites was made to each destination. |
| Total | This entry displays the totals for the destinations above. |

### 35.1.4 Top Blocked Web Sites Drill-Down

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

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

**Figure 258** Security Policy > WEB Blocked > Top Sites > Drill-Down



Top Hosts from 2006-01-23 to 2006-01-25 by Site www.google.com

| Host | Color | Attempts | % of Attempts |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 5 | 100% |
| Total | | 5 | 100% |

Each field is described in the following table.

**Table 226** Security Policy > WEB Blocked > Top Sites > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Attempts | This field displays the number of attempts from each source to the selected destination. |
| % of Attempts | This field displays what percentage of all attempts to access blocked web sites was made by each source to the selected destination. |

**Table 226** Security Policy > WEB Blocked > Top Sites > Drill-Down (continued)

| 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. |

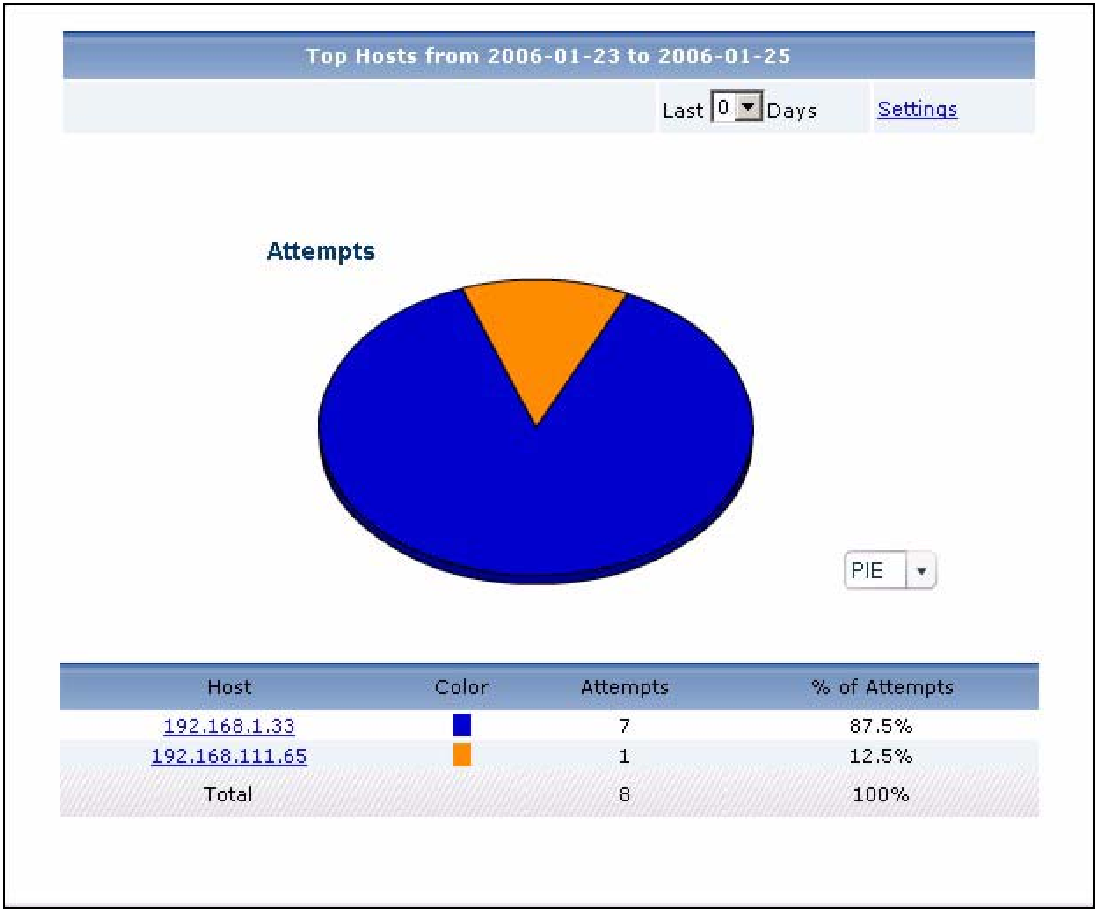
## 35.1.5 Top Blocked Web Hosts

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

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

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

**Figure 259** Security Policy > WEB Blocked > Top Hosts



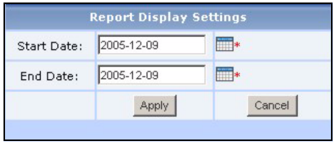
Top Hosts from 2006-01-23 to 2006-01-25

Last 0 Days Settings

| Host | Color | Attempts | % of Attempts |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 7 | 87.5% |
| 192.168.111.65 | 🟧 | 1 | 12.5% |
| Total | | 8 | 100% |

Each field is described in the following table.

**Table 227** Security Policy > WEB Blocked > Top Hosts

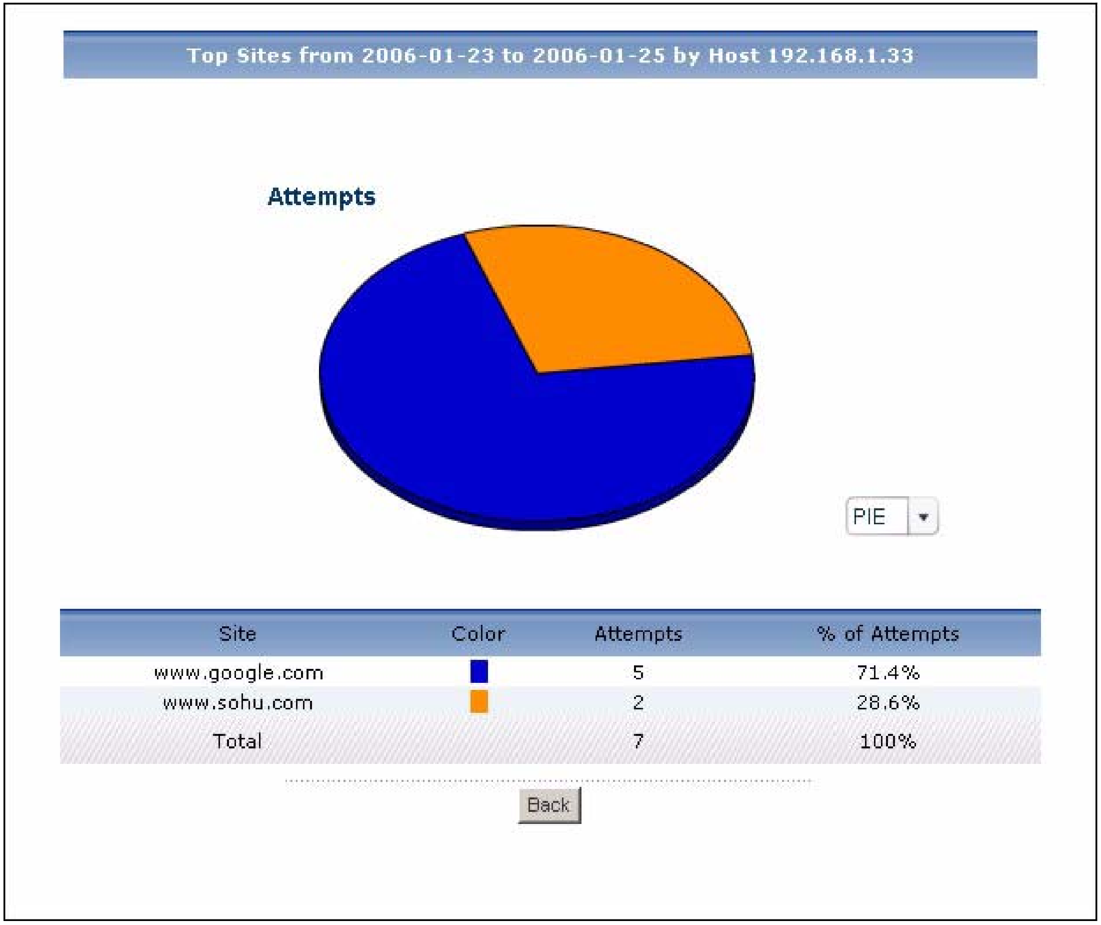
| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of blocked web traffic for the selected source. The **Top Blocked Web Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Attempts | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of Attempts | This field displays what percentage of all attempts to access blocked web sites was made from each source. |
| Total | This entry displays the totals for the sources above. |

## 35.1.6 Top Blocked Web Hosts Drill-Down

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

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

**Figure 260** Security Policy > WEB Blocked > Top Hosts > Drill-Down



Top Sites from 2006-01-23 to 2006-01-25 by Host 192.168.1.33

| Site | Color | Attempts | % of Attempts |
|---|---|---|---|
| www.google.com | 🟦 | 5 | 71.4% |
| www.sohu.com | 🟧 | 2 | 28.6% |
| Total | | 7 | 100% |

Each field is described in the following table.

**Table 228** Security Policy > WEB Blocked > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• 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.<br>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 228** Security Policy > WEB Blocked > Top Hosts > Drill-Down (continued)

| 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. |
| 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. |

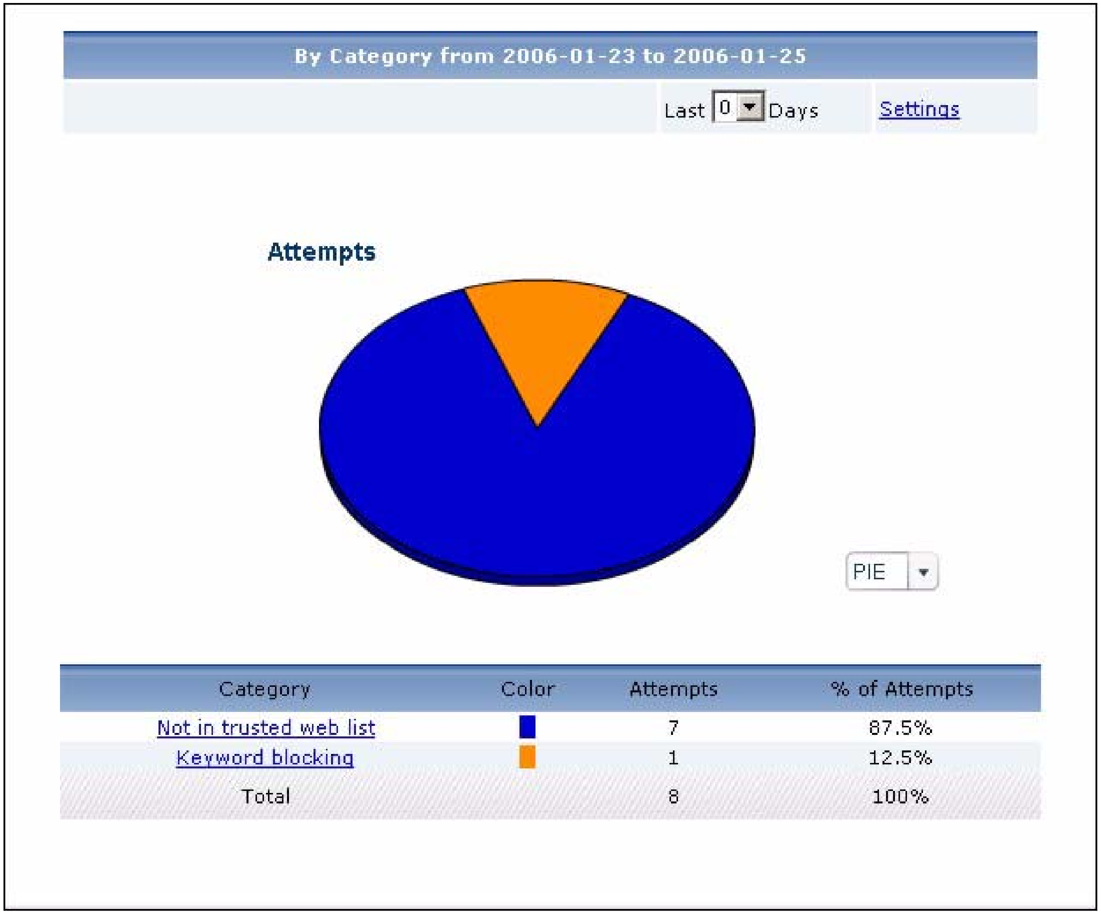
### 35.1.7 Top Blocked Web Categories

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

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

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

**Figure 261** Security Policy > WEB Blocked > By Category



By Category from 2006-01-23 to 2006-01-25

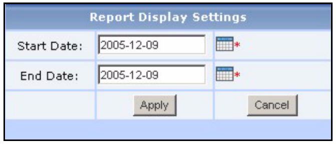
| Category | Color | Attempts | % of Attempts |
|---|---|---|---|
| Not in trusted web list | 🟦 | 7 | 87.5% |
| Keyword blocking | 🟧 | 1 | 12.5% |
| Total | | 8 | 100% |

Each field is described in the following table.

**Table 229** Security Policy > WEB Blocked > By Category

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

**Table 229** Security Policy > WEB Blocked > By Category (continued)

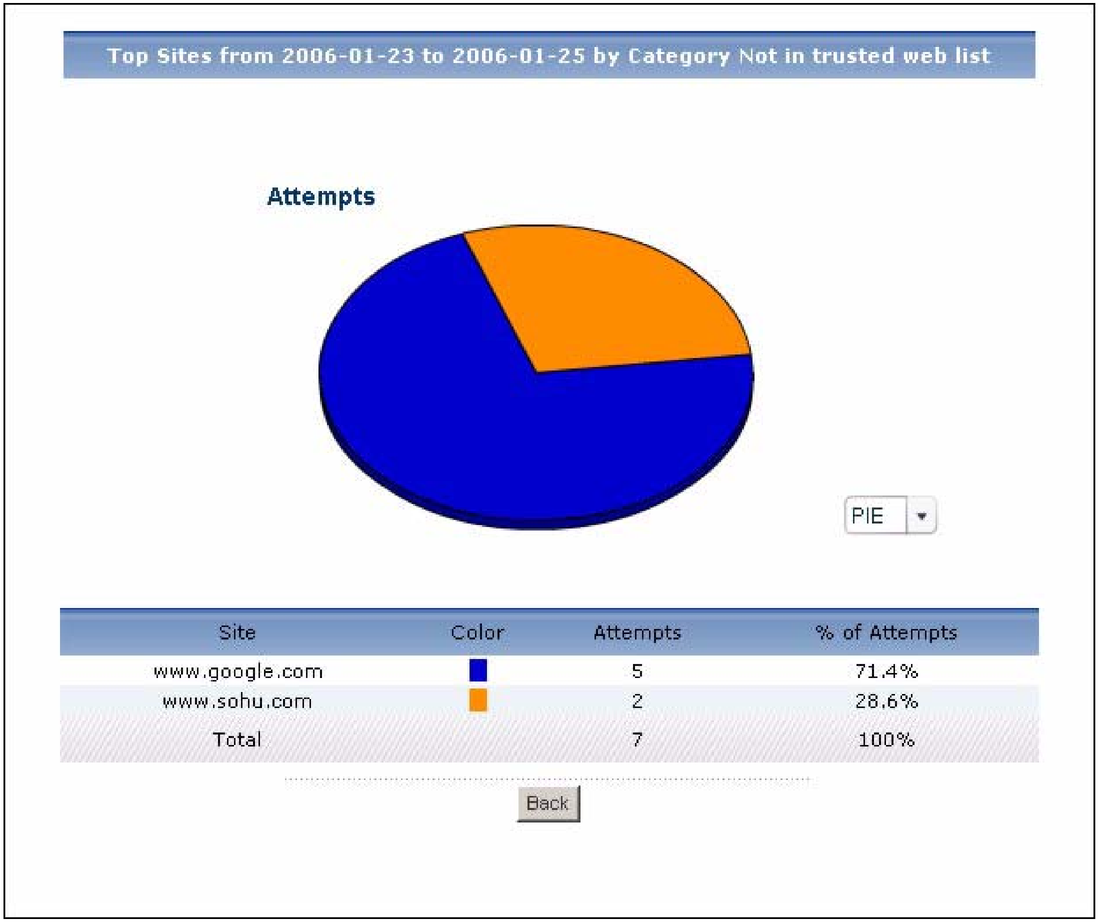
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Category | This field displays the top categories of blocked web traffic in the selected device, sorted by the number of attempts for each one. If the number of categories is less than the maximum number of records displayed in this table, every source is displayed.<br>Click on a source to look at the top destinations of blocked web traffic for the selected category. The **Top Blocked Web Categories Drill-Down** report appears. |
| Color | This field displays what color represents each category in the graph. |
| Attempts | This field displays the number of attempts to access allowed web sites in each category. |
| % of Attempts | This field displays what percentage of all attempts to access blocked web sites belong to each category. |
| Total | This entry displays the totals for the categories above. |

### 35.1.8 Top Blocked Web Categories Drill-Down

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

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

**Figure 262** Security Policy > WEB Blocked > By Category > Drill-Down


Top Sites from 2006-01-23 to 2006-01-25 by Category Not in trusted web list

| Site | Color | Attempts | % of Attempts |
|---|---|---|---|
| www.google.com | 🟦 | 5 | 71.4% |
| www.sohu.com | 🟧 | 2 | 28.6% |
| Total | | 7 | 100% |

Each field is described in the following table.

**Table 230** Security Policy > WEB Blocked > By Category > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Site | This field displays the top destinations of blocked web traffic that belongs to the selected category, sorted by the number of attempts to each one.<br>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. |

**Table 230** Security Policy > WEB Blocked > By Category > Drill-Down (continued)

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

## 35.2 Allowed Web Accesses

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

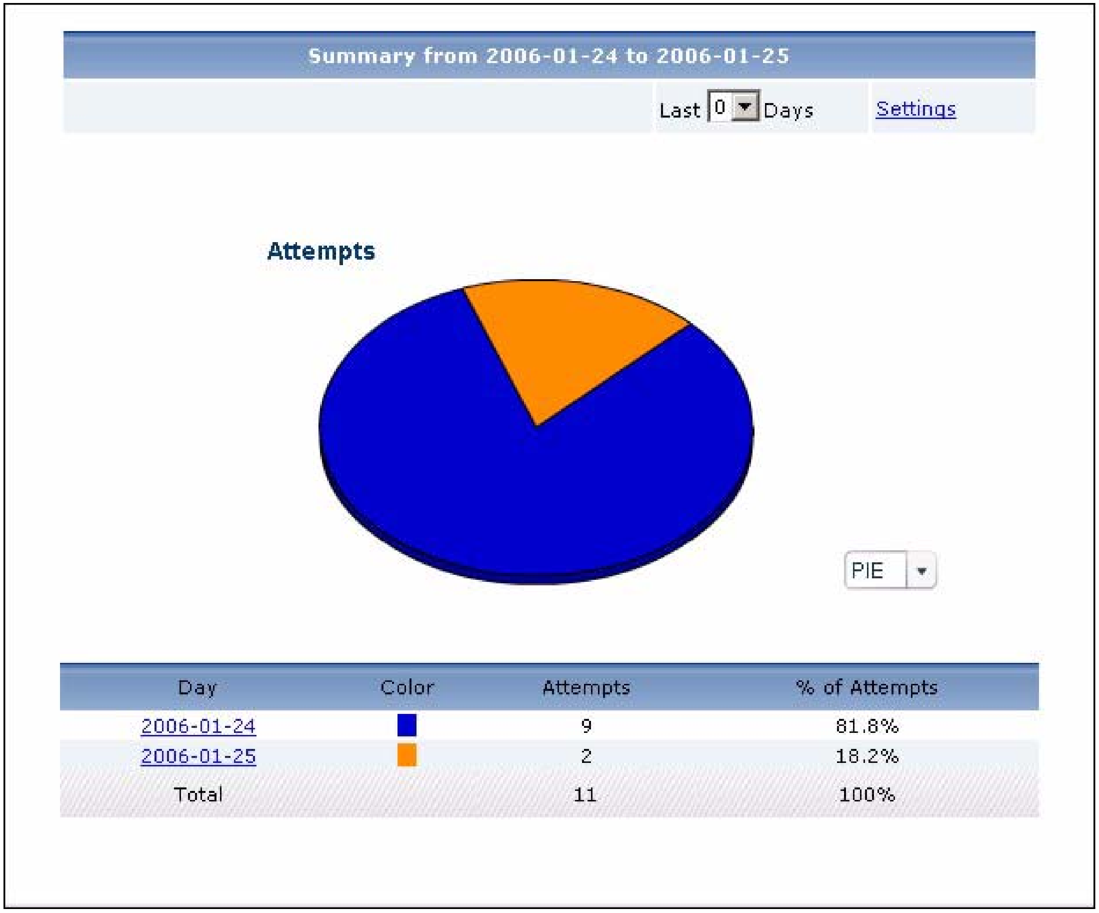
### 35.2.1 Web Allowed Summary

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

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

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

**Figure 263** Security Policy > WEB Allowed > Summary



Summary from 2006-01-24 to 2006-01-25

Last 0 Days Settings

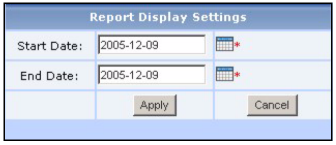
| Day | Color | Attempts | % of Attempts |
|---|---|---|---|
| 2006-01-24 | 🟦 | 9 | 81.8% |
| 2006-01-25 | 🟧 | 2 | 18.2% |
| Total | | 11 | 100% |

Each field is described in the following table.

**Table 231** Security Policy > WEB Allowed > Summary

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

**Table 231** Security Policy > WEB Allowed > Summary (continued)

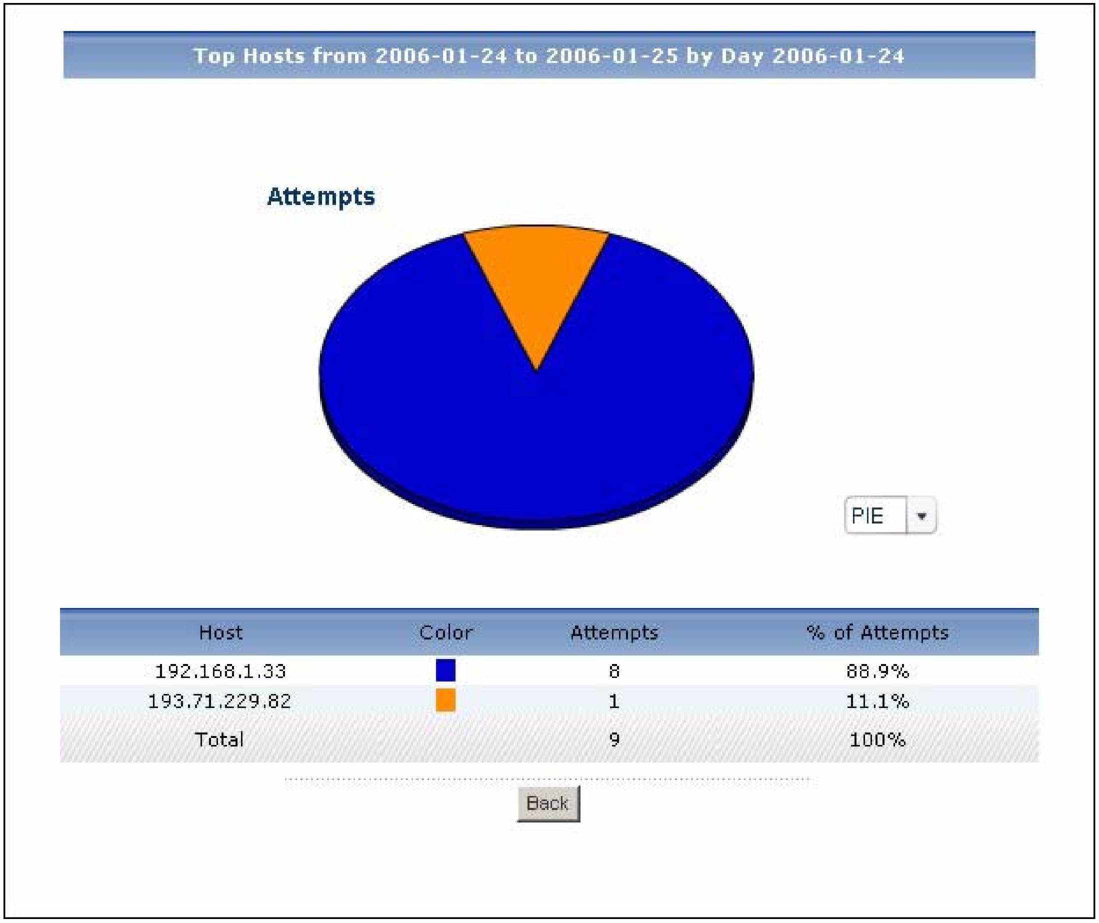
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Hour (Day) | This field displays each time interval in chronological order. If you select one day of historical information or less (in the **Last ... Days** or **Settings** field) and it is in the last seven days (today is day one), the time interval is hours (in 24-hour format). Otherwise, the time interval is days.<br>Click on a time interval to look at the top sources of attempts to access allowed web sites in the selected time interval. The **Web Allowed Summary Drill-Down** report appears. |
| Color | This field displays what color represents each time interval in the graph. |
| Attempts | This field displays the number of attempts to access allowed web sites in each time interval. |
| % of Attempts | This field displays the percentage of all attempts in each time interval. |
| Total | This entry displays the totals for the time intervals above. |

## 35.2.2 Web Allowed Summary Drill-Down

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

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

**Figure 264** Security Policy > WEB Allowed > Summary > Drill-Down



Top Hosts from 2006-01-24 to 2006-01-25 by Day 2006-01-24

| Host | Color | Attempts | % of Attempts |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 8 | 88.9% |
| 193.71.229.82 | 🟧 | 1 | 11.1% |
| Total | | 9 | 100% |

Each field is described in the following table.

**Table 232** Security Policy > WEB Allowed > Summary > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Host | This field displays the top sources of attempts to access allowed web sites in the selected time interval, sorted by the number of attempts by each one.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Attempts | This field displays the number of attempts by each source to access allowed web sites in the selected time interval. |
| % of Attempts | This field displays the percentage of all attempts in the selected time interval attributed to each source. |

**Table 232** Security Policy > WEB Allowed > Summary > Drill-Down (continued)

| 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. |

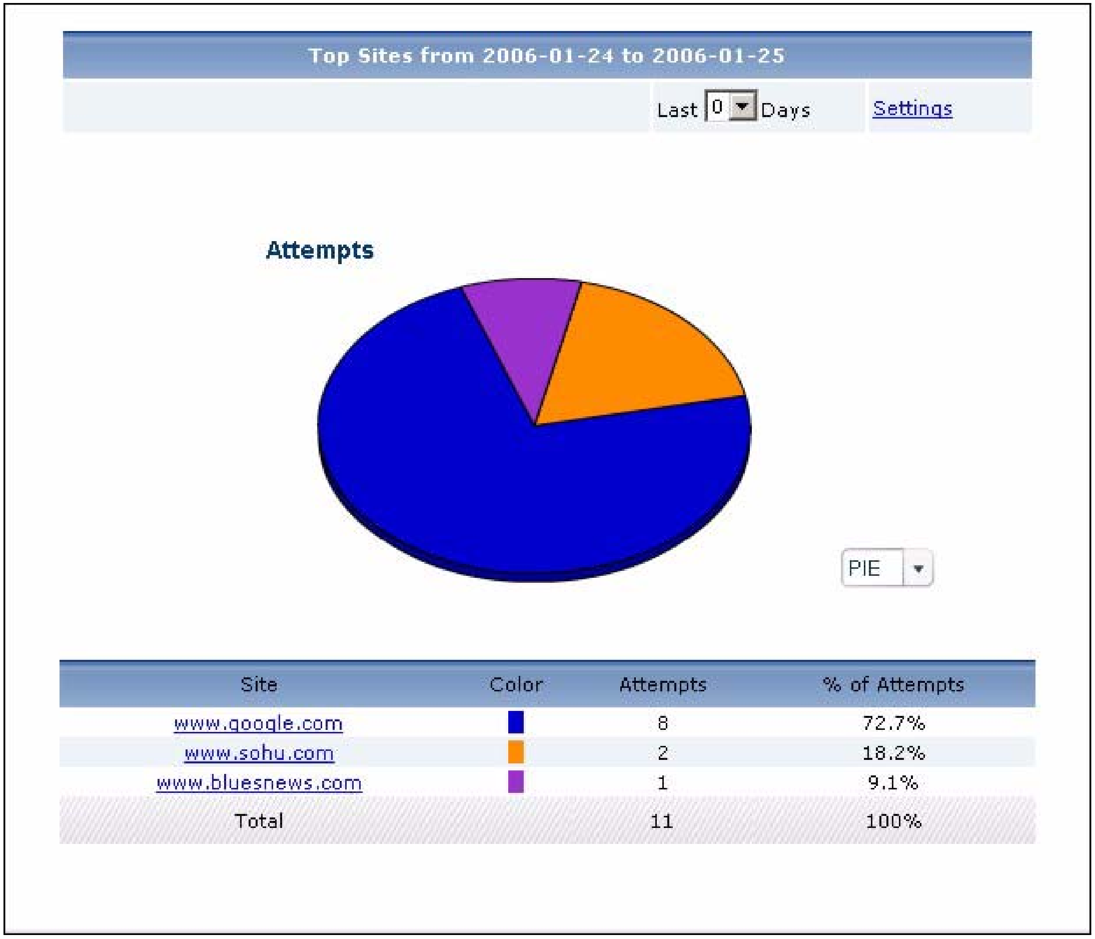
### 35.2.3 Top Allowed Web Sites

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

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

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

**Figure 265** Security Policy > WEB Allowed > Top Sites



Top Sites from 2006-01-24 to 2006-01-25

Last 0 Days Settings

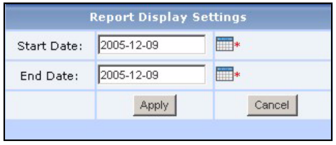
| Site | Color | Attempts | % of Attempts |
|---|---|---|---|
| www.google.com | 🟦 | 8 | 72.7% |
| www.sohu.com | 🟧 | 2 | 18.2% |
| www.bluesnews.com | 🟪 | 1 | 9.1% |
| Total | | 11 | 100% |

Each field is described in the following table.

**Table 233** Security Policy > WEB Allowed > Top Sites

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

**Table 233** Security Policy > WEB Allowed > Top Sites (continued)

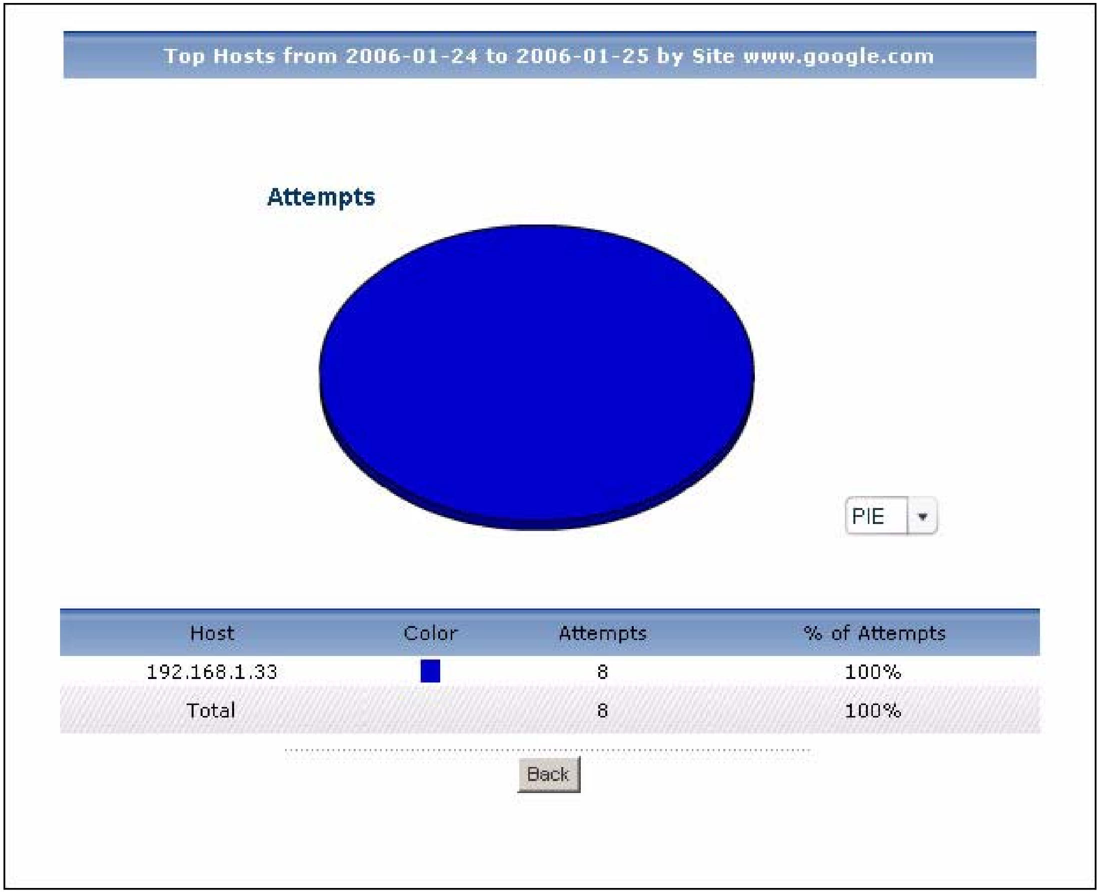
| LABEL | DESCRIPTION |
|---|---|
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Site | This field displays the top destinations of forwarded web traffic in the selected device, sorted by the number of attempts for each one. If the number of destinations is less than the maximum number of records displayed in this table, every destination is displayed.<br>Each destination is identified by its domain name. Click on a destination to look at the top sources of forwarded web traffic for the selected destination. The **Top Forwarded Web Sites Drill-Down** report appears. |
| Color | This field displays what color represents each destination in the graph. |
| Attempts | This field displays the number of attempts for each destination. |
| % of Attempts | This field displays what percentage of all attempts to access allowed web sites was made to each destination. |
| Total | This entry displays the totals for the destinations above. |

## 35.2.4 Top Allowed Web Sites Drill-Down

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

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

**Figure 266** Security Policy > WEB Allowed > Top Sites > Drill-Down



Top Hosts from 2006-01-24 to 2006-01-25 by Site www.google.com

| Host | Color | Attempts | % of Attempts |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 8 | 100% |
| Total | | 8 | 100% |

Each field is described in the following table.

**Table 234** Security Policy > WEB Allowed > Top Sites > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Host | This field displays the top sources of forwarded web traffic to the selected destination, sorted by the number of attempts attributed to each one.<br>Each source is identified by its IP address. |
| Color | This field displays what color represents each source in the graph. |
| Attempts | This field displays the number of attempts from each source to the selected destination. |
| % of Attempts | This field displays what percentage of all attempts to access allowed web sites was made by each source to the selected destination. |

**Table 234** Security Policy > WEB Allowed > Top Sites > Drill-Down (continued)

| 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. |

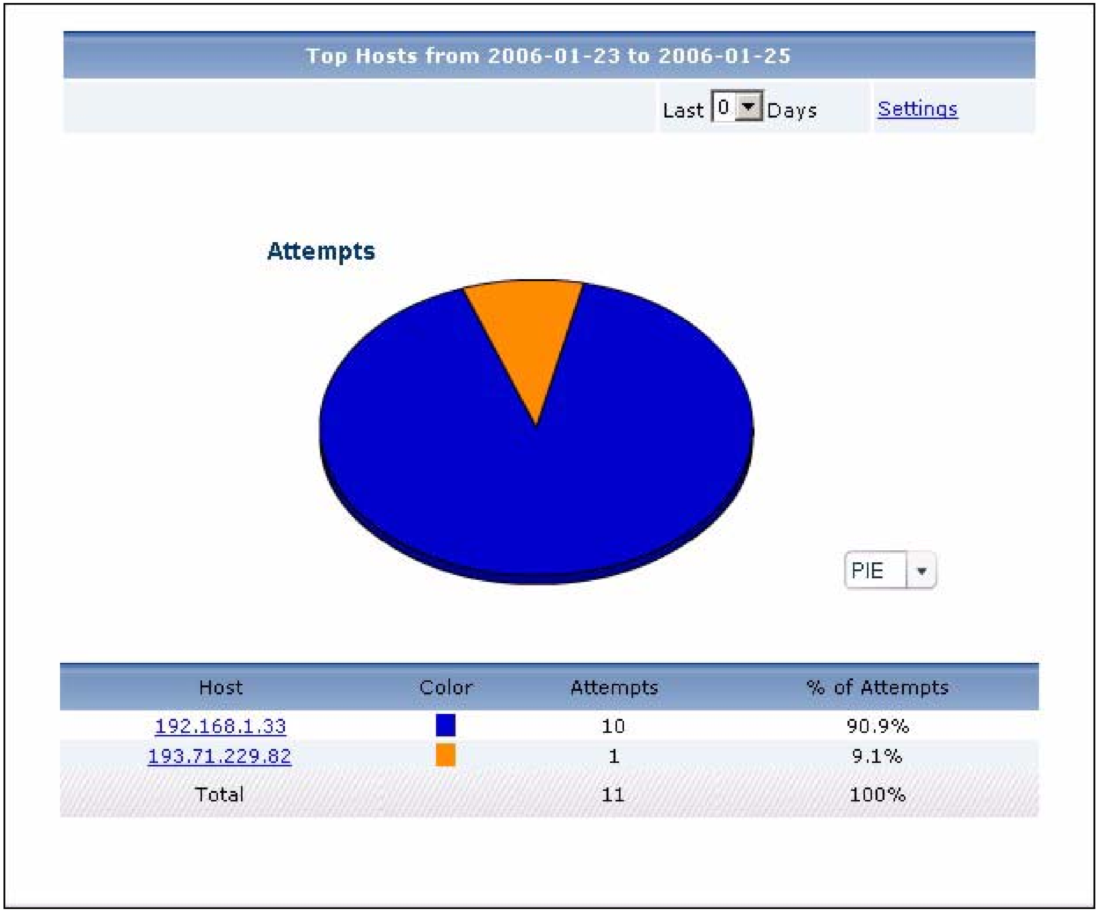
## 35.2.5 Top Allowed Web Hosts

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

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

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

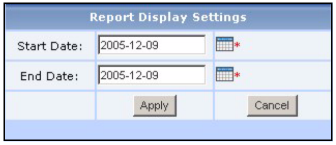
**Figure 267** Security Policy > WEB Allowed > Top Hosts



| Host | Color | Attempts | % of Attempts |
|---|---|---|---|
| 192.168.1.33 | 🟦 | 10 | 90.9% |
| 193.71.229.82 | 🟧 | 1 | 9.1% |
| Total | | 11 | 100% |

Each field is described in the following table.

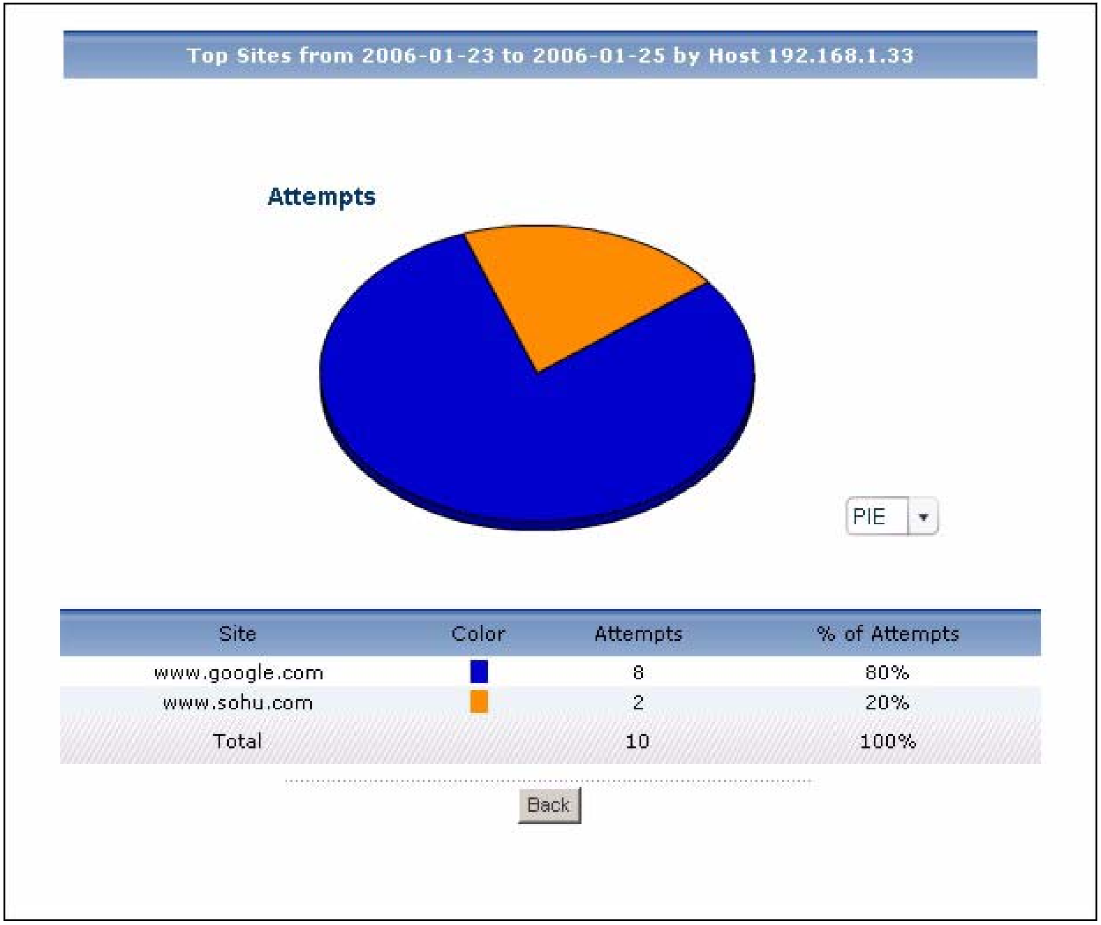
**Table 235** Security Policy > WEB Allowed > Top Hosts

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Use this field or **Settings** to specify what historical information is included in the report. Select how many days, ending (and including) today, you want to include.<br>When you change this field, the report updates automatically. This field returns to zero, so you can refresh the report by selecting it again. You can see the current date range in the title.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| Settings | Use this field or **Last ... Days** to specify what historical information is included in the report. Click **Settings**. The **Report Display Settings** screen appears.<br><br>Report Display Settings<br>Start Date: 2005-12-09<br>End Date: 2005-12-09<br> <br>Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Stored Log Days** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.<br>This field resets to its default value when you click a menu item in the function window (including the menu item for the same report). It does not reset when you open or close drill-down reports. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Host | This field displays the top sources of forwarded web traffic in the selected device, sorted by the number of attempts for each one. If the number of sources is less than the maximum number of records displayed in this table, every source is displayed.<br>Each source is identified by its IP address. Click on a source to look at the top destinations of forwarded web traffic for the selected source. The **Top Forwarded Web Hosts Drill-Down** report appears. |
| Color | This field displays what color represents each source in the graph. |
| Attempts | This field displays how much traffic (in megabytes) the device handled for each source. |
| % of Attempts | This field displays what percentage of all attempts to access allowed web sites was made from each sources. |
| Total | This entry displays the totals for the sources above. |

## 35.2.6 Top Allowed Web Hosts Drill-Down

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

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


Top Sites from 2006-01-23 to 2006-01-25 by Host 192.168.1.33
Attempts
PIE
Back

| Site | Color | Attempts | % of Attempts |
|---|---|---|---|
| www.google.com | 🟦 | 8 | 80% |
| www.sohu.com | 🟧 | 2 | 20% |
| Total | | 10 | 100% |

**Figure 268** Security Policy > WEB Allowed > Top Hosts > Drill-Down

Each field is described in the following table.

**Table 236** Security Policy > WEB Allowed > Top Hosts > Drill-Down

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the drill-down report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| graph | The graph displays the information in the table visually.<br>• Select **PIE** chart or **BAR** chart in the drop-down list box. You can specify the **Default Chart Type** in **System > VRPT Management > Configuration**. See Section 26.8.4 on page 310.<br>• Move your mouse over a slice in the pie chart or a bar in the bar chart. The **yellow conversation box** identifies the slice or bar.<br>• Click on a slice in the pie chart to move it away from the pie chart a little. |
| Site | This field displays the top destinations of forwarded web traffic from the selected source, sorted by the number of attempts attributed to each one.<br>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 236** Security Policy > WEB Allowed > Top Hosts > Drill-Down (continued)

| 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. |
| 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. |

# 36

# Event

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

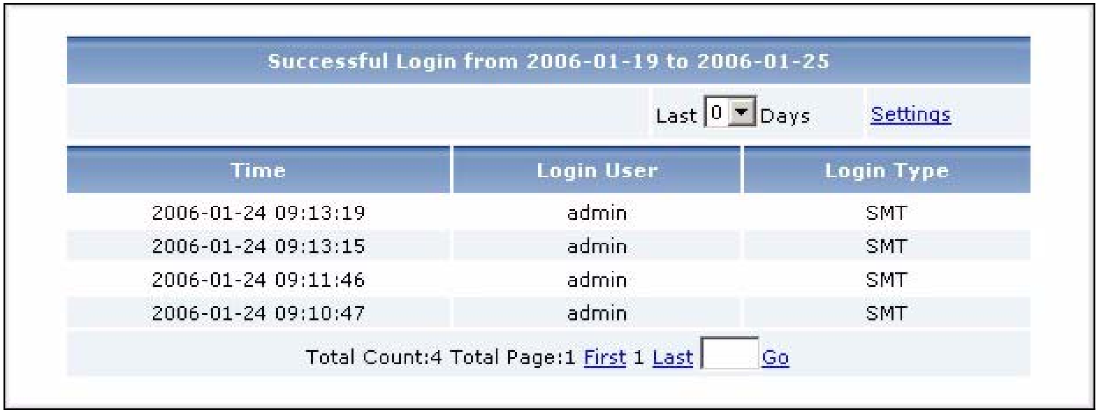
## 36.1 Successful Login Screen

Use this screen to look at who successfully logged into the device (for management or monitoring purposes). See Section 30.4 on page 339 for more information about the source data used by the report.

To use the authentication screens, each device must record authentication successes and failures in its log. See the User's Guide for each device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **System Maintenance** is enabled.

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

**Figure 269** Event > Device Login > Successful Login



Successful Login from 2006-01-19 to 2006-01-25

Last 0 Days Settings

| Time | Login User | Login Type |
|---|---|---|
| 2006-01-24 09:13:19 | admin | SMT |
| 2006-01-24 09:13:15 | admin | SMT |
| 2006-01-24 09:11:46 | admin | SMT |
| 2006-01-24 09:10:47 | admin | SMT |

Total Count:4 Total Page:1 First 1 Last Go

Each field is described in the following table.

**Table 237** Event > Device Login > Successful Login

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Select how many more days of information, ending with current information today, you want to look at. Select 0 if you only want to look at today's information. |
| 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 device, not the time the user logged into the device. |
| Login User | This field displays who logged into the selected device. |
| Login Type | This field displays what type of connection the user used to log into the device. |
| Total Count | This field displays how many records there are for the specified search criteria. |
| Total Page | This field displays how many screens it takes to display all the records. |
| First .. Last | Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.s |
| Go | Enter the page number you want to see, and click **Go**. |

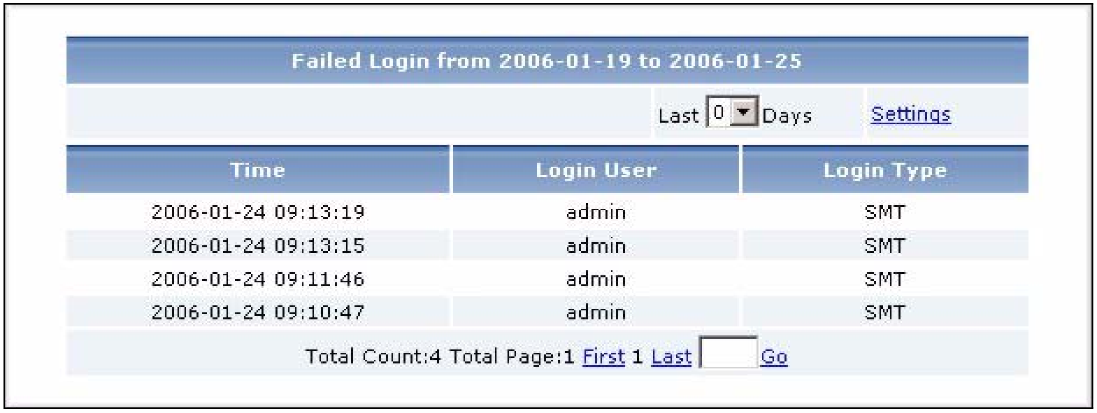
## 36.2 Failed Login Screen

Use this screen to look at who tried to log in into the device (for management or monitoring purposes) but failed. See Section 30.4 on page 339 for more information about the source data used by the report.

To use the authentication screens, each device must record authentication successes and failures in its log. See the User's Guide for each device for more information. In most devices, go to **Logs** > **Log Settings**, and make sure **System Maintenance** is enabled.

Click **Event** > **Device Login** > **Failed Login** to open the **Failed Login** screen.

**Figure 270** Event > Device Login > Failed Login



Failed Login from 2006-01-19 to 2006-01-25

Last 0 Days Settings

| Time | Login User | Login Type |
|---|---|---|
| 2006-01-24 09:13:19 | admin | SMT |
| 2006-01-24 09:13:15 | admin | SMT |
| 2006-01-24 09:11:46 | admin | SMT |
| 2006-01-24 09:10:47 | admin | SMT |

Total Count:4 Total Page:1 First 1 Last Go

Each field is described in the following table.

**Table 238** Event > Device Login > Failed Login

| LABEL | DESCRIPTION |
|---|---|
| title | This field displays the title of the statistical report. The title includes the date(s) you specified in the **Last Days** or **Settings** fields. |
| Last ... Days | Select how many more days of information, ending with current information today, you want to look at. Select 0 if you only want to look at today's information. |
| Settings | Click this if you want to specify the select any **Start Date** and **End Date**. The **Report Display Settings** screen appears. |
| Time | This field displays the time the Vantage Report server received the log entry from the device, not the time the user tried unsuccessfully to log into the device. |
| Login User | This field displays who tried unsuccessfully to log into the selected device. |
| Login Type | This field displays what type of connection the user used to try unsuccessfully to log into the device. |
| Total Count | This field displays how many records there are for the specified search criteria. |
| Total Page | This field displays how many screens it takes to display all the records. |
| First .. Last | Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.s |
| Go | Enter the page number you want to see, and click **Go**. |

# 37

# Log Viewer

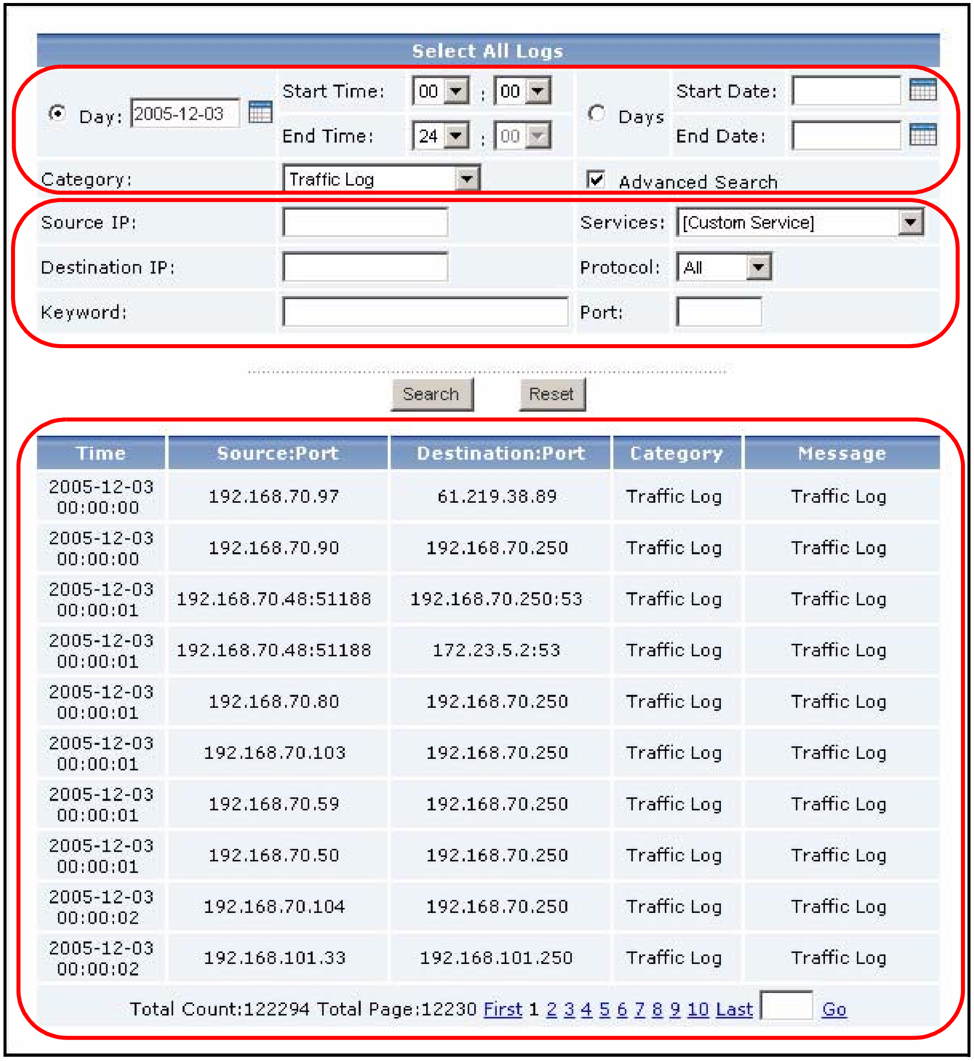
Use these screens to look at log entries for the selected device.

## 37.1 All Logs

See Section 30.3 on page 338 for more information about update frequencies for log entries. See Section 30.4 on page 339 for more information about the source data used by the report. Vantage Report consolidates log entries. See Appendix A on page 515 for Vantage Report's internal log consolidation frequency.

Use this screen to look at log entries for the selected device. To open this screen, click **Log Viewer** > **All Logs**.

**Figure 271** Log Viewer > All Logs



Select All Logs

● Day: 2005-12-03 Start Time: 00 : 00 ○ Days Start Date:

End Time: 24 : 00 End Date:

Category: Traffic Log ☑ Advanced Search

Source IP: Services: [Custom Service]

Destination IP: Protocol: All

Keyword: Port:

Search Reset

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

Total Count:122294 Total Page:12230 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 three rows (above **Search** and **Reset**) appear if you do not select **All Categories** in the **Category** field and if you select **Advanced Search**. The table of log entries appears after you click **Search**, even if there are no log entries for your search criteria. Each field is described in the following table.

**Table 239** Log Viewer > All Logs

| LABEL | DESCRIPTION |
|---|---|
| Day | Select this if you want to look at log entries from one day or part of one day. |
| Start Time | Enter the time of the earliest log entries you want to see, if you select **Day**. |
| End Time | Enter the time of the latest log entries you want to see, if you select **Day**. |
| Days | Select this if you want to look at log entries from more than one day. |
| Start Date | This field is enabled and required if you select **Days**. Enter the date of the earliest log entries you want to see. You can also click the **Calendar** icon to specify the date. |
| End Date | This field is enabled and required if you select **Days**. Enter the date of the latest log entries you want to see. You cannot enter a date earlier than **Start Date**. You can also click the **Calendar** icon to specify the date. |

**Table 239** Log Viewer > All Logs (continued)

| LABEL | DESCRIPTION |
|---|---|
| Category | This field depends on the model of the selected device. Select what type of log entries you want to see. You can also select **All Categories**. |
| Advanced Search | This field is disabled if **Category** is **All Categories**. Select this if you want to use other search criteria to look at log entries. |
| Source IP | Enter the source IP address in the event that generated the log entry. |
| Services | Select the service whose log entries you want to see. If you select **[Custom Service]**, you have to specify the **Protocol** and **Port** too. |
| Destination IP | Enter the destination IP address in the event that generated the log entry. |
| Protocol | This field is enabled if **Services** is **[Custom Service]**. Select the protocol whose log entries you want to see. |
| Keyword | Enter part or all of any value you want to look for in the **Message** field. You can use any printable ASCII character. The search is not case-sensitive. |
| Port | This field is enabled if **Services** is **[Custom Service]**. Select the destination port number whose log entries you want to see. |
| Search | Click this to display the log entries based on the current search criteria. |
| Reset | Click this to set the search criteria to the values they had the last time you clicked **Search**. If you have not clicked **Search** yet, the search criteria return to their default values. |
| Time | This field displays the time the Vantage Report server received the log entry, not the time the log entry was generated. |
| Source:Port | This field displays the source IP address and port (if any) of the event that generated the entry. |
| Destination:Port | This field displays the destination IP address and port (if any) of the event that generated the entry. |
| Category | This field displays the type of log entry. |
| Message | This field displays the reason the log entry was generated. |
| Total Count | This field displays how many log entries there are for the specified search criteria. |
| Total Page | This field displays how many screens it takes to display all the log entries. |
| First .. Last | Click **First**, **Last**, or a specific page number to look at the records on that page. Some choices are not available, depending on the number of pages.s |
| Go | Enter the page number you want to see, and click **Go**. |

# Schedule Report

Use these screens to set up and maintain daily, weekly, and one-time reports that Vantage Report sends by e-mail. See Section 30.2 on page 338 for more information about e-mail in Vantage Report.

## 38.1 Scheduled Report Summary Screen

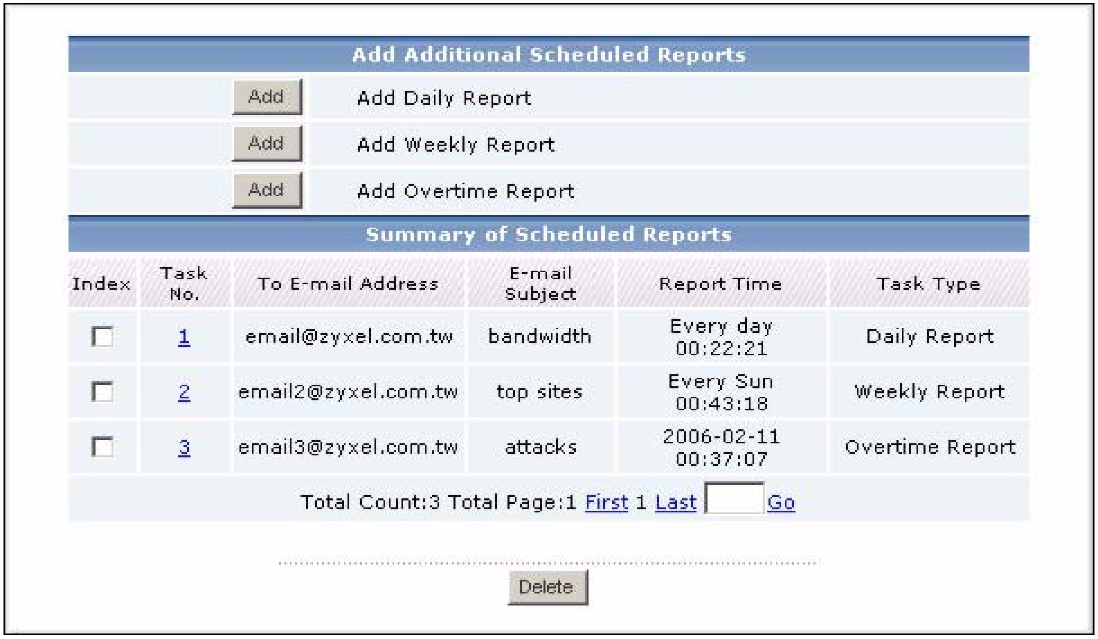
✍ To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 26.8.4 on page 310 for more information.

✍ 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 26.8.4 on page 310 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.

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

**Figure 272** Schedule Reports > Schedule Reports



Add Additional Scheduled Reports

| | |
|---|---|
| Add | Add Daily Report |
| Add | Add Weekly Report |
| Add | Add Overtime Report |

Summary of Scheduled Reports

| Index | Task No. | To E-mail Address | E-mail Subject | Report Time | Task Type |
|---|---|---|---|---|---|
| □ | 1 | email@zyxel.com.tw | bandwidth | Every day 00:22:21 | Daily Report |
| □ | 2 | email2@zyxel.com.tw | top sites | Every Sun 00:43:18 | Weekly Report |
| □ | 3 | email3@zyxel.com.tw | attacks | 2006-02-11 00:37:07 | Overtime Report |

Total Count:3 Total Page:1 First 1 Last Go

Delete

Each field is described in the following table.

**Table 240** Schedule Reports > Schedule Reports

| LABEL | DESCRIPTION |
|---|---|
| Add (Daily Report) | Click this to generate and send one or more statistical reports daily. Each report comes from the previous day's information. The **Customize Scheduled Report** screen appears. |
| Add (Weekly Report) | Click this to generate and send one or more statistical reports weekly. Each report comes from the previous week's information. The **Customize Scheduled Report** screen appears. |
| Add (Overtime Report) | Click this to generate and send one or more statistical reports once, using information from a specified number of days. The **Customize Scheduled Report** screen appears. |
| Summary of Scheduled Reports | |
| Index | Click this, and click **Delete** to delete the scheduled report. |
| Task No. | Click it to edit the scheduled report next to it. The **Customize Scheduled Report** screen appears. Otherwise, this field is a sequential value, and it is not associated with a specific scheduled report. For example, if you delete a scheduled report, the remaining scheduled reports are re-numbered. |
| To E-mail Address | This field displays the first e-mail address to which the scheduled report is sent. If there are more, this field displays a couple punctuation marks at the end. |
| E-mail Subject | This field displays the subject line in the e-mail message Vantage Report sends. |
| Report Time | This field displays how often and when Vantage Report starts generating the scheduled report. It might take over an hour to finish a scheduled report, if there are a lot of reports and a lot of log entries and traffic statistics. For overtime reports, the date is the day after the last day in the report. You cannot change the start time. |
| Task Type | This field displays what type of scheduled report this is. |
| Total Count | This field displays how many scheduled reports there are. |

**Table 240** Schedule Reports > Schedule Reports (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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**. |

## 38.2 Customize Daily Report Screen

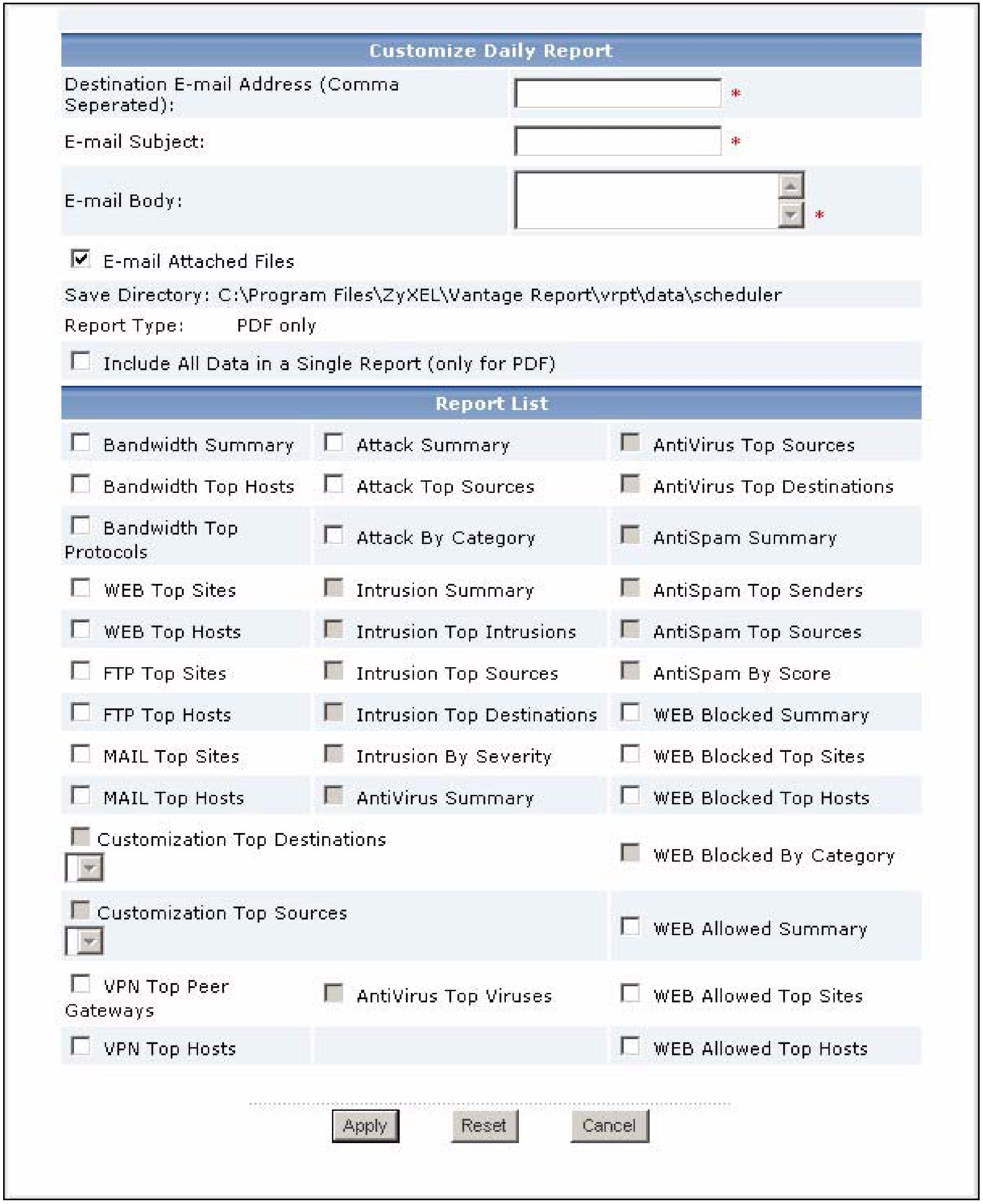
To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 26.8.4 on page 310 for more information.

Scheduled reports are limited by the amount of log and traffic information stored in Vantage Report. For example, if Vantage Report only saves one day of information (today's information), daily reports have no information in them. See Section 26.8.4 on page 310 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** field for more information.

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

**Figure 273** Schedule Reports > Schedule Reports > Add (Daily Report)



Customize Daily Report

|  |  |
|---|---|
| Destination E-mail Address (Comma Seperated): | * |
| E-mail Subject: | * |
| E-mail Body: | * |

☑ E-mail Attached Files

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

Report Type: PDF only

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

Report List

|  |  |  |
|---|---|---|
| □ Bandwidth Summary | □ Attack Summary | □ AntiVirus Top Sources |
| □ Bandwidth Top Hosts | □ Attack Top Sources | □ AntiVirus Top Destinations |
| □ Bandwidth Top Protocols | □ Attack By Category | □ AntiSpam Summary |
| □ WEB Top Sites | □ Intrusion Summary | □ AntiSpam Top Senders |
| □ WEB Top Hosts | □ Intrusion Top Intrusions | □ AntiSpam Top Sources |
| □ FTP Top Sites | □ Intrusion Top Sources | □ AntiSpam By Score |
| □ FTP Top Hosts | □ Intrusion Top Destinations | □ WEB Blocked Summary |
| □ MAIL Top Sites | □ Intrusion By Severity | □ WEB Blocked Top Sites |
| □ MAIL Top Hosts | □ AntiVirus Summary | □ WEB Blocked Top Hosts |
| □ Customization Top Destinations |  | □ WEB Blocked By Category |
| □ Customization Top Sources |  | □ WEB Allowed Summary |
| □ VPN Top Peer Gateways | □ AntiVirus Top Viruses | □ WEB Allowed Top Sites |
| □ VPN Top Hosts |  | □ WEB Allowed Top Hosts |

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

**Table 241** Schedule Reports > Schedule Reports > Add (Daily Report)

| LABEL | DESCRIPTION |
|---|---|
| Destination E-mail Address | Enter the e-mail address(es) to which Vantage Report sends the selected report(s). Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want.<br>Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value. |
| E-mail Subject | Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters.<br>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\schedule` in the Vantage Report installation directory. |
| Save Directory | This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is. |
| Report Type | Select the format(s) of the selected report(s). HTML format looks like the statistical reports you can see online. |
| Include All Data in a Single Report | This field is enabled for if you selected PDF format. Select this if you want to combine all the selected report(s) into one file. |
| Report List | Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. |
| Apply | Click this to save your settings and close the screen. |
| Reset | Click this to change the settings in this screen to the last-saved values. |
| Cancel | Click this to close the screen without saving any changes. |

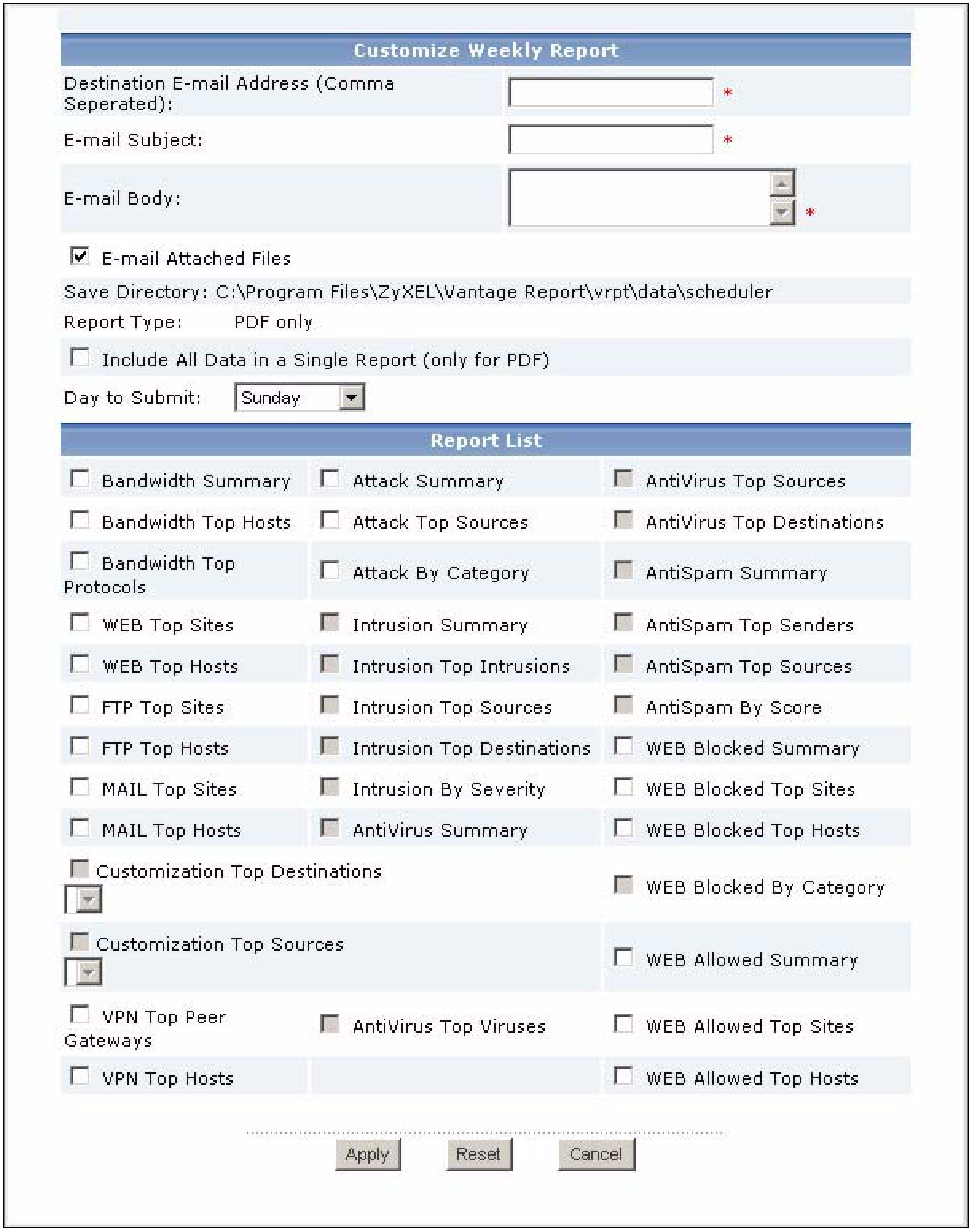
## 38.3 Customize Weekly Report Screen

To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 26.8.4 on page 310 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 26.8.4 on page 310 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** field for more information.

**Figure 274** Schedule Reports > Schedule Reports > Add (Weekly Report)



**Customize Weekly Report**

| | |
|---|---|
| Destination E-mail Address (Comma Seperated): | * |
| E-mail Subject: | * |
| E-mail Body: | * |

☑ E-mail Attached Files

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

Report Type: PDF only

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

Day to Submit: Sunday

**Report List**

| | | |
|---|---|---|
| □ Bandwidth Summary | □ Attack Summary | □ AntiVirus Top Sources |
| □ Bandwidth Top Hosts | □ Attack Top Sources | □ AntiVirus Top Destinations |
| □ Bandwidth Top Protocols | □ Attack By Category | □ AntiSpam Summary |
| □ WEB Top Sites | □ Intrusion Summary | □ AntiSpam Top Senders |
| □ WEB Top Hosts | □ Intrusion Top Intrusions | □ AntiSpam Top Sources |
| □ FTP Top Sites | □ Intrusion Top Sources | □ AntiSpam By Score |
| □ FTP Top Hosts | □ Intrusion Top Destinations | □ WEB Blocked Summary |
| □ MAIL Top Sites | □ Intrusion By Severity | □ WEB Blocked Top Sites |
| □ MAIL Top Hosts | □ AntiVirus Summary | □ WEB Blocked Top Hosts |
| □ Customization Top Destinations | | □ WEB Blocked By Category |
| □ Customization Top Sources | | □ WEB Allowed Summary |
| □ VPN Top Peer Gateways | □ AntiVirus Top Viruses | □ WEB Allowed Top Sites |
| □ VPN Top Hosts | | □ WEB Allowed Top Hosts |

Each field is described in the following table.

**Table 242** Schedule Reports > Schedule Reports > Add (Weekly Report)

| LABEL | DESCRIPTION |
|---|---|
| Destination E-mail Address | Enter the e-mail address(es) to which Vantage Report sends the selected report(s). Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want.<br>Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value. |
| E-mail Subject | Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters.<br>Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value. |
| E-mail Body | Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long. |
| E-mail Attached Files | Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. |
| Save Directory | This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is. |
| Report Type | Select the format(s) of the selected report(s). HTML format looks like the statistical reports you can see online. |
| Include All Data in a Single Report | This field is enabled for if you selected PDF format. Select this if you want to combine all the selected report(s) into one file. |
| Day to Submit | Select the day of the week to generate and send the selected report(s). |
| Function Window | Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. |
| Apply | Click this to save your settings and close the screen. |
| Reset | Click this to change the settings in this screen to the last-saved values. |
| Cancel | Click this to close the screen without saving any changes. |

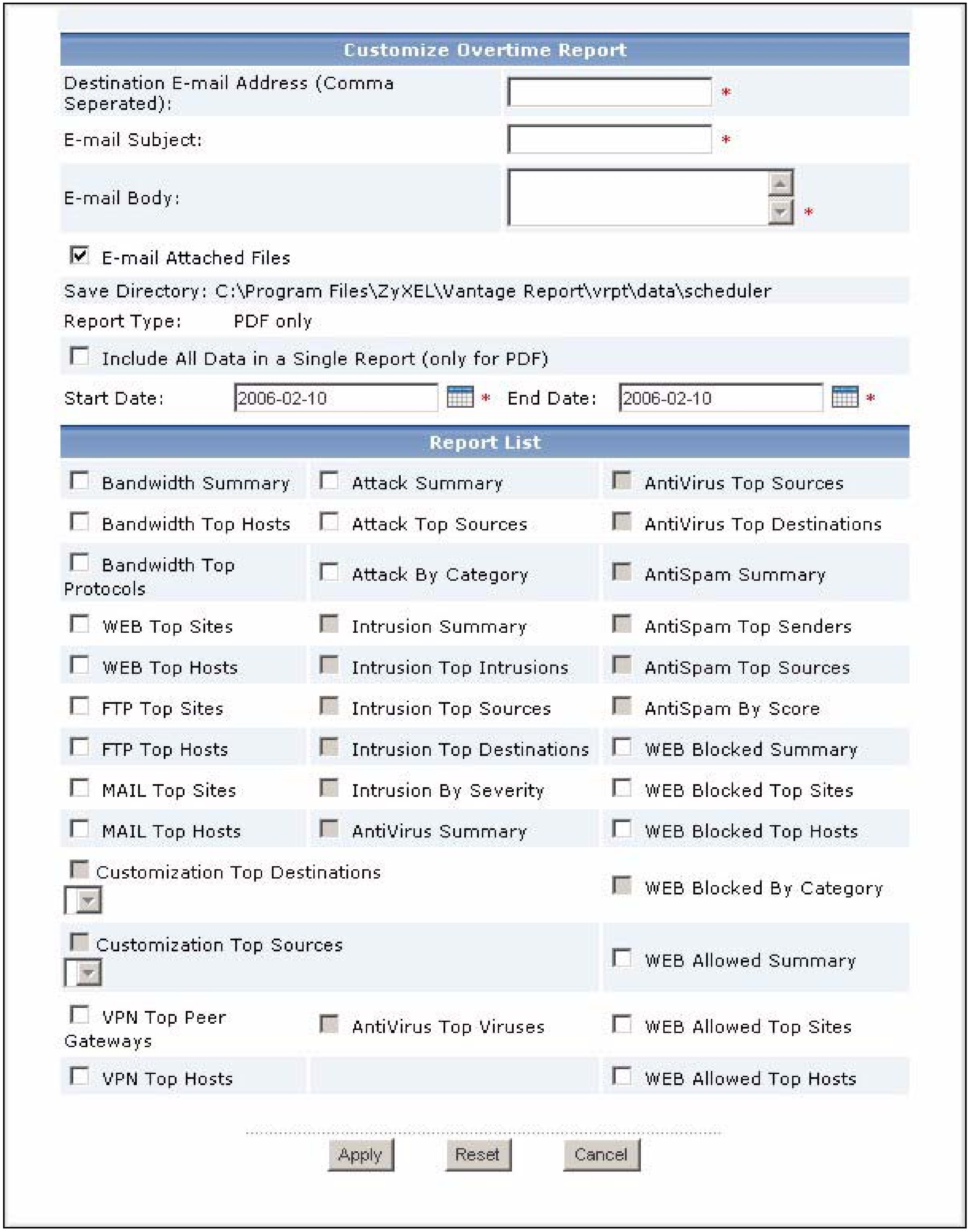
## 38.4 Customize Overtime Report Screen

✍ To send scheduled reports by e-mail, you have to enter the SMTP mail server settings. See Section 26.8.4 on page 310 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 six days of information, overtime reports only consist of information from these six days, not necessarily the whole specified date range. See Section 26.8.4 on page 310 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** field for more information.

**Figure 275** Schedule Reports > Schedule Reports > Add (Overtime Report)



Customize Overtime Report

| | |
|---|---|
| Destination E-mail Address (Comma Seperated): | * |
| E-mail Subject: | * |
| E-mail Body: | * |

☑ E-mail Attached Files

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

Report Type: PDF only

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

Start Date: 2006-02-10 * End Date: 2006-02-10 *

Report List

| | | |
|---|---|---|
| □ Bandwidth Summary | □ Attack Summary | □ AntiVirus Top Sources |
| □ Bandwidth Top Hosts | □ Attack Top Sources | □ AntiVirus Top Destinations |
| □ Bandwidth Top Protocols | □ Attack By Category | □ AntiSpam Summary |
| □ WEB Top Sites | □ Intrusion Summary | □ AntiSpam Top Senders |
| □ WEB Top Hosts | □ Intrusion Top Intrusions | □ AntiSpam Top Sources |
| □ FTP Top Sites | □ Intrusion Top Sources | □ AntiSpam By Score |
| □ FTP Top Hosts | □ Intrusion Top Destinations | □ WEB Blocked Summary |
| □ MAIL Top Sites | □ Intrusion By Severity | □ WEB Blocked Top Sites |
| □ MAIL Top Hosts | □ AntiVirus Summary | □ WEB Blocked Top Hosts |
| □ Customization Top Destinations | | □ WEB Blocked By Category |
| □ Customization Top Sources | | □ WEB Allowed Summary |
| □ VPN Top Peer Gateways | □ AntiVirus Top Viruses | □ WEB Allowed Top Sites |
| □ VPN Top Hosts | | □ WEB Allowed Top Hosts |

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

**Table 243** Schedule Reports > Schedule Reports > Add (Overtime Report)

| LABEL | DESCRIPTION |
|---|---|
| Destination E-mail Address | Enter the e-mail address(es) to which Vantage Report sends the selected report(s). Use a comma to separate each e-mail address. Do not put a space after the comma. You can enter as many valid e-mail addresses as you want.<br>Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value. |
| E-mail Subject | Enter the subject line in the e-mail message Vantage Report sends. The subject must be 1-50 printable ASCII characters.<br>Vantage Report provides an auto-complete feature in this field. As you type, you can see a list of values for this field in other scheduled reports next to the mouse. You can click on one to avoid typing the rest of the value. |
| E-mail Body | Enter the text you want to appear in the main body of the e-mail message Vantage Report sends. The body must be 1-255 printable ASCII characters long. |
| E-mail Attached Files | Select this if you want Vantage Report to send the selected report(s) as attachment(s). Vantage Report also saves the selected report(s) on the Vantage Report server. If you do not select this, Vantage Report only saves the selected report(s) on the Vantage Report server. |
| Save Directory | This field is read-only. Vantage Report saves a copy of the selected report(s) on the Vantage Report server. This field displays where the copy is. |
| Report Type | Select the format(s) of the selected report(s). HTML format looks like the statistical reports you can see online. |
| Include All Data in a Single Report | This field is enabled for if you selected PDF format. Select this if you want to combine all the selected report(s) into one file. |
| Start Date | Select the day to start collecting information for the selected report(s). Vantage Report starts collecting information at the beginning of this day. |
| End Date | Select the day to stop collecting information for the selected report(s). Vantage Report stops collecting information at the end of this day. |
| Function Window | Select which report(s) you want to generate and send in the e-mail message. For some reports, you can select additional options. All the bandwidth reports use the same direction setting. |
| Apply | Click this to save your settings and close the screen. |
| Reset | Click this to change the settings in this screen to the last-saved values. |
| Cancel | Click this to close the screen without saving any changes. |

# 39

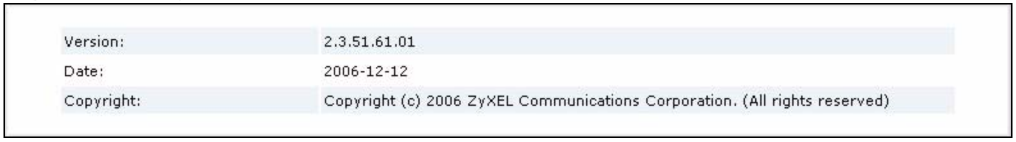
# System

Use this screen to basic information about Vantage Report.

## 39.1 About Screen

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

**Figure 276** System > About



| | |
|---|---|
| Version: | 2.3.51.61.01 |
| Date: | 2006-12-12 |
| Copyright: | Copyright (c) 2006 ZyXEL Communications Corporation. (All rights reserved) |

# 40

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Vantage CNM Access and Login
- Vantage Report

## 40.1 Vantage CNM Access and Login

See the Quick Start Guide for additional suggestions.

?

### I cannot see or access the **Login** screen in the web configurator.

1 Make sure your Internet browser does not block pop-up windows and has Java Scripts and Java enabled. See Appendix C on page 535.

2 Make sure you are using the correct IP address.

3 If the problem continues, contact your local vendor.

?

### I forgot the **root** password.

The default password is **root**. If you have changed it, contact your local vendor.

?

### I can see the **Login** screen, but I cannot log in to the Vantage CNM.

Make sure you have entered the user name and password correctly. The user name and password are case-sensitive, so make sure [Caps Lock] is not on. If this does not work, contact the network administrator or local vendor.

## 40.2 Vantage Report

### There is no information in any report for my device.

1 If you just added the device, wait. See Table 157 on page 338 for the amount of time it takes for information to appear in each report.

2 Click **System** > **VRPT Management** > **General** > **Receiver Monitor**. This screen keeps track of all the log entries received by the Vantage Report server.

- If the MAC address is in the screen, Vantage Report is receiving information from the device. Wait.
- If the MAC address is not in the file, Vantage Report is not receiving information from the device. Make sure you have selected the devices in the **Managed Device List** in the **System** > **VRPT Management** > **General** screen. See Section 26.8.1 on page 306.

3 Check the amount of available disk space on the Vantage Report server. If it is less than the value in Appendix A on page 515, the Vantage Report server stops receiving log entries.

4 Make sure your devices support Vantage Report. Check the release notes for the current firmware version.

5 Check the connections between the devices and Vantage Report server.

6 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 devices support these reports. Check the release notes for the current firmware version.

2 Make sure you have selected the devices in the **Managed Device List** in the **System** > **VRPT Management** > **General** screen. See Section 26.8.1 on page 306.

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.

4 If the problem continues, contact your local vendor.

# PART VIII

# Appendices and Index

# A

# Product Specifications

This appendix summarizes Vantage CNM's and Vantage Report's specifications.

## Vantage CNM Specifications

This section summarizes Vantage CNM's specifications.

**Table 244** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Default User Name | root |
| Default Password | root |
| Object Tree View | Three defined views: Account, Type, and Main<br>Status icons |
| Device Registration | Manual or XML file |
| Building Blocks (BB) | Reusable configurations<br>BB repository |
| Domain Administration | One domain per administrator<br>Multiple administrators per domain<br>Different privileges for each administrator |
| Device Configuration | Vantage CNM's **Configuration** menu<br>Device's web configurator<br>Most device features, including firewall and UTM features |
| Synchronization | Copy device's configuration to Vantage CNM<br>Copy Vantage CNM's configuration to device |
| One-click VPN | Drag-and-drop in graphical interface |
| Configuration File Management | Back up, restore, and reset one or more devices |
| Firmware Upgrade | Upload firmware to one or more devices<br>Upgrade scheduler<br>Upgrade report |
| Monitoring and Notifications | Alarm monitor<br>Status monitor for urgent alerts<br>E-mail alerts |
| Logs | Vantage CNM logs<br>Vantage Report for device logs |

**Table 244** Firmware Specifications (continued)

| FEATURE | DESCRIPTION |
|---|---|
| Data Maintenance | Back up and restore entire Vantage CNM configuration |
| System Management | Vantage CNM server IP address<br>FTP server<br>Mail server<br>Idle timeout<br>Brute-force password protection<br>Notification recipients<br>Administrator privileges |

**Table 245** Feature Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Number of Vantage CNM Log Entries | 1,000,000 |

**Table 246** Supported Devices

| FEATURE | DESCRIPTION |
|---|---|
| Prestige 653HWI-17 | 3.40 |
| P-662H-D1 | 3.40 |
| Prestige 662H-61 | 3.40 |
| P-662HW-D1 | 3.40 |
| Prestige 662HW-61/63 | 3.40 |
| ZyWALL P1 | 3.64 |
| ZyWALL 2 | 3.62 |
| ZyWALL 2 Plus | 4.00, 4.01 |
| ZyWALL 5 | 3.64, 4.00, 4.01 |
| ZyWALL 10W | 3.62 |
| ZyWALL 35 | 3.64, 4.00, 4.01 |
| ZyWALL 70 | 3.65, 4.00, 4.01 |
| ZyWALL 1050 | 1.02(XL.0) |

**Table 247** Trusted CAs (Keystore type: jks, Keystore provider: SUN)

| CA | DATE | MD5 FINGERPRINT |
|---|---|---|
| equifaxsecureebusinessca1 | Jul 19, 2003 | `64:9C:EF:2E:44:FC:C6:8F:52:07:D0:51:73:8F:CB:3D` |
| verisignclass1g3ca | Mar 26, 2004 | `B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73` |
| verisignclass2g2ca | Mar 26, 2004 | `2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1` |
| verisignclass3g3ca | Mar 26, 2004 | `CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09` |
| godaddyclass2ca | Jan 12, 2005 | `91:DE:06:25:AB:DA:FD:32:17:0C:BB:25:17:2A:84:67` |
| entrustglobalclientca | Jan 9, 2003 | `9A:77:19:18:ED:96:CF:DF:1B:B7:0E:F5:8D:B9:88:2E` |

**Table 247** Trusted CAs (Keystore type: jks, Keystore provider: SUN) (continued)

| CA | DATE | MD5 FINGERPRINT |
|---|---|---|
| mykey | Nov 30, 2006 | 8D:E9:89:DB:7F:CC:5E:3B:FD:DE:2C:42:08:13:EF:43 |
| gtecybertrustglobalca | May 10, 2002 | CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB |
| entrustgsslca | Jan 9, 2003 | 9D:66:6A:CC:FF:D5:F5:43:B4:BF:8C:16:D1:2B:A8:99 |
| thawtepersonalbasicca | Feb 13, 1999 | E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41 |
| verisignclass1ca | Mar 26, 2004 | 97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62 |
| verisignclass1g2ca | Mar 26, 2004 | DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83 |
| entrustsslca | Jan 9, 2003 | DF:F2:80:73:CC:F1:E6:61:73:FC:F5:42:E9:C5:7C:EE |
| thawtepersonalfreemailca | Feb 13, 1999 | 1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9 |
| verisignclass3ca | Oct 27, 2003 | 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67 |
| gtecybertrustca | May 10, 2002 | C4:D7:F0:B2:A3:C5:7D:61:67:F0:04:CD:43:D3:BA:58 |
| verisignclass2g3ca | Mar 26, 2004 | F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6 |
| thawteserverca | Feb 13, 1999 | C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D |
| thawtepersonalpremiumca | Feb 13, 1999 | 3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D |
| equifaxsecureca | Jul 19, 2003 | 67:CB:9D:C0:13:24:8A:82:9B:B2:17:1E:D1:1B:EC:D4 |
| verisignclass3g2ca | Mar 26, 2004 | A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9 |
| thawtepremiumserverca | Feb 13, 1999 | 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A |
| entrust2048ca | Jan 9, 2003 | BA:21:EA:20:D6:DD:DB:8F:C1:57:8B:40:AD:A1:FC:FC |
| entrustclientca | Jan 9, 2003 | 0C:41:2F:13:5B:A0:54:F5:96:66:2D:7E:CD:0E:03:F4 |
| verisignserverca | Jun 30, 1998 | 74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93 |
| baltimorecybertrustca | May 10, 2002 | AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4 |
| valicertclass2ca | Jan 12, 2005 | A9:23:75:9B:BA:49:36:6E:31:C2:DB:F2:E7:66:BA:87 |
| geotrustglobalca | Jul 19, 2003 | F7:75:AB:29:FB:51:4E:B7:77:5E:FF:05:3C:99:8E:F5 |

**Table 247** Trusted CAs (Keystore type: jks, Keystore provider: SUN) (continued)

| CA | DATE | MD5 FINGERPRINT |
|---|---|---|
| gtecybertrust5ca | May 10, 2002 | `7D:6C:86:E4:FC:4D:D1:0B:00:BA:22:BB:4E:7C:6A:8E` |
| starfieldclass2ca | Jan 12, 2005 | `32:4A:4B:BB:C8:63:69:9B:BE:74:9A:C6:DD:1D:46:24` |
| baltimorecodesigningca | May 10, 2002 | `90:F5:28:49:56:D1:5D:2C:B0:53:D4:4B:EF:6F:90:22` |
| equifaxsecureglobalebusinessca1 | Jul 19, 2003 | `8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9B:CC` |
| equifaxsecureebusinessca2 | Jul 19, 2003 | `AA:BF:BF:64:97:DA:98:1D:6F:C6:08:3A:95:70:33:CA` |
| verisignclass2ca | Oct 27, 2003 | `B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E` |

# Vantage Report Specifications

This section summarizes Vantage Report's specifications. See Table 157 on page 338 for specifications about the time it takes the Vantage Report server to process information from devices.

**Table 248** Port Number Specifications

| FEATURE | SPECIFICATION |
|---|---|
| MySQL port number | 3316 |

**Table 249** System Notifications Specifications

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

**Table 250** Feature Specifications

| FEATURE | SPECIFICATION |
|---|---|
| Number of supported devices | Up to 25 |
| Number of scheduled reports | 500 |
| Maximum Number of Entries in the Table at the Bottom of Each Statistical Report | 10 |
| Log Consolidation Frequency | 4 minutes |

B

# Setting up Your Computer's IP Address

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

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

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

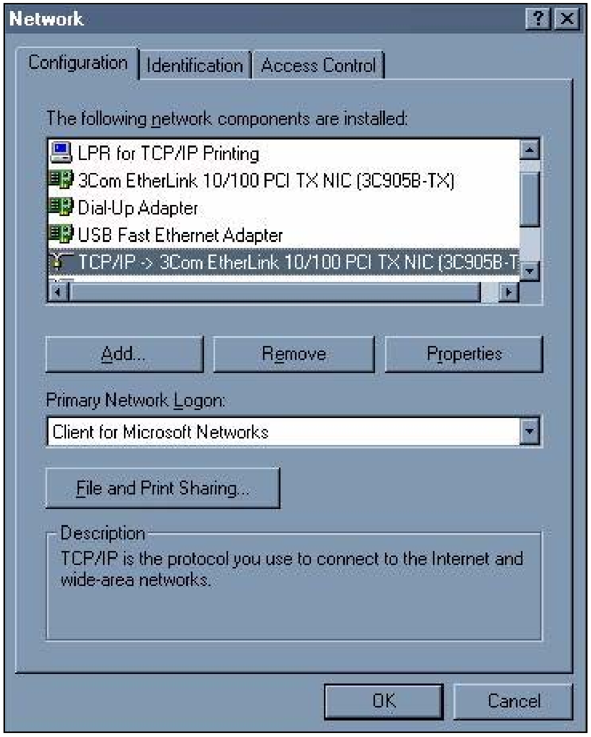
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 277** WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:

Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

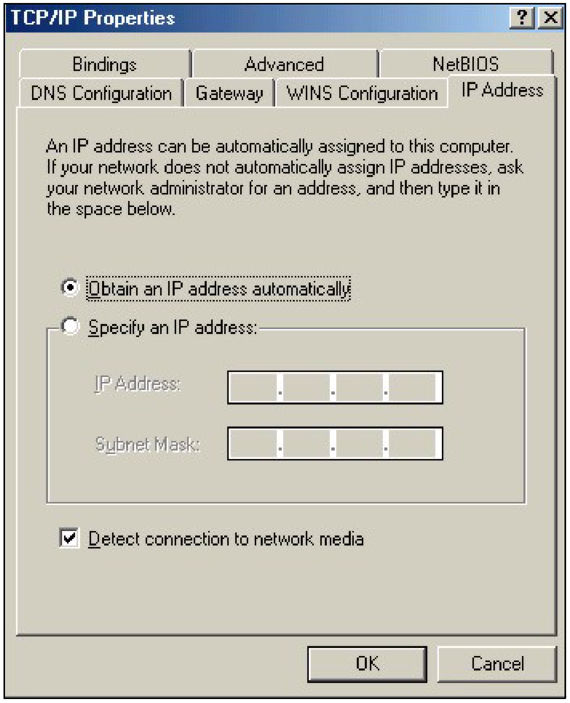
## Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 278** Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

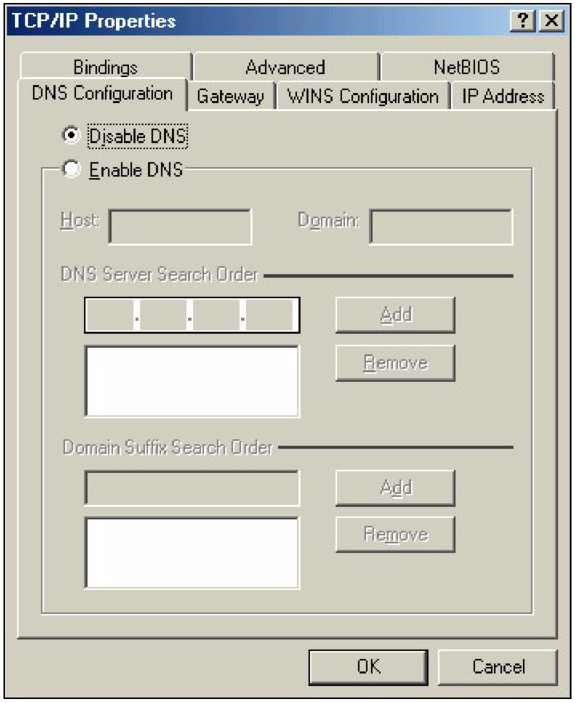
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 279** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

- If you do not know your gateway’s IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your device and restart your computer when prompted.

### Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

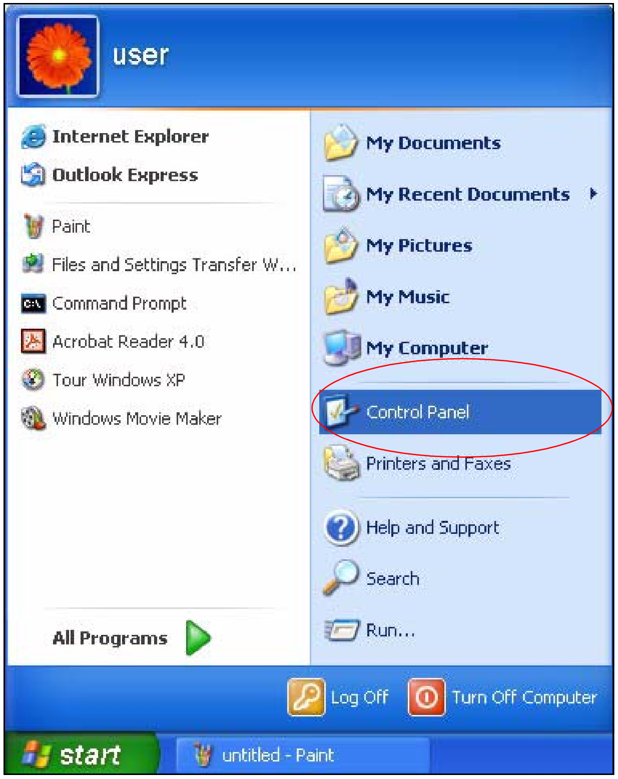
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

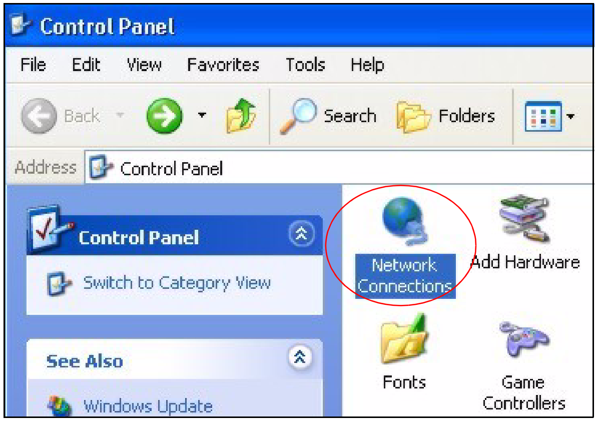
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 280** Windows XP: Start Menu



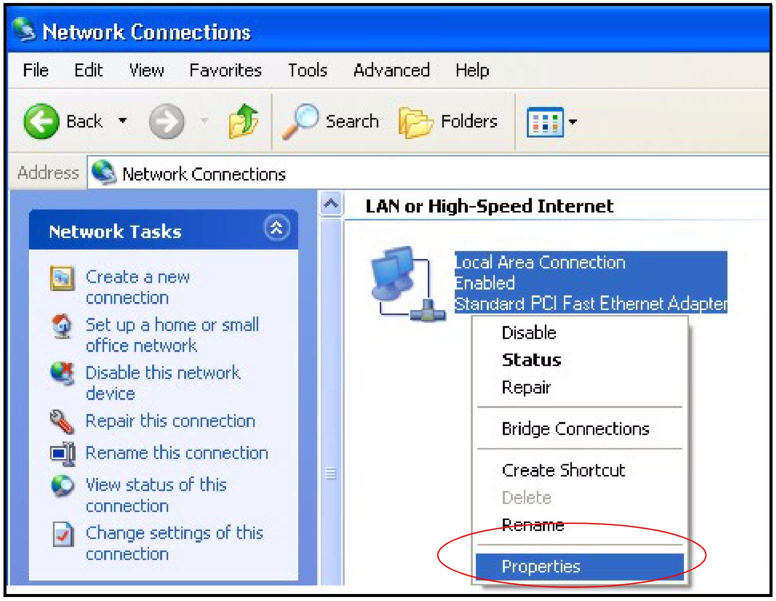
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 281** Windows XP: Control Panel



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

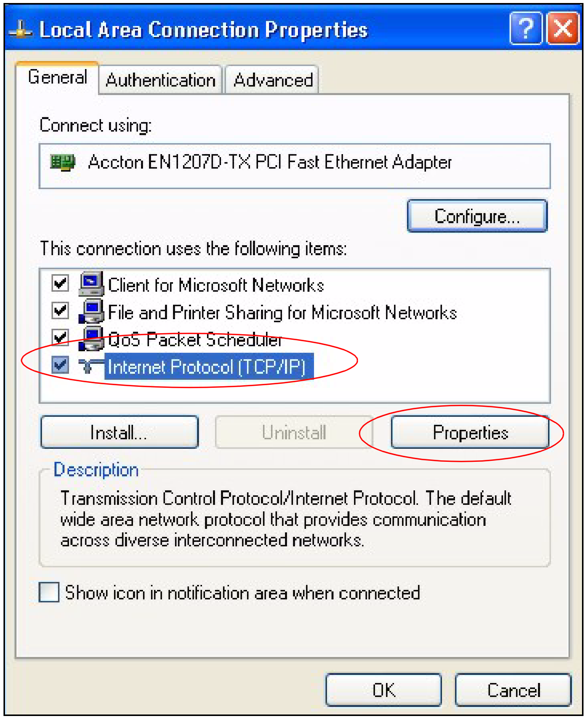
**Figure 282** Windows XP: Control Panel: Network Connections: Properties



Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter

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

**Figure 283** Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

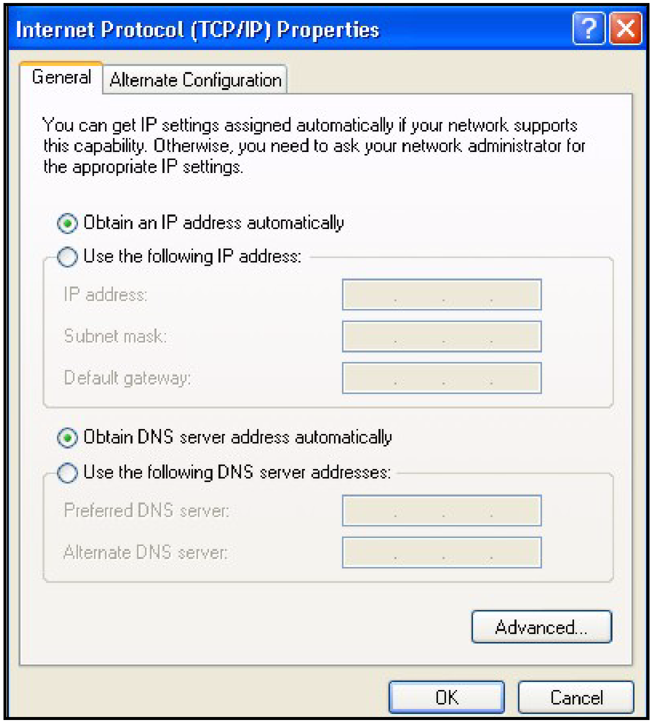
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

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

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

**Figure 284** Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

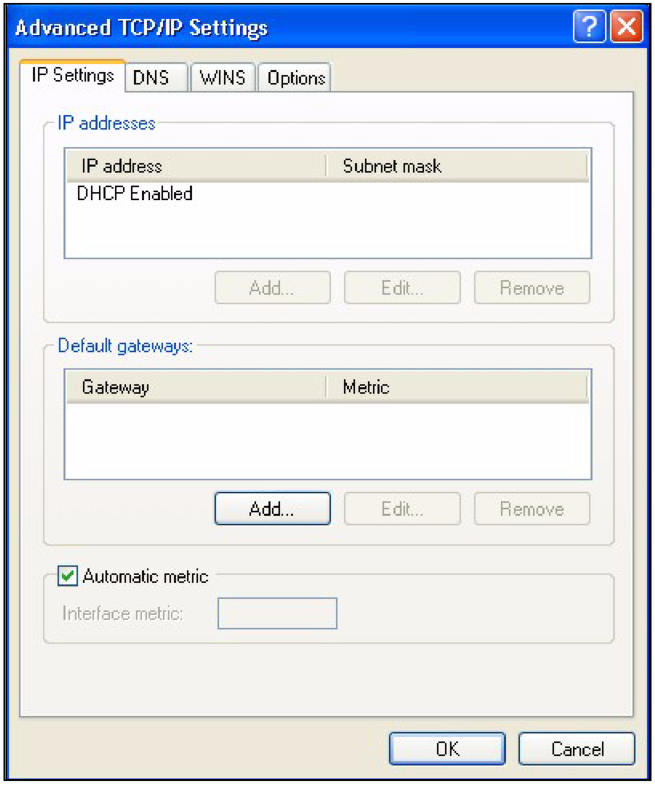
Alternate DNS server: . . .

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

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

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

**Figure 285** Windows XP: Advanced TCP/IP Properties



| IP address | Subnet mask |
|---|---|
| DHCP Enabled | |

| Gateway | Metric |
|---|---|

☑ Automatic metric

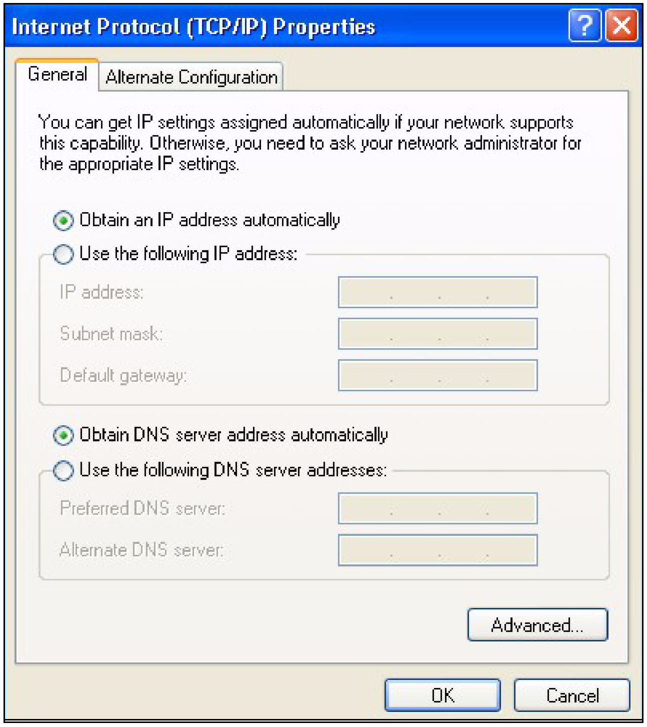
Interface metric:

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

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

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

**Figure 286** Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your device and restart your computer (if prompted).

### Verifying Settings

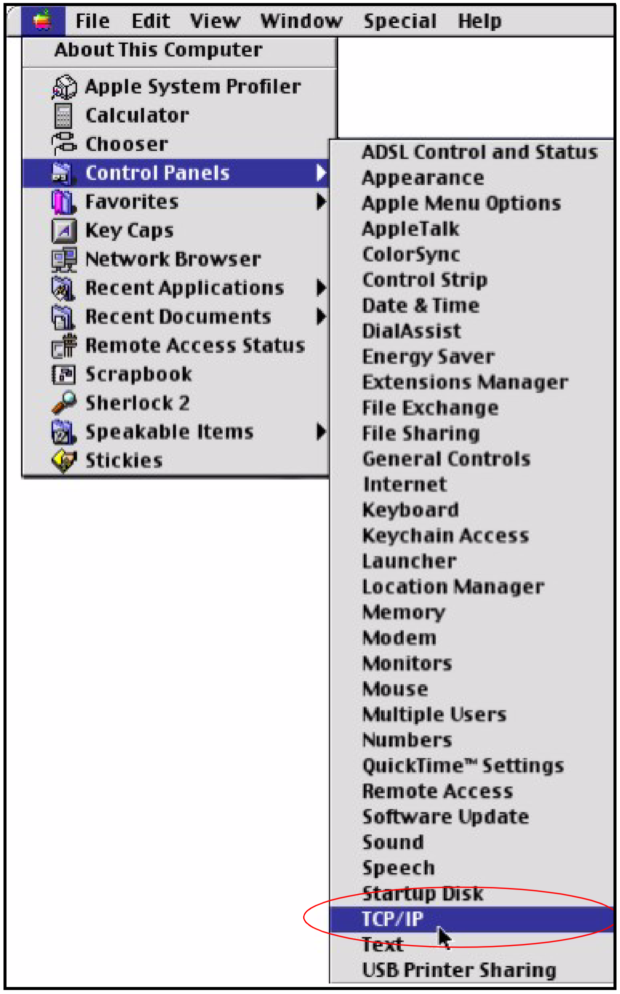
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

## Macintosh OS 8/9

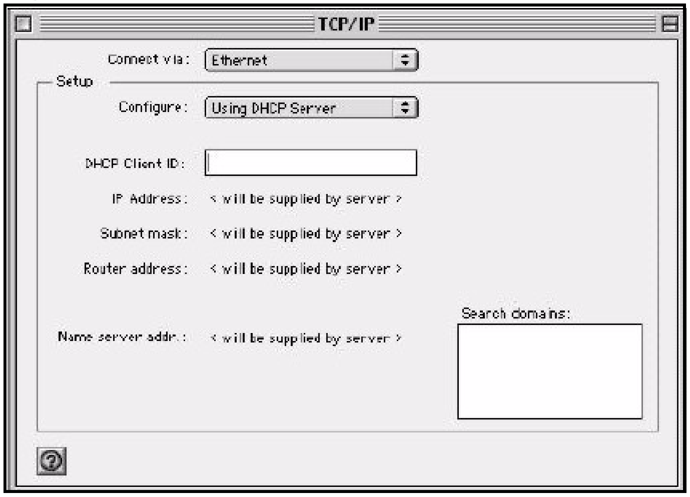
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 287** Macintosh OS 8/9: Apple Menu



**2** Select **Ethernet built-in** from the **Connect via** list.

**Figure 288** Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

Name server addr.: < will be supplied by server >

**3** For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your device and restart your computer (if prompted).

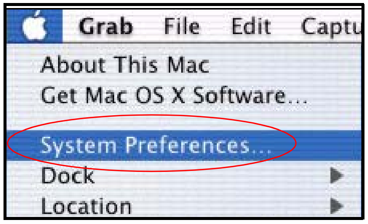
### Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 289 Macintosh OS X: Apple Menu

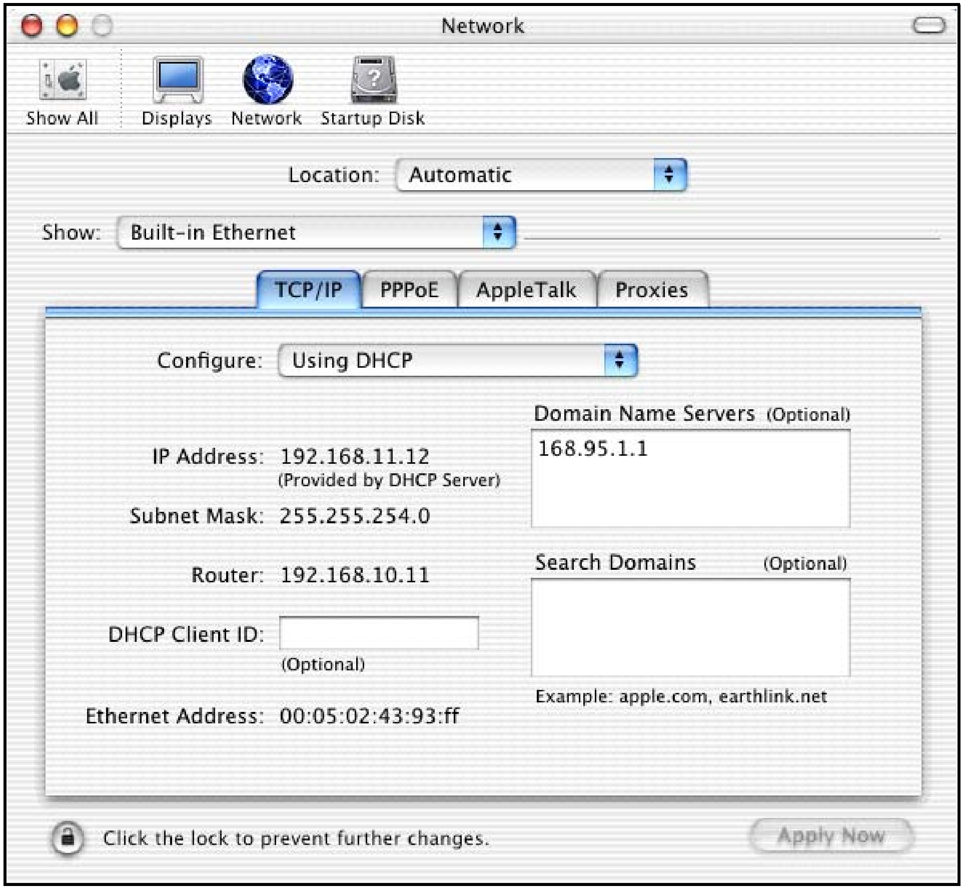


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 290** Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your device and restart your computer (if prompted).

### Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer’s TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

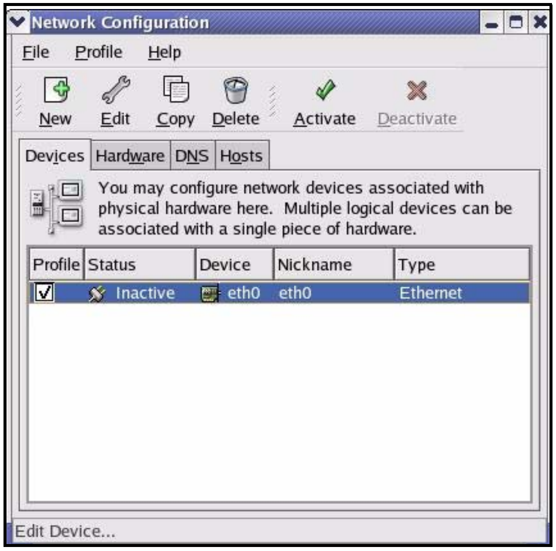
Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 291** Red Hat 9.0: KDE: Network Configuration: Devices



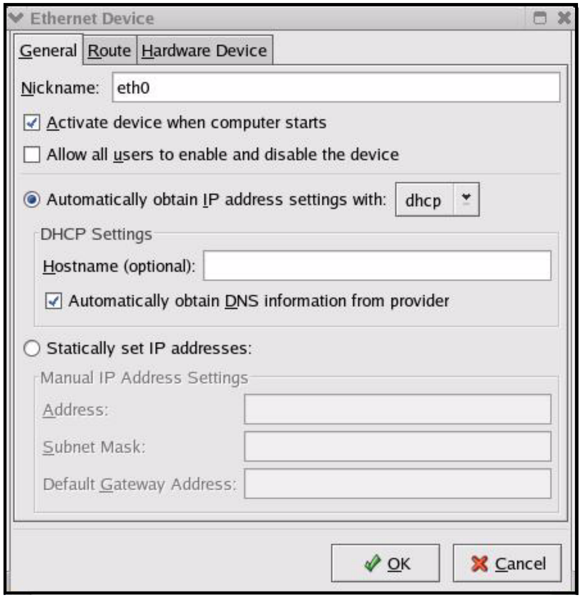
You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

| Profile | Status | Device | Nickname | Type |
|---|---|---|---|---|
| ☑ | Inactive | eth0 | eth0 | Ethernet |

Edit Device...

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 292** Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

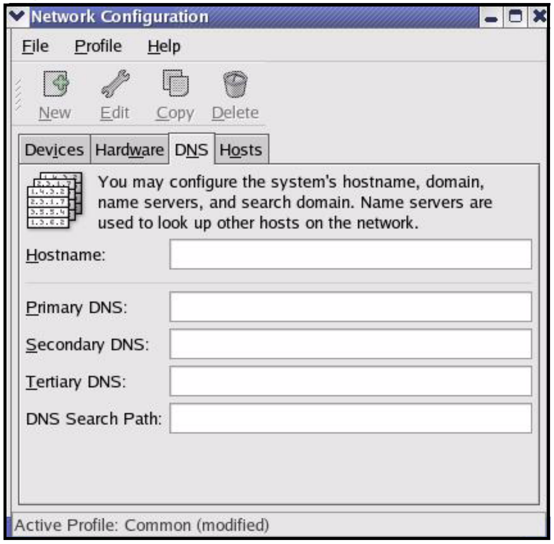
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 293** Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

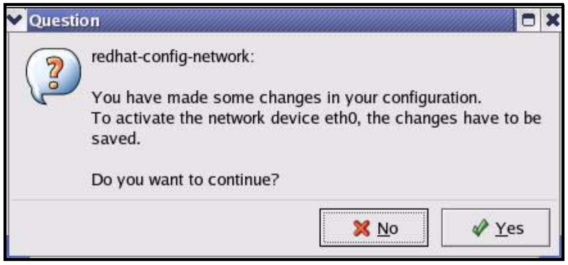
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

**Figure 294** Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 295** Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 296** Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 297** Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 298** Red Hat 9.0: Restart Ethernet Card

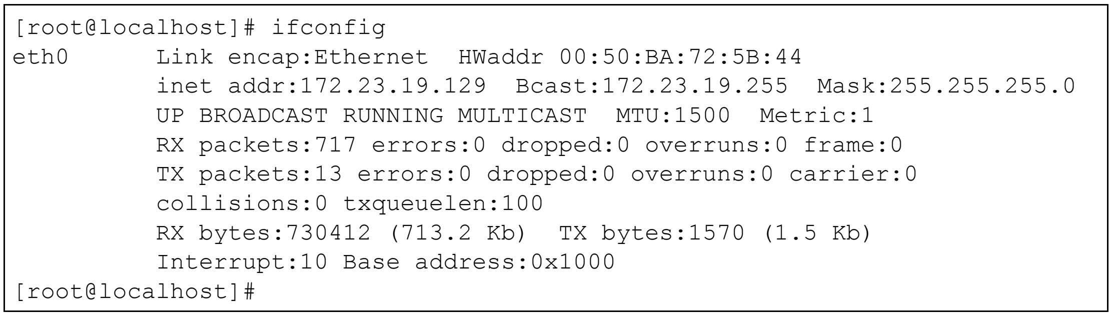
```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 299** Red Hat 9.0: Checking TCP/IP Properties



```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

C

# Pop-up Windows, Java Scripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- Java Scripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

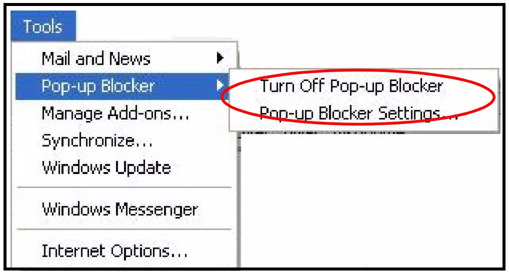
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 300** Pop-up Blocker

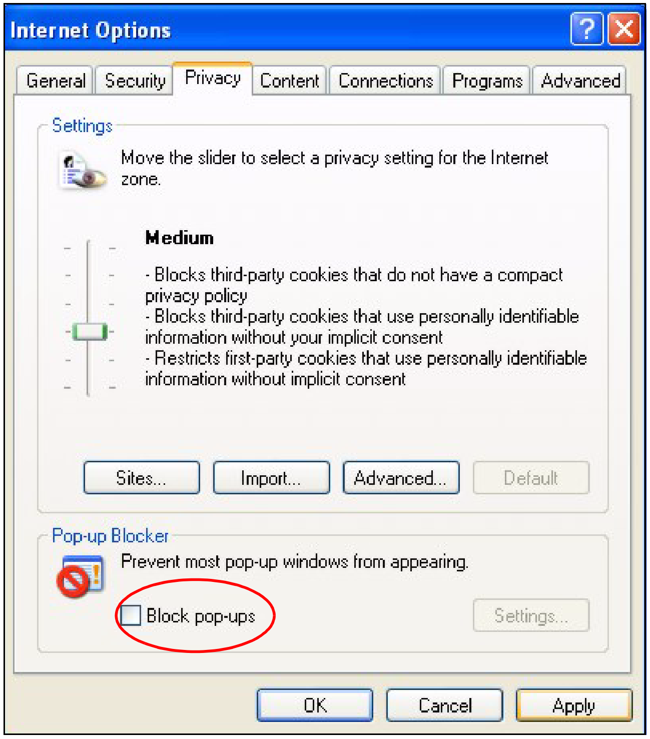


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 301** Internet Options: Privacy



Settings

Move the slider to select a privacy setting for the Internet zone.

**Medium**

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

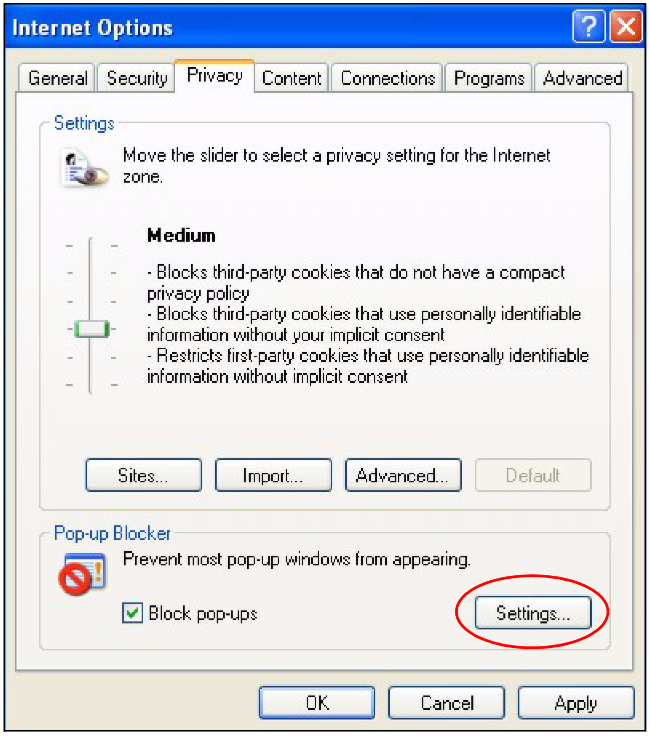
## Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

**Figure 302** Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

**Medium**

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

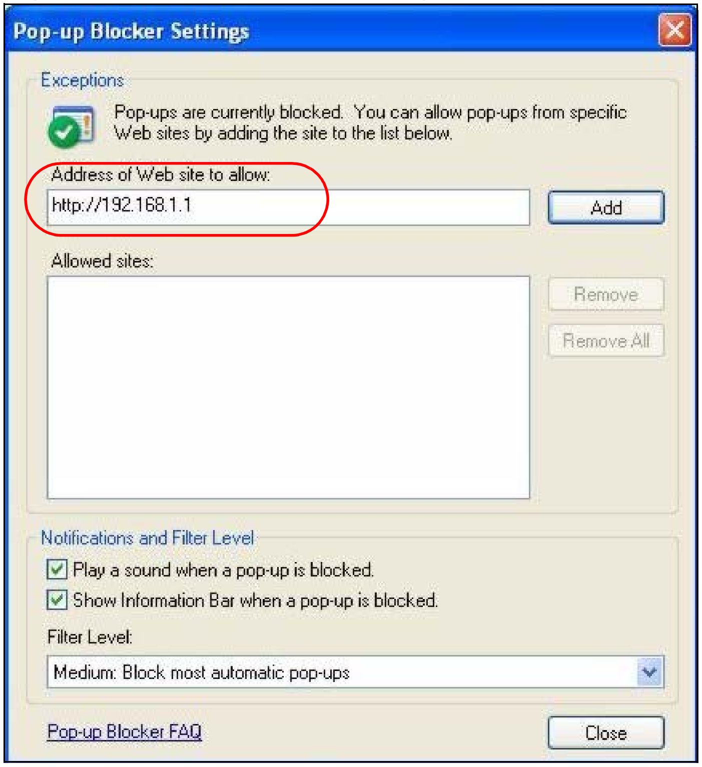
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 303** Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

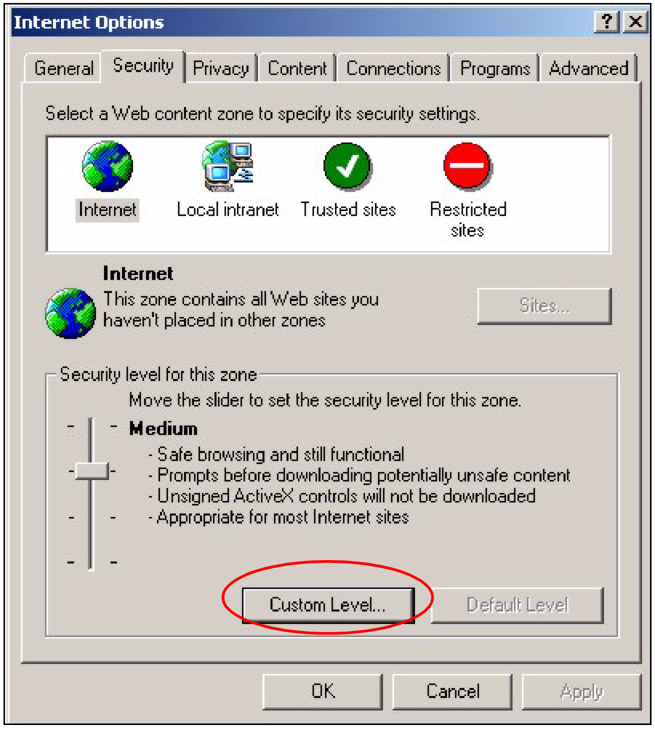
6 Click **Apply** to save this setting.

## Java Scripts

If pages of the web configurator do not display properly in Internet Explorer, check that Java Scripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 304** Internet Options: Security


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Select a Web content zone to specify its security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Internet
This zone contains all Web sites you haven't placed in other zones
Sites...
Security level for this zone
Move the slider to set the security level for this zone.
Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites
Custom Level...
Default Level
OK
Cancel
Apply

2 Click the **Custom Level...** button.

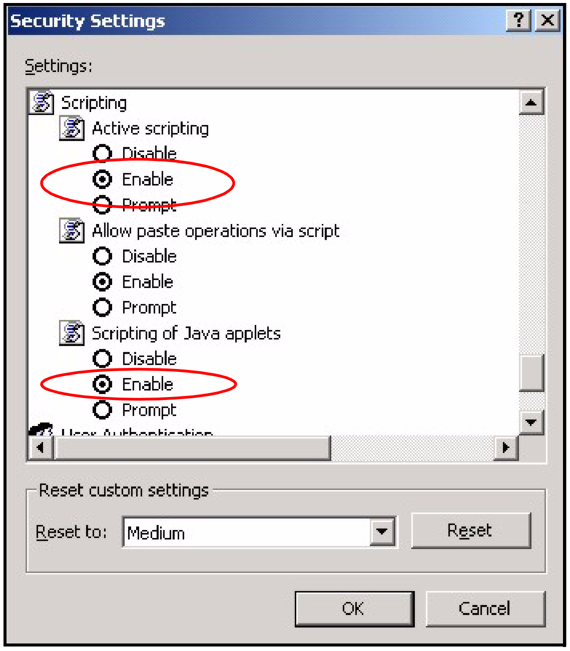
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

**Figure 305** Security Settings - Java Scripting



Scripting
Active scripting
○ Disable
● Enable
○ Prompt
Allow paste operations via script
○ Disable
● Enable
○ Prompt
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication

Reset to: Medium

## Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

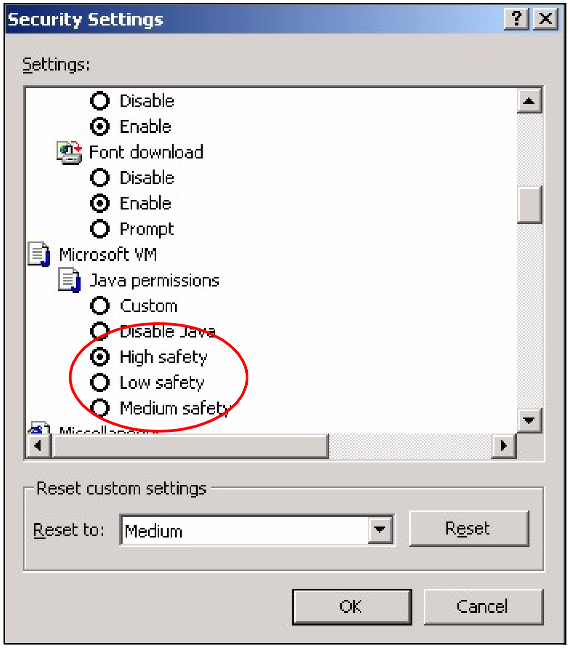
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

**Figure 306** Security Settings - Java



○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety
Miscellaneous

Reset to: Medium

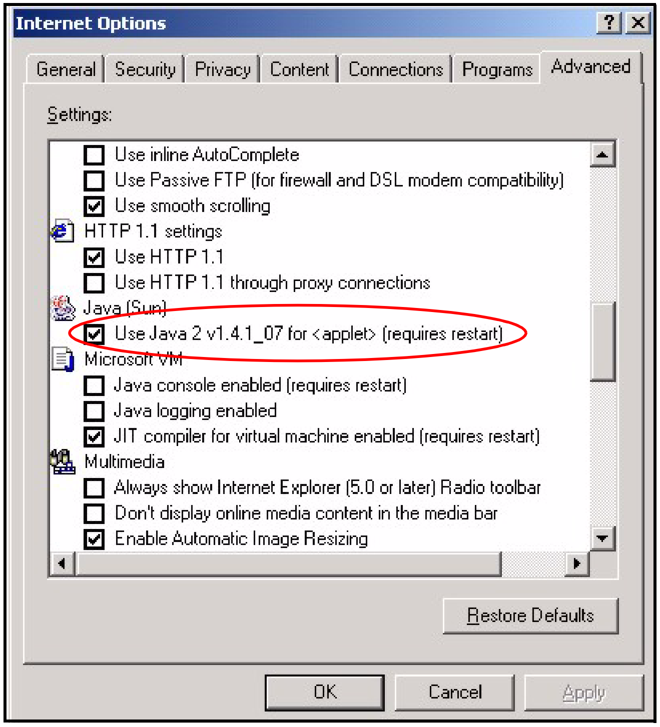
## JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

**Figure 307** Java (Sun)



Settings:

- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

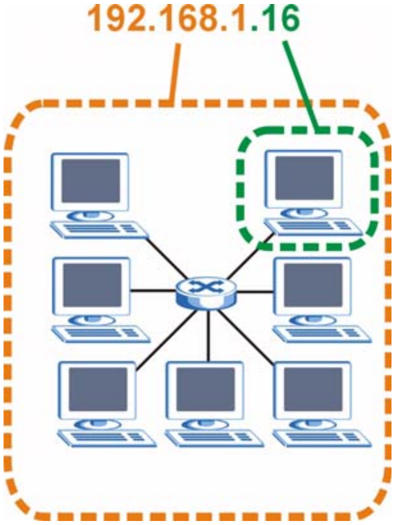
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 308** Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 251** IP Address Network Number and Host ID Example

| | 1ST OCTET: (192) | 2ND OCTET: (168) | 3RD OCTET: (1) | 4TH OCTET (2) |
|---|---|---|---|---|
| IP Address (Binary) | 11000000 | 10101000 | 00000001 | 00000010 |
| Subnet Mask (Binary) | **11111111** | **11111111** | **11111111** | 00000000 |
| Network Number | **11000000** | **10101000** | **00000001** | |
| Host ID | | | | 00000010 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 252** Subnet Masks

| | BINARY | | | | DECIMAL |
|---|---|---|---|---|---|
| | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET | |
| 8-bit mask | 11111111 | 00000000 | 00000000 | 00000000 | 255.0.0.0 |
| 16-bit mask | 11111111 | 11111111 | 00000000 | 00000000 | 255.255.0.0 |
| 24-bit mask | 11111111 | 11111111 | 11111111 | 00000000 | 255.255.255.0 |
| 29-bit mask | 11111111 | 11111111 | 11111111 | 11111000 | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 253** Maximum Host Numbers

| SUBNET MASK | | HOST ID SIZE | | MAXIMUM NUMBER OF HOSTS |
|---|---|---|---|---|
| 8 bits | 255.0.0.0 | 24 bits | $2^{24} – 2$ | 16777214 |
| 16 bits | 255.255.0.0 | 16 bits | $2^{16} – 2$ | 65534 |
| 24 bits | 255.255.255.0 | 8 bits | $2^{8} – 2$ | 254 |
| 29 bits | 255.255.255.248 | 3 bits | $2^{3} – 2$ | 6 |

# Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 254** Alternative Subnet Mask Notation

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 | 0 |
| 255.255.255.128 | /25 | 1000 0000 | 128 |

**Table 254** Alternative Subnet Mask Notation (continued)

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.192 | /26 | 1100 0000 | 192 |
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 255.255.255.252 | /30 | 1111 1100 | 252 |

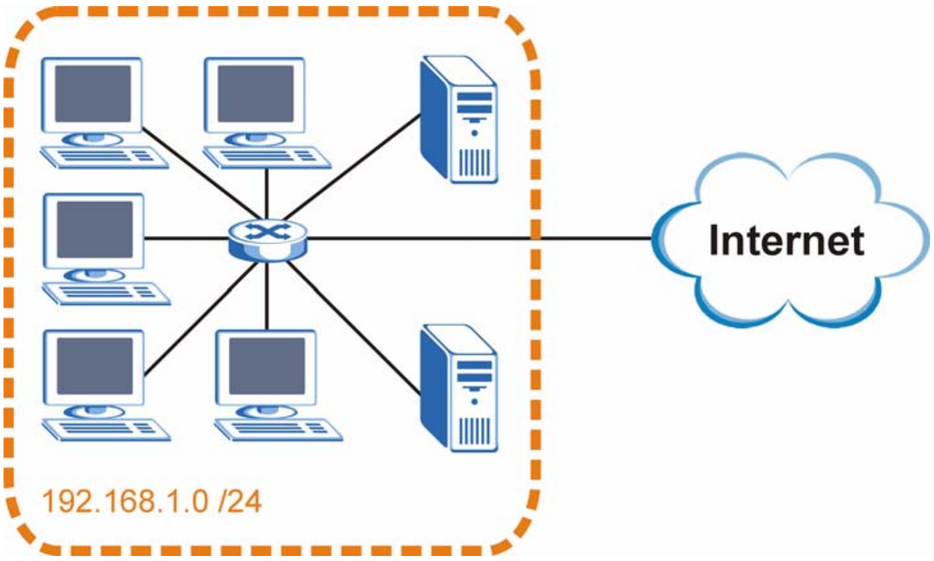
# Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 – 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 309** Subnetting Example: Before Subnetting

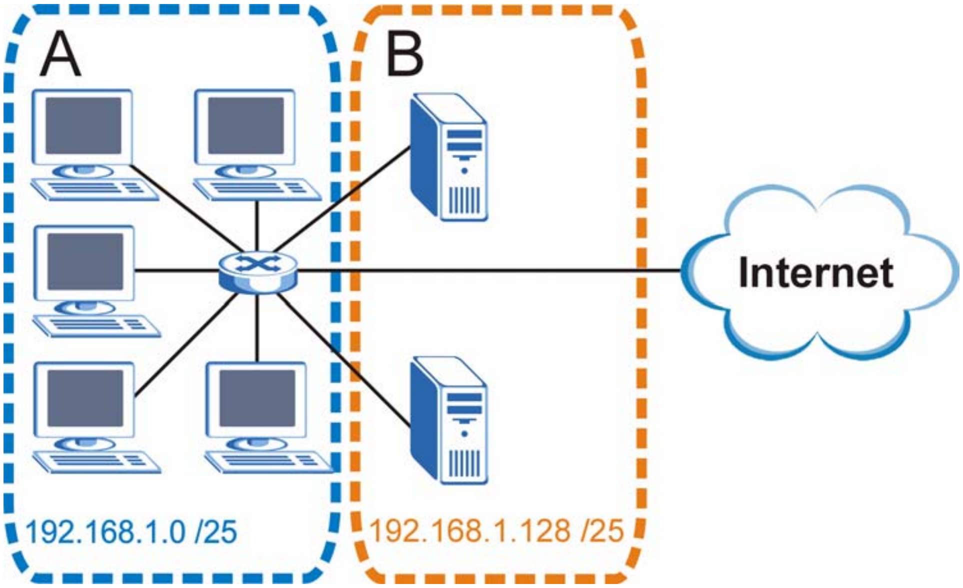


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 310** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6$ - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 255** Subnet 1

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address (Decimal) | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 256** Subnet 2

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address:<br>192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address:<br>192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Table 257** Subnet 3

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address:<br>192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address:<br>192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Table 258** Subnet 4

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address:<br>192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address:<br>192.168.1.255 | Highest Host ID: 192.168.1.254 | |

# Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 259** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |

**Table 259** Eight Subnets (continued)

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 225 | 254 | 255 |

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 260** 24-bit Network Number Subnet Planning

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.255.128 (/25) | 2 | 126 |
| 2 | 255.255.255.192 (/26) | 4 | 62 |
| 3 | 255.255.255.224 (/27) | 8 | 30 |
| 4 | 255.255.255.240 (/28) | 16 | 14 |
| 5 | 255.255.255.248 (/29) | 32 | 6 |
| 6 | 255.255.255.252 (/30) | 64 | 2 |
| 7 | 255.255.255.254 (/31) | 128 | 1 |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 261** 16-bit Network Number Subnet Planning

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |
| 13 | 255.255.255.248 (/29) | 8192 | 6 |

**Table 261** 16-bit Network Number Subnet Planning (continued)

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

# Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the device.

Once you have decided on the network number, pick an IP address for your device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the device unless you are instructed to do otherwise.

## Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

E

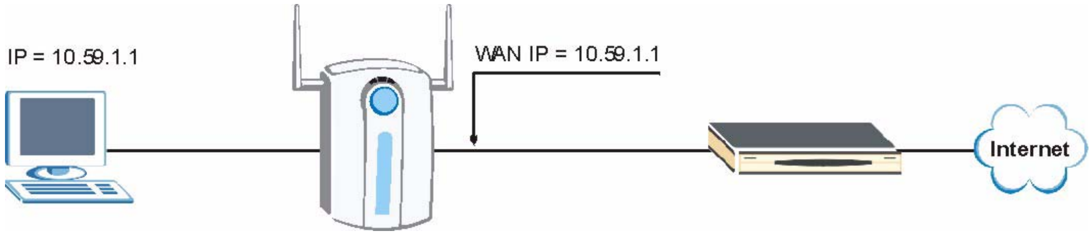
# IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

## Case A: The device is using the same LAN and WAN IP addresses

The following figure shows an example where the device is using a WAN IP address that is the same as the IP address of a computer on the LAN.

**Figure 311** IP Address Conflicts: Case A

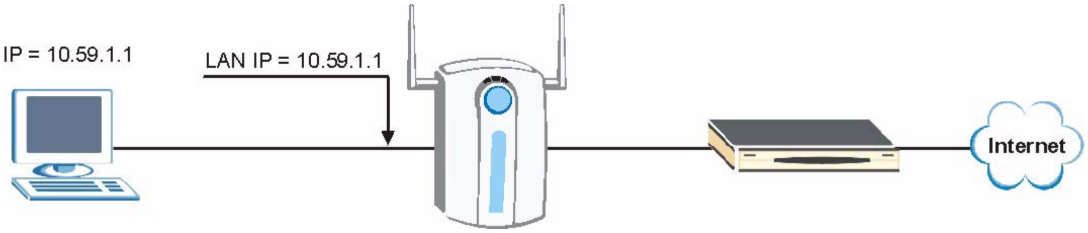


You must set the device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the device use a public WAN IP address.

## Case B: The Device LAN IP address conflicts with the DHCP client IP address

In the following figure, the device is acting as a DHCP server. The device assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

**Figure 312** IP Address Conflicts: Case B

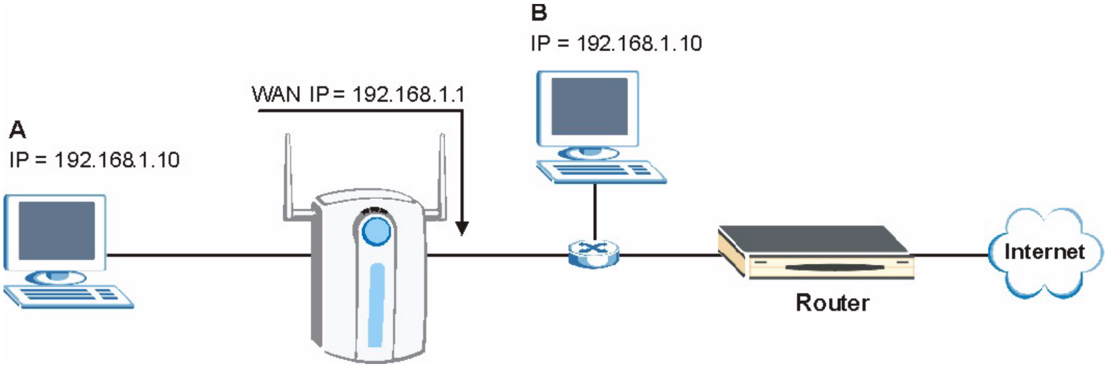


To solve this problem, make sure the device LAN IP address is not in the DHCP IP address pool.

## Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the device.

**Figure 313** IP Address Conflicts: Case C



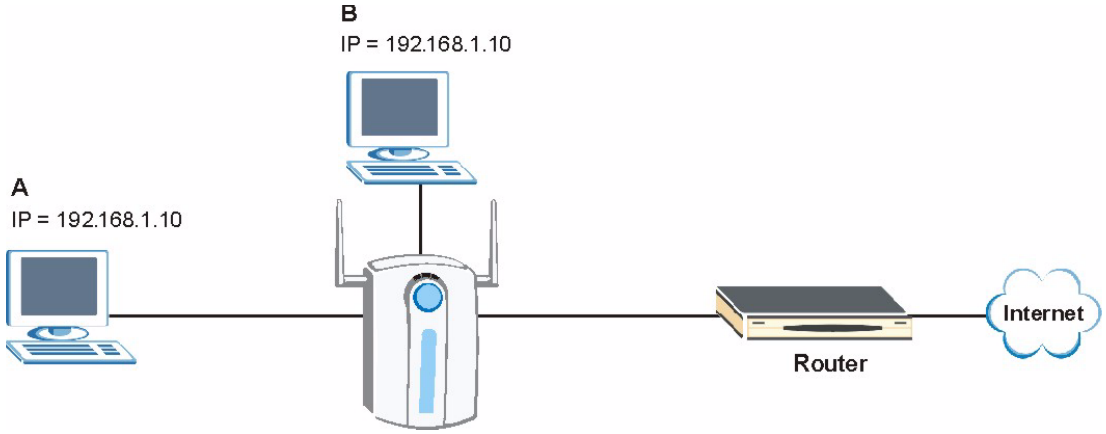
You must set the device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the device uses a public WAN IP address.

## Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the device allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the device DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

**Figure 314** IP Address Conflicts: Case D



This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

# F

# Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 262** Commonly Used Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM/New-ICQ | TCP | 5190 | AOL's Internet Messenger service. It is also used as a listening port by ICQ. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP<br>UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |

**Table 262** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/ server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |

**Table 262** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/ IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP | 7000 | Another videoconferencing solution. |

# G

# Importing Certificates

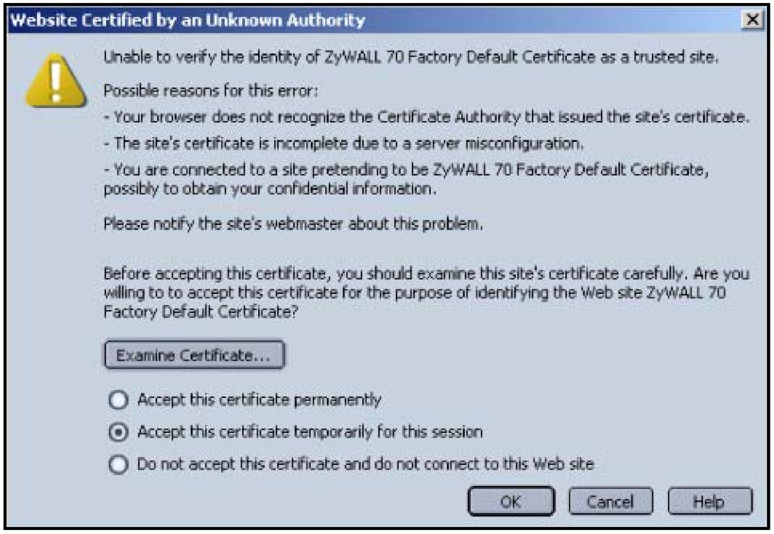
This appendix shows importing certificates examples using Internet Explorer 5.

## Import Vantage CNM Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the Vantage CNM's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

**Figure 315** Security Certificate



Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site

## Importing the Vantage CNM's Certificate into Internet Explorer

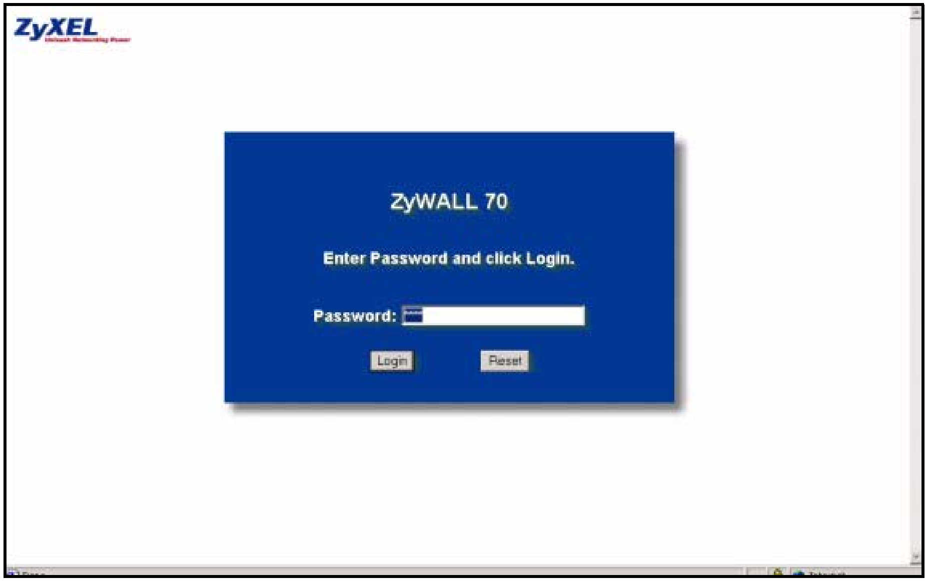
For Internet Explorer to trust a self-signed certificate from Vantage CNM, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a Vantage CNM certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the Vantage CNM's (self-signed) server certificate into your operating system as a trusted certification authority.

1 In Internet Explorer, double click the lock shown in the following screen.

Figure 316 Login Screen

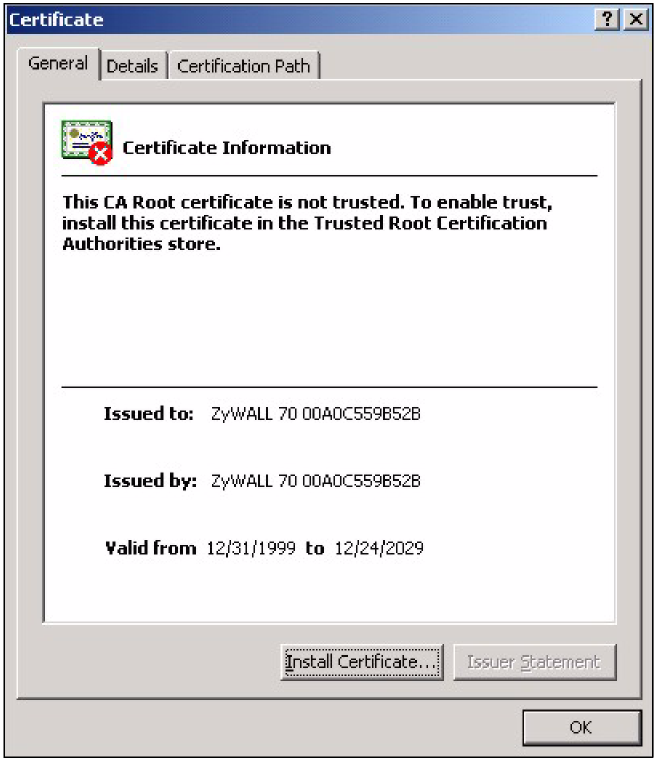


Enter Password and click Login.

Password:

2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 317 Certificate General Information before Import



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

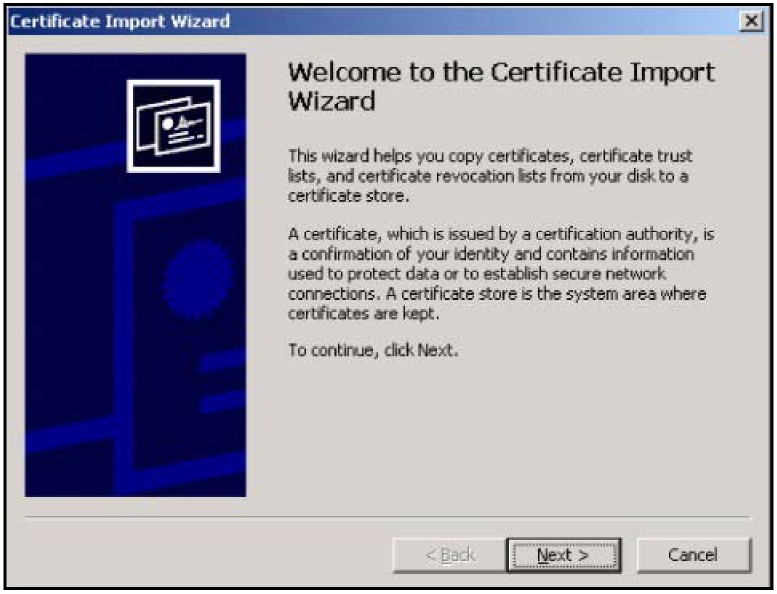
Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 to 12/24/2029

3 Click **Next** to begin the **Install Certificate** wizard.

Figure 318   Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

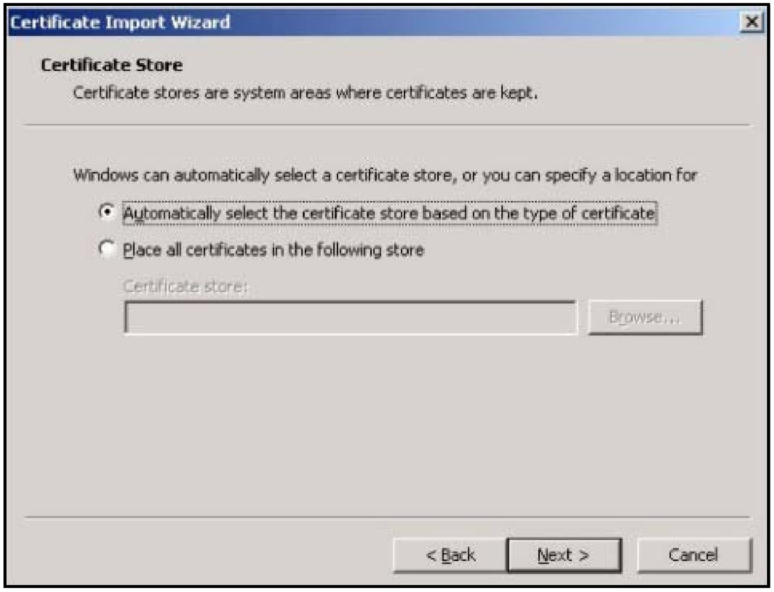
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4  Select where you would like to store the certificate and then click **Next**.

Figure 319   Certificate Import Wizard 2



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

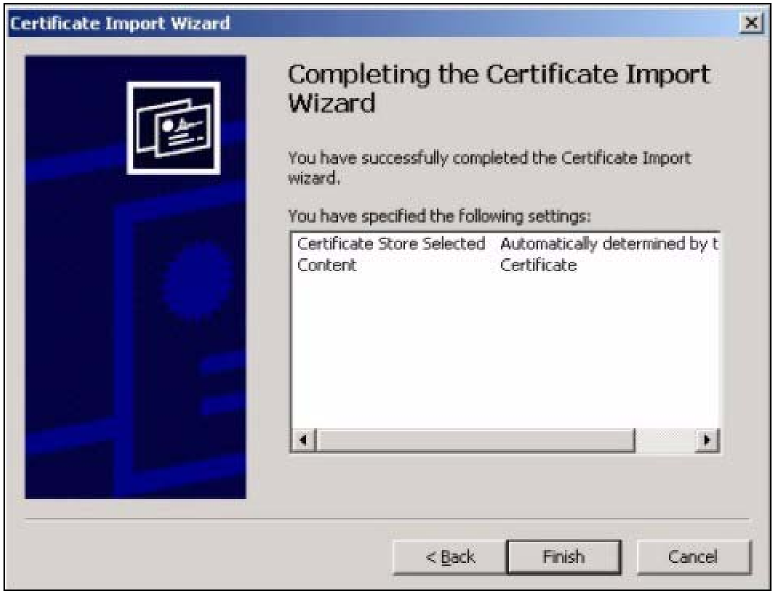
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5  Click **Finish** to complete the **Import Certificate** wizard.

**Figure 320** Certificate Import Wizard 3



Certificate Import Wizard

Completing the Certificate Import Wizard

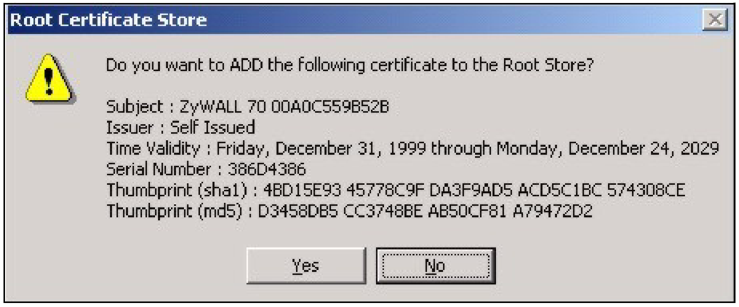
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected | Automatically determined by t |
| Content | Certificate |

6 Click **Yes** to add the Vantage CNM certificate to the root store.

**Figure 321** Root Certificate Store

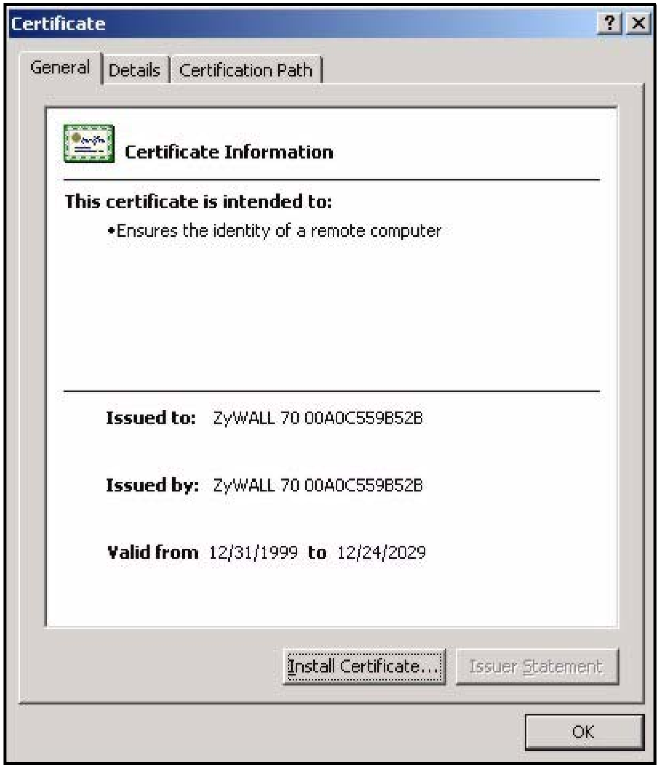


Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : ZyWALL 70 00A0C559B52B
Issuer : Self Issued
Time Validity : Friday, December 31, 1999 through Monday, December 24, 2029
Serial Number : 386D4386
Thumbprint (sha1) : 4BD15E93 45778C9F DA3F9AD5 ACD5C1BC 574308CE
Thumbprint (md5) : D3458DB5 CC3748BE AB50CF81 A79472D2

**Figure 322** Certificate General Information after Import



Certificate Information

This certificate is intended to:

•Ensures the identity of a remote computer

Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 to 12/24/2029

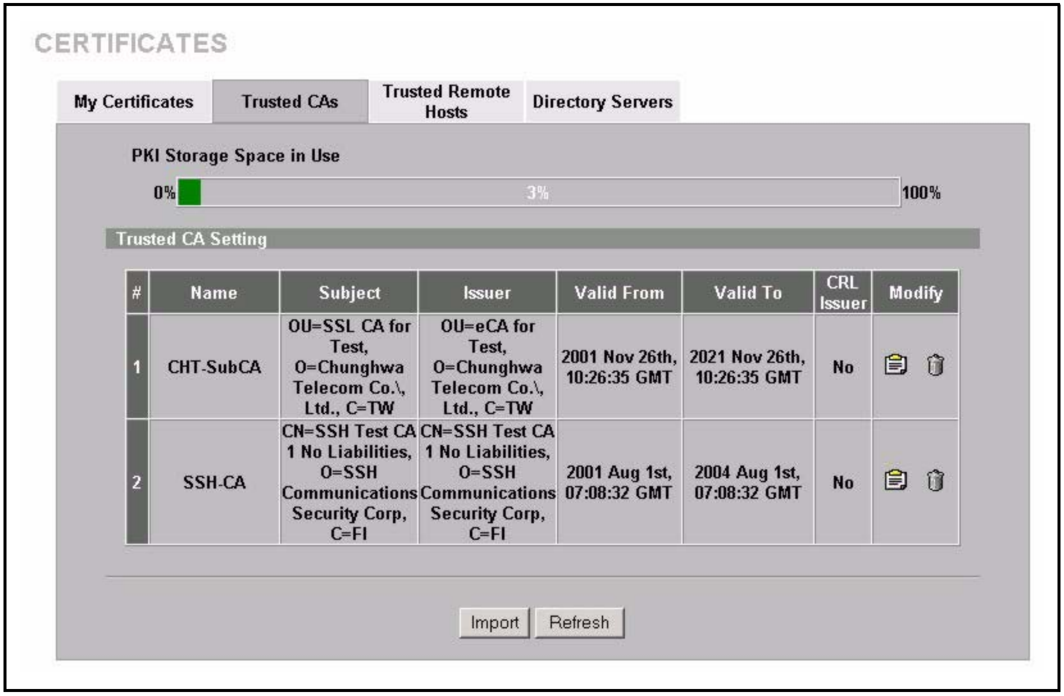
# Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the device.

You must have imported at least one trusted CA to the device in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the device (see the device’s **Trusted CA** web configurator screen).

**Figure 323** Device's Trusted CA Screen



CERTIFICATES

PKI Storage Space in Use

Trusted CA Setting

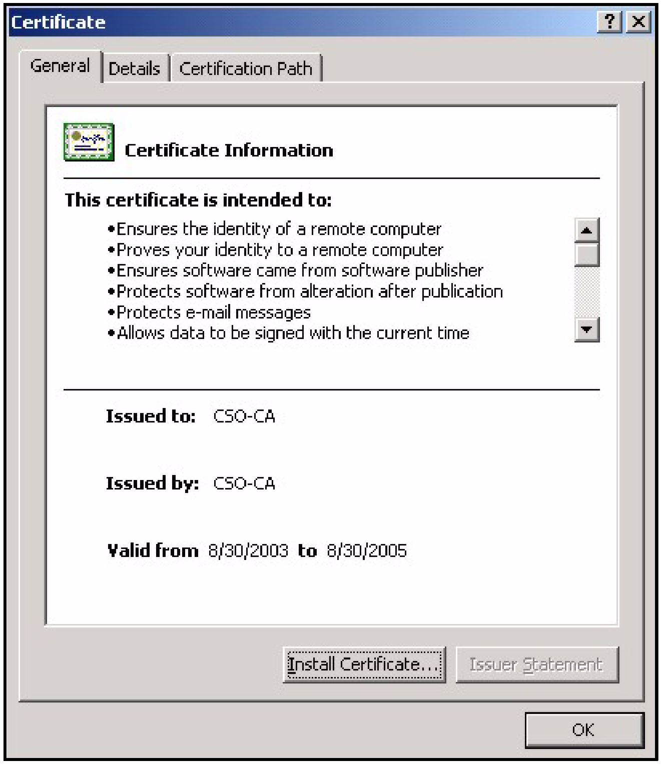
| # | Name | Subject | Issuer | Valid From | Valid To | CRL Issuer | Modify |
|---|---|---|---|---|---|---|---|
| 1 | CHT-SubCA | OU=SSL CA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW | OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW | 2001 Nov 26th, 10:26:35 GMT | 2021 Nov 26th, 10:26:35 GMT | No | 📝 🗑 |
| 2 | SSH-CA | CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI | CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI | 2001 Aug 1st, 07:08:32 GMT | 2004 Aug 1st, 07:08:32 GMT | No | 📝 🗑 |

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

## Installing the CA's Certificate

**1** Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 324** CA Certificate Example



Certificate

**Certificate Information**

**This certificate is intended to:**

- •Ensures the identity of a remote computer
- •Proves your identity to a remote computer
- •Ensures software came from software publisher
- •Protects software from alteration after publication
- •Protects e-mail messages
- •Allows data to be signed with the current time

**Issued to:** CSO-CA

**Issued by:** CSO-CA

**Valid from** 8/30/2003 **to** 8/30/2005

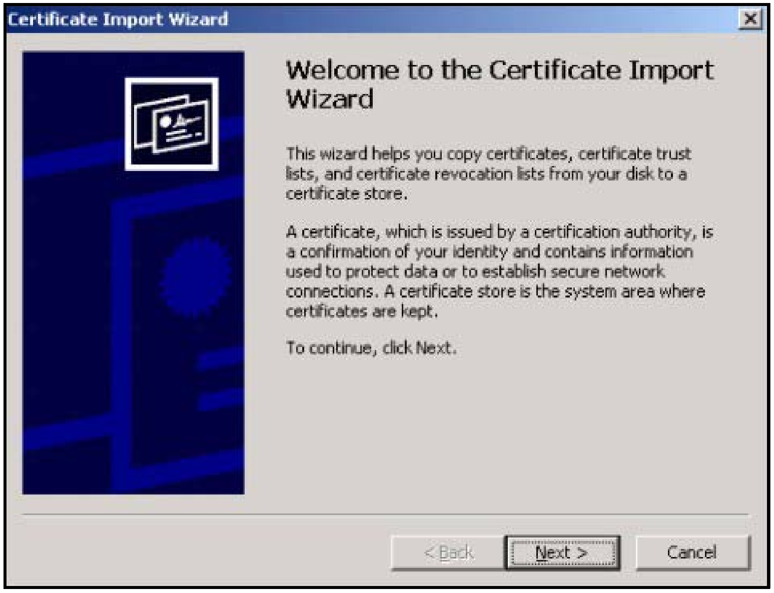
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

## Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

**Figure 325** Personal Certificate Import Wizard 1



Certificate Import Wizard

Welcome to the Certificate Import Wizard

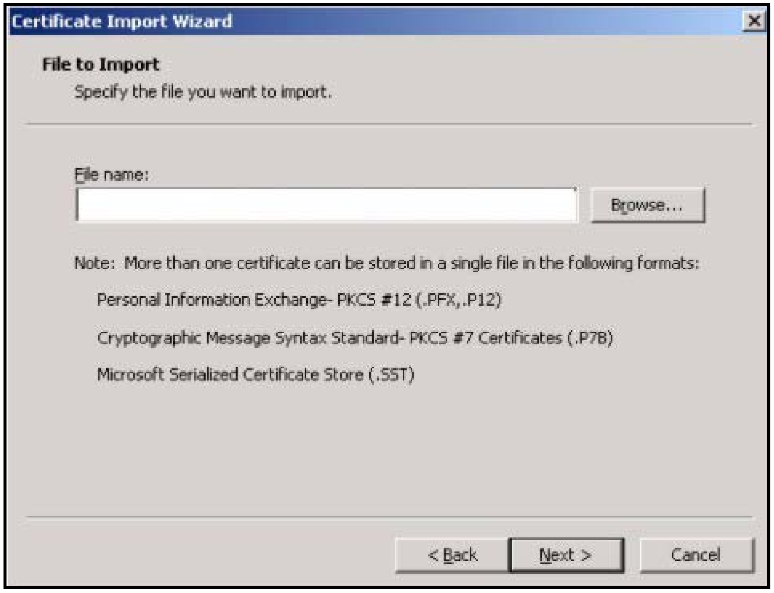
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

**Figure 326** Personal Certificate Import Wizard 2



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

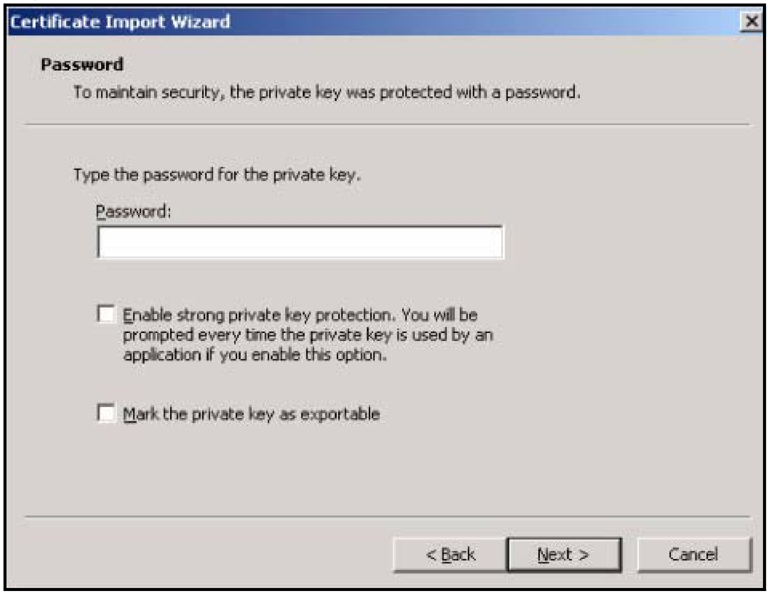
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

**Figure 327** Personal Certificate Import Wizard 3



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

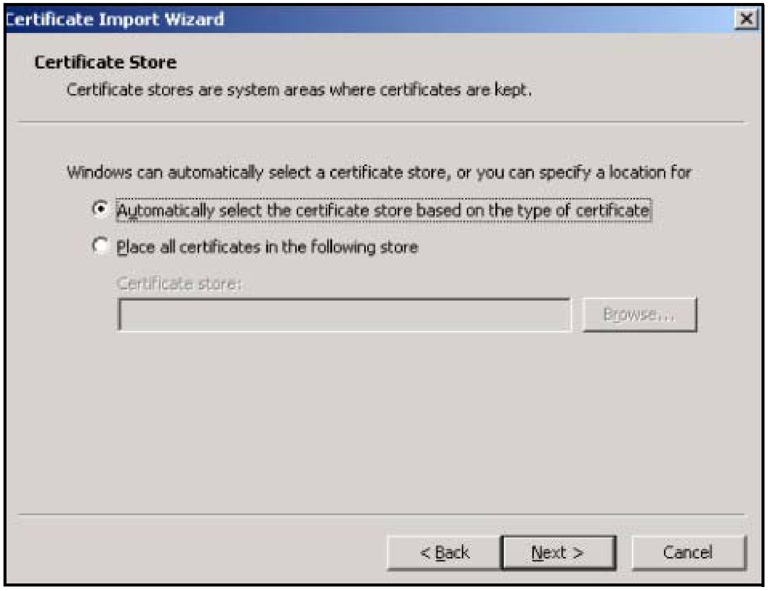
Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark the private key as exportable

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 328** Personal Certificate Import Wizard 4



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

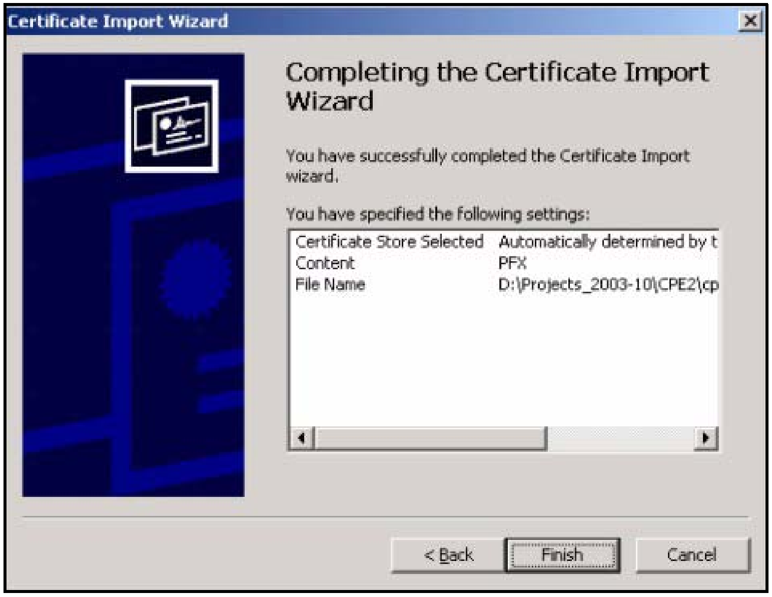
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the wizard and begin the import process.

**Figure 329** Personal Certificate Import Wizard 5



Certificate Import Wizard

Completing the Certificate Import Wizard

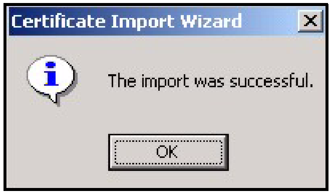
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected | Automatically determined by t |
| Content | PFX |
| File Name | D:\Projects_2003-10\CPE2\cp |

6 You should see the following screen when the certificate is correctly installed on your computer.

**Figure 330** Personal Certificate Import Wizard 6



Certificate Import Wizard

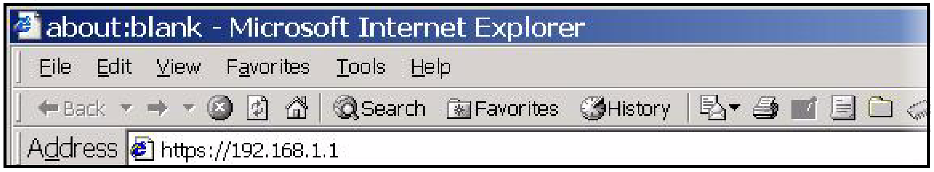
The import was successful.

## Using a Certificate When Accessing the Device Example

Use the following procedure to access the device via HTTPS.

1 Enter ‘https://device IP Address/ in your browser’s web address field.

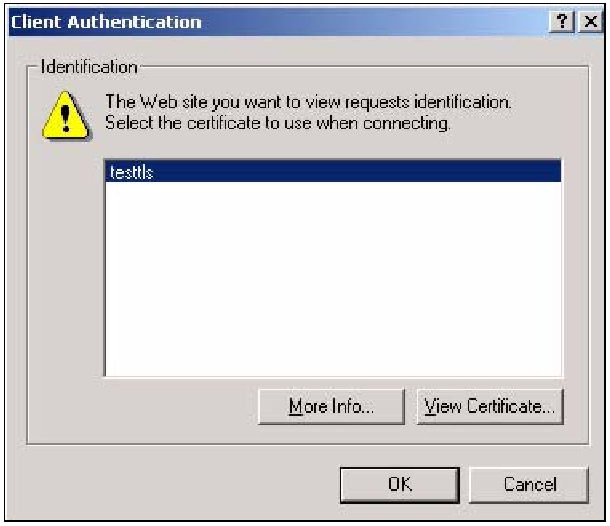
Figure 331 Access the Device Via HTTPS


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History

Address https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the device, the following screen asks you to select a personal certificate to send to the device. This screen displays even if you only have a single certificate as in the example.

Figure 332 SSL Client Authentication


Client Authentication

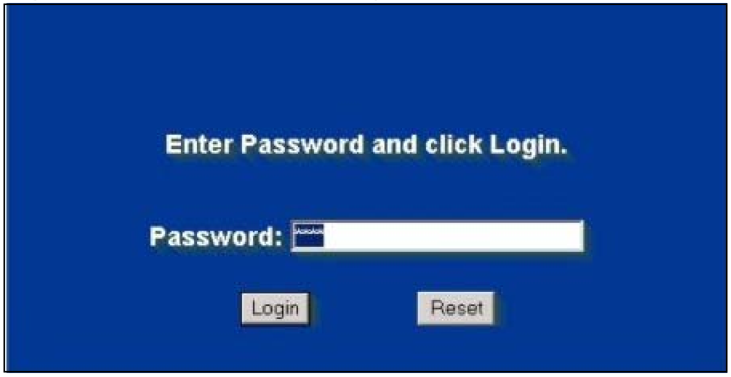
Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

testtls

3 You next see the device login screen.

Figure 333 Device Secure Login Screen


Enter Password and click Login.

Password:

# Open Software Announcements

**Notice**

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Castor under below license

**Copyright (C) 1999-2001 Intalio, Inc. All Rights Reserved.**

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "ExoLab" must not be used to endorse or promote products derived from this Software without prior written permission of ExoLab Group. For written permission, please contact info@exolab.org.

4. Products derived from this Software may not be called "ExoLab" nor may "ExoLab" appear in their names without prior written permission of ExoLab Group. Exolab is a registered trademark of ExoLab Group.

5. Due credit should be given to the ExoLab Group (http://www.exolab.org).

THIS SOFTWARE IS PROVIDED BY INTALIO, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF ERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL INTALIO, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes ant-contrib 1.0b3 version, axis 1.2.1 version, a[ache-commoms quartz 1.5.2 version, log4j 102014 version, j2sh, xerces 2.8.1 version, apache-any 1.6.5 version, and apache-tomcat 5.0 version under Apache Software License

**Apache License**

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

This Product includes hibernate 3.1.3 version and j2sh under LGPL

Copyright (C) 2002 Lee David Painter. All right reserved

**GNU LESSER GENERAL PUBLIC LICENSE**

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root

function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS

This Product includes MySQL database and j2sh under GPL

**GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes JavaMail 1.3.2 version under the license by Sun Development Network

**Copyright 1994-2006 Sun Microsystems, Inc. All Rights Reserved.**

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sun Microsystems, Inc. or the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You acknowledge that this software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

This Product includes JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0 1.5.0 version of Java Software technologies

**TECHNOLOGY LICENSE FROM SUN MICROSYSTEMS, INC. TO DOUG LEA**

Whereas Doug Lea desires to utilize certain Java Software technologies in the util.concurrent technology; and Whereas Sun Microsystems, Inc. ("Sun") desires that Doug Lea utilize certain Java Software technologies in the util.concurrent technology; Therefore the parties agree as follows, effective May 31, 2002:

"Java Software technologies" means

classes/java/util/ArrayList.java, and

classes/java/util/HashMap.java.

The Java Software technologies are Copyright (c) 1994-2000 Sun Microsystems, Inc. All rights reserved.

Sun hereby grants Doug Lea a non-exclusive, worldwide, non-transferrable license to use, reproduce, create derivative works of, and distribute the Java Software and derivative works thereof in source and binary forms as part of a larger work, and to sublicense the right to use, reproduce and distribute the Java Software and Doug Lea's derivative works as the part of larger works through multiple tiers of sublicensees provided that the following conditions are met:

-Neither the name of or trademarks of Sun may be used to endorse or promote products including or derived from the Java Software technology without specific prior written permission; and

-Redistributions of source or binary code must contain the above copyright notice, this notice and the following disclaimers:

THIS SOFTWARE IS PROVIDED "AS IS," WITHOUT A WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR

DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN MICROSYSTEMS, INC. OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You acknowledge that Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

signed [Doug Lea] dated

**JAVA Software Technologies**

**Copyright 1994-2000 Sun Microsystems, Inc. All right reserved**

JAVA(TM) 2 SOFTWARE DEVELOPMENT KIT (J2SDK), STANDARD EDITION, VERSION 1.4.1_X SUPPLEMENTAL LICENSE TERMS

These supplemental license terms ("Supplemental Terms") add to or modify the terms of the Binary Code License Agreement (collectively, the "Agreement"). Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the binary form of the Software complete and unmodified for the sole purpose of designing, developing, testing, and running your Java applets and applications intended to run on Java-enabled general purpose desktop computers and servers ("Programs").

2. License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree.

3. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional

software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement.

4. Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of he "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

5. Notice of Automatic Software Updates from Sun. You acknowledge that the Software may automatically download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun ("Software Updates"), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

6. Notice of Automatic Downloads. You acknowledge that, by your use of the Software and/or by requesting services that require use of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Software Development Kit, Standard Edition, Version 1.4.1; (iv) The Software must be reproduced in its entirety.

8. Trademarks and Logos. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

9. Source Code. Software may contain source code that is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

10. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A (LFI#134402/Form ID#011801)

This Product includes Spring 2.0 version under Spring license

Revision 62, 1.5 kB (checked in by jacob, 1 year ago)

Changed name on LICENSE to be lawyerriffic

Line

Copyright (c) 2005, the Lawrence Journal-World
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Django nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

20 WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

21 DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR

22 ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

23 (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

24 LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON

25 ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

26 (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS

NOTE: Some components of the Vantage CNM 2.3 incorporate source code covered under the Apache License, GPL License, LGPL License, Sun License, and Castor License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at ZyXEL Technical Support.

**End-User License Agreement for Vantage CNM 2.3**

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF

BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED $1,000. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9. Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

I

# 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

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. 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 ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

### 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.

# J

# Customer Support

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

## Required Information

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

## Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

## Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

## Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

### Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-0
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

### Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

### North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: ftp.us.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

### Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

### Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

### Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

### United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

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

# Index